



# Digital.NSW ICT Purchasing Framework

## ICT Agreement (ICTA)

between

**Department of Communities and Justice (ABN 36 433 875 185) for and on behalf of the State of New South Wales**

and

**Fujitsu Australia Limited, ABN # 19001011427**

**JusticeLink Support and Maintenance Agreement**

**ICTA Module: Services**

**Agreement Reference No: PRJ\_5302**

## Contents

<b>PART A: PRELIMINARIES .....</b>	<b>1</b>
<b>1. Definitions and Agreement documents .....</b>	<b>1</b>
1.1 Defined terms and interpretation .....	1
1.2 Agreement documents .....	1
1.3 Order of precedence .....	2
1.4 Role of the Master ICT Agreement .....	2
1.5 Supplier's Documents .....	2
<b>2. Supplier's acknowledgments .....</b>	<b>3</b>
<b>3. Purchasing Services and/or Deliverables by Order .....</b>	<b>4</b>
3.1 Order Form .....	4
3.2 Electronic execution .....	4
3.3 Additional Orders .....	4
3.4 No exclusivity or minimum commitment .....	5
3.5 Additional Conditions .....	5
3.6 Reseller arrangements .....	5
<b>4. Relationship and governance .....</b>	<b>6</b>
4.1 General .....	6
4.2 Nature of relationship .....	6
4.3 Governance .....	6
<b>5. Term .....</b>	<b>6</b>
5.1 Initial Term .....	6
5.2 Renewal Period .....	6
<b>PART B: SUPPLIER'S ACTIVITIES .....</b>	<b>7</b>
<b>6. Performance of the Supplier's Activities .....</b>	<b>7</b>
6.1 General .....	7
6.2 Customer Supplied Items .....	7
6.3 ICT Accessibility .....	8
6.4 Co-operation with the Customer and Other Suppliers .....	8
6.5 Project management .....	9
6.6 Staged implementation .....	9
6.7 Delays .....	10
6.8 Extension of time .....	10
6.9 Delay costs .....	11
6.10 Site .....	12
<b>7. Transition-In .....</b>	<b>13</b>
7.1 Application .....	13
7.2 Transition-In Plan .....	13
7.3 Transition-In Services .....	13
<b>8. Document Deliverables .....</b>	<b>14</b>
8.1 General .....	14
8.2 Review .....	14
8.3 No obligation .....	15
8.4 User Documentation .....	15
<b>9. Defects .....</b>	<b>16</b>
<b>10. Change Control Procedure .....</b>	<b>17</b>
10.1 Change Requests .....	17

10.2	Process for submitting and agreeing to Change Requests .....	17
10.3	Electronic transactions .....	18
10.4	Acknowledgements .....	18
<b>11.</b>	<b>Personnel .....</b>	<b>19</b>
11.1	Nominated Personnel.....	19
11.2	Replacement of Nominated Personnel.....	19
11.3	Supplier's Personnel .....	20
11.4	Deed of Confidentiality and Privacy .....	21
11.5	Subcontracting .....	21
11.6	Background checks.....	22
11.7	Compliance with employment Laws .....	23
11.8	Non-solicitation .....	23
<b>12.</b>	<b>Compliance .....</b>	<b>23</b>
12.1	Compliance with Laws and directions .....	23
12.2	Policies, Codes and Standards .....	24
12.3	Policy Changes .....	24
12.4	Work health and safety.....	25
12.5	Work health and safety where Supplier's Activities include construction work.....	25
12.6	The environment .....	26
12.7	Conflicts of Interest.....	26
<b>13.</b>	<b>Modern Slavery .....</b>	<b>26</b>
13.1	Core Modern Slavery Obligations .....	26
13.2	Price .....	27
13.3	Systems and policies .....	27
13.4	Disclosure .....	27
13.5	Information .....	27
13.6	Response to Modern Slavery incident.....	28
13.7	Termination .....	28
<b>14.</b>	<b>Acceptance Testing.....</b>	<b>29</b>
14.1	General .....	29
14.2	Testing by Supplier .....	29
14.3	Testing by the Customer .....	29
14.4	Effect of failure to meet Acceptance Criteria .....	30
14.5	Effect of Acceptance Certificate .....	31
<b>15.</b>	<b>Performance.....</b>	<b>31</b>
15.1	Performance obligations.....	31
15.2	Service standards and Service Levels .....	32
15.3	Consequences for failing to meet a Service Level.....	33
15.4	Performance reports .....	33
15.5	Performance reviews .....	34
15.6	Notice .....	34
15.7	Meetings.....	34
<b>16.</b>	<b>Liquidated Damages.....</b>	<b>34</b>
<b>17.</b>	<b>Intellectual Property .....</b>	<b>35</b>
17.1	Ownership of Existing Materials .....	35
17.2	Licence to use Existing Materials .....	35
17.3	Ownership of New Materials .....	36
17.4	Customer licence to use Supplier owned New Materials .....	36
17.5	Licence term.....	37
17.6	Supplier Licence to use Customer owned New Materials .....	37
17.7	Third party Intellectual Property Rights .....	37
17.8	Open Source Software .....	38
17.9	Consents and Moral Rights .....	38

17.10	Prohibited activities .....	39
17.11	Additional obligations .....	39
17.12	Warranties and acknowledgements .....	39
17.13	Replacement of Deliverables .....	39
<b>18.</b>	<b>Escrow .....</b>	<b>40</b>
<b>PART C: DATA AND SECURITY .....</b>		<b>40</b>
<b>19.</b>	<b>Customer Data .....</b>	<b>40</b>
19.1	Obligations in relation to Customer Data .....	40
19.2	Security of Customer Data .....	41
19.3	Location of Customer Data .....	41
19.4	Backup of Customer Data .....	42
19.5	Restoration of lost Customer Data .....	42
19.6	Rights to access, use, extract and retrieve Customer Data .....	42
19.7	Record, retention, return and destruction of the Customer Data .....	43
19.8	General .....	43
<b>20.</b>	<b>Privacy .....</b>	<b>44</b>
20.1	Protection and use of Personal Information .....	44
20.2	Data Management and Protection Plan .....	45
20.3	No limitation of obligations .....	45
<b>21.</b>	<b>Security .....</b>	<b>45</b>
21.1	Scope of the Supplier's security obligations .....	46
21.2	Supplier's security obligations .....	46
21.3	Audits and compliance .....	47
<b>22.</b>	<b>Security Incidents .....</b>	<b>48</b>
22.1	Notification of Security Incidents .....	48
22.2	Actions required in relation to a Security Incident .....	49
<b>23.</b>	<b>Confidentiality .....</b>	<b>50</b>
<b>PART D: FEES AND PAYMENT .....</b>		<b>51</b>
<b>24.</b>	<b>Payment and invoicing .....</b>	<b>51</b>
24.1	Price .....	51
24.2	Benchmarking .....	51
24.3	Outcome of benchmarking .....	52
24.4	Invoicing .....	53
24.5	Payment .....	54
24.6	Payment disputes .....	54
24.7	Set off .....	54
24.8	Taxes .....	54
<b>PART E: RISK ALLOCATION AND MANAGEMENT .....</b>		<b>55</b>
<b>25.</b>	<b>Business contingency and Disaster recovery .....</b>	<b>55</b>
25.1	Business contingency .....	55
25.2	Business Contingency Plan .....	55
25.3	Disasters .....	56
<b>26.</b>	<b>Step-in .....</b>	<b>56</b>
26.1	Step-In Rights .....	56
26.2	Conclusion of Step-In .....	57
26.3	No prejudice .....	58
<b>27.</b>	<b>Insurance .....</b>	<b>58</b>
<b>28.</b>	<b>Performance Guarantee and Financial Security .....</b>	<b>59</b>


28.1	Performance Guarantee .....	59
28.2	Financial Security .....	59
28.3	Costs .....	59
<b>29.</b>	<b>Termination .....</b>	<b>59</b>
29.1	Termination for cause by the Customer .....	59
29.2	Termination for convenience by the Customer .....	60
29.3	Consequences of reduction of scope .....	61
29.4	Termination for cause by the Supplier .....	61
29.5	Dispute resolution .....	61
29.6	Survival of rights on termination or reduction in scope .....	61
<b>30.</b>	<b>Suspension .....</b>	<b>62</b>
<b>31.</b>	<b>Transition-Out Services .....</b>	<b>62</b>
31.1	Application of this clause .....	62
31.2	Transition-Out Plan .....	62
31.3	General .....	63
<b>32.</b>	<b>Consequences of expiry or termination .....</b>	<b>63</b>
32.1	Extracting or retrieving Customer Data .....	63
32.2	Confidential Information and intellectual property .....	63
<b>33.</b>	<b>Warranties .....</b>	<b>64</b>
33.1	Mutual warranties .....	64
33.2	General Supplier warranties .....	64
33.3	Warranties in relation to Supplier's Activities .....	64
33.4	Implied warranties .....	65
<b>34.</b>	<b>Indemnities and liability .....</b>	<b>65</b>
34.1	Indemnities .....	65
34.2	Third Party IP Claims .....	65
34.3	Indemnities not affected by insurance .....	66
34.4	Status of indemnities .....	66
34.5	Liability cap .....	66
34.6	Exclusions of liability .....	67
34.7	Application and contribution .....	68
34.8	Mitigation .....	68
<b>35.</b>	<b>Dispute resolution .....</b>	<b>68</b>
35.1	General .....	68
35.2	Escalation .....	69
35.3	Alternative dispute resolution .....	69
35.4	Acknowledgment .....	69
35.5	Costs .....	69
35.6	Continue to perform .....	69
<b>36.</b>	<b>Force Majeure .....</b>	<b>69</b>
36.1	Force Majeure Event .....	69
36.2	Notification and diligence .....	70
36.3	Liability not relieved .....	70
36.4	Prolonged Force Majeure Event .....	70
<b>37.</b>	<b>Reports and audits .....</b>	<b>71</b>
37.1	Records and reports .....	71
37.2	Audits and inspections .....	71
37.3	Conduct of audits and inspections .....	72
37.4	Survival .....	73
<b>38.</b>	<b>Proportionate liability .....</b>	<b>73</b>
<b>PART F: GENERAL PROVISIONS .....</b>	<b>73</b>	

<b>39.</b>	<b>General .....</b>	<b>73</b>
39.1	Government information .....	73
39.2	Personal Property Securities Act .....	74
39.3	No use of the Customer's name or logo .....	74
39.4	Prior work .....	74
39.5	Entire agreement .....	75
39.6	Variation .....	75
39.7	Survival and merger .....	75
39.8	Severability .....	75
39.9	Waiver .....	75
39.10	Cumulative rights .....	75
39.11	Further assurances .....	75
39.12	Assignment, novation and other dealings .....	76
39.13	Notices .....	76
39.14	Construction .....	77
39.15	Expenses .....	77
39.16	English language .....	77
39.17	Governing Law .....	77
	<b>Schedule 1 - Definitions and interpretation .....</b>	<b>79</b>
	<b>Schedule 2 - Order Form .....</b>	<b>95</b>
	<b>Statement of Work – Software Support Services and Other Professional Services .....</b>	<b>120</b>
	<b>Annexure C to Order Form – Supplementary Customer Requirements .....</b>	<b>135</b>
	<b>Annexure D to Order Form – Additional Conditions .....</b>	<b>144</b>
	<b>Annexure E to Order Form - Customer Policies .....</b>	<b>148</b>
	<b>Schedule 4 - Payment Schedule .....</b>	<b>150</b>
	<b>Schedule 5 - Change Request Form .....</b>	<b>151</b>
	<b>Schedule 6 - Deed of Confidentiality and Privacy .....</b>	<b>152</b>
	<b>Schedule 7 - Escrow Deed – Not Applicable .....</b>	<b>159</b>
	<b>Schedule 8 - Performance Guarantee – Not applicable .....</b>	<b>159</b>
	<b>Schedule 9 - Financial Security – Not applicable .....</b>	<b>159</b>

# ICT Agreement (ICTA)

- Parties**
- The party identified at Item 1 of the Order Form (**Customer**)

The party identified at Item 4 of the Order Form (**Supplier**)



**Guidance note:** The parties' names and (where applicable) ABNs should be clearly described in the relevant parts of the Order Form, relevant Schedules and the execution clauses.

## Background

- A.

The New South Wales Government's Digital.NSW ICT Purchasing Framework (**ICT Purchasing Framework**) is a suite of template documents which sets out standard terms and conditions to be used by Eligible Customers for the procurement of ICT related goods and services.
- B.

The Supplier acknowledges and agrees that the New South Wales Procurement Board has directed that Government Agencies must, subject to applicable New South Wales Procurement Board Directions, use the ICT Purchasing Framework for the procurement of ICT related goods and services.
- C.

This Agreement forms part of the ICT Purchasing Framework and contains the terms and conditions on which the Supplier agrees to carry out the Supplier's Activities.
- D.

The Supplier has represented to the Customer that it has the relevant skills and experience to provide the Supplier's Activities.
- E.

The Customer has agreed to appoint the Supplier, on a non-exclusive basis, to carry out the Supplier's Activities, subject to the Supplier's ongoing compliance with the terms and conditions of this Agreement, and the Supplier has agreed to accept that appointment.

## PART A: PRELIMINARIES

### 1. Definitions and Agreement documents


#### 1.1 Defined terms and interpretation

In this Agreement the definitions and interpretation provisions set out in Schedule 1 apply.

#### 1.2 Agreement documents

This Agreement comprises the following documents:

- (a) any Additional Conditions;



**Guidance note:** Subject to relevant New South Wales Procurement Board Directions, Additional Conditions may be used to implement special requirements applicable to a particular ICT procurement or to augment or enhance the terms of this Agreement to address bespoke matters or risks. Where Additional Conditions are used, they will take priority over all other Agreement documents.

- (b) these Core Terms and Schedule 1;
- (c) the applicable Module Terms;

- (d) the Order Form and Payment Schedule (excluding any Additional Conditions or Supplier's Documents);
- (e) any other schedule, attachment or annexure to this Agreement (excluding any documents forming part of the Order Form);
- (f) any other document expressly incorporated into this Agreement as set out in the Order Form; and
- (g) any Supplier's Documents.



**Guidance note:** Where the parties agree to incorporate certain terms proposed by the Supplier into this Agreement, these should be clearly identified and introduced as Supplier's Documents pursuant to the process set out in clause 1.5 and not characterised as "Additional Conditions".

1.3 Order of precedence

In the event of any conflict or inconsistency between the documents set out in clause 1.2, the document listed higher in the list will prevail over the document listed lower in the list to the extent of such conflict or inconsistency, regardless of anything to the contrary in those documents.

1.4 Role of the Master ICT Agreement

Where this Agreement is made under a MICTA, the Supplier acknowledges that its MICTA with the Contract Authority constitutes a standing offer under which it offers to supply the deliverables, services and/or activities specified in the MICTA to Eligible Customers, including the Customer:

- (a) pursuant to the terms of the MICTA and this Agreement; and
- (b) at rates and prices which are the same as or less than those set out in the MICTA (and, upon the commencement of any Renewal Period, at rates and prices which are the same as or less than any reduced rates and prices then applying under the MICTA at the time of such renewal).



**Guidance note:** A Contract Authority may make a standing offer arrangement by agreeing a MICTA with a Supplier for the supply of particular ICT related goods, services and/or other activities by that Supplier to Eligible Customers.

Where a MICTA applies in relation to particular ICT goods, services and/or other activities supplied by a Supplier, all Eligible Customers who purchase ICT goods, services and/or other activities from that Supplier must (subject to the terms of the MICTA) do so pursuant to the terms of the MICTA and this Agreement (which is the contract agreed under that MICTA).

Where the MICTA does not apply, the Customer may acquire Deliverables and Services from the Supplier under this Agreement without reference to the MICTA.

1.5 Supplier's Documents

- (a) The parties acknowledge that the intent of incorporating any Supplier's Documents into this Agreement, where so agreed, is to supplement and elaborate the detail and specifications of particular Services and Deliverables and not to amend or contradict the terms set out in any of the documents listed in clauses 1.2(a) to 1.2(f).
- (b) The Supplier represents that the Supplier's Documents:



- (i) set out specific details regarding how the Customer may access, use and interact with particular Services or Deliverables; and
  - (ii) may describe other elements of the Services or Deliverables which the Supplier offers to provide to the Customer, such as technical and functional specifications, service characteristics and performance standards.
- (c) No Supplier's Documents will be incorporated into this Agreement except to the extent expressly specified in, and attached to, Annexure A of the Order Form.
- (d) Notwithstanding the incorporation of Supplier's Documents under clause 1.5(c), those Supplier's Documents do not apply to the extent that they:
  - (i) deal with the same or similar subject matter as a provision of the Core Terms, Module Terms or any Additional Conditions (for example, provisions in the Supplier's Documents that deal with limitations of liability will not apply, in whole, as the Core Terms also deal with this subject matter);
  - (ii) are inconsistent, or in conflict, with the Core Terms, Module Terms or any Additional Conditions;
  - (iii) alter, or seek to alter, the legal obligations of, or relationship between, the Customer and the Supplier, as set out in the Core Terms, Module Terms or any Additional Conditions;
  - (iv) impose additional obligations or requirements on the Customer, beyond those set out in the Core Terms, Module Terms or any Additional Conditions; or
  - (v) limit any rights or remedies of the Customer or relieve the Supplier from any of its obligations or responsibilities under the Core Terms, Module Terms or any Additional Conditions.
- (e) Where any of the Supplier's Documents purport to override or otherwise vary the Core Terms, Module Terms or any Additional Conditions those terms will have no legal effect.
- (f) Except to the extent expressly set out in the Module Terms, no subsequent changes, amendments or updates to the Supplier's Documents will have any effect other than where made pursuant to a written variation under clause 39.6.

---

## 2. Supplier's acknowledgments

- (a) The Supplier warrants, represents, acknowledges and agrees that it:
  - (i) has the expertise to carry out the Supplier's Activities;
  - (ii) has satisfied itself about, and has obtained all information necessary to enable it to understand, the Customer's requirements under this Agreement in so far as they relate to the Supplier's Activities;
  - (iii) has satisfied itself as to the availability and suitability of the Materials, labour and resources necessary to perform its obligations under this Agreement;

- (iv) has satisfied itself of the nature and extent of the Supplier's Activities and its obligations under this Agreement;
  - (v) did not in any way rely on:
    - A. any information, data, representation, statement or document made by the Customer or its Personnel or provided to the Supplier by the Customer or its Personnel; or
    - B. the accuracy, adequacy, suitability or completeness of any such information, data, representation, statement or document,for the purposes of entering into this Agreement, except to the extent that any such information, data, representation, statement or document forms part of this Agreement;
  - (vi) entered into this Agreement based on its own investigations, interpretations, deductions, information and determinations; and
  - (vii) is aware that the Customer has entered into this Agreement relying upon the warranties given by the Supplier under this Agreement, including in clauses 2(a)(i) to 2(a)(vi), 17.12, 33.2, 33.3 and in the Module Terms.
- (b) The Supplier further acknowledges and agrees that, where this Agreement is entered into under a MICTA, the Customer may appoint or delegate the enforcement of any of its rights from time to time under this Agreement to the Contract Authority.

---

### 3. Purchasing Services and/or Deliverables by Order

#### 3.1 Order Form

The Supplier must provide all Services and/or Deliverables specified in the Order Form and carry out all other Supplier's Activities on the terms of this Agreement.

#### 3.2 Electronic execution

Subject to applicable Laws, the parties may execute this Agreement and any document entered into under it, electronically (including through an electronic platform) and in one or more counterparts. Notwithstanding the manner in which a document under this Agreement is submitted or accepted, the terms of this Agreement will apply and any click-wrap, "pop-up" or other like terms and conditions of the Supplier appearing in the course of such submittal or acceptance will have no force or effect.



**Guidance note:** Electronic signatures and audio-visual witnessing is an evolving area of law. Where necessary, seek legal advice as to whether there are any legal restrictions that may apply to electronic execution (including through an electronic platform).

#### 3.3 Additional Orders

- (a) This clause applies where it is specified in Item 10 of the Order Form that the Customer may place Additional Orders for Services and/or Deliverables within the scope of this Agreement.
- (b) If, at any time during the Term, the Customer wishes to increase the volume or quantum of Services and/or Deliverables, the Customer may, in its sole discretion, do so by submitting a written notice to the Supplier for those increased Services

and/or Deliverables. The written notice will be in the form required by the Customer and will include information relating to the Additional Order, including the number of additional Services and/or Deliverables required.

- (c) Except to the extent agreed by the parties in writing, any increased Deliverables and/or Services will be supplied for the same rates and charges specified in the Payment Particulars.
- (d) The parties agree that each time the Customer submits an Additional Order to the Supplier:
  - (i) that Additional Order forms part of this Agreement, and will not constitute a separate contractual relationship between the parties; and
  - (ii) the Supplier must increase the supply of the Deliverables and/or Services in accordance with that Additional Order, subject to any reasonable qualifications specified in Item 10 of the Order Form.

3.4 No exclusivity or minimum commitment

The Supplier acknowledges and agrees that:

- (a) except to the extent expressly set out in the Payment Particulars, the Customer is under no obligation to acquire any minimum volumes of Services or Deliverables or to meet any minimum spend level under this Agreement; and
- (b) the Supplier is not an exclusive provider of the Supplier's Activities (nor activities which are the same as or similar to them) to the Customer, and the Customer is not, by executing this Agreement, restricted in any way from engaging any other person to provide activities which are the same as, or similar to, the Supplier's Activities.

3.5 Additional Conditions

The parties agree to comply with any Additional Conditions.



**Guidance note:** Any applicable directions of the New South Wales Procurement Board should be checked and complied with when agreeing Additional Conditions that alter, or are in addition to, those terms and conditions specified in any of the Core Terms or Module Terms. Any Additional Conditions must be consistent with all applicable New South Wales procurement Laws and policies and New South Wales Procurement Board Directions.

3.6 Reseller arrangements

Where specified in Item 12 of the Order Form, the parties agree that the Supplier may provide particular Services and/or Deliverables in the Supplier's capacity as a reseller and subject to any Additional Conditions relating to the reseller arrangement.



**Guidance note:** Reseller arrangements take different forms. The terms and conditions that apply to reseller arrangements will differ depending on the Services and Deliverables and the type of reseller arrangement. Each reseller arrangement needs to be considered on a case by case basis and tailored Additional Conditions developed subject to relevant governmental approvals.

---

**4. Relationship and governance**

**4.1 General**

The parties must perform their respective roles and responsibilities as set out in the Order Documents.



**Guidance note:** The Order Documents are defined in Schedule 1 and include not only the Order Form but also the Payment Schedule, all applicable Plans and the relevant Module Terms. Please note that certain Order Documents (namely, certain Plans) may come into effect after the Commencement Date.

**4.2 Nature of relationship**

Nothing in this Agreement creates or is intended to constitute a relationship between the parties of employer and employee, principal and agent, partnership or joint venturers, and neither party has authority to bind the other party. Neither party may hold itself out in any manner which is contrary to this clause 4.2.

**4.3 Governance**

- (a) Each party agrees to comply with any governance arrangements specified in the Order Documents, including any governance framework approved by the Customer pursuant to clause 4.3(b) (**Governance Framework**).
- (b) If specified in the Order Form, the Supplier must prepare and submit to the Customer for its approval a Governance Framework that contains the details specified in the Order Form. The Governance Framework must be submitted by the Supplier to the Customer's Representative by the time specified in the Order Form or such other time as reasonably required by the Customer's Representative.

---

**5. Term**

**5.1 Initial Term**

This Agreement begins on the Commencement Date and continues for the Initial Term, unless terminated earlier by agreement in writing between the parties or in accordance with the terms of this Agreement.

**5.2 Renewal Period**

- (a) Where a Renewal Period has been specified in Item 9 of the Order Form, the Customer may, in its sole discretion, extend the Term for a period not exceeding the relevant Renewal Period (up to, if any, the maximum number of renewals specified in that Item), by giving the Supplier a notice in writing at least 15 Business Days prior to the end of the then current Term (or such other notice period as may be specified in Item 9 of the Order Form).
- (b) Subject to clause 1.4(b), any Renewal Period exercised in accordance with clause 5.2(a) will be on the same terms and conditions of this Agreement as in effect at the end of the then current Term, unless the parties agree to amend this Agreement in accordance with clause 39.6.

**PART B: SUPPLIER'S ACTIVITIES**

---

**6. Performance of the Supplier's Activities****6.1 General**

The Supplier must carry out the Supplier's Activities in accordance with the timeframes, Specifications and requirements of this Agreement, including all requirements specified in the Order Documents.

**6.2 Customer Supplied Items**

- (a) Other than any CSI or any items expressly specified in the Order Documents or the Additional Conditions to be provided by an Other Supplier in connection with this Agreement, the Supplier must provide all necessary Materials and resources to carry out the Supplier's Activities in accordance with this Agreement.
- (b) The Supplier acknowledges and agrees that:
  - (i) unless the Customer agrees otherwise in writing, the Supplier will only receive access to the CSI specified in the Order Form;
  - (ii) the Supplier will obtain no title or interest to any CSI;
  - (iii) it is the Supplier's responsibility to inspect and assess any CSI before the Supplier or its Personnel use it to ensure the CSI is suitable and contains no defects; and
  - (iv) the Customer provides no warranty or representation about the suitability or fitness of any CSI for the Supplier's Activities or any other use (except to the extent the Order Form expressly contemplates CSI being put to a particular use or function in relation to this Agreement).
- (c) The following will not be a breach of this Agreement by the Customer, but in relation to Critical CSI, may entitle the Supplier to an extension of time if clause 6.8 applies:
  - (i) the Customer failing to supply the CSI at the times and in accordance with any requirements specified in this Agreement;
  - (ii) the Customer failing to maintain the CSI to any minimum standards specified in the Order Documents; or
  - (iii) any Other Supplier failing to supply items in accordance with any requirements specified in this Agreement.
- (d) The Supplier must:
  - (i) take all reasonable care of all CSI, including accounting for, preserving and handling all CSI in accordance with any requirements in the Order Form;
  - (ii) take reasonable steps to protect the CSI from any loss, destruction or damage;
  - (iii) not use any CSI other than:
    - A. for the purpose for which the CSI was designed and manufactured;

- B. for the purpose of carrying out the Supplier's Activities in accordance with this Agreement; and
- C. in accordance with any applicable third party terms and conditions relating to the use of, or dealing with, such CSI;
- (iv) not modify or adapt any CSI without the prior written consent of the Customer;
- (v) promptly inform the Customer's Representative of any loss, destruction or damage to any CSI and (to the extent known) its cause and comply with any directions of the Customer in relation to such CSI;
- (vi) not part with possession of any CSI unless the Customer has provided its prior written consent to do so, nor create or allow the creation of any lien, security interest or mortgage over any CSI; and
- (vii) if specified in the Order Form, pay the costs for the CSI as stated in the Order Form, and pay those costs in accordance with the timeframes for payment set out in the Order Form or otherwise agreed by the Customer.
- (e) Unless other arrangements have been agreed by the Customer in writing, the Supplier must, at its cost, return any CSI to the Customer (or otherwise deal with CSI as directed by the Customer's Representative in writing) once it is no longer required for the purposes of this Agreement.
- (f) The Supplier is liable to the Customer for any loss, destruction or damage to CSI to the extent that any such loss, destruction or damage is caused or contributed to by the Supplier or its Personnel or resulted from the failure of the Supplier to comply with its obligations under this clause 6.2.

### 6.3 ICT Accessibility

- (a) The Supplier acknowledges that the Customer is committed to:
  - (i) meeting Accessibility Standard AS EN 301 549 (**Accessibility Standard**); and
  - (ii) ensuring that the Services and Deliverables support access to information and communications technology for all Customer Users, regardless of disability.
- (b) Without limiting any other obligation under this Agreement, the Supplier must ensure that, to the extent reasonably practicable, all Services and Deliverables:
  - (i) are available to Customer Users on a non-discriminatory accessible basis and do not infringe anti-discrimination Laws; and
  - (ii) meet the Accessibility Standard and any other accessibility requirements to the extent specified in the Order Documents (unless otherwise required by the Order Form).

### 6.4 Co-operation with the Customer and Other Suppliers

- (a) Each party agrees to reasonably co-operate with the other party and its Personnel to promote the timely progress of the activities contemplated by this Agreement.
- (b) The Supplier acknowledges that the Customer may require the Supplier to co-operate and work collaboratively with any Other Suppliers in connection with the provision of the Supplier's Activities.

- (c) Where stated in the Order Documents or at the reasonable request of the Customer, the Supplier must:
- (i) permit any Other Suppliers to carry out their work;
  - (ii) reasonably co-operate with any Other Suppliers;
  - (iii) carefully co-ordinate and interface the Supplier's Activities with the services and work being carried out by any Other Suppliers in a manner that:
    - A. is as efficient and non-disruptive as reasonably practicable;
    - B. integrates, where applicable, with the services, works and deliverables that the Supplier and any Other Suppliers will provide; and
    - C. minimises the need for the Customer to be involved in resolving service problems or managing the tasks that the Supplier and Other Suppliers perform;
  - (iv) carry out the Supplier's Activities in a manner that minimises disruption or delay to the work of Other Suppliers; and
  - (v) comply with any additional requirements with respect to Other Suppliers or interfacing arrangements as specified in the Order Documents.

## 6.5 Project management

- (a) The parties must perform their obligations in accordance with any initial project plan that is included in the Order Documents or such other project plan that is approved by the Customer pursuant to this clause 6.5 (**Project Plan**).
- (b) Where specified in the Order Form, the Supplier must prepare and submit to the Customer's Representative for the Customer's approval a Project Plan that contains the details specified in the Order Form or in an Order Document.
- (c) The Supplier must submit the Project Plan by the date specified in the Order Documents or, where no date is specified, within 20 Business Days following the Commencement Date.
- (d) The Supplier agrees to update the Project Plan at the times or intervals set out in the Order Documents or at such other times as reasonably required by the Customer, including to reflect any Change Requests.
- (e) For clarity, the Project Plan is a Document Deliverable. Clause 8 therefore applies to the Project Plan, including any updates to it.

## 6.6 Staged implementation

- (a) Where the Order Documents specify that the Supplier's Activities will be carried out in different Stages, the Supplier must:
  - (i) carry out each Stage in accordance with the requirements and staging so specified in the Order Documents; and
  - (ii) not commence work on a Stage until it receives written notice from the Customer to proceed with the work in that Stage. Unless otherwise agreed by the parties in writing, the execution of this Agreement by the Supplier and the Customer is deemed to be sufficient notice to proceed with work on any first Stage described in the Order Documents.

- (b) Without limiting the Customer's rights under clause 6.6(c), at any time during the Term, the parties may:
  - (i) change the order of any Stages; or
  - (ii) vary the Supplier's Activities by removing one or more Stages from the scope of the Supplier's Activities,
 by following the Change Control Procedure under this Agreement.
- (c) The Customer may, at any time during the Term, and without having to comply with clause 6.6(b) and the Change Control Procedure, by written notice to the Supplier, remove from the scope of this Agreement any future Stages in respect of which approval to commence work has not been given by the Customer under clause 6.6(a)(ii).
- (d) The Customer will have no liability to the Supplier in respect of any Stage(s) that may be removed from the scope of the Supplier's Activities, except for those costs stated in Item 28 of the Order Form (if any) as being recoverable by the Supplier in such circumstance or as otherwise agreed by the parties in writing.
- (e) Nothing in this clause 6.6 will prevent the parties adopting a different project delivery methodology to that described in clause 6.6 (including involving agile, iterative and/or parallel development activities or other project methodology which is not Stage-based). Where an alternative project delivery methodology is specified in the Order Form, the Supplier must carry out the Supplier's Activities in accordance with the requirements for that alternative methodology as specified in the Order Form.

## 6.7 Delays

- (a) The Supplier must manage the Supplier's Activities, including to:
  - (i) anticipate and identify potential failures to meet a Date for Delivery, Key Milestone or other timeframe under this Agreement (**Delay**) (including, to the extent known or able to be reasonably anticipated, those Delays that may arise due to the Customer or an Other Supplier); and
  - (ii) take all necessary steps within its reasonable control to avoid or mitigate those potential Delays.
- (b) The parties must keep each other informed of anything that they become aware of which is likely to cause a Delay.

## 6.8 Extension of time

- (a) If a Delay occurs and that Delay was beyond the reasonable control of the Supplier, the Supplier may request an extension of time on the terms of this clause 6.8.
- (b) To request an extension of time under clause 6.8(a), the Supplier must within five Business Days of the commencement of the occurrence of the Delay, give the Customer's Representative written notice of the:
  - (i) particulars of the Delay and the occurrence causing the Delay; and
  - (ii) extension of time claimed in days, together with the basis for calculating that period.
- (c) The Customer will reasonably consider any Supplier request to extend a Date for Delivery or Key Milestone where the applicable Delay was beyond the reasonable control of the Supplier, could not have been reasonably mitigated or worked



around, and the Supplier has given notice as required by clause 6.8(b). The Customer may reduce any extension of time to the extent that the Supplier or its Personnel contributed to the Delay or the Supplier failed to take steps necessary both to preclude the cause of the Delay and to avoid or minimise the consequences of the Delay. In all other circumstances, the Customer may grant, decline or impose conditions on the granting of such request in its sole discretion.

(d) Where the Supplier requests an extension of time under clause 6.8(b) and that Delay has arisen because of:

- (i) the Customer's breach of this Agreement;
- (ii) a failure to provide any Critical CSI; or
- (iii) the acts or omissions of an Other Supplier,

the Customer must grant an extension of time, of a duration reasonably determined by the Customer having regard to the extent to which the Delay was attributable to the relevant breach, failure, acts or omissions.

(e) Whether or not the Supplier has made, or is entitled to make, a Claim for an extension of time under clause 6.8(a), the Customer may, in its sole discretion, at any time by written notice to the Supplier, unilaterally extend a Date for Delivery or Key Milestone by written notice to the Supplier. For clarity, no extension of time granted by the Customer will result in an increase or decrease to the Price, unless separately agreed pursuant to an agreed Change Request.

(f) Notwithstanding clause 35.1, where:

- (i) any dispute or difference arises between the parties in relation to this clause 6.8 or its subject matter; and
- (ii) a project management committee or other governance forum, which meets at least monthly, is provided for in the Order Documents,

then the party claiming the dispute or difference has arisen must not issue a Dispute Notice pursuant to clause 35.1(b) in relation to that dispute or difference unless it has first raised and sought to resolve that dispute or difference in the next occurring meeting of that committee or forum, without resolution at such meeting.

## 6.9 Delay costs

(a) To the extent a Delay arises which is attributable to the Customer's breach of this Agreement, a failure to provide any Critical CSI or the acts or omissions of an Other Supplier, the Supplier:

- (i) may advise the Customer of any proposed changes to the Price, the quantum of which must not exceed any additional, incremental cost and expense (calculated on a cost-only basis) directly attributable to:
  - A. undertaking and implementing any workarounds or remedial measures which are within the Supplier's control to implement or adopt, and which would minimise or lessen the impact of that Delay; and
  - B. any increase in the Supplier's Activities, or in the cost of the Supplier's Activities, as a result of that Delay,

**(Additional Activities);**

- (ii) must accompany any advice under clause 6.9(a)(i) with sufficient supporting evidence to substantiate the calculation of its proposed changes to the Price in accordance with the principles set out in that clause; and
  - (iii) may prepare and submit to the Customer a Change Request Form, which complies with clause 10, in respect of the Additional Activities referred to in clause 6.9(a)(i).
- (b) The parties will comply with the Change Control Procedure in relation to the Change Request initiated by that Change Request Form, including any approval, rejection or request for further information. For clarity, however (and subject to clause 6.9(c)), the Supplier is not required to perform any of the Additional Activities unless the Change Request is approved by the Customer.
- (c) Nothing in clause 6.9(b) will prevent the parties reaching some other written agreement in relation to the Additional Activities, for example, the Supplier performing aspects of the Additional Activities on an urgent and/or interim time and materials basis, subject to the subsequent formalisation of a detailed Change Request.

## 6.10 Site

- (a) Where specified in Item 16 of the Order Form, the Supplier must carry out the Supplier's Activities at the locations or sites specified in that Item (**Site**).
- (b) Where physical delivery of any Deliverables to a Site is required, the Supplier must, at no additional cost to the Customer, deliver any Deliverables:
  - (i) to the delivery area at the Site specified in the Order Form; and
  - (ii) on the Date for Delivery and between the hours stated in the Order Form,

or as otherwise agreed in writing between the parties.
- (c) The Supplier warrants, represents and undertakes that it has, and it will be deemed to have, done everything that would be expected of a prudent, competent and experienced supplier in assessing the risks which it is assuming under this Agreement in relation to carrying out the Supplier's Activities at the Site, including visiting and inspecting the Site and its surroundings and making its own assessment of the risks associated with the conditions at the Site and its surroundings.
- (d) Any failure of the Supplier to do any of the matters mentioned in clause 6.10(c) will not relieve the Supplier of its obligations to carry out the Supplier's Activities in accordance with this Agreement.
- (e) The Customer:
  - (i) is not obliged to:
    - A. provide the Supplier with sole access to the Site; or
    - B. carry out any work or provide any facilities or Materials to the Supplier (other than CSI or such other items specified in the Order Form) which may be necessary to enable the Supplier to obtain adequate access to carry out the Supplier's Activities; and

- (ii) may engage Other Suppliers to work upon, or in the vicinity of, the Site at the same time as the Supplier.
  - (f) In carrying out the Supplier's Activities, the Supplier must:
    - (i) minimise disruption or inconvenience to:
      - A. the Customer, occupiers, tenants and potential tenants of the Site in their occupation, use of or attendance upon any part of the Site; and
      - B. others having a right of access to the Site;
    - (ii) comply with all Policies, Codes and Standards of the Customer applicable to access to and attendance at the Site and any additional requirements specified in Item 16 of the Order Form;
    - (iii) at all reasonable times give the Customer's Representative, the Customer and any person authorised by the Customer access to the Supplier's Activities located at, or being carried out at, the Site (as applicable) or any location where the Supplier's Activities are being carried out; and
    - (iv) facilitate the Customer's supervision, examination or assessment of the Supplier's Activities at the Site or any location where the Supplier's Activities are being carried out.
- 

## **7. Transition-In**

### **7.1 Application**

This clause 7 applies if specified in the Order Form that the Supplier is required to provide any Transition-In Services as part of any Stage or part of the Supplier's Activities.

### **7.2 Transition-In Plan**

- (a) If the Order Form specifies that a Transition-In Plan must be prepared with respect to the Supplier's Activities, by the date specified in the Order Documents, the Supplier must prepare, and submit to the Customer's Representative for the Customer's approval, a plan setting out how the Supplier will carry out the Transition-In Services.
- (b) For clarity, the Transition-In Plan is a Document Deliverable. Clause 8 therefore applies to the Transition-In Plan, including any updates to it.

### **7.3 Transition-In Services**

- (a) The Supplier must supply any Transition-In Services specified in the Order Documents or in any Transition-In Plan that is developed pursuant to clause 7.2.
- (b) The Transition-In Services must be provided by the Supplier for the period specified in the Order Documents. Where no period is specified in the Order Documents, the Transition-In Services must be provided in a prompt and timely manner that will ensure that the Supplier can meet the Dates for Delivery, Key Milestones and other timeframes under this Agreement.

---

## 8. Document Deliverables

### 8.1 General

- (a) The process in this clause 8.1 applies to all Deliverables that comprise written, printed, digital or electronic Materials on which there is writing or other text or symbols, including all Plans (**Documents**) and which are subject to the Customer's approval under this Agreement.
- (b) The Supplier must submit all Document Deliverables to the Customer for approval in accordance with this clause 8 and by the dates specified in this Agreement or the Order Documents.
- (c) Document Deliverables must be submitted to the Customer's Representative, unless otherwise directed by the Customer in writing.
- (d) The Document Deliverables must:
  - (i) be in English;
  - (ii) be fit for their intended purpose;
  - (iii) be free of Defects;
  - (iv) in relation to any User Documentation, be current, complete, accurate and sufficient to enable the Customer and its Personnel to make full and proper use of the applicable Services and/or Deliverables; and
  - (v) comply with any applicable Specifications and any other requirements in the Order Documents.
- (e) A Document Deliverable will not be deemed approved by the Customer until the Customer notifies the Supplier in writing that it approves the relevant Document Deliverable, except where clause 8.2(f) applies.

### 8.2 Review

- (a) The Customer may:
  - (i) review any Document Deliverable (including any resubmitted Document Deliverable) prepared and submitted by the Supplier; and
  - (ii) within 15 Business Days of the submission by the Supplier of such Document Deliverable or resubmitted Document Deliverable (or any alternative timeframe set out in the Order Documents or otherwise agreed between the parties in writing):
    - A. approve the Document Deliverable; or
    - B. reject the Document Deliverable if, in its reasonable opinion, the Document Deliverable does not comply with the Specifications and other requirements of this Agreement.
- (b) The Customer will accompany any rejection under clause 8.2(a)(ii)B with a description of why the relevant Document Deliverable does not comply with the Specifications and other requirements of this Agreement.
- (c) A Document Deliverable does not fail to comply with the Specifications and other requirements of this Agreement exclusively because of:

- (i) any opinion expressed in the Document Deliverable, provided that the opinion expressed is the professional opinion held by the Supplier;
  - (ii) the style, formatting or layout of the Document Deliverable, unless the style, formatting or layout is of a nature that it:
    - A. fails to meet the requirements in clause 8.1(d); or
    - B. affects the readability or useability of the Document Deliverable; or
  - (iii) semantics which do not impact the interpretation of the substantive matters conveyed in the Document Deliverable.
- (d) If the Customer gives the Supplier a notice rejecting a Document Deliverable under clause 8.2(a)(ii)B, the Supplier must, within five Business Days (or any alternative timeframe set out in the Order Documents or otherwise agreed between the parties in writing), prepare a revised version of the Document Deliverable which addresses all of the amendments and issues required by the Customer.
- (e) The parties must repeat the process in this clause 8.2 until the Customer approves each Document Deliverable in accordance with clause 8 or terminates this Agreement.
- (f) Where the period referred to in clause 8.2(a)(ii) elapses without the Customer approving or rejecting the Document Deliverable, the Supplier must submit to the Customer's Representative a written reminder notice identifying the Document Deliverable in respect of which it requires a decision by the Customer. If the Customer does not approve or reject the relevant Document Deliverable or otherwise communicate with the Supplier in relation to that reminder notice within 10 Business Days of its receipt, then the relevant Document Deliverable will be deemed to have been approved by the Customer.

### 8.3 No obligation

- (a) The Customer does not assume or owe any duty of care to the Supplier to review any Document or Document Deliverable for errors, omissions or compliance with this Agreement.
- (b) No review, acceptance or approval of, comments upon, rejection of, or failure to review or comment upon or reject, any Document or Document Deliverable provided by the Supplier to the Customer under this Agreement or any other direction by the Customer about that Document or Document Deliverable will:
  - (i) relieve the Supplier from, or alter or affect, the Supplier's liabilities or responsibilities whether under this Agreement or otherwise at Law; or
  - (ii) prejudice the Customer's rights against the Supplier whether under this Agreement or otherwise at Law.

### 8.4 User Documentation

- (a) The Supplier must, at its sole cost, provide the User Documentation to the Customer's Representative except where otherwise specified in the Order Form.
- (b) The User Documentation must be supplied in an electronic format and by the time specified in the Order Documents or, where no timeframe is specified, where reasonably required by the Customer.
- (c) Where it is specified in the Order Form that the Customer also requires any User Documentation in a hard copy format (or where otherwise requested by the

Customer), the Supplier must provide the Customer's Representative with at least one copy of the User Documentation at no additional charge to the Customer.

- (d) The Supplier must ensure that any User Documentation that is supplied to the Customer's Representative:
  - (i) provides adequate instructions on how to enable the Customer and Customer Users to utilise the Services and Deliverables (as applicable) without reference to the Supplier; and
  - (ii) complies with the same requirements as specified in clause 8.1(d) in relation to Document Deliverables.
- (e) The Supplier must update the User Documentation as is needed for the Customer and Customer Users to be able to use the Services and Deliverables (as applicable) in an efficient and effective manner.

---

## 9. Defects

- (a) If, prior to the expiry of the Warranty Period, the Customer discovers or is informed that there is a Defect, the Customer may give the Supplier an instruction (with which the Supplier will comply) specifying the Defect and doing one or more of the following:
  - (i) requiring the Supplier to correct the Defect, or any part of it;
  - (ii) advising the Supplier that the Customer will accept the Deliverable or Service, or any part thereof, despite the Defect; or
  - (iii) advising the Supplier that the Customer will accept the Deliverable or Service, or any part thereof, despite the Defect, in exchange for a reasonable reduction in, or adjustment to, the cost of the Deliverables or Services which were impacted by the Defect,

and pursuing any other remedy it may have at Law or under this Agreement subject to compliance with the dispute resolution procedure in clause 35.
- (b) If, prior to the expiry of the Warranty Period, the Supplier identifies a Defect, the Supplier must notify the Customer in writing within one Business Day of identifying the Defect.
- (c) If, prior to the expiry of the Warranty Period, the Supplier identifies a Defect or an instruction is given under clause 9(a)(i), the Supplier must, at no cost to the Customer, correct the Defect:
  - (i) in accordance with all applicable Service Levels, or if no applicable Service Levels apply, within 15 Business Days after the date on which the non-compliance was notified to, or identified by, the Supplier (or such other timeframe as agreed between the parties in writing); and
  - (ii) in a manner which will cause as little inconvenience to the Customer and Customer Users as is reasonably possible.
- (d) The parties acknowledge that where the Defect relates to any Services, the Customer may request that the Supplier, and the Supplier must, supply the affected Services again.
- (e) If multiple Defects are identified, the Customer may request the Supplier to prioritise the rectification of such Defects, and the Supplier must comply with any such

request. However, for clarity, any prioritisation must remain consistent with any applicable Service Levels.

- (f) Unless otherwise agreed between the parties in writing, the Warranty Period will be increased by a period of time equivalent to the time that the relevant Services and Deliverables were unavailable or their functionality materially decreased due to a Defect.
- (g) The Customer's rights under this Agreement and at Law will not be affected or limited by:
  - (i) the rights conferred upon the Customer by this clause;
  - (ii) the failure by the Customer or the Customer's Representative to exercise any such rights; or
  - (iii) any instruction of the Customer under this Agreement.
- (h) For clarity, the Warranty Period will not be deemed to exclude or restrict any guarantee that is provided at Law with respect to any Deliverable or Service.

---

## **10. Change Control Procedure**

### **10.1 Change Requests**

- (a) Either party may request a variation to the Supplier's Activities, including:
  - (i) varying the Specifications or the nature, quality or scope of the Deliverables and Services, the sequence or time in which they are performed or substituting alternative Materials (if applicable);
  - (ii) varying the order of any Stages or removing one or more Stages from the scope of the Supplier's Activities;
  - (iii) increasing, decreasing, omitting, deleting or removing any Deliverables and/or Services;
  - (iv) varying the CSI and/or any responsibilities or dependencies attributable to the Customer; and/or
  - (v) any change resulting in the Supplier providing services and/or deliverables that are materially different to the Services and Deliverables specified in the Order Form,

**(Change Request).**
- (b) Except to the extent expressly specified in the Module Terms, no Change Request is binding on either party or to be carried out by the Supplier until the Change Control Procedure specified in this clause 10 is followed.

### **10.2 Process for submitting and agreeing to Change Requests**

- (a) Each Change Request must be submitted in a form substantially similar to the Change Request Form included at Schedule 5 (or such other form approved by the Customer) and containing the details specified in that Change Request Form or such other details as may be reasonably required by the Customer.
- (b) Where rates and charges for any Change Requests, and/or a pricing methodology, have been specified in the Payment Particulars, then the Prices in the relevant Change Request must not exceed those rates and charges and must be based on

any applicable pricing methodology specified in the Payment Particulars. Where no rates, charges or methodology are specified, prices must be based on those costs and expenses reasonably and necessarily incurred by the Supplier to implement the relevant Change Request.

- (c) The party receiving the draft Change Request Form must notify the other party in writing as to whether it:
  - (i) approves or rejects the Change Request; or
  - (ii) requires further information in relation to any aspect of the Change Request.
- (d) The parties must respond to Change Requests and requests for information regarding Change Requests within seven Business Days of receiving the request or such other timeframe as reasonably agreed between the parties having regard to the nature and substance of the work required by the relevant request.
- (e) Each party will act reasonably in preparing, submitting, reviewing, considering and assessing Change Requests.
- (f) If a Change Request is approved, the:
  - (i) parties must promptly execute the relevant Change Request Form; and
  - (ii) Supplier must perform the Supplier's Activities in accordance with the executed Change Request Form.
- (g) No Change Request is binding on either party or to be carried out by the Supplier until the relevant Change Request Form is executed by both parties in accordance with this clause 10.

### **10.3 Electronic transactions**

- (a) The parties may submit and execute Change Request Forms electronically (including through an electronic platform) and in one or more counterparts.
- (b) Unless otherwise directed by the Customer, either party may also submit Change Request Forms through its designated electronic ordering portal to which it may give the other party access from time to time.

### **10.4 Acknowledgements**

The parties acknowledge and agree that:

- (a) the Change Control Procedure does not apply to changes to the Core Terms, the Module Terms or any Additional Conditions, which must be effected in accordance with the variation procedure specified in clause 39.6;
- (b) the Customer does not need to follow the Change Control Procedure with respect to:
  - (i) Additional Orders submitted in accordance with clause 3.3; or
  - (ii) the Customer's exercise of its unilateral right to:
    - A. remove from the scope of this Agreement any future Stages pursuant to clause 6.6(c); or
    - B. reduce the scope of this Agreement pursuant to clause 29;



- (c) the Customer is not obliged to pay the Supplier for implementing any Change Request unless the parties have complied with this clause 10;
- (d) the Customer is under no obligation to place Change Requests;
- (e) if any Change Request made pursuant to the Change Control Procedure omits or removes any part of the Supplier's Activities, the Customer may thereafter either provide those Supplier's Activities itself or employ or engage third parties to do so;
- (f) the Customer may, in its sole discretion, agree or reject a Change Request;
- (g) no Change Request will invalidate, or amount to a repudiation of, this Agreement; and
- (h) each party must bear its own costs in preparing, submitting and negotiating any Change Request.

---

## **11. Personnel**

### **11.1 Nominated Personnel**

- (a) The Supplier must ensure that:
  - (i) each of its Nominated Personnel is made available to perform their role/responsibilities as set out in Item 18 of the Order Form; and
  - (ii) it immediately notifies the Customer's Representative if the Supplier becomes unable or unwilling to comply with this clause 11.1 or otherwise breaches this clause 11.1.
- (b) The Supplier must not remove or replace any of the Nominated Personnel unless the:
  - (i) Customer requests that the Nominated Personnel are replaced pursuant to clause 11.3(e); or
  - (ii) Nominated Personnel are no longer available to carry out the Supplier's Activities due to a substantial change in the relevant Nominated Personnel's personal circumstances (including compassionate leave, carers' leave or other extended leave, serious illness, injury, death, termination of employment by the Supplier or resignation).

### **11.2 Replacement of Nominated Personnel**

If the Supplier is required to replace any Nominated Personnel in accordance with clauses 11.1(b) or 11.3(e), the Supplier must ensure that any replacement is:

- (a) approved by the Customer. The Customer must act reasonably in granting or withholding approval, or granting approval subject to conditions. If requested by the Customer, the Supplier must provide the Customer with such information as the Customer requires concerning any proposed replacement of any Nominated Personnel (including a resume and an opportunity to interview them); and
- (b) of equal or superior ability to, and has the required experience of, the original Nominated Personnel and meets the Personnel requirements specified in this Agreement.

### 11.3 Supplier's Personnel

- (a) The Supplier must ensure that all of its Personnel engaged or employed by the Supplier in carrying out the Supplier's Activities:
  - (i) are aware of, and comply with, the Supplier's obligations under this Agreement as if they were the Supplier;
  - (ii) prior to carrying out any part of the Supplier's Activities, are properly trained and qualified and have the requisite competencies, skills, qualifications and experience to:
    - A. perform the duties allocated to them; and
    - B. understand the Supplier's obligations under this Agreement, including with respect to privacy, security, confidentiality and safety; and
  - (iii) are provided with regular training to ensure that the Supplier's Personnel's skills and qualifications are maintained in accordance with all applicable Best Industry Practice.
- (b) On the Customer's request or as part of any audit conducted pursuant to clause 37.2, the Supplier must promptly provide the Customer or its nominee with evidence that the obligations under this clause 11.3 have been complied with (including with respect to the training of the Supplier's Personnel).
- (c) The Supplier must ensure that all of its Personnel, when on the Customer's premises or when accessing Customer Data or the Customer's systems, equipment or facilities, comply with the reasonable requirements and directions of the Customer (including with regard to the Customer's safety and security requirements).
- (d) The Supplier must ensure that its Personnel when entering any Site comply with any conditions of entry or other Site specific requirements as specified in the Order Documents or notified by the Customer to the Supplier from time to time.
- (e) The Customer may, acting reasonably and in its discretion, give notice in writing requiring the Supplier to remove any of its Personnel (including Nominated Personnel) from work in respect of this Agreement, together with its reasons for removal. The Supplier must promptly arrange for the removal of such Personnel and their replacement with Supplier Personnel reasonably acceptable to the Customer.
- (f) The Supplier must ensure that it (and where appropriate, its outgoing Personnel) effects a process that:
  - (i) minimises any adverse impact on, or delay in, the performance of the Supplier's Activities; and
  - (ii) effects a smooth transition between the outgoing and replacement Personnel, including by identifying and recording:
    - A. any processes and systems in place (or proposed) to manage the provision of the Supplier's Activities; and
    - B. the detail of any outstanding issues in relation to the Supplier's Activities,

for which any of the outgoing Supplier's Personnel were responsible.

- (g) The process for transition to the replacement Personnel by the Supplier must be performed as expeditiously as possible with regard to the Supplier's Activities, the Dates for Delivery and other timeframes under this Agreement, and to the reasonable satisfaction of the Customer.
- (h) The Supplier will be solely responsible, at its sole cost, for compliance with clause 11.2, including finding and replacing Supplier's Personnel in accordance with clause 11.3(e).
- (i) The Supplier must properly manage its Personnel resourcing (including any planned absences) to maintain a sufficient level of Personnel engaged or employed in the provision of the Supplier's Activities (both in terms of quality and quantity of such Personnel) to ensure that all relevant roles are, and continue to be, adequately resourced and that the Supplier's Activities are provided in accordance with this Agreement.

#### 11.4 Deed of Confidentiality and Privacy

- (a) If specified in Item 19 of the Order Form or at the request of the Customer's Representative, the Supplier's Personnel involved in the provision of the Supplier's Activities (or who may receive or have access to the Customer's Confidential Information or Personal Information in connection with this Agreement), must sign a deed in substantially the same form as the document in Schedule 6 or such other deed as required by the Customer (**Deed of Confidentiality and Privacy**).
- (b) Where the Customer requires an alternate Deed of Confidentiality and Privacy to that specified in Schedule 6, it must include obligations that are consistent with the privacy and confidentiality obligations under this Agreement.
- (c) Unless otherwise agreed by the Customer in writing, the Deed of Confidentiality and Privacy must be signed and returned to the Customer's Representative prior to the Supplier's Personnel commencing the Supplier's Activities or being provided with access to the Customer's Confidential Information or Personal Information.

#### 11.5 Subcontracting

- (a) The Supplier must not subcontract any of its obligations under this Agreement unless specified in Item 20 of the Order Form (or otherwise pre-approved by the Customer in writing). Such approval may also be given in respect of classes or categories of subcontractor or types of subcontracted activities and made subject to any applicable conditions. The use of permitted subcontractors may be withheld or given on such conditions as specified in the Order Form or otherwise notified by the Customer to the Supplier in writing.
- (b) If the Customer consents to the engagement of any subcontractor on a conditional basis, then the Supplier must comply with those conditions when it engages that subcontractor.
- (c) A permitted subcontractor may not further subcontract the relevant obligations to another person without the Customer's prior written consent.
- (d) The Customer may, by written notice to the Supplier, revoke its consent to any permitted subcontractor if the Customer, acting reasonably, has concerns about that permitted subcontractor's or its personnel's:
  - (i) performance of the Supplier's Activities; or
  - (ii) compliance with (or ability to comply with) the terms of this Agreement.
- (e) Where practicable to do so, the Customer must engage in reasonable advance consultation with the Supplier in relation to its concerns regarding a permitted

subcontractor's (or its personnel's) performance or compliance, including whether those concerns may be otherwise addressed or remediated, before the Customer gives a notice of revocation under clause 11.5(d).

- (f) The Supplier is solely responsible for managing its supply chains and any risks in its supply chains, including ensuring any permitted subcontractor's compliance with clause 13.
- (g) Any subcontracting by the Supplier does not relieve the Supplier of any of its obligations under this Agreement.
- (h) The Supplier must ensure that each of its subcontractors comply with all of the terms of this Agreement to the extent that they are relevant to the subcontractor.
- (i) The Supplier is responsible for its subcontractors, and liable for their acts and omissions, as though they were the acts and omissions of the Supplier.
- (j) If specified in the Order Form or if required by the Customer as a condition of granting consent to the Supplier's use of any subcontractor, the Supplier must arrange for its subcontractors to enter into a subcontractor deed on terms consistent with, and no less onerous than, the parts of this Agreement applicable to the subcontractor's activities.
- (k) The Order Form may specify additional procurement policy requirements which the parties have agreed will apply to, or be prioritised in, any subcontracting arrangement by the Supplier, including the Policies, Codes and Standards. The parties agree to comply with any such requirements.

## 11.6 Background checks

- (a) The Supplier must:
  - (i) prior to involving any of its Personnel in carrying out the Supplier's Activities, undertake all necessary background checks of those Personnel to ensure that they are fit and proper to provide the Supplier's Activities; and
  - (ii) monitor and assess its Personnel throughout their involvement in the Supplier's Activities to ensure that they remain fit and proper to provide the Supplier's Activities.
- (b) Without limiting the generality of clause 11.6(a), if specified in Item 22 of the Order Form or where not so specified in that Item but reasonably required by the Customer, the Supplier must:
  - (i) carry out any specific background checks of its Personnel as specified in Item 22 of the Order Form or as requested by the Customer, including criminal record and "Working with Children" checks; and
  - (ii) provide the results of those checks to the Customer's Representative within the timeframe specified in Item 22 of the Order Form, or if no time is specified, within five Business Days of receipt (or within such other time as reasonably required by the Customer).
- (c) Where the outcome of a background check reveals that any of the Supplier's Personnel are not fit and proper to be involved in the provision of the Supplier's Activities, the Supplier must not use those Personnel with respect to such activities.
- (d) The Supplier acknowledges and agrees that:

- (i) all background checks will be undertaken at the Supplier's sole cost, unless otherwise agreed by the Customer in writing;
- (ii) the Customer may provide the results of any background checks to the Contract Authority or any other Government Agency; and
- (iii) the Supplier is solely responsible for obtaining all necessary consents, in accordance with the Privacy Laws, in connection with the conduct of any background checks and the sharing and use of those background checks as contemplated under this clause 11.6.

**11.7 Compliance with employment Laws**

- (a) The Supplier undertakes to comply with all applicable employment Laws in relation to itself and its Personnel, including in relation to workers' compensation, payroll tax, fringe benefits tax, PAYG tax, group tax, superannuation contributions, leave entitlements and any other employment or related benefit or entitlement.
- (b) The Supplier acknowledges and agrees that:
  - (i) it is solely responsible for the obligations under clause 11.7(a); and
  - (ii) neither the Supplier, nor its Personnel have, pursuant to this Agreement, any entitlement from the Customer in relation to any form of employment or related benefit.

**11.8 Non-solicitation**

- (a) Neither party may, without the prior written consent of the other party, engage, employ, induce or cause a third party to induce the other party's Personnel engaged in the performance of this Agreement to enter into a contract for service or a contract of employment with it.
- (b) The restrictions in clause 11.8(a) will apply during the Term and for a period of six months after the end of the Term.
- (c) General solicitation for employment which is placed in good faith, such as on a jobs website or in a newspaper advertisement, will not constitute a breach of this clause 11.8.
- (d) The parties agree that the restrictions in this clause 11.8 are necessary to protect the legitimate interests of each party.

---

**12. Compliance**

**12.1 Compliance with Laws and directions**

While carrying out the Supplier's Activities, the Supplier must:

- (a) acquire and maintain all Authorisations necessary for the performance of the Supplier's Activities;
- (b) ensure that the Supplier's Activities comply with all applicable Laws (including all applicable Australian Laws, even if the Supplier is not domiciled in Australia); and
- (c) comply with any reasonable directions made by the Customer in relation to the Supplier's Activities.

## 12.2 Policies, Codes and Standards

- (a) Without limiting the generality of clause 12.1, the Supplier must, in performing its obligations under this Agreement, comply with all Policies, Codes and Standards.
- (b) Where it is specified in Item 17 of the Order Form that this clause 12.2(b) applies, the Supplier:
  - (i) must comply with the Aboriginal Participation Plan and all relevant Aboriginal participation and reporting requirements under the Aboriginal Procurement Policy and clause 37.1(b)(ii);
  - (ii) acknowledges and agrees that Training Services NSW has established the Aboriginal participation fund to receive payments when the Supplier does not meet contracted Aboriginal participation requirements; and
  - (iii) acknowledges and agrees that where the Supplier does not meet its Aboriginal participation requirements under this Agreement, the Agency may, in accordance with the Aboriginal Procurement Policy, withhold payments due to the Supplier pursuant to this Agreement and direct the funds to an account held by Training Services NSW.

## 12.3 Policy Changes

- (a) If there is:
  - (i) any change to any of the Policies, Codes and Standards specified in this Agreement (including with respect to any security requirements); or
  - (ii) the introduction of any new Policies, Code and Standards in addition to those specified in this Agreement,

with which the Customer requires the Supplier to comply (**Policy Change**), then (without limiting any other express rights of the Customer or obligations of the Supplier under this Agreement) where:

  - (iii) the Supplier's compliance with that Policy Change can, with the Supplier's best efforts, be achieved without the incurrence of material additional cost and expense to the Supplier; or
  - (iv) irrespective of the cost of complying with the Policy Change, the Supplier's compliance with its obligations under clause 12.1 would involve the Supplier complying with that Policy Change in any event,

then the Supplier must comply with the Policy Change at no additional cost to the Customer.
- (b) If neither clauses 12.3(a)(iii) nor 12.3(a)(iv) apply and the Supplier cannot comply with a Policy Change without incurring material additional cost and expense, then:
  - (i) the Supplier must promptly notify the Customer in writing of the additional, incremental cost and expense (calculated on a cost-only and zero-margin basis) that would be directly attributable to its compliance with the Policy Change, accompanied with evidence to substantiate the additional, incremental costs and expenses (including information as to how those costs and expenses have been calculated); and
  - (ii) following receipt of such notification, the Customer may:
    - A. approve the incurrence of the costs and expenses notified to it under clause 12.3(b)(i), in which case the Supplier must

comply with the relevant Policy Change and, subject to so complying, will be entitled to invoice the Customer for such costs and expenses;

- B. reject the incurrence of the costs and expenses notified to it under clause 12.3(b)(i), in which case, the Supplier will not be required to incur those costs or to comply with the Policy Change; or
- C. require the Supplier to, in which case the Supplier must, participate in reasonable good faith discussions with the Customer in relation to an alternative approach to managing the Policy Change.

## 12.4 Work health and safety

Without limiting the Supplier's obligations under any other provision of this Agreement, the Supplier must:

- (a) comply, and must ensure that its Personnel comply, with the WHS Legislation (including any obligation under the WHS Legislation to consult, co-operate and coordinate activities with all other persons who have a work health and safety duty in relation to the same matter);
- (b) if requested by the Customer's Representative or required by the WHS Legislation, demonstrate compliance with the WHS Legislation, including providing evidence of any approvals, prescribed qualifications or experience, or any other information relevant to work health and safety matters;
- (c) notify the Customer's Representative promptly (and in any event within 12 hours of such matter arising) of all work health, safety and rehabilitation matters arising out of, or in any way in connection with, the Supplier's Activities;
- (d) insofar as the Supplier, in carrying out the Supplier's Activities, is under any duty imposed by the WHS Legislation, do everything necessary to comply with any such duty;
- (e) ensure that it does not do anything or fail to do anything that would cause the Customer to be in breach of the WHS Legislation; and
- (f) comply with any additional work health and safety requirements specified in the Order Form or as otherwise reasonably required by the Customer from time to time.

## 12.5 Work health and safety where Supplier's Activities include construction work

- (a) This clause applies where construction work forms part of the Supplier's Activities.
- (b) In this clause 12.5, the terms "**construction work**", "**principal contractor**" and "**workplace**" have the same meanings assigned to those terms under the WHS Legislation.
- (c) Where the Customer engages the Supplier as the principal contractor:
  - (i) the Customer authorises the Supplier to have management and control of each workplace at which construction work is to be carried out and to discharge the duties of a principal contractor, under the WHS Legislation;

- (ii) the Supplier accepts the engagement as principal contractor and agrees to discharge the duties imposed on a principal contractor by the WHS Legislation; and
- (iii) the Supplier's engagement and authorisation as principal contractor will continue until:
  - A. the Supplier delivers the Supplier's Activities in accordance with this Agreement;
  - B. the Supplier achieves Acceptance in respect of each Deliverable subject to Acceptance Testing under this Agreement; and
  - C. any rectification work that is "construction work" that is carried out during the Warranty Period is completed,

unless sooner revoked by the Customer, including by terminating this Agreement at Law or pursuant to this Agreement.

**12.6 The environment**

Where applicable to the performance of the Supplier's Activities, the Supplier must:

- (a) provide all Supplier's Activities in a manner that does not cause or threaten to cause pollution, contamination or environmental harm to, on or outside a Site or other location;
- (b) ensure that it and its Personnel comply with all applicable environmental Laws and Policies, Codes and Standards; and
- (c) follow New South Wales Government policies and guidelines concerning the safe disposal of any hazardous substances.

**12.7 Conflicts of Interest**

- (a) The Supplier must:
  - (i) promptly notify the Customer in writing if a Conflict of Interest arises or is likely to arise during its performance of the Supplier's Activities; and
  - (ii) take all necessary action as may be reasonably required by the Customer to avoid or minimise such a Conflict of Interest.
- (b) If such a Conflict of Interest, in the Customer's view, significantly affects the interests of the Customer, and the Supplier is unable to resolve the Conflict of Interest to the satisfaction of the Customer within 14 days of receipt of a notice from the Customer, then the Customer will be entitled to terminate this Agreement under clause 29.1(d).

---

**13. Modern Slavery**

**13.1 Core Modern Slavery Obligations**

- (a) For the purpose of this clause 13 and any Modern Slavery terms in the Module Terms, the definition of "Personnel" is extended to include any other workers (howsoever described) who may be engaged for the purposes of this Agreement, but are not employed by the relevant party including but not limited to independent contractors, secondees, and consultants.



- (b) Each party must:
- (i) not engage in Modern Slavery;
  - (ii) take Reasonable Steps to ensure that it, its Personnel, and in the case of the Supplier its Related Bodies Corporate, comply with Modern Slavery Laws as applicable;
  - (iii) take Reasonable Steps to ensure that its relevant Personnel include provisions equivalent to the Core Modern Slavery Obligations (including this sub-clause) in any contracts with their suppliers; and
  - (iv) take Reasonable Steps to ensure that its relevant Personnel provide their respective directors, officers, employees and suppliers with at least the minimum level of wages and other entitlements required by law
- (together, the **Core Modern Slavery Obligations**).

### 13.2 Price

Each party acknowledges and agrees that the Price supports each party to comply with its Core Modern Slavery Obligations.

### 13.3 Systems and policies

Each party agrees that it will establish, implement, and maintain for the term of this Agreement, appropriate systems and policies as required to meet its Core Modern Slavery Obligations.

### 13.4 Disclosure

The Supplier represents, warrants and undertakes that, as at the Commencement Date and on a continuing basis for the term of this Agreement, the Supplier has disclosed:

- (a) to the extent the Supplier is aware, any:
- (i) actual or reasonably suspected Modern Slavery engaged in; and
  - (ii) notices, investigations, proceedings or claims arising in any jurisdiction in relation to any actual or reasonably suspected breach of Modern Slavery Laws,
- by the Supplier, any of the Supplier's Personnel, or the Supplier's Related Bodies Corporate, while performing any contract with the Supplier, whether or not the Modern Slavery arises in the performance of this Agreement; and
- (b) all actions taken to remedy said Modern Slavery or breach of Modern Slavery Laws.

### 13.5 Information

- (a) For the purpose of this clause 13.5, "Information" may include (as applicable) information as to any risks of, actual or suspected occurrences of, and remedial action taken in respect of, Modern Slavery but excludes Personal Information.
- (b) Each party must, subject to any restrictions under any applicable Laws by which it is bound, and without limiting the obligations in this Agreement, provide, and use reasonable endeavours to ensure each party's Personnel (and Related Bodies Corporate in the case of the Supplier) provide, to the other party any Information and other assistance, as reasonably requested by the requesting party, to enable the other party to meet any of its obligations under the Modern Slavery Laws and

associated regulatory requirements (for example, in the case of the Customer, any applicable annual reporting requirements and New South Wales Procurement Board Directions), including co-operating in any Modern Slavery audit undertaken by the Customer or the NSW Audit Office and providing reasonable access to the Customer's and/or Audit Office's auditors to interview the Supplier's Personnel.

- (c) The Supplier must notify the Customer in writing as soon as it becomes aware of a material change to any of the Information it has provided to the Customer in relation to Modern Slavery under clause 13.5(b).
- (d) The Supplier may provide any Information or report requested by the Customer in the form of a previously-prepared statement or re-purposed report, for example a statement provided in response to a similar request for Information from another Australian public sector agency, or refer the Customer to its publicly available Modern Slavery Statement, provided that such statement or report provides generally the same Information as that sought by the Customer.
- (e) The Supplier must, during the Term and for a period of seven years thereafter:
  - (i) maintain; and
  - (ii) upon the Customer's reasonable request, give the Customer access to, and/or copies of,

records in the possession or control of the Supplier to trace, so far as practicable, the supply chains of all Services and Deliverables provided under this Agreement and to enable the Customer to assess the Supplier's compliance with this clause 13.

### **13.6 Response to Modern Slavery incident**

- (a) Where one party forms the view that there has been a breach of the obligations under this clause 13 that is reasonably capable of being remedied, the parties must promptly develop a remediation plan to take Reasonable Steps to remedy the breach in accordance with this Agreement.
- (b) Each party must make reasonable efforts proportionate to their contribution to the breach to implement this remediation plan, as determined by the Customer in its sole discretion.

### **13.7 Termination**

- (a) In addition to any other rights or remedies under this Agreement or at Law, the Customer may terminate this Agreement, upon written notice and with immediate effect if, in the Customer's reasonable view, the Supplier has:
  - (i) failed to notify the Customer as soon as it became aware of an actual or suspected occurrence of Modern Slavery in its operations or supply chains (or in those of any entity that it owns or controls);
  - (ii) failed to take Reasonable Steps to respond to an actual or suspected occurrence of Modern Slavery in its operations or supply chains (or in those of any entity that it owns or controls) including a failure to implement a remediation plan; or
  - (iii) otherwise committed a breach of its obligations under this clause 13 and the breach (or breaches) is not remedied within 15 days of the Supplier receiving a notice to remedy.
- (b) Before exercising its termination rights under clause 13.7(a) of this Agreement, the Customer must consult with relevant stakeholders on whether Modern Slavery may

arise from such termination and the Reasonable Steps to prevent or mitigate such risk of Modern Slavery.

---

## **14. Acceptance Testing**

### **14.1 General**

- (a) Unless otherwise specified in the Order Form, this clause 14 will apply in relation to the supply of any Deliverables that are not Documents.
- (b) Where the parties have agreed further details as to the form or the conduct of Acceptance Tests in the Order Documents, those details apply in addition to this clause 14, except to the extent expressly stated in the Order Form.

### **14.2 Testing by Supplier**

- (a) Before delivery by the Supplier to the Customer of any Deliverable (or any component thereof) that is subject to Acceptance Testing, the Supplier must:
  - (i) carry out the tests in accordance with any Test Plan and to ensure that the Deliverable meets the Acceptance Criteria for the Deliverable;
  - (ii) following testing, supply the Customer with the test results in accordance with the requirements and timeframes in the Test Plan and Order Documents, or where no requirements or timeframes are specified in those documents, promptly on completion of each test;
  - (iii) if the Supplier determines that a Deliverable (or component thereof) does not meet any Acceptance Criteria, promptly remedy that non-compliance; and
  - (iv) when appropriate, notify the Customer that the relevant Deliverable (or applicable component thereof) is ready for Acceptance Testing by the Customer.
- (b) Where directed by the Customer, the Supplier must:
  - (i) permit the Customer or its nominee to witness any tests conducted pursuant to this clause 14.2; and
  - (ii) provide the Customer with evidence as reasonably required by the Customer,

to demonstrate that the tests have been successfully completed in accordance with clause 14.2.

### **14.3 Testing by the Customer**

- (a) The Customer may carry out Acceptance Tests in respect of each Deliverable to which Acceptance Testing applies and the Supplier must provide all reasonable assistance required by the Customer in connection with the Customer's Acceptance Testing.
- (b) If the Customer carries out Acceptance Tests, the Customer must conclude the Acceptance Tests in accordance with any timeframes specified in the Order Documents or, where no timeframes are specified, within a time reasonably determined by the Customer.
- (c) Following completion of the Customer's Acceptance Testing in respect of a Deliverable, the Customer must either:

- (i) provide to the Supplier an Acceptance Certificate in respect of that Deliverable; or
  - (ii) notify the Supplier that the Acceptance Criteria in respect of that Deliverable have not been met.
- (d) Neither the full or partial Acceptance of any Deliverable nor any exercise by the Customer of any option or other right under this clause 14 will:
  - (i) operate as a sole or exclusive remedy; or
  - (ii) limit or prejudice any rights or remedies of the Customer under this Agreement or at Law.
- (e) Where the Deliverable meets the Acceptance Criteria, the Customer must issue the Acceptance Certificate no later than 10 Business Days from completion of the Acceptance Testing, or within such other timeframe specified in the Order Documents.
- (f) Where the period referred to in clause 14.3(e) elapses without the Customer either providing an Acceptance Certificate to the Supplier in respect of that Deliverable or notifying the Supplier that the Acceptance Criteria have not been met, the Supplier must submit to the Customer's Representative a written reminder notice identifying the Deliverable in respect of which it requires a decision by the Customer. If the Customer does not take one of the actions referred to in clause 14.3(c) or otherwise communicate with the Supplier in relation to that reminder notice within 15 Business Days of its receipt, then the relevant Deliverable will be deemed to have been Accepted by the Customer.

#### **14.4 Effect of failure to meet Acceptance Criteria**

- (a) If the Acceptance Criteria in respect of a Deliverable have not been met, the Customer may, at its option, do any of the following:
  - (i) issue a notice to the Supplier that requires the Supplier to comply with clause 14.4(b), accompanied with a description of the areas in which the relevant Deliverable has failed to meet the Customer's Acceptance Testing;
  - (ii) Accept the Deliverable subject to a reasonable reduction in the Price as reasonably agreed between the parties or, in the absence of agreement, as reasonably determined by the Customer to reflect the greater of the:
    - A. cost to the Customer of correcting the Defects in the Deliverable; or
    - B. reduced features, functionality or quality of operation as a result of those Defects; or
  - (iii) if the Deliverable contains a Material Defect that, in the Customer's reasonable opinion, is incapable of remedy or the Supplier has failed to remedy that Material Defect within 20 Business Days after delivery of the Deliverable (or such other time as specified in the Order Form or agreed between the parties in writing), immediately terminate this Agreement or reduce its scope pursuant to clause 29.1(d).
- (b) If the Supplier receives a notice under clauses 14.4(a)(i) or 14.4(c)(i), the Supplier must, at its cost, within 20 Business Days (or such other time as specified in the Order Form or agreed between the parties in writing) after the date of the notice:

- (i) supply such additional services to rectify any Defect in the Deliverable as may be necessary to enable the Deliverable to meet the Acceptance Criteria, including, if necessary, replacing the Deliverable;
  - (ii) co-operate with the Customer with respect to any repeat Acceptance Testing; and
  - (iii) provide all assistance required by the Customer in relation to the repeated Acceptance Tests.
- (c) If the Acceptance Criteria in respect of a Deliverable have not been met following repeat Acceptance Testing, the Customer may, at its option, do any of the following:
  - (i) require the Supplier to again comply with clause 14.4(b);
  - (ii) Accept the Deliverable subject to a reduction in the Price as reasonably agreed between the parties or, in the absence of agreement, as reasonably determined by the Customer in accordance with the same principles as described in clause 14.4(a)(ii); or
  - (iii) immediately terminate or reduce the scope of this Agreement pursuant to clause 29.1(d).
- (d) The Customer reserves the right to remedy any Defects or to appoint third parties to do so if the Supplier fails to correct any Defect that has been notified by the Customer to the Supplier and which the Supplier has not corrected within the timeframe required by this clause 14.4. At the Customer's request, the Supplier must reimburse the Customer for the costs incurred by the Customer in relation to the remediation of the relevant Defects, based on commercially reasonable rates and charges.

**14.5 Effect of Acceptance Certificate**

An Acceptance Certificate will constitute Acceptance for the purposes of this clause 14, but will not be taken as an admission or evidence that the Deliverables comply with, or that the Supplier has performed its obligations under, this Agreement.

---

**15. Performance**

**15.1 Performance obligations**

The Supplier must:

- (a) carry out the Supplier's Activities:
  - (i) in accordance with this Agreement, including the Order Documents;
  - (ii) with all due skill, care and diligence and in a proper, regular and timely manner;
  - (iii) in a manner that encourages the most efficient use of resources and promotes the achievement of any Customer objectives specified in the Order Documents;
  - (iv) to a high standard and in accordance with Best Industry Practice for work of a similar nature to the Supplier's Activities;
  - (v) in a manner that is safe to both people and the environment;

- (vi) in a manner that minimises any disruption, interference or inconvenience to the Customer or its operations, Personnel or Other Suppliers;
- (vii) to enable all Deliverables to operate in accordance with this Agreement, and to meet the Acceptance Criteria applicable to them;
- (viii) to ensure that all timeframes under this Agreement are met, including all Key Milestones and Dates for Delivery;
- (ix) in accordance with any relevant Statement of Work;
- (x) in accordance with the Specifications; and
- (xi) otherwise in accordance with the other requirements of this Agreement; and
- (b) provide Deliverables to the Customer which:
  - (i) are of high quality and are fit for the purpose for which they are required as detailed in, or reasonably ascertainable from, the Order Documents;
  - (ii) achieve Acceptance;
  - (iii) where applicable, will (on delivery, or at the time of performance of the relevant Supplier's Activities in relation to the applicable Deliverable(s)):
    - A. have been tested and verified, in accordance with Best Industry Practice, to be free from any Viruses; and
    - B. be compatible and interoperable with those features or characteristics of the Customer Environment described in the Order Documents and will not detrimentally affect the operation or performance of the Customer Environment or any part thereof.

## 15.2 Service standards and Service Levels

- (a) The Supplier must carry out the Supplier's Activities in a manner that meets or exceeds any Service Levels or, if none are specified in the Order Documents, in a timely and efficient manner taking into account the Supplier's obligations under this Agreement.
- (b) Unless otherwise specified in the Order Documents, the Supplier agrees to:
  - (i) measure its performance under this Agreement against any Service Levels;
  - (ii) provide the Customer with the results of all performance reviews;
  - (iii) use appropriate measurement and monitoring tools and procedures to measure performance accurately; and
  - (iv) provide the Customer with sufficient information in relation to the Supplier's assessment and monitoring of its performance pursuant to this clause 15.
- (c) The Supplier's liability under clause 15.2(a) is reduced to the extent that the failure to meet or exceed a Service Level was caused or contributed to by the:
  - (i) breach or negligence of the Customer;

- (ii) unavailability or failure of any Critical CSI; or
- (iii) acts or omissions of an Other Supplier.

### 15.3 Consequences for failing to meet a Service Level

- (a) If the Supplier fails to meet any applicable Service Levels, it will:
  - (i) notify the Customer of the Service Level failure in accordance with clause 15.6;
  - (ii) provide timely updates to the Customer's Representative, in accordance with the incident notification requirements in the Service Levels or on request by the Customer, in relation to the progress being made in rectifying the failure;
  - (iii) promptly take whatever action that is commercially reasonable to minimise the impact of the failure;
  - (iv) correct the failure as soon as practicable;
  - (v) promptly take all necessary actions to prevent the recurrence of the failure and any other failure resulting from the same facts, circumstances or root cause(s); and
  - (vi) where requested by the Customer or specified in the Order Documents, promptly investigate the facts, circumstances or root cause(s) of the failure and promptly following conclusion of the investigation, deliver to the Customer a written report identifying such facts, circumstances or root cause(s) in the form requested by the Customer.
- (b) Without limiting any right or remedy available to the Customer under this Agreement or at Law, if the Supplier does not meet a Service Level, then the consequences for failing to meet a Service Level will be as set out in the Order Documents (such as service credits, service rebates or termination rights).
- (c) The parties acknowledge and agree that any service credits or service rebates calculated in accordance with the Order Documents:
  - (i) reflect the provision of a lower level of service than is required under this Agreement; and
  - (ii) are reasonable and represent a genuine pre-estimate of the diminution in value the Customer will suffer, as represented by an adjustment to the Price, as a result of the delivery by the Supplier of a lower level of service than that required by the applicable Service Level, but are not an exclusive remedy with respect to other categories of Loss.

### 15.4 Performance reports

The Supplier must provide to the Customer's Representative the following written or electronic reports and reporting tools:

- (a) a monthly (unless a different frequency is specified in the Order Form) report on the performance and availability of the Services and/or Deliverables in respect of the immediately preceding month, including detail relating to:
  - (i) the quantity of Services and/or Deliverables supplied to the Customer (including, where applicable, the rates of utilisation);

- (ii) the total Price paid by the Customer in respect of that reporting period and cumulatively over the Term to date, tracked over time and usage, including any applicable discounts, credits, rebates and other benefits; and
  - (iii) any other matters specified in the Order Form;
- (b) a monthly report of the Supplier's performance against any Service Levels, including any accrued service credits or service rebates;
- (c) the additional reports specified in the Module Terms and Order Form for the time period specified in those documents (which may include, where so specified, access to real-time or near-real time reporting capability); and
- (d) any other reports as reasonably requested by the Customer from time to time, including as may be required by the Customer to enable the Customer to meet its internal or New South Wales Government compliance, regulatory and operational reporting obligations.

## 15.5 Performance reviews

- (a) If it is stated in Item 25 of the Order Form that the parties must conduct a service and performance review of the Supplier's performance under this Agreement, then the parties must conduct such reviews at the intervals and in accordance with any requirements in the Order Form (or as otherwise agreed between the parties).
- (b) All reviews must be undertaken by representatives of both parties who have the authority, responsibility and relevant expertise in financial and operational matters appropriate to the nature of the review. Where this Agreement is made under a MICTA, either party may request the involvement of the Contract Authority in any review.

## 15.6 Notice

The Supplier must notify the Customer immediately if it becomes aware that it is not able to, or reasonably anticipates that it is not able to, perform the Supplier's Activities in accordance with the performance standards and requirements specified in this Agreement.

## 15.7 Meetings

- (a) The Supplier's Representative must meet with the Customer's Representative or other Personnel at the times and at the locations specified in the Order Form or as otherwise agreed between the parties in writing.
- (b) The parties agree that meetings may be held by video or teleconference if required by the Customer.

---

## 16. Liquidated Damages

- (a) This clause 16 applies if Item 29 of the Order Form provides for Liquidated Damages to be payable in relation to a failure by the Supplier to meet a Key Milestone.
- (b) If the Supplier fails to meet a Key Milestone, the Supplier must pay the Customer the amount of Liquidated Damages set out in, or otherwise calculated in accordance with, Item 29 of the Order Form in relation to the period between the relevant Key Milestone and the date on which the:
  - (i) Supplier achieves the relevant Key Milestone; or



- (ii) Customer terminates the relevant Order (or this Agreement),  
  
but subject always to the maximum number of days (if any) for which Liquidated Damages are payable, or maximum percentage of the value of applicable Prices, as may be specified in Item 29 of the Order Form.
- (c) The Supplier acknowledges that the Liquidated Damages payable under this clause 16 are a reasonable and genuine pre-estimate of the Loss likely to be suffered by the Customer in respect of a failure by the Supplier to meet the relevant Key Milestone. However, they do not limit the rights or remedies of the Customer to claim Loss from the Supplier in the event that the amount of Loss actually incurred by the Customer exceeds such genuine pre-estimate, in the amount of the difference between such Loss actually incurred and the Liquidated Damages payable under this clause 16.
- (d) The Supplier will not be liable to pay Liquidated Damages to the extent that the Supplier's failure to achieve a Key Milestone was caused or contributed to by the:
  - (i) breach or negligence of the Customer;
  - (ii) unavailability or failure of any Critical CSI; or
  - (iii) acts or omissions of an Other Supplier.

---

**17. Intellectual Property**

**17.1 Ownership of Existing Materials**

Unless otherwise specified in Item 37 of the Order Form, the parties agree that nothing in this Agreement will affect the ownership of the Intellectual Property Rights in any Existing Materials.

**17.2 Licence to use Existing Materials**

- (a) Unless otherwise specified in the applicable Module Terms or in Item 37 of the Order Form, the Supplier grants to the Customer an irrevocable, non-exclusive, worldwide, transferable, royalty-free licence to use, copy, adapt, translate, reproduce, modify, communicate and distribute any Intellectual Property Rights in the Supplier's Existing Materials for any purpose in connection with the:
  - (i) Customer performing its obligations and exercising its rights under this Agreement;
  - (ii) full use of any Services and/or Deliverables in which the Supplier's Existing Material is incorporated, including installing, operating, upgrading, modifying, supporting, enhancing and maintaining the Deliverables or integrating them with any other software, systems, equipment or infrastructure owned, operated or maintained by the Customer or a Government Agency;
  - (iii) performance of tests and other quality assurance processes, including Acceptance Tests, in relation to the Deliverables and systems that may integrate or interoperate with the Deliverables; or
  - (iv) carrying out, or exercise, of the functions or powers of the Customer, a Government Agency or the Crown, including any statutory requirements concerning State records or auditing.
- (b) Where:

- (i) the Supplier's Existing Material is incorporated into any New Materials; and
- (ii) clause 17.4(b) applies in respect of those New Materials,

then the licence granted in clause 17.2(a) will also include, in respect of the Supplier's Existing Materials, an equivalent right and licence to that described in clause 17.4(b), to the extent required to support the exploitation and commercialisation of the Intellectual Property Rights in the relevant New Materials under that clause (but excluding commercial exploitation of the Supplier's Existing Materials independently of the New Materials in which they are incorporated).

- (c) The rights and licences granted by the Supplier to the Customer under clause 17.2(a):

- (i) do not permit the Customer to sell, monetise or commercialise the Supplier's Existing Materials, except as otherwise stated in Item 37 of the Order Form; and
- (ii) are sub-licensable by the Customer (on the same terms, for the same period and for the same purposes as set out in clause 17.2(a)), without additional charge to any:
  - A. contractor, subcontractor or outsourced service provider (subject to such persons being under reasonable obligations of confidentiality owed to the Customer or another Government Agency) acting on behalf of, or providing products and/or services for the benefit of, the Customer or a Government Agency; or
  - B. Government Agency.

- (d) Unless otherwise specified in Item 37 of the Order Form, the Customer grants to the Supplier, a non-exclusive, non-transferable, revocable, worldwide, royalty-free licence to use the Intellectual Property Rights in the Customer's Existing Materials, to the extent required for the Supplier to perform, and solely for the purposes of the Supplier performing, its obligations under this Agreement.

### **17.3 Ownership of New Materials**

- (a) Unless otherwise specified in Item 37 of the Order Form, where the Supplier creates New Materials in carrying out the Supplier's Activities, the ownership of all Intellectual Property Rights in those New Materials vests in, or is transferred or assigned to, the Supplier immediately on creation.
- (b) If the parties agree in Item 37 of the Order Form that the Intellectual Property Rights in any New Materials will be owned by the Customer, then ownership of all Intellectual Property Rights in those New Materials vests in the Customer immediately on creation or is transferred or assigned by the Supplier to the Customer immediately on creation, free of any encumbrances, security interests and third party rights.

### **17.4 Customer licence to use Supplier owned New Materials**

- (a) Where the Supplier owns the Intellectual Property Rights in any New Materials, unless otherwise specified in the applicable Module Terms or in Item 37 of the Order Form, the Supplier grants to the Customer an irrevocable, non-exclusive, worldwide, transferable, royalty-free licence to use, copy, adapt, translate, reproduce, modify, communicate and distribute the Intellectual Property Rights in such New Materials, for any purpose in connection with the:

- (i) Customer performing its obligations and exercising its rights under this Agreement;
  - (ii) full use of any Services and/or Deliverables in which New Material is incorporated, including installing, operating, upgrading, modifying, supporting, enhancing and maintaining the Deliverables or integrating them with any other software, systems, equipment or infrastructure owned, operated or maintained by the Customer or a Government Agency;
  - (iii) performance of tests and other quality assurance processes, including Acceptance Tests, in relation to the Deliverables and systems that may integrate or interoperate with the Deliverables; or
  - (iv) carrying out, or exercise, of the functions or powers of the Customer, a Government Agency or the Crown, including any statutory requirements concerning State records or auditing.
- (b) Where specified in Item 37 of the Order Form, the licence granted in clause 17.4(a) will also include the right and licence to exploit and commercialise the Intellectual Property Rights in New Materials for the purposes specified in clause 17.4(a) or such other purposes specified in Item 37 of the Order Form.
- (c) The rights and licences granted by the Supplier to the Customer under clauses 17.4(a) and 17.4(b) are sub-licensable by the Customer (on the same terms and for the same purposes as set out in those clauses) to any person, without additional charge, including to any:
- (i) contractor, subcontractor or outsourced service provider (subject to such persons being under reasonable obligations of confidentiality owed to the Customer or another Government Agency (as applicable)) acting on behalf of, or providing products and/or services for the benefit of, the Customer or a Government Agency; or
  - (ii) Government Agency.

## 17.5 Licence term

Except where otherwise specified in Item 37 of the Order Form or in the applicable Module Terms, the licences granted under clauses 17.2 and 17.4 will be perpetual in relation to the purposes specified in those clauses.

## 17.6 Supplier Licence to use Customer owned New Materials

Where it is specified in Item 37 of the Order Form that Intellectual Property Rights in any New Materials are owned by the Customer, then to the extent required to enable the Supplier to perform its obligations under this Agreement, the Customer grants to the Supplier, a non-exclusive, non-transferable, revocable, worldwide, royalty-free licence to use the Intellectual Property Rights in those New Materials, to the extent required for the Supplier to perform, and solely for the purposes of the Supplier performing, its obligations under this Agreement.

## 17.7 Third party Intellectual Property Rights

Unless stated otherwise in Item 37 of the Order Form or the applicable Module Terms, the Supplier must, in respect of any third party Intellectual Property Rights used in the production of Deliverables, included in any Deliverables, or required by the Customer to receive the Services:

- (a) ensure that it procures for the Customer a licence on terms no less favourable than:
  - (i) the terms set out in this clause 17 or any applicable Module Terms; or

- (ii) on such other terms specified in Item 37 of the Order Form;
- (b) ensure that the use of such third party Intellectual Property Rights does not constrain the Customer's use of the Services or any Deliverables; and
- (c) otherwise, not use any third party Intellectual Property Rights in the provision of the Services or the production of any Deliverables.

## 17.8 Open Source Software

- (a) The Supplier must not, without the prior written consent of the Customer:
  - (i) develop or enhance any Deliverable using Open Source Software; or
  - (ii) incorporate any Open Source Software into any Deliverable.
- (b) In requesting any consent from the Customer under clause 17.8(a), the Supplier must provide the Customer with:
  - (i) complete and accurate copies of any licence agreement, the terms and conditions of which would apply to the proposed use or incorporation of the Open Source Software into a relevant Deliverable; and
  - (ii) a description of how such use or incorporation may affect the provision of the Supplier's Activities, the Customer's licence rights under this Agreement and the Customer's and Customer Users' uses or other dealings with the relevant Deliverable,

for the Customer's review and consideration.
- (c) Where the Customer provides its consent in relation to the use or incorporation of any Open Source Software under clause 17.8(a) the:
  - (i) Customer must comply with the terms and conditions notified to it in clause 17.8(b)(i) in relation to the use of that Open Source Software; and
  - (ii) Supplier must ensure that the use of that Open Source Software will not:
    - A. result in an obligation to disclose, licence or otherwise make available any part of the Customer Environment, software of the Customer, Customer Data or Confidential Information to any third party; or
    - B. diminish the Supplier's obligations or the Customer's rights under this Agreement.

## 17.9 Consents and Moral Rights

- (a) Prior to provision to the Customer or use in connection with this Agreement, the Supplier must ensure that it obtains all necessary consents from all authors of all Materials and Deliverables provided or licenced to the Customer under this Agreement to any use, modification or adaptation of such Materials and Deliverables to enable the Customer to fully exercise its Intellectual Property Rights under this Agreement, including:
  - (i) the use, modification or adaptation of the Materials or Deliverables; or
  - (ii) any other dealing which might otherwise constitute an infringement of the author's Moral Rights.

- (b) To the extent the Customer provides any CSI for use by the Supplier and that CSI incorporates any Intellectual Property Rights, the Customer must procure all necessary:
  - (i) licences of Intellectual Property Rights in that CSI; and
  - (ii) Moral Rights consents from all authors of that CSI,
 to the extent required to enable the Supplier to perform, and solely for the purposes of the Supplier performing, its obligations under this Agreement with respect to that CSI.

## 17.10 Prohibited activities

The licences granted to the Customer under clauses 17.2 and 17.4 do not permit the Customer to disassemble, decompile or reverse engineer any software-based elements of the materials licensed under those clauses, provided that this restriction shall not apply to the extent it would not be permissible under the *Copyright Act 1968* (Cth) in relation to particular acts conducted for certain purposes, as specified in that legislation.

## 17.11 Additional obligations

The Supplier must, at its cost, do all acts (and procure that all relevant persons do all acts) as may be necessary to give effect to the intellectual property provisions in this clause 17, including by executing (or procuring the execution of) any required documents or effecting any required registrations.

## 17.12 Warranties and acknowledgements

- (a) The Supplier represents, warrants and undertakes that:
  - (i) it has all the Intellectual Property Rights and has procured the necessary Moral Rights consents required to:
    - A. carry out the Supplier's Activities; and
    - B. enable the Customer and each Customer User (or other permitted licensee) to use the requisite Services and/or Deliverables in the manner envisaged by this Agreement; and
  - (ii) its supply of the requisite Services and/or Deliverables to the Customer, and the Customer's, Customer Users' (and other permitted licensees') use of them in the manner envisaged by this Agreement will not infringe any Intellectual Property Rights or Moral Rights.
- (b) The Supplier acknowledges and agrees that the Intellectual Property Rights and licences (as applicable) granted under this Agreement (including this clause 17) do not limit or reduce the Supplier's or its Personnel's obligations under this Agreement with respect to the Customer's Confidential Information, Personal Information and Customer Data.

## 17.13 Replacement of Deliverables

Without limiting the Customer's rights under clause 34.1(c), if any Claim of the kind described in that clause is made or brought in respect of Intellectual Property Rights or Moral Rights, the Supplier must, at its election and at no additional cost to the Customer:

- (a) procure for the Customer the right to continue to use the Services and/or Deliverables on terms no less favourable than those set out in this Agreement;

- (b) promptly replace or modify the Services and/or Deliverables so that the alleged infringement ceases and the replaced or modified Services and/or Deliverables provides the Customer with no less functionality and performance as that required by this Agreement; or
- (c) only where the options in paragraphs (a) and (b) are not reasonably possible and subject to prior consultation with and receipt of approval from the Customer, accept return of the affected Deliverable or cease to provide the affected Service (as applicable) and, within 30 days, refund the Customer any fees paid for the relevant Service and/or Deliverable, subject to any reasonable deduction for any in-production use already made by the Customer of the relevant Service and/or Deliverable.

---

## 18. Escrow

- (a) If specified in Item 38 of the Order Form (or if otherwise agreed between the parties in writing) that any Escrow Materials are to be held in escrow, the Supplier must arrange for:
  - (i) itself, the Customer and an escrow agent approved by the Customer to enter into an escrow agreement in substantially the same form as Schedule 7 (or such other form as may be prescribed by the relevant escrow agent and agreed by the parties in writing); or
  - (ii) the Customer to become a party to an escrow arrangement which already covers the Escrow Materials which the Customer regards as a satisfactory arrangement.
- (b) Any escrow arrangement to which the Customer becomes a party under clause 18(a) must continue in effect for at least the period stated in Item 38 of the Order Form, unless otherwise agreed between the parties in writing.
- (c) The Supplier must consult with, and comply with the reasonable directions of, the Customer in any negotiations with the escrow agent arising under clause 18(a).
- (d) Any escrow arrangement must be entered into by the timeframe specified in Item 38 of the Order Form, or if no timeframe is specified, as otherwise reasonably required by the Customer.

## PART C: DATA AND SECURITY

---

### 19. Customer Data

#### 19.1 Obligations in relation to Customer Data

- (a) This clause 19 applies where the Supplier or its Personnel obtains access to, or collects, uses, holds, controls, manages or otherwise processes, any Customer Data in connection with this Agreement.
- (b) The Supplier acknowledges and agrees that it obtains no right, title or interest with respect to any Customer Data, other than a right to use Customer Data for the sole purpose of, and only to the extent required for, the carrying out of the Supplier's Activities in accordance with this Agreement.
- (c) As between the Supplier and Customer, all rights in and in relation to Customer Data remain with the Customer at all times and the Supplier assigns all rights, title and interest in the Customer Data to the Customer on creation. The Supplier agrees to do all things necessary to assign or vest ownership of all rights in Customer Data to the Customer on creation.

- (d) The Supplier must:
- (i) not use any Customer Data for any purpose other than for the sole purpose of, and only to the extent required for, carrying out the Supplier's Activities in accordance with this Agreement;
  - (ii) not sell, assign, lease or commercially transfer or exploit any Customer Data;
  - (iii) not perform any data analytics on Customer Data, except to the sole extent permitted by this Agreement;
  - (iv) ensure that all of its Personnel who access, or have the ability to access, Customer Data are appropriate to do so, including passing any background or security checks as required by this Agreement;
  - (v) apply to the Customer Data the level of security and (if applicable) encryption that is required under this Agreement;
  - (vi) apply technical and organisational controls which are appropriate to ensure that all Customer Data is at all times protected from any unauthorised access, modification or disclosure and only handled and processed in accordance with the terms of this Agreement and any other security requirements reasonably specified by the Customer; and
  - (vii) ensure that Customer Data is at all times managed in accordance with the *State Records Act 1998* (NSW) (to the extent applicable); and
  - (viii) ensure that its Personnel (including subcontractors) comply with this clause 19.1(d) and manage and safeguard Customer Data in accordance with all other requirements of this Agreement.

## 19.2 Security of Customer Data

- (a) The Supplier must comply with the security requirements set out in this Agreement, including in the Order Documents (**Information Security Requirements**) in carrying out the Supplier's Activities.
- (b) The Supplier must establish, maintain, enforce and continuously improve its safeguard and security measures, and take all reasonable steps, to ensure that Customer Data is protected against misuse, interference and loss, and from unauthorised access, modification or disclosure.
- (c) The Supplier must immediately notify the Customer where it is or may be required by Law to disclose any Customer Data to any third party contrary to the terms of this Agreement.

## 19.3 Location of Customer Data

- (a) The Supplier must not:
  - (i) transfer, store, process, access, disclose or view Customer Data; or
  - (ii) perform any of its obligations under this Agreement which could involve Customer Data being stored, processed, accessed, disclosed or viewed, outside of New South Wales, Australia, except in accordance with clause 19.3(b).
- (b) Notwithstanding clause 19.3(a), the Supplier may transfer, store, process, access, disclose or view Customer Data outside of New South Wales:

- (i) if permitted under the Order Form or any relevant Module Terms;
- (ii) at the locations specified in the Order Documents (or as otherwise agreed to in writing in advance by the Customer); and
- (iii) subject to the Supplier's and its Personnel's compliance with the Data Location Conditions.

#### **19.4 Backup of Customer Data**

- (a) If specified in the Order Documents that the Supplier is required to make and store backup copies of Customer Data as part of the Services, the Supplier must make and store backup copies of the Customer Data in accordance with all requirements (including as to frequency, maturity of backup and approved locations) set out or referenced in this Agreement (including the Module Terms and Order Form) or as otherwise reasonably required by the Customer by notice to the Supplier.
- (b) Where clause 19.4(a) applies, the Supplier must check the integrity of all backup Customer Data annually (or at such other time required by the Order Form).

#### **19.5 Restoration of lost Customer Data**

Notwithstanding any other rights the Customer may have under this Agreement, if as a result of any act or omission of the Supplier or its Personnel in the carrying out of the Supplier's Activities or in discharging their privacy or security obligations under this Agreement:

- (a) any Customer Data is lost; or
- (b) there is any unauthorised destruction or alteration of Customer Data,

the Supplier must take all practicable measures to immediately restore the Customer Data (including, where applicable, in accordance with any requirements specified in the Order Documents). Any such measures will be at the Supplier's sole cost where and to the extent such loss, destruction or alteration to the Customer Data was caused or contributed to by an act or omission of the Supplier or any of its Personnel.

#### **19.6 Rights to access, use, extract and retrieve Customer Data**

Where Customer Data is in the Supplier's possession or control, the Supplier must enable the Customer to:

- (a) access, use and interact with the Customer Data (which may be through access controls identified in the Order Documents); and
- (b) extract, retrieve and/or permanently and irreversibly delete those copies of the Customer Data which are in the Supplier's possession or control (which may be performed by self-service tools), or otherwise provide the Customer Data to the Customer:
  - (i) in accordance with all applicable timeframes and requirements under this Agreement;
  - (ii) at no additional charge to the Customer;
  - (iii) in a human readable, commonly accepted format which does not require the Customer to purchase additional licences it does not already hold, or in the same format as the Customer Data was uploaded (for example, a semi-structured format); and



- (iv) in order to maintain the relationships and integrity of those copies of the Customer Data.

## **19.7 Record, retention, return and destruction of the Customer Data**

- (a) If specified in the Order Form, the Supplier must:
  - (i) establish, keep and maintain complete, accurate and up-to-date records of all Customer Data accessed, collected or changed by it; and
  - (ii) make copies of the records referred to in clause 19.7(a)(i) available to the Customer immediately upon request.
- (b) On the date that any Customer Data is no longer needed for the purposes of the Supplier carrying out the Supplier's Activities (or should the Customer notify the Supplier that the Customer Data is no longer needed), the Supplier must at its sole cost:
  - (i) immediately stop using the relevant Customer Data (except as permitted under this Agreement); and
  - (ii) at the Customer's direction (subject to clause 19.7(c)):
    - A. securely and permanently destroy all records and backups of the Customer Data in accordance with the timeframes under this Agreement and supply the Customer's Representative with a certificate of destruction that confirms that this has occurred; or
    - B. securely return all records of Customer Data to the Customer in accordance with the timeframes under this Agreement.
- (c) The Supplier will be entitled to retain copies of records of Customer Data to the extent, and only for the period, that such retention is mandated by any Laws to which the Supplier is subject.
- (d) The Supplier acknowledges and agrees that:
  - (i) where the Order Documents specify additional requirements for the capture and retention of audit log data, including categories of data and periods of retention, the Supplier must comply with those requirements; and
  - (ii) notwithstanding anything to the contrary in this Agreement, no Customer Data should be destroyed until the Supplier has met the data retrieval requirements under clause 32.1.

## **19.8 General**

- (a) If requested by the Customer, the Supplier must provide the Customer with a report setting out how it will comply, and has complied, with its obligations under this clause 19.
- (b) Where applicable, the Supplier must comply with any additional obligations relating to Customer Data as may be specified in the Order Documents.
- (c) For clarity, nothing in this clause 19 relieves the Supplier of its obligations under clause 20.

---

## 20. Privacy

### 20.1 Protection and use of Personal Information

- (a) If the Supplier or its Personnel obtains access to, or collects, uses, holds, controls, manages or otherwise processes, any Personal Information in connection with this Agreement (regardless of whether or not that Personal Information forms part of the Customer Data), the Supplier must (and must ensure that its Personnel):
- (i) comply with all Privacy Laws, as though it were a person subject to those Privacy Laws;
  - (ii) only use that Personal Information for the sole purpose of carrying out the Supplier's Activities;
  - (iii) not disclose the Personal Information to any other person without the Customer's prior written consent, which may be given in respect of classes or categories of subcontractors or types of subcontracted activities and made subject to any applicable conditions;
  - (iv) not transfer the Personal Information outside New South Wales, Australia or access it, or allow it to be accessed, from outside New South Wales, Australia unless permitted in the Order Form or relevant Module Terms and subject to the Supplier's and its Personnel's compliance with the Data Location Conditions;
  - (v) protect the Personal Information from loss, unauthorised access, use, disclosure, modification and other misuse and in accordance with the security requirements under this Agreement;
  - (vi) if it becomes aware, or has reasonable grounds to suspect, that there has been a Security Incident involving Personal Information:
    - A. immediately make all reasonable efforts to contain the Security Incident involving Personal Information;
    - B. comply with clause 22;
    - C. unless otherwise directed by the Customer, comply with the Customer's published data breach policy and any data breach procedures and documentation specified in the Order Form, as well as any other Policies, Codes and Standards relevant to the management, mitigation and response to a Security Incident;
    - D. comply with any reasonable direction (including as to timeframes) from the Customer with respect to a Security Incident involving Personal Information (which may include, for example, activities to support the Customer's response to the incident and compliance with the New South Wales mandatory notification of data breach scheme); and
    - E. take all reasonable steps to prevent such Security Incident involving Personal Information from recurring; and
  - (vii) notify the Customer as soon as reasonably possible if the Supplier is approached by any privacy commissioner or other Authority concerning any Personal Information.

- (b) Where the Supplier is required by Law to produce or disclose any information or to develop or provide any response or explanation to an Authority in relation to any incident (including any privacy breach) concerning the handling, management, safekeeping or protection of any Personal Information in connection with this Agreement, it must (to the extent such action is permitted by Law), provide notice to the Customer as soon as reasonably possible of the nature and content of the information to be produced or disclosed and, prior to providing a response to the Authority or disclosing any Personal Information, engage in reasonable consultation with the Customer regarding its proposed response or explanation.

**20.2 Data Management and Protection Plan**

- (a) Where the Supplier or its Personnel collects, uses, discloses, holds or otherwise processes any Personal Information in connection with this Agreement, the Supplier must, for the duration of those activities, have and maintain (and prepare and implement, if not already in existence) a Data Management and Protection Plan that caters for the handling of that Personal Information.
- (b) The Data Management and Protection Plan must be provided to the Customer's Representative within five Business Days following the Commencement Date or such other time as agreed between the parties in writing.
- (c) The Data Management and Protection Plan must:
  - (i) set out measures for how the Supplier and its Personnel will:
    - A. comply with the Privacy Laws; and
    - B. protect Personal Information;
  - (ii) be consistent with the Privacy Laws and the security and privacy requirements under this Agreement, provided that, where the Privacy Laws and the security and privacy requirements under this Agreement both address standards in respect of same subject matter, the Data Management and Protection Plan must reflect the higher standard; and
  - (iii) cover such other matters as reasonably required by the Customer.
- (d) The Supplier must review and update the Data Management and Protection Plan annually or at such other times as reasonably required by the Customer to address a Security Incident or breach of this Agreement.
- (e) The Supplier must comply with its latest Data Management and Protection Plan and provide the latest copy of that Plan to the Customer's Representative on request.

**20.3 No limitation of obligations**

Nothing in this clause 20 is intended to limit any obligations that the Supplier has at Law with respect to privacy and the protection of Personal Information.

---

**21. Security**



**Guidance note:** Additional security requirements or standards may be specified in an Order Form.

## 21.1 Scope of the Supplier's security obligations

- (a) Without limiting any other security obligation under this Agreement, the Supplier's security obligations under this clause apply to:
  - (i) the Supplier's Activities; and
  - (ii) Customer Data and Personal Information, where and to the extent that the Supplier or its Personnel is in the possession of, controls, or is able to control, such data and information.
- (b) For the purposes of this clause 21, "**control**" includes controlling, managing, processing, generating, capturing, collecting, transferring, transmitting, deleting and destroying.

## 21.2 Supplier's security obligations

- (a) The Supplier must implement, maintain and enforce a formal program of technical and organisational security measures (including an audit and compliance program) relating to ICT security and cyber security that is in accordance with:
  - (i) this clause 21; and
  - (ii) the standards or requirements specified in Item 40 of the Order Form,

**(Security Program)**, provided that, where clause 21 and the standards or requirements specified in the Order Form both address standards in respect of the same subject matter, the Security Program must reflect the higher standard.
- (b) The Security Program must be designed to:
  - (i) monitor, audit, detect, identify, report and protect against Security Incidents, Viruses, and any other threats or hazards to the security or integrity of the Customer's operations or the Services and Deliverables in carrying out the Supplier's Activities;
  - (ii) ensure the security (including the confidentiality, availability and integrity) of the Services and Deliverables in accordance with the requirements of this Agreement;
  - (iii) ensure the continuity of the Customer's access to, and use of, the Services and Deliverables and in a manner that achieves any applicable Service Levels. This includes continuity of access and use during any business continuity event, Disaster recovery event, scheduled or unscheduled maintenance and similar events;
  - (iv) manage any potential security risks in the Supplier's supply chains that bear upon the Supplier's Activities;
  - (v) monitor, detect, identify and protect against fraud and corruption by the Supplier's organisation and the Supplier's Personnel; and
  - (vi) ensure that the Security Program is comprehensive in covering all components of the Supplier's Activities and protects data in accordance with this Agreement.
- (c) Without limiting its obligations under clause 21.2(a), the Supplier must ensure its Security Program complies, and is consistent, with the Policies, Codes and Standards (to the extent applicable to security).

- (d) The Supplier must regularly review and continuously improve the Security Program to ensure it remains current and up-to-date and continues to satisfy the requirements of this clause 21.2 and is in accordance with Best Industry Practice.
- (e) If specified in Item 40 of the Order Form, the Supplier must have, obtain and maintain from the Commencement Date and for the duration of the Supplier's Activities the security certifications specified or referenced in Item 40 of the Order Form from an accredited, independent, third party register or accredited, independent third party certification body. Unless otherwise specified in Item 40 of the Order Form, the certifications must be updated at least annually and must comply with any specific certification requirements set out in the Order Form.
- (f) Without limiting this clause 21.2, the Supplier must comply with any additional security obligations or standards specified in the Order Form.

### **21.3 Audits and compliance**

- (a) The Supplier must audit its compliance with its Security Program and security obligations under this Agreement in accordance with any timeframes specified in the Order Documents and, where no such timeframes are specified, on an annual basis.
- (b) The Supplier must provide the Customer, at the Customer's request, with electronic copies of:
  - (i) any security certifications required by this clause 21 and a copy of each renewal of these certifications;
  - (ii) a description of the Supplier's information security management system and cyber security management system;
  - (iii) all reports relating to:
    - A. any external or internal audits of the Supplier's security systems (to be provided for the most recent period available), including follow-up reports on audit action items; and
    - B. where applicable, the integrity of any data backups required to be undertaken as part of the Supplier's Activities;
  - (iv) evidence that a vulnerability and security management process is in place within its organisation that includes ongoing and routine vulnerability scanning, patching and coverage verification, with a frequency commensurate with any applicable security requirements specified in the Order Form, or where no requirements are specified, Best Industry Practice. This can include copies of relevant policies, scan results, vulnerability reports, registers of vulnerabilities and patch reports;
  - (v) evidence that (if applicable) penetration and security testing (including any Acceptance Tests set out in the Order Form) are carried out:
    - A. prior to, and directly after, new systems are moved into production or in the event of a significant change to the configuration of any existing system; or
    - B. at such other times specified in the Order Form; and
  - (vi) evidence that high and extreme Inherent Risks identified in audits, vulnerability scans and tests have been remediated,

which must contain (at a minimum) full and complete details of information and reports insofar as they relate to the Supplier's Activities. Where the Supplier is not permitted to provide the Customer with any of the foregoing (due to confidentiality obligations to third parties or because to do so would cause the Supplier to breach any Law or relevant security certification that the Supplier is subject to), the Supplier may (acting reasonably) redact those components that it is not permitted to provide to the Customer but only to the fullest extent needed to prevent the Supplier's non-compliance.

- (c) Without limiting clause 11.3(a)(ii), the Supplier must run initial and annual mandatory security awareness training for all of the Supplier's Personnel involved in carrying out the Supplier's Activities under this Agreement and ensure that those Personnel have completed the initial training prior to carrying out the Supplier's Activities.
- (d) At the Customer's request, the Supplier must implement any audit findings or recommendations arising from an audit conducted under clause 21.3(a) and reasonably demonstrate to the Customer the implementation of such findings and recommendations.

---

**22. Security Incidents**

**22.1 Notification of Security Incidents**

- (a) If the Supplier becomes aware, or has reasonable grounds to suspect, that there has been a Security Incident, the Supplier must immediately:
  - (i) notify the Customer, and also notify the Contract Authority where this Agreement is made pursuant to a MICTA; and
  - (ii) at the same time as providing notice pursuant to clause 22.1(a)(i) provide to the Customer, to the extent known at the time, the following information:
    - A. date of the Security Incident;
    - B. a description of the Security Incident (including whether the Security Incident involved any Personal Information);
    - C. how the Security Incident occurred;
    - D. where the Security Incident involves Personal Information, the following:
      - 1) the type of breach that occurred;
      - 2) the amount of time the Personal Information was disclosed for; and
      - 3) the total (or estimated total) number of individuals affected or likely to be affected by the breach;
    - E. whether the Security Incident is a cyber incident, and if so, details of the cyber incident; and
    - F. such other information relating to the Security Incident that the Customer or its Personnel requires to comply with the Privacy Laws (and as notified to the Supplier).

- (b) Where the information set out under clause 22.1(a)(ii) is not known by the Supplier at the time of providing notice pursuant to clause 22.1(a)(i), the Supplier must expeditiously take steps to investigate and identify the information and promptly provide the outstanding information to the Customer's Representative once known.

## 22.2 Actions required in relation to a Security Incident

- (a) Where the:

- (i) Supplier becomes aware, or has reasonable grounds to suspect, that there has been a Security Incident; or
- (ii) Customer notifies the Supplier that the Customer has reasonable grounds to suspect that a Security Incident has occurred or is about to occur,

then, the Supplier must:

- (iii) comply with clause 22.1;
- (iv) expeditiously assess, investigate and diagnose the Security Incident (including to identify the root cause of the Security Incident, the risks posed by the Security Incident and identify how these risks could be addressed) and, on the Customer's request, provide the results of that assessment and investigation to the Customer's Representative within the timeframe requested by the Customer;
- (v) manage and contain the Security Incident and mitigate the impact of the Security Incident (working on a 24 x 7 basis if required);
- (vi) develop and adopt a remediation Plan addressing the rectification of, and the prevention of the future recurrence of the facts and circumstances giving rise to, the Security Incident (**Remediation Plan**);
- (vii) cooperate with the Customer, the Customer's Personnel or any assessor appointed by the Customer in connection with the assessment, investigation, diagnosis, response and resolution of the Security Incident (including so as to ensure the Customer is able to satisfy its notification and reporting obligations within the timeframes and requirements under the Privacy Laws); and
- (viii) comply with any additional plans, actions and requirements relating to the Security Incident as specified in Item 42 of the Order Form, the Order Documents or as required by Law or any Authority.

- (b) The Supplier must:

- (i) within 48 hours after the Supplier's initial awareness or notification of the Security Incident in accordance with clause 22.1(a)(i) (or such earlier period agreed by the parties to enable Customer to comply with Laws), provide to the Customer, to the extent known at that time:
  - A. a list of actions taken by the Supplier to date to mitigate the impact of the Security Incident;
  - B. a summary of the records impacted, or which may be impacted, and any Customer Data and other information that has been or may have been lost, accessed or disclosed as a result of the Security Incident; and
  - C. the estimated time to resolve the Security Incident;

- (ii) provide any assistance reasonably required by the Customer or any Authority in relation to any criminal, regulatory or other investigation or inquiry relating to the Security Incident;
- (iii) promptly update the Remediation Plan to address any concerns reasonably raised by the Customer, following which the Supplier must implement the Remediation Plan in accordance with the timeframes agreed by the Customer;
- (iv) following implementation of the Remediation Plan (or upon the earlier resolution of the Security Incident), provide to the Customer:
  - A. a list of all actions taken by the Supplier to mitigate and remediate the Security Incident; and
  - B. evidence verifying (where applicable) that the remediation activities undertaken have successfully resolved the underlying cause of the Security Incident (for example, by sharing the results of relevant penetration tests or vulnerability scans); and
- (v) review and learn from the Security Incident to improve security and data handling practices and prevent future Security Incidents from occurring.
- (c) For clarity, nothing in this clause 22:
  - (i) requires the Supplier to provide the Customer with specific details that relate to the Supplier's other customers or would breach any applicable Laws; and
  - (ii) limits the Supplier's obligations at Law with respect to the notification and resolution of Security Incidents.

---

## 23. Confidentiality

- (a) Where either party (**Recipient**) receives or otherwise possesses Confidential Information of the other party (**Discloser**), the Recipient must:
  - (i) keep it confidential;
  - (ii) in the case of the Supplier or its Personnel, only use it where required to exercise its rights or perform its obligations under this Agreement; and
  - (iii) not disclose it to anyone other than:
    - A. with the prior consent of the Discloser and on the condition that the subsequent recipient is bound by the same or substantively equivalent confidentiality requirements as specified in this Agreement;
    - B. where required by the GIPA Act (or any other similar Laws) which may require the Customer to publish or disclose certain information concerning this Agreement;
    - C. where required by any other Laws, provided that the Recipient gives the Discloser reasonable notice of any such legal requirement or order to enable the Discloser to seek a protective order or other appropriate remedy (unless it would be in violation of a court order or other legal requirement);



- D. in the case of the Customer, to:
    - 1) the Contract Authority or responsible Minister (where this Agreement is made under a MICTA); or
    - 2) any Government Agency or Eligible Customer or responsible Minister for a Government Agency or an Eligible Customer; or
  - E. to its Personnel and directors, officers, lawyers, accountants, insurers, financiers and other professional advisers where the disclosure is in connection with advising on, reporting on, or facilitating the party's exercise of its rights or performance of its obligations under this Agreement.
- (b) The Supplier must not issue any press release or make any other public statement regarding this Agreement or the Supplier's Activities without the prior written consent of the Customer, except as required by Law.
  - (c) This clause 23 does not preclude the Customer from disclosing any information (including Confidential Information) of the Supplier to the extent that this Agreement otherwise permits the disclosure of such information.

PART D: FEES AND PAYMENT

24. Payment and invoicing

24.1 Price

- (a) In consideration for the performance of the Supplier's Activities in accordance with this Agreement, the Customer agrees to pay to the Supplier the Price set out in the Payment Particulars, subject to any additional discounts, rebates, credits or other similar benefits specified in the Payment Particulars. Other than as expressly set out in this Agreement, such amounts are the only amounts payable by the Customer in respect of the Supplier's performance of the Supplier's Activities and its other obligations under this Agreement.
- (b) Subject to clause 1.4(b), the Price and any rates or charges specified in the Payment Particulars will be fixed for the Term, unless otherwise specified in the Payment Particulars.

24.2 Benchmarking

- (a) Clauses 24.2 and 24.3 apply if it is specified in the Order Form that benchmarking applies.
- (b) No more than once per annum during the Term and commencing on the first anniversary of the Commencement Date, the Customer may, in its sole discretion, notify the Supplier in writing (**Benchmarking Notice**) that the Customer is seeking to implement a formal independent benchmarking of the cost of the Supplier's Activities in order to consider whether the rates and prices under this Agreement are competitive with the current Australian market for like deliverables and services (**Benchmarking Activities**).
- (c) An independent benchmarker may be agreed between the parties. If the parties cannot agree upon an independent benchmarker within 10 Business Days of the Benchmarking Notice, the Customer may appoint an independent third party benchmarker which the Customer reasonably considers to possess the adequate

expertise to carry out the Benchmarking Activities, subject to such third party not being a direct competitor of the Supplier.

- (d) The parties will work together in good faith to expeditiously develop terms of reference which will form the basis of joint instructions for the benchmarker to follow in conducting the Benchmarking Activities. Those terms of reference must, unless otherwise agreed by the parties, be based on the following principles:
  - (i) a "like-for-like" comparison in respect of the Supplier's Activities, conducted by reference to one or both of:
    - A. a "whole of offering" basis in relation to all Services and Deliverables; and
    - B. a product and service category basis; and
  - (ii) appropriate normalisation, including with respect to volumes, method of delivery, quality of service and, in respect of clause 24.2(d)(i)B, taking into account any cross-subsidies offered between different product and service categories.
- (e) The parties will instruct the benchmarker to:
  - (i) conduct the Benchmarking Activities on an objective and independent basis; and
  - (ii) use reasonable efforts to access and rely on recent, accurate and verifiable data in respect of its Benchmarking Activities.
- (f) The parties must ensure that the benchmarker signs a confidentiality deed in favour of the Supplier and the Customer (in a form acceptable to the Customer) prior to undertaking any Benchmarking Activities pursuant to this Agreement.
- (g) Unless otherwise agreed by the parties in writing, the Customer will bear the cost of engaging a benchmarker to undertake the Benchmarking Activities under this clause.
- (h) The parties must each appoint a reasonable number of Personnel to work under the direction of the benchmarker in collecting data necessary for the purposes of the benchmarking exercise.
- (i) The parties agree that the benchmarker may, in its own discretion, determine the information required to carry out the Benchmarking Activities and may carry out the benchmark as he or she sees fit (including by determining the benchmarking methodology).
- (j) The parties must reasonably co-operate with the benchmarker in connection with the Benchmarking Activities carried out under this clause 24.2.

### 24.3 Outcome of benchmarking

- (a) The benchmarker will be required to deliver a benchmarking report (**Benchmarking Report**) to the parties within 60 days of the Benchmarker's appointment, or within such other period as agreed by the parties in writing.
- (b) If the Benchmarking Report concludes that the rates and prices (or certain rates and prices) under this Agreement exceed the rates and prices offered by the current Australian market for comparable goods, services and activities, then the parties must use all reasonable endeavours to agree on an adjustment to the Payment Particulars to reduce the relevant rates and/or prices to align with the conclusions of the Benchmarking Report.

- (c) If the parties are unable to agree on adjustments to the rates and prices in the Payment Particulars in accordance with clause 24.3(b) within 20 Business Days of the issue of the Benchmarking Report, then, subject to the Supplier's rights under clause 24.3(g), the Customer may, acting reasonably, determine the adjustments required to reduce the rates and prices in the Payment Particulars to reflect the conclusions contained in the Benchmarking Report.
- (d) If the Customer determines that an adjustment to the rates and prices in the Payment Particulars is required in accordance with clause 24.3(c), the Customer may issue a notice to the Supplier notifying it of the adjustment (**Adjustment Notice**).
- (e) The parties acknowledge and agree that if an adjustment to the rates and prices in the Payment Particulars is determined under clauses 24.3(b) or 24.3(c), the Payment Particulars will be deemed to have been amended to reflect the relevant adjustment, on and from the date:
  - (i) on which the parties reach an agreement in respect of the adjustment to the rates and prices under clause 24.3(b); or
  - (ii) specified in an Adjustment Notice issued by the Customer under clause 24.3(d), provided that the Customer will not specify a retrospective date in the Adjustment Notice.
- (f) A party may dispute the results of the Benchmarking Report if it reasonably considers that the findings in, and/or the conclusions of, the Benchmarking Report are based on incorrect facts, assumptions or comparisons. Any such dispute must be notified within 20 Business Days of the issue of the Benchmarking Report and must be resolved in accordance with clause 35.
- (g) The Supplier may dispute an Adjustment Notice if it reasonably considers that the adjustment to the rates and prices proposed in that notice are materially inconsistent with the conclusions contained in the Benchmarking Report. Any such dispute must be notified within 20 Business Days of the issue of the relevant Adjustment Notice and must be resolved in accordance with clause 35.

## 24.4 Invoicing

- (a) The Supplier must Invoice the Customer at the time stated in the Order Form or Payment Particulars or, if the time for payment is not stated, then the Supplier must Invoice the Customer within 30 days from the end of the calendar month in which the relevant Deliverables or Services are provided to the Customer in accordance with this Agreement.
- (b) The Supplier must:
  - (i) ensure that its Invoice is a valid tax invoice for the purposes of the GST Law;
  - (ii) together with any Invoice provided under clause 24.4(a), provide the Customer with a subcontractor's statement regarding workers' compensation, payroll tax and remuneration in the form specified at <https://www.revenue.nsw.gov.au/help-centre/resources-library/opt011.pdf> (or such other site or form as advised by the Customer from time to time); and
  - (iii) provide any further details in regard to an Invoice that are set out in the Order Form or reasonably required by the Customer.

## 24.5 Payment

- (a) Subject to the Supplier satisfying any conditions precedent to payment specified in Item 46 of the Order Form, the Customer will pay any Correctly Rendered Invoice:
  - (i) by electronic funds transfer to the bank account details nominated by the Supplier in Item 46 of the Order Form, or as otherwise stipulated in writing by the Supplier from time to time; and
  - (ii) within 30 days following receipt of the Correctly Rendered Invoice, or such other time as specified in the Order Form.
- (b) The making of a payment is not an acknowledgment that the Supplier's Activities have been provided in accordance with this Agreement.
- (c) If the Supplier has overcharged the Customer in any Invoice, the Supplier must promptly refund any amounts that the Supplier has overcharged the Customer, and adjust current Invoices that have not been paid by the Customer to ensure that the Customer is only liable to pay the correct amount.

## 24.6 Payment disputes

If the Customer disputes or is unable to reconcile part of an Invoice, the Customer may withhold payment for the amount in dispute or in discrepancy until such dispute or discrepancy is resolved. In such case, the Customer must promptly notify the Supplier of the amount in dispute and the reasons for disputing it.

## 24.7 Set off

- (a) The Customer may, on notice to the Supplier, deduct from any amount otherwise due to the Supplier and from any security held by the Customer:
  - (i) any debt or other liquidated amount due from the Supplier to the Customer; or
  - (ii) any Claim to money which the Customer may have against the Supplier whether for damages (including Liquidated Damages) or otherwise,under or in connection with this Agreement.
- (b) The rights given to the Customer under this clause 24.7 are in addition to and do not limit or affect any other rights of the Customer under this Agreement or at Law. Nothing in this clause 24.7 affects the right of the Customer to recover from the Supplier the whole of the debt or Claim in question or any balance that remains owing.

## 24.8 Taxes

- (a) Subject to clause 24.8(b), the Price is inclusive of, and the Supplier is responsible for paying, all Taxes levied or imposed in connection with the provision of the Supplier's Activities under this Agreement.
- (b) Unless otherwise specified, all amounts specified in this Agreement are exclusive of GST.
- (c) The Customer must, subject to receipt from the Supplier of a Correctly Rendered Invoice, pay any GST that is payable in respect of any taxable supply made under this Agreement in addition to the amount payable (exclusive of GST) for the taxable supply. GST is payable at the same time as the amount payable for the taxable supply to which it relates.

- (d) Where the Customer is required by any applicable Law to withhold any amounts from the payments made by it to the Supplier under this Agreement, the Customer:
  - (i) may withhold such amounts and will not be required to gross-up its payments to the Supplier for any amounts withheld; however
  - (ii) will provide the Supplier with a certificate of withholding or such other reasonable evidence of such withholding, to facilitate the Supplier's claims or deductions with the relevant taxing authority.

## PART E: RISK ALLOCATION AND MANAGEMENT

---

### 25. Business contingency and Disaster recovery

#### 25.1 Business contingency

While carrying out the Supplier's Activities, the Supplier must have reasonable business continuity and contingency measures and procedures in place to ensure business continuity and no disruption to the Customer or any Customer User.

#### 25.2 Business Contingency Plan

- (a) If stated in the Order Form that a business contingency plan is required, the Supplier must, within the timeframe stated in the Order Form or as otherwise agreed in writing by the parties, have in place (and prepare and implement, if not already in existence) a Business Contingency Plan for the approval of the Customer (**Business Contingency Plan**).
- (b) The Business Contingency Plan must:
  - (i) specify the procedures and plans to predict, avoid, remedy and mitigate internal or external problems (including any Disasters) that may have an adverse effect on the Supplier's Activities;
  - (ii) comply with the security standards, requirements and certifications required by this Agreement, including under clause 21; and
  - (iii) include any other details specified in the Order Documents or as otherwise reasonably required by the Customer.
- (c) In developing the Business Contingency Plan, the Supplier must undertake a careful and informed assessment of the likely events and circumstances which may affect the Supplier's ability to carry out its obligations under this Agreement (including those in existence at the Commencement Date or notified by the Customer to the Supplier in writing).
- (d) The Business Contingency Plan must be reviewed and tested by the Supplier in accordance with the timeframes stated in the Order Form, or if no timeframes are stated, at least annually. The Supplier must provide the results of any review or test of its Business Contingency Plan to the Customer upon request.
- (e) If any updates to the Business Contingency Plan are required as a result of any review or test of the Business Contingency Plan, the Supplier must make those updates and re-submit the Business Contingency Plan to the Customer for approval.
- (f) The Supplier must comply with the latest Business Contingency Plan that has been approved by the Customer pursuant to clause 8.

- (g) For clarity, the Business Contingency Plan is a Document Deliverable. Clause 8 therefore applies to the Business Contingency Plan, including any updates to it.

25.3 Disasters

On the occurrence of a Disaster, the Supplier must immediately:

- (a) notify the Customer's Representative that a Disaster has occurred; and
- (b) implement any measures set out in the Business Contingency Plan or such other measures as reasonably required by the Customer to mitigate and respond to the Disaster.

---

26. Step-in

26.1 Step-In Rights

- (a) This clause 26 applies where specified in Item 48 of the Order Form that the Customer may exercise Step-In Rights.
- (b) Without limiting any other right or remedy under this Agreement or at Law, if the Customer reasonably forms the opinion that:
  - (i) the Supplier is unable or unwilling to provide any of the Supplier's Activities in accordance with this Agreement;
  - (ii) a Disaster or emergency has occurred, which the Supplier is unable to prevent or overcome and which will or does materially affect the operations of the Customer;
  - (iii) a Security Incident has occurred and the Supplier has failed to take, or delayed in taking, the actions required in relation to the Security Incident under clause 22.2; or
  - (iv) the Supplier has materially breached its obligations under this Agreement or there is a real and reasonable prospect of the Supplier materially breaching its obligations under this Agreement,the Customer may give written notice to the Supplier that it intends to exercise its rights under this clause 26 (**Step-In Rights**).
- (c) To the extent reasonably practicable, before exercising Step-In Rights the Customer agrees to consult with the Supplier in relation to measures to mitigate or manage the impact of events and circumstances giving rise to the Step-In Rights.
- (d) For the purpose of exercising Step-In Rights, the Customer:
  - (i) will be entitled to act as the Supplier's agent under all contracts entered into by the Supplier that relate to the Supplier's Activities and are necessary for the Customer to exercise the Step-In Rights; and
  - (ii) may:
    - A. give reasonable instructions to any employee of the Supplier (and the Supplier must ensure that such requests are complied with); and
    - B. contract with any of the subcontractors engaged by the Supplier,

as is reasonably required by the Customer to exercise the Step-In Rights.

- (e) Upon receiving notice from the Customer stating that the Customer is exercising the Step-In Rights, the Supplier must:
  - (i) at the Customer's request, allow the Customer or a third party engaged by the Customer to provide part or all of the Supplier's Activities; and
  - (ii) maintain all third party agreements, consents and approvals necessary to enable the Customer to exercise its rights under this clause 26.
- (f) If the Customer exercises its Step-In Rights under this clause 26:
  - (i) the Customer will be relieved from paying any component of the Price that relates to those Supplier's Activities in respect of which it has exercised Step-In Rights, for the period of such exercise, however will continue to pay those components of the Price which relate to Supplier's Activities unaffected by the Step-In Rights; and
  - (ii) the Supplier must pay to the Customer on demand an amount equal to:
    - A. any costs incurred by the Customer in connection with the exercise of its Step-In Rights (including any costs relating to the Customer or its Personnel providing any part or all of the Supplier's Activities) under clause 26.1(e)(i)); and
    - B. the quantum of any increase in the fees or costs paid by the Customer to any third party (including any substitute supplier) in respect of the period of the exercise of the Step-In Rights.
- (g) The Customer will use its reasonable efforts to minimise the quantum of any increase under clause 26.1(f)(ii)B.
- (h) The Supplier will not be responsible for any default or delay in the delivery of the Supplier's Activities to the extent that it was caused by the Customer or any third party providing part or all of the Supplier's Activities as contemplated in clause 26.1(e)(i), except to the extent contributed to by the Supplier or any of its Personnel.
- (i) If the Customer exercises its Step-In Rights for 60 days or more (or such other period as specified in Item 48 of the Order Form), then the Customer may, at its sole discretion, elect to terminate this Agreement or reduce its scope pursuant to clause 29.1(d).

## 26.2 Conclusion of Step-In

- (a) The Customer may cease to exercise its Step-In Rights at any time by giving the Supplier at least five Business Days written notice or such other period specified in Item 48 of the Order Form (**Step-Out Notice**).
- (b) Upon the Customer ceasing to exercise a Step-In Right, the Supplier must recommence performance of the Supplier's Activities on the date specified in the Step-Out Notice.
- (c) The Customer must relinquish the control and possession of any of the Supplier's resources utilised for the performance of the Step-In Rights and must provide the Supplier with details of its actions taken during the period in which the Customer was exercising its Step-In Rights.

### 26.3 No prejudice

The parties acknowledge and agree that:

- (a) except as specified in clause 26.1(g), nothing in this clause 26 will prejudice the rights of the Customer (including with respect to termination) or relieve the Supplier of its liabilities or responsibilities whether under this Agreement or otherwise according to Law; and
- (b) the Customer is under no obligation to exercise Step-In Rights before it exercises any termination rights under this Agreement.

---

## 27. Insurance

- (a) Unless otherwise specified in Item 49 of the Order Form, the Supplier must hold and maintain each of the following types of insurances, for the periods and in the amounts specified below:
  - (i) public liability insurance with a limit of cover of at least [REDACTED] in respect of each occurrence, to be held for the duration of the Supplier's Activities;
  - (ii) product liability insurance with a limit of cover of at least [REDACTED] in respect of each occurrence and in the aggregate, to be held for the duration of the Supplier's Activities and for at least seven years thereafter;
  - (iii) workers' compensation insurance as required by Law;
  - (iv) professional indemnity insurance with a limit of cover of at least [REDACTED] in respect of each occurrence and in the aggregate, to be held for the duration of the Supplier's Activities and for at least seven years thereafter; and
  - (v) such other insurances as specified in Item 49 of the Order Form.
- (b) Without limiting clause 27(a), where specified in the Order Form, the Supplier must hold and maintain:
  - (i) cyber security insurance with a limit of cover of at least [REDACTED] in respect of each claim (or such other amount specified in Item 49 of the Order Form), to be held for the duration of the Supplier's Activities; and
  - (ii) insurance that covers Losses that may be suffered as a result of a data security breach or the wrongful disclosure and use of Personal Information by the Supplier or its Personnel.
- (c) Within 10 Business Days following a request from the Customer, the Supplier must provide the Customer with:
  - (i) a certificate of currency issued by its insurer or insurance broker (or other form of evidence acceptable to the Customer) confirming that all insurance policies required by this Agreement are current and that the insurance has the required limits of cover; and
  - (ii) any information reasonably requested by the Customer regarding the policies for each of the insurances required to be held and maintained by the Supplier under clauses 27(a) and 27(b) (which may include reasonably redacted policy provisions or summarised policy terms where



disclosure of the full policy terms is restricted by confidentiality obligations owed by the Supplier to third parties).

---

**28. Performance Guarantee and Financial Security**

**28.1 Performance Guarantee**

If specified in Item 50 of the Order Form, the Supplier must arrange for a guarantor approved in writing by the Customer to enter into an agreement with the Customer in substantially the same form as the document in Schedule 8 or such other document reasonably acceptable to the Customer. This Performance Guarantee must be provided to the Customer within 15 Business Days following the Commencement Date or at such other time as specified in Item 50 of the Order Form.

**28.2 Financial Security**

- (a) If specified in Item 51 of the Order Form, the Supplier must provide a financial security in the amount stated in the Order Form and in substantially the same form as the document in Schedule 9 or such other document reasonably acceptable to the Customer (**Financial Security**). The Financial Security must be provided to the Customer within 15 Business Days following the Commencement Date or at such other time as specified in Item 51 of the Order Form.
- (b) If the Prices payable for the Supplier's Activities are increased pursuant to this Agreement (including due to a Change Request approved under clause 10), the Customer may, acting reasonably, direct the Supplier to provide additional security in an amount that is proportionate to the increase in Price, and the Supplier must promptly comply with such a direction.
- (c) Subject to its rights to have recourse to the Financial Security, the Customer must release the Financial Security on the sooner of:
  - (i) one year from the date of issue of the Acceptance Certificate for the last Deliverable under the Order Form, or if no Acceptance Tests were required, one year following the termination or expiry of this Agreement (or such other period specified in the Order Documents);
  - (ii) the date the Customer and the Supplier agree in writing to release the issuer of the Financial Security; and
  - (iii) the date the Customer notifies the issuer of the Financial Security in writing that the Financial Security is no longer required.

**28.3 Costs**

Unless otherwise specified in the Order Form, the Supplier will be responsible for the costs that it incurs in complying with its obligations under this clause 28.

---

**29. Termination**

**29.1 Termination for cause by the Customer**

The Customer may (in its sole discretion) immediately terminate this Agreement or reduce its scope by written notice to the Supplier:

- (a) if the Supplier breaches a term of this Agreement which is:
  - (i) not capable of remedy; or

- (ii) capable of remedy, but the Supplier fails to remedy it within 30 days of receiving a notice to do so;
- (b) if an Insolvency Event occurs in respect of the Supplier, to the extent there is no prohibition at Law in respect of such termination;
- (c) if the Supplier or any parent company of the Supplier involved in the performance of the Supplier's Activities undergoes a Change in Control or Other Changes, without the Customer's prior written consent; or
- (d) in any of those circumstances specified in clauses 12.7(b), 13.6, 14.4(a)(iii), 14.4(c)(iii), 26.1(i) and 36.4 or as otherwise set out in this Agreement, including the Additional Conditions,

in which circumstances the Customer's sole liability will be to pay the Supplier (subject to substantiation by the Supplier and the Supplier submitting a Correctly Rendered Invoice in accordance with this Agreement) for work carried out prior to the date of termination or reduction in scope.

## 29.2 Termination for convenience by the Customer

- (a) Without prejudice to the Customer's other rights, the Customer may for its sole convenience, and for any reason, by written notice to the Supplier immediately terminate this Agreement or reduce its scope, effective from the time stated in the Customer's notice, or if no such time is stated, at the time notice is given to the Supplier.
- (b) If the Customer terminates this Agreement or reduces its scope under clause 29.2(a), the Supplier:
  - (i) must take all reasonably practicable steps to mitigate the costs referred to in clause 29.2(b)(ii); and
  - (ii) will be entitled to payment of the following amounts, subject to substantiation by the Supplier, being:
    - A. for:
      - 1) work carried out prior to the time of termination or reduction in scope; and
      - 2) third party costs and disbursements duly incurred, with the authorisation of the Customer, but only to the extent referable to the period prior to the effective time of termination,

which would have been payable if this Agreement had not been terminated or reduced in scope and the Supplier submitted an Invoice for the work carried out prior to this date; and
    - B. such other specific costs itemised in Item 52 of the Order Form (if any),

but in no case will the total amount payable to the Supplier be more than the total Price that would have been payable by the Customer had this Agreement not been terminated.
- (c) The amount to which the Supplier is entitled under this clause 29.2 will be a limitation on the Customer's liability to the Supplier arising out of, or in connection with, the termination or reduction in scope of this Agreement and the Supplier may

not make any Claim against the Customer with respect to this, other than for the amount payable under this clause 29.2.

### **29.3 Consequences of reduction of scope**

If the Customer exercises its right to reduce the scope of this Agreement pursuant to clause 29, the parties agree that the Price will be reduced proportionately and in accordance with any methodology specified in the Payment Particulars.

### **29.4 Termination for cause by the Supplier**

- (a) The Supplier may immediately terminate this Agreement by written notice to the Customer if:
  - (i) the Customer has not paid an amount due and payable by it under this Agreement and the:
    - A. amount has been properly invoiced in a Correctly Rendered Invoice and is not the subject of any unresolved dispute under clause 24.6;
    - B. Supplier has issued a notice to the Customer, stating that the amount is overdue and that the Supplier intends to terminate unless the amount is paid; and
    - C. Customer does not pay the amount within 90 days of the date it receives the Supplier's notice under clause 29.4(a)(i)B; or
  - (ii) the Customer has:
    - A. breached this Agreement in a manner which results in the Supplier being in breach of a Law; or
    - B. intentionally and wilfully:
      - 1) breached clauses 17.10 or 23; or
      - 2) misappropriated the Intellectual Property Rights of the Supplier in its Existing Materials in a manner that is contrary to the Intellectual Property Rights granted or licenced to the Customer under this Agreement,
- and the Customer does not cease the relevant conduct within 60 days of receiving a written notice from the Supplier requesting it to do so.
- (b) This clause 29.4 exhaustively sets out the Supplier's rights to terminate this Agreement.

### **29.5 Dispute resolution**

For clarity, the processes described in clause 35 are independent of, may be undertaken contemporaneously with, and do not constrain or delay, a party exercising its rights under this clause 29.

### **29.6 Survival of rights on termination or reduction in scope**

Termination of this Agreement will be without prejudice to any other rights or obligations which may have accrued under this Agreement on or before termination.

---

## 30. Suspension

- (a) The Customer may direct the Supplier in writing to:
  - (i) suspend the performance or carrying out of; and/or
  - (ii) after a suspension has been instructed, re-commence the performance or carrying out of,

all or part of the Supplier's Activities, at any time. Any such suspension will be effective on and from the date specified in the Customer's direction.
- (b) The Supplier must comply with any direction issued by the Customer under clause 30(a).
- (c) If a suspension under this clause 30 is instructed by the Customer as a result of any breach by the Supplier, the Supplier's failure or delay in carrying out any of its obligations in accordance with this Agreement or because of any event of the kind described in clause 29.1, such suspension will be without any liability to the Customer and the Supplier will not be entitled to make any Claim against the Customer arising out of, or in connection with, the suspension.
- (d) If a suspension is instructed by the Customer under clause 30(a) other than for the reasons described in clause 30(c), then:
  - (i) unless otherwise agreed by the parties, the Supplier will be entitled to Invoice the Customer the direct, reasonable and substantiated costs (excluding any profit, profit component or overheads) necessarily incurred by the Supplier as a result of implementing the suspension as directed by the Customer, to the extent such costs could not have been reasonably mitigated or avoided;
  - (ii) the Supplier must take all reasonable steps to mitigate those costs incurred by it as a result of such suspension; and
  - (iii) the Supplier will not be entitled to make any Claim against the Customer arising out of or in connection with the suspension other than as described in clause 30(d)(i).

---

## 31. Transition-Out Services

### 31.1 Application of this clause

This clause 31 applies if it is specified in the Order Form that the Supplier is required to provide Transition-Out Services as part of any Stage or part of the Supplier's Activities.

### 31.2 Transition-Out Plan

- (a) If the Order Form specifies that a Transition-Out Plan must be prepared by the Supplier with respect to the Supplier's Activities, by any date specified in the Order Form or otherwise promptly on request, the Supplier must prepare, and submit to the Customer's Representative for the Customer's approval in accordance with clause 8, a plan setting out how the Supplier will effect:
  - (i) the orderly disablement of the Supplier's Activities; or
  - (ii) where applicable, the transfer of the performance of the Supplier's Activities under this Agreement to the Customer or a third party, including complying with the obligations set out in this clause 31.

- (b) The Supplier must ensure that the Transition-Out Plan sets out:
  - (i) the timeframes within which the Supplier will perform its obligations under the Transition-Out Plan;
  - (ii) any specific transition-out or disengagement obligations specified in the Order Documents; and
  - (iii) any charges, or the basis or methodology for the calculation of charges, which the Customer will pay the Supplier to perform the Services described in the Transition-Out Plan (if not otherwise specified in the Order Documents).
- (c) The Supplier must:
  - (i) review and update the Transition-Out Plan periodically throughout its engagement under this Agreement or at the Customer's reasonable request; and
  - (ii) make any updates to the Transition-Out Plan that are reasonably requested by the Customer.
- (d) For clarity, the Transition-Out Plan is a Document Deliverable. Clause 8 therefore applies to the Transition-Out Plan, including any updates to it.

### 31.3 General

The Supplier must for the duration of the Transition-Out Period (or such other period as agreed between the parties in writing):

- (a) carry out all transition-out or disengagement Services specified in the Module Terms and other Order Documents or that are necessary to ensure the smooth transition of the Supplier's Activities to the Customer or its nominee;
- (b) if a Transition-Out Plan has been approved by the Customer, perform its obligations as set out in the Transition-Out Plan; and
- (c) co-operate with the Customer and its Personnel in relation to the performance of all Transition-Out Services.

---

## 32. Consequences of expiry or termination

### 32.1 Extracting or retrieving Customer Data

The Supplier must enable the Customer to extract or retrieve Customer Data, or otherwise provide the Customer Data to the Customer, in accordance with the requirements of this Agreement, for a minimum period of up to six months after the expiry or termination of this Agreement (or such other period as specified in the Order Documents or agreed between the parties in writing).

### 32.2 Confidential Information and intellectual property

Subject to clauses 23 and 32.1 and any requirements at Law applicable to the parties, on the expiry or termination of this Agreement, the Supplier and its Personnel must cease to access, and at the Customer's election, securely:

- (a) return; or
- (b) destroy,

the Customer's:

- (c) Confidential Information; and
- (d) Existing Materials, New Materials and other Materials that comprise the Customer's Intellectual Property Rights.

---

### **33. Warranties**

#### **33.1 Mutual warranties**

Each party represents, warrants and undertakes to the other party that:

- (a) as at the date that this Agreement is entered into, it is properly constituted and has sufficient power, capacity and authority to enter into this Agreement and perform the activities required under it;
- (b) in so far as it uses Personnel to perform activities on its behalf under this Agreement, those Personnel are duly authorised by it; and
- (c) it will reasonably co-operate with the other party and its respective Personnel to promote timely progress and fulfilment of this Agreement.

#### **33.2 General Supplier warranties**

Without limiting any other warranty under this Agreement, the Supplier represents, warrants and undertakes to the Customer that:

- (a) to the best of its knowledge and belief after making due and reasonable enquiries, there is no Conflict of Interest in respect of itself and its Personnel, which relates to the Supplier's ability to perform its obligations under this Agreement;
- (b) the information that is provided to the Customer in terms of the structure, viability, reliability, insurance cover, capacity, experience and expertise of the Supplier and its Personnel is, to the best of the Supplier's knowledge and belief, correct and not misleading as at the date it was (or is to be) supplied to the Customer;
- (c) it is not aware of any information which, if it had provided that information to the Customer, may reasonably be expected to have had a material effect on the decision made by the Customer to enter into this Agreement;
- (d) the office holders of the Supplier and any associate of the Supplier (as defined under section 11 of the Corporations Act) or its Related Body Corporate are of good fame and character; and
- (e) the Supplier has all the Authorisations necessary to perform its obligations under this Agreement.

#### **33.3 Warranties in relation to Supplier's Activities**

Without limiting any other warranty under this Agreement, the Supplier represents and warrants to the Customer that:

- (a) the Supplier's Activities will be carried out with due skill, care and diligence;
- (b) the Supplier's Activities (including Deliverables repaired or replaced or Services re-performed under this Agreement) will meet the Specifications and other requirements of this Agreement;

- (c) the Supplier's Activities will only be carried out by Supplier's Personnel who meet the Personnel requirements under this Agreement; and
- (d) it will perform the Supplier's Activities in accordance with all applicable Laws.

### **33.4 Implied warranties**

The express warranties given by the Supplier under this Agreement are provided by the Supplier to the exclusion of any implied representations or warranties not set out in this Agreement, provided that this Agreement (including clause 33.4) does not operate to exclude any statutorily implied representations, warranties, conditions or guarantees which cannot legally be excluded. To the extent that any such statutorily non-excludable representations, warranties, conditions or guarantees apply, the Supplier limits its liability for their breach to the maximum amount permitted by Law.

---

## **34. Indemnities and liability**

### **34.1 Indemnities**

The Supplier indemnifies the Indemnified Entities against any Loss arising out of, or connected with any:

- (a) personal injury or death to any person or damage to, or loss of any real or tangible property to the extent caused or contributed to by an act or omission of the Supplier or any of the Supplier's Personnel;
- (b) breach of the Supplier's or its Personnel's obligations under clauses 19.1 (Obligations in relation to Customer Data), 19.2 (Security of Customer Data), 20 (Privacy), 21 (Security), 22 (Security Incident notification) or 23 (Confidentiality);
- (c) Claim brought by a third party arising out of, or in connection with, any actual or alleged infringement of Intellectual Property Rights or Moral Rights in the Deliverables or Services or associated with the Supplier's Activities, or any breach by the Supplier of the warranties in clause 17.12; or
- (d) of the Supplier's or its Personnel's fraud, recklessness or Wilful Misconduct.

### **34.2 Third Party IP Claims**

In relation to Claims of the kind referred to in clause 34.1(c), the parties agree that the Supplier's liability under the indemnity under that sub-clause is reduced to the extent that Loss arising under that indemnity is caused or contributed to by:

- (a) the Customer's combination, operation or use of a Deliverable or Service with any other product, equipment, software or document of the Customer or a third party, except where:
  - (i) such combination, operation or use is authorised under this Agreement;
  - (ii) the Supplier supplied the Deliverable or Service on the basis that it can be combined, operated or used with the Customer's or the relevant third party's products; or
  - (iii) such combination, operation or use should have been reasonably anticipated by the Supplier having regard to the nature and purpose of the Deliverable or Service;
- (b) the Customer's unauthorised modification of a Deliverable without the knowledge of the Supplier, except where such modification was contemplated in the Order

Documents or reasonably anticipated having regard to the nature and purpose of the Deliverable; or


- (c) in relation to Licensed Software:
  - (i) the Supplier following the Customer's written technical directions in relation to the coding and configuration of the Licensed Software, to the extent that verifying or validating such directions is not within the scope of the Supplier's Activities; or
  - (ii) the Customer's continued use of old versions of the Licensed Software after the Supplier has notified the Customer in writing of the relevant infringement and provided the Customer (at no additional cost) a remedial software version, patch or correction, or a replacement part or other correction, that would have overcome the relevant infringement without affecting the performance or availability of the Licensed Software.

34.3 Indemnities not affected by insurance

For clarity, the Supplier's obligations and liability to indemnify the Indemnified Entities under this Agreement or otherwise, will not be affected in any way by any terms of insurance or any refusal by the insurer to indemnify the Supplier under the policies of insurance.

34.4 Status of indemnities

The Supplier's obligations to indemnify any Indemnified Entities who are not the Customer, under this Agreement or otherwise, are held on trust by the Customer and may be fully and effectively enforced by the Customer on behalf of those other entities.



**Guidance note:** In the Order Form, there is an ability to adjust certain aspects of the liability framework, including the matters that are carved-out of the liability cap. Adjustments which are non-beneficial to the Customer should only be considered where supported by clear operational and commercial requirements and must align with the risk profile of the relevant procurement. Non-beneficial changes will require governance approval in accordance with relevant New South Wales Procurement Board Directions.

34.5 Liability cap

- (a) Subject to clauses 34.5(c) and 34.5(d), the liability of each party under this Agreement, howsoever arising and whether for breach, in tort (including negligence) or for any other common law or statutory cause of action is limited to the Limitation Amount.
- (b) In clause 34.5(a), the "**Limitation Amount**" means the amount specified in Item 53 of the Order Form, which may be:
  - (i) a fixed amount;
  - (ii) a multiple of the total amounts paid or payable by the Customer under this Agreement; or
  - (iii) an amount determined by reference to any other mechanism,in the aggregate or otherwise, provided that where no such amount is specified or Item 53 of the Order Form is left blank, the Limitation Amount (in that case, being the aggregate liability of a party under this Agreement), will be the Default Amount. The "**Default Amount**" will be determined in accordance with the table below:



Total Fees Paid or Payable*	Default Amount
Under \$1,000,000 (including GST)	\$2,000,000
\$1,000,000 and above (including GST)	Two times the total fees paid or payable by the Customer under this Agreement.
* "Paid or payable" includes amounts that at the relevant time have not been paid but which would have become payable if the parties performed all of their obligations under this Agreement. It is not limited to amounts that at the relevant time have become due and payable.	

- (c) The Supplier's liability under this Agreement is uncapped, and the limitation of liability set out in clause 34.5(a) does not apply in relation to each of the following:
- (i) liability arising:
    - A. under any of the indemnities in clause 34.1; or
    - B. in respect of any of the matters referenced in that clause,except to the extent that the parties expressly agree to, in Item 53 of the Order Form, an alternative approach in relation to regulating the quantum of any such liability; or
  - (ii) the Supplier's abandonment or repudiation of its obligations under this Agreement.
- (d) Where the Supplier is a current member of a relevant scheme approved under the Professional Standards Legislation, and that scheme applies to limit the liability of the Supplier in accordance with that scheme, then the Supplier's liability will not be regulated by clauses 34.5(a) and 34.5(c) but will instead be limited only to the extent specified under that scheme. For clarity, to the extent that any such scheme does not apply, the Supplier's liability will continue to be determined in accordance with the other provisions of this clause 34.

**34.6 Exclusions of liability**

- (a) In no event will either party's liability to the other party, howsoever arising and whether for breach, in tort (including negligence) or for any other common law or statutory cause of action, include any liability for special, indirect, incidental or consequential loss or damage.
- (b) Nothing in clause 34.6(a) will preclude a party from recovering:
- (i) Loss which may fairly and reasonably be considered to arise naturally, in the usual course of things, from the breach or other act or omission giving rise to the relevant liability; and
  - (ii) any kinds of Loss which the parties expressly agree, in Item 53 of the Order Form, will be treated as Loss of the kind referred to in clause 34.6(b)(i),
- and where the Customer is the recovering party:
- (iii) any Loss against which the Supplier is required to indemnify the Indemnified Entities under clause 34.1, to the extent such Loss relates to

monies, amounts or liabilities owed, due, paid or payable, or obligations owed, to a third party; and

- (iv) subject to applicable common law tests in respect of the recovery of Loss, any costs and expenses relating to any of the following activities (which, for clarity, will be treated as loss of the kind referred to in clause 34.6(b)(i)):
  - A. repairing or replacing the relevant Deliverable or Licensed Software or re-supplying any Services, including the cost of procuring replacement deliverables or services of equivalent functionality and performance internally or from a third party;
  - B. implementing any reasonably necessary temporary workaround in relation to the Licensed Software, Services or Deliverables;
  - C. engaging labour resources to reload any lost or corrupt data to the extent caused or contributed by the Supplier, from the last backup made of such data (regardless of whether the Supplier is responsible for backup of that data as part of the Supplier's Activities); and
  - D. activities undertaken by, or on behalf of, the Customer in connection with the mitigation of Loss.

**34.7 Application and contribution**

- (a) Each party's liability will be reduced proportionately to the extent caused or contributed by the other party.
- (b) The limitations and exclusions of liability in this clause 33.4 only apply to the extent permitted by Law.

**34.8 Mitigation**

The Supplier's obligation to indemnify the Indemnified Entities against Loss under clause 34.1 is reduced to the extent that the relevant Loss arose due to a failure of the relevant Indemnified Entity to take reasonable steps to mitigate that Loss.

---

**35. Dispute resolution**

**35.1 General**

- (a) The parties agree to resolve any dispute between them that arises out of, or in connection with, this Agreement in accordance with the procedure set out in clauses 35.2 to 35.3 or such other procedure set out in Item 54 of the Order Form.
- (b) Either party may give written notice of a dispute to the other party setting out the particulars of the dispute and, where the notice is issued by the Customer, indicating whether the Contract Authority is to be involved in the dispute resolution process (**Dispute Notice**).
- (c) Nothing in this clause 35 limits the ability of either party to commence legal action against the other party for urgent interlocutory relief.

**35.2 Escalation**

- (a) Within 10 Business Days of a party receiving a Dispute Notice, the Customer's Representative and the Supplier's Representative must meet and try to resolve the dispute in good faith.
- (b) If the parties have not:
  - (i) resolved the dispute; or
  - (ii) met,within the period specified in clause 35.2(a), a senior executive of each party must meet and try to resolve the dispute in good faith within 10 Business Days or such other period as may be agreed by the parties in writing.

**35.3 Alternative dispute resolution**

- (a) Unless otherwise specified in the Order Form, if the dispute remains unresolved after 20 Business Days of the date of the Dispute Notice (or such longer period as may be agreed by the parties in writing), then either party may issue a notice in writing to the other party requiring the dispute to be determined by mediation in accordance with, and subject to, the Resolution Institute Mediation Rules or any equivalent and replacement rules.
- (b) If the dispute still remains unresolved 20 Business Days after a party becomes entitled to issue a notice in writing under clause 35.3(a) requiring the dispute to be determined by mediation, and by that time:
  - (i) *neither party has referred the dispute to mediation*: then either party may commence any other form of dispute resolution, including court proceedings, to determine the dispute; or
  - (ii) *the dispute has been referred to mediation*: then neither party may commence any other form of dispute resolution to determine the dispute, until a further 10 Business Days has elapsed following the commencement of mediation.

**35.4 Acknowledgment**

The parties acknowledge and agree that neither party may commence any other form of dispute resolution to determine the dispute, until the procedure set out in clauses 35.2 to 35.3 (or such other procedure set out in Item 54 of the Order Form) has been complied with in relation to the dispute.

**35.5 Costs**

Each party will bear its own costs in respect of complying with this clause 35.

**35.6 Continue to perform**

Notwithstanding the existence of a dispute, the parties must continue to perform their obligations under this Agreement.

---

**36. Force Majeure**

**36.1 Force Majeure Event**

Subject to clauses 36.2 and 36.3, non-performance as a result of a Force Majeure Event by a party of any obligation required by this Agreement to be performed by it will, during the time,

and to the sole extent, that such performance is prevented, wholly or in part, by that Force Majeure Event:

- (a) be excused; and
- (b) not give rise to any liability to the other party for any Losses arising out of, or in any way connected with, that non-performance.

## **36.2 Notification and diligence**

A party which is, by reason of a Force Majeure Event, unable to perform any obligation required by this Agreement to be performed will:

- (a) notify the other party as soon as possible giving:
  - (i) full particulars of the event or circumstance of the Force Majeure Event;
  - (ii) the date of commencement of the Force Majeure Event and an estimate of the period of time required to enable it to resume full performance of its obligations where these particulars are available at the time of the Force Majeure Event notice; and
  - (iii) where possible, the means proposed to be adopted to remedy or abate the Force Majeure Event;
- (b) use all reasonable diligence and employ all reasonable means to remedy or abate the Force Majeure Event as expeditiously as possible;
- (c) resume performance as expeditiously as possible after termination of the Force Majeure Event or after the Force Majeure Event has abated to an extent which permits resumption of performance;
- (d) notify the other party when the Force Majeure Event has terminated or abated to an extent which permits resumption of performance to occur; and
- (e) notify the other party when resumption of performance will occur.

## **36.3 Liability not relieved**

A Force Majeure Event affecting a party's performance under this Agreement will not relieve that party of liability in the event, and to the extent that:

- (a) its negligence, failure to comply with any applicable Business Contingency Plan or breach of this Agreement (which was not caused by the Force Majeure Event) caused or contributed to its failure to perform under this Agreement; or
- (b) it failed to use all reasonable endeavours to remedy the situation and to remove the event or circumstances giving rise to the Force Majeure Event.

## **36.4 Prolonged Force Majeure Event**

If a Force Majeure Event prevents or inhibits the Supplier's performance of any obligation required to be performed under this Agreement for 60 days or more (or such other period as specified in the Order Form), then the Customer may, at its sole discretion, elect to terminate this Agreement or reduce its scope pursuant to clause 29.1(d).

---

## **37. Reports and audits**

### **37.1 Records and reports**

- (a) The Supplier must keep and maintain true and accurate records and accounts of:
  - (i) all of the Supplier's Activities performed under this Agreement, including all records specified in the Module Terms;
  - (ii) the Supplier's compliance with its obligations under this Agreement; and
  - (iii) all associated records and accounts, including all supporting material, used to generate and substantiate the Invoices that it submits under this Agreement.
- (b) Without limiting clause 37.1(a), the Supplier must provide the Customer with quarterly reports containing details of:
  - (i) the Supplier's compliance with the SME Policies, including (to the extent that the SME Policies apply):
    - A. the SMEs (as defined in the SME Policies) engaged in the Supplier's Activities;
    - B. the amounts paid to any such SMEs;
    - C. the Supplier's compliance with any plans developed or updated in accordance with the SME Policies; and
    - D. such other matters as required under the SME Policies; and
  - (ii) the Supplier's compliance with the Aboriginal Procurement Policy, including identifying (to the extent that the Aboriginal Procurement Policy applies) the:
    - A. Aboriginal-owned businesses engaged to perform the Supplier's Activities under this Agreement;
    - B. Supplier's compliance with the Aboriginal Participation Plan; and
    - C. amounts paid to any Aboriginal owned businesses under this Agreement.

### **37.2 Audits and inspections**

- (a) The Customer or its nominee (which may be an advisor, consultant or other third party engaged by the Customer) may conduct audits and inspections of the Supplier's and its Personnel's performance of its obligations under this Agreement, including the:
  - (i) Supplier's and any of the Supplier's subcontractors' operational practices and procedures as they relate to this Agreement;
  - (ii) accuracy of the Supplier's Invoices and reports submitted under this Agreement; and
  - (iii) Supplier's and its Personnel's compliance with its other obligations under this Agreement.

- (b) For the purpose of conducting an audit or inspection under clause 37, or for the purposes of an inspection, examination or audit undertaken by or on behalf of the Auditor-General in accordance with its powers to assess the expenditure of public money related to this Agreement, the Customer, Auditor-General or their nominees may, on giving reasonable advance notice to the Supplier (at reasonable times and during Business Hours where practicable):
  - (i) access the premises and facilities of the Supplier to the extent reasonably required to carry out the audit or inspection;
  - (ii) to the extent relating to the Supplier's Activities, access, inspect and copy documents, resources and books and records, however stored, in the possession or control of the Supplier or its Personnel; and
  - (iii) require assistance in respect of any inquiry into or concerning the Supplier's Activities, including any parliamentary or statutory review or inquiry.
- (c) If an audit will involve the Supplier being required to produce documents, resources or books and records, the Customer will accompany its notice under clause 37.2(b) with a general description of the scope and purpose of the audit.
- (d) To the extent an audit involves physical access to the premises or facilities of the Supplier the:
  - (i) Customer will limit the exercise of its audit or inspection rights to no more than once per calendar year, unless the audit arises from the Supplier's breach of this Agreement or the Customer forming, on a reasonable basis, a view that such breach may have occurred; and
  - (ii) Customer or its nominee must comply with the Supplier's reasonable security requirements during such physical access.
- (e) The Supplier must provide all reasonable access, assistance and co-operation required by the Customer or its nominee in carrying out an audit under this clause 37.2.
- (f) Without limiting any rights or remedies of the Customer, if an audit shows that the Supplier or its Personnel has:
  - (i) breached, or is in breach of, this Agreement, the Supplier must promptly do all things necessary to remedy that breach and prevent it from recurring at no cost to the Customer; or
  - (ii) overcharged the Customer in any Invoice, the Supplier must promptly refund any amounts that the Supplier has overcharged the Customer, and adjust all of the current invoices that have not been paid by the Customer to ensure that the Customer is only liable to pay the correct amount. Where the overcharging discrepancy identified exceeds 10% of the amount that should have been correctly invoiced, the Supplier must also promptly reimburse the Customer for the reasonable costs (including internal costs) of conducting the audit.
- (g) Subject to clause 37.2(f)(ii), each party must bear its own costs of executing its rights under, or complying with, this clause 37.

### **37.3 Conduct of audits and inspections**

The Customer and its nominee must, in conducting an audit or inspection under this clause 37:

- (a) to the extent it obtains any Confidential Information of the Supplier as a result of such audit or inspection, treat that information in accordance with clause 23; and
- (b) not delegate the conduct of an audit or inspection under this clause to any person who may reasonably be considered to be a direct competitor of the Supplier in relation to the Supplier's Activities (unless such person is otherwise approved by the Supplier, acting reasonably).

### 37.4 Survival

This clause 37 survives for the Term and a period of seven years following the termination or expiry of this Agreement.

---

## 38. Proportionate liability

- (a) To the extent permitted by Law, Part 4 of the *Civil Liability Act 2002* (NSW) (and any equivalent statutory provision in any other state or territory) is excluded in relation to all and any rights, obligations or liabilities of either party under or in any way in connection with this Agreement whether such rights, obligations or liabilities are sought to be enforced in contract, tort or otherwise.
- (b) Without limiting clause 38(a), the rights, obligations and liabilities of the Customer and the Supplier under this Agreement with respect to proportionate liability are as specified in this Agreement and are not otherwise, whether such rights, obligations or liabilities are sought to be enforced in contract, in tort or otherwise.

## PART F: GENERAL PROVISIONS

---

## 39. General

### 39.1 Government information

- (a) The Supplier acknowledges that the Customer is subject to the GIPA Act and agrees that the Customer may disclose any part or all of this Agreement on its nominated website established for GIPA Act disclosures. The Supplier irrevocably consents to the Customer acting in accordance with this clause 39.
- (b) To the extent that section 121 of the GIPA Act applies, the Supplier must, upon receipt of a written request by the Customer, provide the Customer with immediate access to the following information contained in records held by the Supplier:
  - (i) information that relates directly to the performance of the Supplier's Activities;
  - (ii) information collected by the Supplier from members of the public to whom it provides, or offers to provide, any aspect of the Supplier's Activities; and
  - (iii) information received by the Supplier from the Customer to enable it to carry out the Supplier's Activities.
- (c) For the purposes of clause 39.1(b), information does not include information that:
  - (i) discloses or would tend to disclose the Supplier's financing arrangements, financial modelling, cost structure or profit margin;
  - (ii) the Supplier is prohibited from disclosing to the Customer by provision made by or under any Act, whether of any State or Territory, or of the Commonwealth; or

- (iii) if disclosed to the Customer, could reasonably be expected to place the Supplier at a substantial commercial disadvantage in relation to the Customer whether at present or in the future.
- (d) The Supplier must provide copies of any of the information referred to in clause 39.1(b), as requested by the Customer, at the Supplier's own expense and in such medium as the Customer may reasonably require.
- (e) Without limiting any other provision of this clause 39.1, the Supplier:
  - (i) authorises the Customer to make information concerning the Supplier available to other Government Agencies or Eligible Customers (including to the relevant head of any Government Agency or Eligible Customer and any responsible Minister of a Government Agency) for any purpose in connection with facilitating the Customer's exercise of its rights under this Agreement or the carrying out, or exercise, of the functions or powers of the Customer, any Government Agency, Eligible Customer or the Crown. Such information may include any information provided by the Supplier to the Customer and any information relating to the Supplier's performance under this Agreement (including any reports provided under clause 15.4);
  - (ii) acknowledges that information about the Supplier from any source, including substantiated reports of unsatisfactory performance, or any conduct including, any civil and/or criminal or alleged criminal conduct, by any officers or associates of the Supplier or a Related Body Corporate may be taken into account by Government Agencies and Eligible Customers considering whether to offer the Supplier future opportunities for working with those entities, for assessing the terms of their own contracts (or proposed contracts) with the Supplier or any other third party, for governance or reporting purposes or for any other reasonable business or government purposes;
  - (iii) agrees that the communication of such information to any Government Agency is a communication falling within section 30 of the *Defamation Act 2005* (NSW); and
  - (iv) releases and indemnifies the Customer and the State of New South Wales from and against any Claim in respect of any matter arising out of such communications, including the use of such information by the recipient.

### 39.2 Personal Property Securities Act

To the extent the *Personal Property Securities Act 2009* (Cth) applies to any Materials or Deliverables supplied by the Supplier to the Customer, the Supplier represents, warrants and undertakes that the supply of the Materials and Deliverables to the Customer:

- (a) does not breach any security agreement the Supplier has with a third party; and
- (b) is within the ordinary course of the Supplier's business.

### 39.3 No use of the Customer's name or logo

The Supplier must not use the Customer's name or any of the Customer's logos, trade marks or branding, without the prior written consent of the Customer.

### 39.4 Prior work

Except as otherwise agreed between the parties in writing:



- (a) the terms of this Agreement apply to all of the work performed by the Supplier in connection with the Supplier's Activities even if it was performed prior to entry into this Agreement; and
- (b) any payment made to the Supplier by the Customer in connection with this Agreement or the Supplier's Activities prior to entry into this Agreement will be treated as a payment under this Agreement and will be in part discharge of the Customer's obligation to pay the Price.

### **39.5 Entire agreement**

This Agreement is the entire agreement between the parties about its subject matter and replaces all previous agreements, understandings, representations and warranties about that subject matter.

### **39.6 Variation**

No variation to this Agreement is effective unless made in writing and executed by each party.

### **39.7 Survival and merger**

- (a) No term of this Agreement merges on completion of any transaction contemplated by this Agreement.
- (b) The following provisions survive the termination and expiry of this Agreement:
  - (i) 9, 13, 17, 18, 19, 20, 21, 23, 27(a)(iv), 29.5, 31, 32, 33.4, 34.8, 37, 38 and this clause 39; and
  - (ii) any other provisions that are expressed to or which by their nature survive termination or expiry.

### **39.8 Severability**

Any term of this Agreement which is wholly or partially void or unenforceable is severed to the extent that it is void or unenforceable. The validity or enforceability of the remainder of this Agreement is not affected.

### **39.9 Waiver**

- (a) No waiver of a right or remedy under this Agreement is effective unless it is in writing and signed by the party granting it. It is only effective in the specific instance and for the specific purpose for which it is granted.
- (b) A single or partial exercise of a right or remedy under this Agreement does not prevent a further exercise of that or of any other right or remedy. Failure to exercise or a delay in exercising a right or remedy under this Agreement does not operate as a waiver or prevent further exercise of that or of any other right or remedy.

### **39.10 Cumulative rights**

Except as expressly provided in the Additional Conditions, the rights and remedies of a party under this Agreement (including under an indemnity) are in addition to and do not exclude or limit any other rights or remedies provided by Law.

### **39.11 Further assurances**

Each party must do all things, and execute all further documents, necessary to give full effect to this Agreement.

**39.12 Assignment, novation and other dealings**

- (a) The Supplier must not, in whole or in part, assign or novate this Agreement or otherwise deal with the benefit of it or a right under it, or purport to do so without obtaining the prior written consent of the Customer, which consent may be withheld at the Customer's sole discretion.
- (b) The Supplier acknowledges that the Customer may conduct financial and other inquiries or checks on the entity proposing to take an assignment or novation of this Agreement before determining whether or not to give consent to an assignment or novation.
- (c) Subject to clause 39.12(d), the Customer must not, in whole or in part, assign or novate this Agreement or otherwise deal with the benefit of it or a right under it, or purport to do so, without the prior written consent of the Supplier, which consent may not be unreasonably withheld.
- (d) Notwithstanding clause 39.12(c), the Customer may, at its sole discretion, assign or novate this Agreement in whole or in part:
  - (i) to any other Eligible Customer, by notice in writing to the Supplier; or
  - (ii) for machinery of government changes, including if, by operation of Law, the Customer is reconstituted into a new body or legal entity or the functions of the Customer, relevant to this Agreement, are transferred to a different body or legal entity.
- (e) The Supplier agrees to co-operate in good faith and provide all reasonable assistance to the Customer in respect of any such assignment or novation made by the Customer under this clause 39.12.
- (f) The Supplier must (to the extent permitted by Law):
  - (i) notify the Customer if the Supplier or any parent company of the Supplier is about to undergo a Change in Control or Other Changes, as soon as it becomes aware that the Change in Control or Other Changes will or may occur; and
  - (ii) provide the Customer with all information reasonably requested by the Customer in respect of the Change in Control or Other Changes, including in respect of any incoming owner or other person who is to obtain control over the Supplier or any parent company.

**39.13 Notices**

- (a) A notice, consent or other communication under this Agreement (**Notice**) is only effective if it is in writing and received in full and legible form at the addressee's address or email address.
- (b) For the purposes of this clause 39.13, a party's address and email address is that set out in the Order Form (as applicable), unless the party has notified a changed address, then the notice, consent, approval or other communication must be sent to that address.
- (c) A Notice will be regarded as received at the time and on the day it is actually received, but if it is received on a day that is not a Business Day or after 5:00pm on a Business Day it is regarded as received at 9:00am on the following Business Day.
- (d) Unless there is evidence to the contrary:

- (i) a letter sent by post will be taken to be received on the fifth Business Day after posting (or seventh, if posted to or from a place outside of Australia);
- (ii) in the case of email:
  - A. production of a delivery notification statement from the computer from which the email was sent which indicates that the email was sent in its entirety to the email address of the recipient will be prima facie evidence that the email has been received;
  - B. where there is no delivery notification statement from the computer from which the email was sent, the date and the time of dispatch of the email will be prima facie evidence of the date and time that the email was received; and
  - C. where a delivery error or similar response is returned in response to that email, the email will not be taken to be received and the sender must use an alternative method of giving that notice in accordance with this clause 39.13.

#### **39.14 Construction**

No rule of construction applies to the disadvantage of a party because that party was responsible for the preparation of this Agreement.

#### **39.15 Expenses**

Except as otherwise expressly provided in this Agreement, each party must pay its own costs and expenses in connection with the negotiation, preparation and execution of this Agreement.

#### **39.16 English language**

All communications between the parties and all documentation provided in connection with this Agreement and the Supplier's Activities must be in the English language.

#### **39.17 Governing Law**

This Agreement is governed by the Laws applicable in the State of New South Wales, Australia. The Supplier irrevocably and unconditionally submits to the sole and exclusive jurisdiction of the courts of New South Wales, Australia and the courts entitled to hear appeals from those courts.

Executed as an agreement:

**Signed** for and on behalf of **the State of New South Wales, represented by the Department of Communities and Justice (ABN 36 433 875 185),** by its authorised representative, but not so as to incur personal liability, in the presence of:

**Refer to the DocuSign on Last Page**

Signature of authorised representative

**Jay Huntley, A/CDIO**

Name of authorised representative in full

**Refer to the DocuSign on Last Page**

Date

**Executed by Fujitsu Australia Ltd (ABN 19 001 011 427)** in accordance with section 127 of the *Corporations Act 2001* (Cth):

Signature of Director

Name of Director in full

07-Apr-2025

**Refer to the DocuSign on Last Page**

Date

## Schedule 1 - Definitions and interpretation

### 1.1 Definitions

In this Agreement, unless the contrary intention appears:

**Aboriginal Participation Plan** means the plan of that name developed pursuant to the Aboriginal Procurement Policy and attached to, or referenced in, the Order Form.

**Aboriginal Procurement Policy** means the New South Wales Government's Aboriginal Procurement Policy published at <https://buy.nsw.gov.au/policy-library/policies/aboriginal-procurement-policy> (or such other link as notified by the Customer).

**Acceptance** in respect of a Deliverable, means the issuing by the Customer of an Acceptance Certificate for that Deliverable. **Accept** and **Accepted** have a corresponding meaning.

**Acceptance Certificate** means an acceptance notice or certificate issued by the Customer pursuant to clause 14.3 to confirm that a Deliverable meets the Acceptance Criteria.

**Acceptance Criteria** in respect of a Deliverable, means the compliance of that Deliverable with any criteria set out in the Order Form and such other requirements as the Customer reasonably considers necessary to determine whether that Deliverable complies with the applicable Specifications and the other requirements set out in this Agreement.

**Acceptance Tests** or **Testing** in respect of a Deliverable, means acceptance tests carried out in accordance with clause 14 to verify whether the Acceptance Criteria in respect of that Deliverable has been met, including any such tests specified in the Order Documents.

**Accessibility Standard** has the meaning given to that term in clause 6.3(a)(i).

**Additional Activities** has the meaning given to that term in clause 6.9(a)(i).

**Additional Conditions** means any terms or conditions that vary or are additional to the terms and conditions set out in the Core Terms or Module Terms and which are stated or referenced in Items 11 or 66 of the Order Form.

**Additional Order** means an Additional Order for Services and/or Deliverables that is placed in accordance with clause 3.3.

**Adjustment Notice** has the meaning given to that term in clause 24.3(d).

**Agreement** means this agreement and includes any schedule and attachment to this agreement.

**Authorisations** means any consent, registration, filing, agreement, notarisation, certificate, licence, approval, permit, authority or exemption from, by or with a Government Agency.

**Authority** includes any Government Agency, governmental or semi-governmental or local government authority, administrative, regulatory or judicial body or tribunal, department, commission, public authority, agency, Minister, statutory corporation or instrumentality.

**Benchmarking Activities** has the meaning given to that term in clause 24.2(b).

**Benchmarking Notice** has the meaning given to that term in clause 24.2(b).

**Benchmarking Report** has the meaning given to that term in clause 24.3(a).

**Best Industry Practice** means a standard of service or deliverable, in terms of quality, productivity, performance, cost and timeliness of delivery, that, when considered collectively, is equal to or better than the commonly accepted best practice being provided at the relevant

time by a supplier of like or similar services, deliverables and activities to the Supplier's Activities throughout the world.

**Business Contingency Plan** has the meaning given to that term in clause 25.2(a).

**Business Day** means a day other than a Saturday, Sunday or gazetted public holiday in New South Wales, Australia.

**Business Hours** means the hours between 9:00am and 5:00pm on any Business Day.

**Change Control Procedure** means the procedure to be followed with respect to Change Requests as specified in clause 10.

**Change in Control** means, in respect of an entity, the occurrence of any circumstances or events following which the entity, who was not so controlled before, is controlled by another person, alone or together with any Related Body Corporate, and:

- (a) includes, in respect of the entity, a change of a direct holding of at least fifteen percent of the voting shares in that entity or a holding company of that entity; however
- (b) excludes an internal solvent corporate reorganisation occurring exclusively within the group of companies comprised of the Supplier and its Related Bodies Corporate.

**Change Request** has the meaning given to that term in clause 10.1(a).

**Change Request Form** means a document in substantially the same form as that in Schedule 5 or such other form approved by the Customer.

**Claim** means any allegation, cause of action, liability, claim, proceeding, suit or demand of any nature, whatsoever arising, and whether present or future, fixed or unascertained, actual or contingent and whether at Law, under statute or otherwise.

**Commencement Date** means the date specified as such in the Order Form.

**Confidential Information** means information that:

- (a) is by its nature confidential;
- (b) is communicated by the discloser of the information (**Discloser**) to the recipient of the information (**Recipient**) as confidential;
- (c) the Recipient knows or ought to know is confidential; or
- (d) relates to or comprises the:
  - (i) financial, corporate or commercial information of any party;
  - (ii) affairs of a third party; or
  - (iii) strategies, practices or procedures of the State of New South Wales or any information in the Supplier's possession relating to a Government Agency,

but excludes information:

- (e) in the public domain, unless it came into the public domain due to a breach of confidentiality;
- (f) independently developed by the Recipient; or

- (g) in the possession of the Recipient without breach of confidentiality by the Recipient or other person.

**Conflict of Interest** means the Supplier or its Personnel:

- (a) engaging in any activity;
- (b) obtaining any interest, whether pecuniary or non-pecuniary; or
- (c) being involved in any actual or threatened litigation or investigation,

whether proven or alleged, which is likely to, has the potential to, or could be perceived to, present a conflict of interest in the Supplier or its Personnel performing its obligations under this Agreement.

**Contract Authority** means the entity named as such in the Order Form and who has entered into a MICTA.

**Core Modern Slavery Obligations** has the meaning given to that term in clause 13.1.

**Core Terms** means clauses 1 to 39 of this Agreement.

**Corporations Act** means the *Corporations Act 2001* (Cth).

**Correctly Rendered Invoice** means an Invoice which:

- (a) specifies an amount that is due for payment and correctly calculated in accordance with this Agreement;
- (b) is itemised and identifies the GST exclusive amount, the GST component and the GST inclusive amount (as applicable) and enables the Customer to ascertain what the Invoice covers and the amount payable;
- (c) includes (where available) the relevant purchase order number notified by the Customer to the Supplier and this Agreement reference number;
- (d) where relating to an amount that is payable subject to Acceptance, is accompanied by documentary evidence that signifies that Acceptance (where appropriate) has occurred in accordance with this Agreement;
- (e) is in the right form (which may be an electronic or digital form where agreed to by the Customer); and
- (f) complies with clauses 24.4(a) to 24.4(b) and satisfies any additional criteria relating to Invoices specified in the Order Form.

**Critical CSI** means any:

- (a) CSI that is critical to the Supplier's ability to carry out the Supplier's Activities and without which the Supplier would be materially restricted in its ability to carry out the Supplier's Activities in accordance with the requirements of this Agreement; or
- (b) any CSI specified as "Critical CSI" in the Order Form.

**Crown** means the Crown in right of the State of New South Wales.

**Customer** means the entity named as such in Item 1 of the Order Form.

**Customer Data** means all data (including metadata) and information relating to the Customer or any Government Agency and the operations, facilities, customers, clients, personnel, assets and programs of the Customer and any Government Agency, including Personal Information,

in whatever form that information may exist and whether created, captured, collected, entered into, stored in, generated by, controlled, managed, retrieved, transferred, transmitted, printed, processed or produced as part of carrying out the Supplier's Activities, but excluding any Performance Data.

**Customer Environment** means the combination of hardware, software, systems and network infrastructure and services used by the Customer from time to time, including those specified in the Order Documents.

**Customer's Representative** means the person nominated in Item 2 of the Order Form or as advised in writing by the Customer to the Supplier from time to time, to act on behalf of the Customer in connection with this Agreement.

**Customer Supplied Items** or **CSI** means the Materials, equipment, resources or items specified in the Order Form to be provided by the Customer to the Supplier.

**Customer User(s)** means any Personnel of the Customer or any other person that the Customer authorises to use the Deliverables or Services.

**Data Location Conditions** means:

- (a) compliance with the Information Security Requirements;
- (b) ensuring that Customer Data and Personal Information is at all times handled and processed in accordance with all applicable Laws, including the Privacy Laws and the *State Records Act 1998* (NSW) (to the extent applicable);
- (c) not transferring any Customer Data and Personal Information to a jurisdiction that is the subject of any sanction, embargo, export control or similar Laws;
- (d) ensuring that Customer Data and Personal Information is at all times protected in accordance with the terms of this Agreement including clauses 19, 20 and 21; and
- (e) compliance with any other requirements or conditions with respect to the location of Customer Data and Personal Information as specified in Item 39 of the Order Form or in the Module Terms.

**Data Management and Protection Plan** means the Supplier's written plan with respect to data management and protection that complies with clause 20.2.

**Date for Delivery** means the date(s) (including any Key Milestones) by which the Supplier must provide the relevant Deliverables and/or Services to the Customer or complete the relevant Supplier's Activities, as stated in the Order Documents and as may be adjusted under this Agreement.

**Deed of Confidentiality and Privacy** has the meaning given to that term in clause 11.4(a).

**Default Amount** means the amount determined as such according to clause 34.5(b).

**Defect** means a fault, error, failure, degradation, deficiency or malfunction that causes the relevant Deliverable or Service to not meet the Specifications and the other requirements of this Agreement or any other aspect of a Deliverable or Service that is not in accordance with the requirements of this Agreement.

**Delay** has the meaning given to that term in clause 6.7(a)(i).

**Deliverable** means all things or items (including Documents) to be supplied by the Supplier under this Agreement as set out in the Order Documents.

**Denial of Service (DoS) Attack** means an attack that shuts down or substantially degrades the Deliverables and/or Services, resulting in the Deliverables and/or Services (or any



functionality forming part of the Deliverables and/or Services) being unable to be used by the Customer or Customer Users in the manner intended to be used under this Agreement, including as to any Service Levels or key performance indicators.

**Disaster** means any disaster, accident, emergency, degradation, damage, interruption or other event which impacts on the continuity of the Supplier's Activities (including any Force Majeure Event impacting the Supplier).

**Dispute Notice** has the meaning given to that term in clause 35.1(b).

**Document** has the meaning given to that term in clause 8.1(a).

**Document Deliverable** means any Deliverable which is, or is required to be, in the form of a Document.

**Eligible Customer** means any Government Agency or Eligible Non-Government Body.

**Eligible Non-Government Body** includes the following public bodies that are not Government Agencies (as identified under clause 6 of the *Public Works and Procurement Regulation 2019* (NSW)):

- (a) a private hospital;
- (b) a local council or other local authority;
- (c) a charity or other community non-profit organisation;
- (d) a private school or a college;
- (e) a university;
- (f) a public authority of the Commonwealth or any other State or Territory;
- (g) a public authority of any other jurisdiction (but only if it carries on activities in the State of New South Wales); or
- (h) any contractor to a public authority (but only in respect of things done as such a contractor).

**Escrow Materials** means the software code and programming Materials specified in Item 38 of the Order Form or otherwise specified as constituting "Escrow Materials" in Schedule 7.

**Existing Materials** means any Materials in which Intellectual Property Rights subsist (which, in the case of the Supplier, are incorporated into a Deliverable or Service or to which the Customer otherwise requires a licence in order to enjoy the benefit of this Agreement or any obligations performed for the Customer under it):

- (a) belonging to a party that are pre-existing as at the Commencement Date; or
- (b) that are brought into existence, by or on behalf of a party, other than in connection with the performance of that party's obligations under this Agreement,

and includes any enhancements, modifications and developments to such Materials, to the extent not comprising New Materials.

**Financial Security** has the meaning given to that term in clause 28.2(a).

**Force Majeure Event** means any of the following events or circumstances to the extent not within the reasonable control of the party affected by it (**Affected Party**):

- (a) acts of God, including storms, cyclones, landslides, epidemics, earthquakes, floods, and other natural disasters;
- (b) strikes, stoppages, labour restraints and other industrial disturbances, except for those only affecting the Personnel of the Affected Party;
- (c) acts of the public enemy, including wars, blockades and insurrections; and
- (d) riots, malicious damage, sabotage, civil disturbance and acts of terrorism,

the incidence of which is not (or would not be reasonably expected to be) generally known to the Affected Party as at the Commencement Date and which the Affected Party is not reasonably able to prevent or overcome, or the effects of which the Affected Party is not reasonably able to predict and take measures to avoid, by the exercise of reasonable diligence and prudence.

**GIPA Act** means the *Government Information (Public Access) Act 2009* (NSW).

**Governance Framework** has the meaning given to that term in clause 4.3(a).

**Government Agency** means any of the following:

- (a) a government sector agency (within the meaning of the *Government Sector Employment Act 2013* (NSW));
- (b) a New South Wales Government agency;
- (c) any other public authority that is constituted by or under an Act or that exercises public functions for or on behalf of the State of New South Wales (other than a State owned corporation); or
- (d) any State owned corporation prescribed by regulations under the *Public Works and Procurement Act 1912* (NSW).

**GST Law** means *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

**ICT** means information and communication technologies.

**ICT Purchasing Framework** means the suite of New South Wales Government template documents which sets out standard terms and conditions to be used by Eligible Customers for the procurement of ICT related goods and services.

**Indemnified Entities** means the Customer, Customer Users, the State of New South Wales, the Customer's Personnel and, in relation to a Government Agency, the relevant head of the Government Agency and its responsible Minister.

**Information Security Requirements** has the meaning given to that term in clause 19.2(a).

**Inherent Risks** means the level of risks that exists in an organisation prior to the adoption or implementation of internal security controls or measures designed to avoid or mitigate them.

**Initial Term** means the period specified as such in the Order Form.

**Insolvency Event** means the occurrence of any one or more of the following events in relation to any person:

- (a) an application is made to a court for an order, or an order is made, that it be wound up, declared bankrupt or that a provisional liquidator or receiver, or receiver and manager, be appointed;
- (b) a liquidator or provisional liquidator is appointed;

- (c) an administrator is appointed to it under sections 436A, 436B or 436C of the Corporations Act;
- (d) a Controller (as defined in section 9 of the Corporations Act) is appointed to it or any of its assets;
- (e) a receiver is appointed to it or any of its assets;
- (f) it enters into an arrangement or composition with one or more of its creditors, or an assignment for the benefit of one or more of its creditors, in each case other than to carry out a reconstruction or amalgamation while solvent;
- (g) it proposes a winding-up, dissolution or reorganisation, moratorium, deed of company arrangement or other administration involving one or more of its creditors;
- (h) it is insolvent as disclosed in its accounts or otherwise, states that it is insolvent, is presumed to be insolvent under Law (including under sections 459C(2) or 585 of the Corporations Act) or otherwise is, or states that it is, unable to pay all its debts as and when they become due and payable;
- (i) it is taken to have failed to comply with a statutory demand as a result of section 459F(1) of the Corporations Act;
- (j) a notice is issued under sections 601AA or 601AB of the Corporations Act;
- (k) a writ of execution is levied against it or a material part of its property;
- (l) it ceases to carry on business or threatens to do so; or
- (m) anything occurs under the Law of any jurisdiction which has a substantially similar effect to any of the events set out in the above clauses of this definition.

**Intellectual Property Rights** means all intellectual property rights, including:

- (a) copyright, patent, design, semi-conductor or circuit layout rights, registered design, trade marks or trade names and other protected rights, or related rights, existing worldwide; and
- (b) any licence, consent, application or right to use or grant the use of, or apply for the registration of, any of the rights referred to in paragraph (a),

but does not include the right to keep Confidential Information confidential, Moral Rights, business names, company names or domain names.

**Invoice** means a tax invoice issued under the GST Law.

**Item** means an item in Parts A to E of the Order Form.

**Key Milestone** means a Date for Delivery of a Deliverable, or for the completion of a particular Service or other Supplier's Activity, that is specified as such in the Payment Particulars or Order Documents, as may be adjusted under this Agreement.

**Laws** means any legally binding law, legislation, statute, act, regulation, subordinate legislation, rule, by-law, order, proclamation, decree, ordinance, directive or code which is enacted, issued or promulgated from time to time in any relevant jurisdiction (including the Commonwealth or any State or Territory government) and any applicable common law and rule or principle of equity.

**Licensed Software** means the software set out in the Order Documents that the Supplier is to provide to the Customer, or provide the Customer access to (as applicable) under this

Agreement and includes any Updates or New Releases of that software that may be provided to the Customer from time to time in accordance with this Agreement.

**Limitation Amount** has the meaning given to that term in clause 34.5.

**Liquidated Damages** means any damages specified as such in an Order Form which, where applicable, will be applied in accordance with clause 16.

**Loss** means any loss, damage, liability, cost (including all legal and other professional costs on a full indemnity basis), charge, expense, Claim, outgoing, fine or payment of any nature or kind.

**Material Defect** means any Defect which represents a material departure from the Specifications or other requirements of this Agreement in respect of that Deliverable or prevents the proper operation of the Deliverable.

**Materials** means all property, materials, documents, information and items in whatever form, and includes equipment, hardware, computer software (including development tools and object libraries), concepts, approaches, tools, methodologies, processes, know-how, data, Documentation, manuals and anything else which is the subject matter of Intellectual Property Rights.

**MICTA** means (if any) the master ICT agreement between the Contract Authority and the Supplier under which there is a standing offer to provide particular ICT-related goods, services and/or other activities (including the Deliverables and Services) to Eligible Customers.

**Modern Slavery** means:

- (a) mean any conduct that constitutes or would constitute any offence listed in Schedule 2 of the Modern Slavery Act 2018 (NSW), including an offence of attempting or incitement to commit such an offence;
- (b) includes any conduct that constitutes or would constitute an offence under any of the Modern Slavery Laws as amended from time to time, including an offence of attempting or incitement to commit such an offence;
- (c) includes conduct engaged in elsewhere than in New South Wales that, if it occurred in New South Wales, would constitute a modern slavery offence under paragraphs (a) or (b); and
- (d) includes any form of slavery, servitude, forced labour, human trafficking, debt bondage, organ trafficking, forced marriage and exploitation of children.

**Modern Slavery Guidance** means the document titled 'NSW Anti-slavery Commissioner's Guidance on Reasonable Steps to Manage Modern Slavery Risks in Operations and Supply-Chains' published by the Office of the NSW Anti-slavery Commissioner as updated, replaced or superseded from time to time.

**Modern Slavery Laws** means:

- (a) the *Modern Slavery Act 2018* (Cth);
- (b) the *Modern Slavery Act 2018* (NSW);
- (c) Divisions 270 and 271 of the Commonwealth Criminal Code;
- (d) section 176(1A) of the *Public Works and Procurement Act 1912* (NSW);
- (e) section 438ZE of the *Local Government Act 1993* (NSW); and

- (f) any other laws, regulations, codes and international conventions aimed at combatting modern slavery, forced labour or human trafficking, from time to time in force in or ratified by Australia and, where relevant, in or by other jurisdictions in which the parties operate,

each as amended from time to time.

**Modern Slavery Statement** means a modern slavery statement as required or volunteered under the Modern Slavery Laws.

**Module** means the applicable Module(s) which apply to the specific Services and/or Deliverables as identified in the Order Form.

**Module Terms** means the terms and conditions in respect of the applicable Module(s) as set out in the Module(s).

**Moral Rights** means a person's moral rights as defined in the *Copyright Act 1968* (Cth) and any other similar rights existing under any other laws.

**New Materials** means Materials in which Intellectual Property Rights subsist that are created or which arise in the course of performing this Agreement, excluding Customer Data.

**New Releases** means software (including the latest current version) which has been produced primarily to extend, alter or improve the Licensed Software by providing additional functionality or performance enhancement (whether or not Defects in that Licensed Software are also corrected) while still retaining the original designation of the Licensed Software. A New Release does not include any software that is generally licensed by the Supplier to its customers as a different product.

**Nominated Personnel** means the key Personnel of the Supplier who are required to undertake the provision of the Supplier's Activities or part of the work constituting the Supplier's Activities, as stated in Item 18 of the Order Form or otherwise agreed by the Customer in writing.

**Notice** has the meaning given to that term in clause 39.13.

**Open Source Software** means software available under a licence which:

- (a) meets the criteria of the Open Source Definition published by the Open Source Initiative at <http://www.opensource.org>, and includes the forms of creative commons licences published as the Creative Commons Legal Code for Australia at <http://www.creativecommons.org>; or
- (b) contains any term or condition which mandates the re-licensing or redistribution to the public (whether free of charge or for a fee) of any software code, in any circumstance.

**Order** means an order for the Services and/or Deliverables and other Supplier's Activities as set out in an Order Form, and includes an Additional Order.

**Order Documents** means:

- (a) the Order Form;
- (b) the Payment Schedule;
- (c) all applicable Plans; and
- (d) the relevant Module Terms identified as applicable in Item 13 of the Order Form.

**Order Form** means:

- (a) the document set out at Schedule 2;
- (b) any Additional Order;
- (c) any Statement of Work or Supplier's Documents incorporated within or attached to an Order Form in accordance with this Agreement; and
- (d) any schedules, annexures or attachments expressly incorporated into any of the above documents.

**Other Changes** means any actual or proposed change in the Supplier's circumstances, operations or supply chains (including a change to the Supplier's Personnel) that could reasonably be considered to:

- (a) create a security risk for the Customer or the State of New South Wales; or
- (b) adversely affect the:
  - (i) Supplier's ability to fulfil its obligations under this Agreement; or
  - (ii) reputation of the Customer or the State of New South Wales.

**Other Supplier** means any supplier, contractor, consultant or other person engaged to provide services or deliverables to the Customer, other than the Supplier or its subcontractors and suppliers.

**Payment Particulars** means the pricing and payment regime for the completion of the Supplier's Activities as set out in the Payment Schedule, the Statement of Work or in Item 43 of the Order Form.

**Payment Schedule** means the schedule of Prices and payment regime specified in Schedule 4.

**Performance Data** means automatically generated metadata, not including any Personal Information or Confidential Information of the Customer or a Government Agency that:

- (a) is incidentally generated by a computer system in the course of its normal operation;
- (b) relates to the performance or operation of that computer system; and
- (c) arises in the course of the performance of the Supplier's Activities.

**Performance Guarantee** has the meaning given to that term in clause 28.1.

**Personal Information** means:

- (a) information or an opinion about an identified individual (that is, a natural person) or an individual who is reasonably identifiable whether the information or opinion is:
  - (i) true or not; and
  - (ii) recorded in a material form or not; and
- (b) information defined as such under applicable Privacy Laws.

**Personnel** means a party's employees, officers, agents and subcontractors and:

- (a) in the case of the Supplier, includes any persons carrying out the Supplier's Activities on the Supplier's behalf; and

- (b) in the case of the Customer, includes any Customer Users permitted or enabled by the Customer to use the Deliverables and Services, but excludes the Supplier and its Personnel.

**Plans** means any:

- (a) Project Plan;
- (b) Business Contingency Plan;
- (c) Data Management and Protection Plan;
- (d) Test Plan;
- (e) Transition-In Plan and Transition-Out Plan; and
- (f) any additional plans specified in Item 27 of the Order Form or required to be complied with under this Agreement.

**Policies, Codes and Standards** means:

- (a) all applicable SME Policies and associated requirements;
- (b) the other policies, codes, standards and guidelines and associated requirements specified in this Agreement, including within:
  - (i) clauses 12.2(b) and 37.1(b); and
  - (ii) the Order Form; and
- (c) any Policy Changes with which the Supplier is or becomes required to comply with under clause 12.3.

**Policy Change** has the meaning given to that term in clause 12.3(a).

**Price** means the total amount payable by the Customer for the Deliverables and/or Services and the carrying out of the other Supplier's Activities under this Agreement as stated in the Payment Particulars, as may be adjusted under this Agreement.

**Privacy Laws** means:

- (a) the *Privacy Act 1988* (Cth);
- (b) the *Privacy and Personal Information Protection Act 1998* (NSW);
- (c) the *Health Records and Information Privacy Act 2002* (NSW);
- (d) any legislation (to the extent that such legislation applies to the Customer or the Supplier or any other recipient of Personal Information) from time to time in force in:
  - (i) any Australian jurisdiction (which includes the Commonwealth of Australia and any State or Territory of Australia); and
  - (ii) any other jurisdiction (to the extent that the Customer or any Personal Information or the Supplier is subject to the laws of that jurisdiction),

affecting privacy or Personal Information, provided that the Supplier ensures that it complies at all times with the Privacy Laws applicable in New South Wales; and

- (e) any ancillary rules, guidelines, orders, directions, directives, codes of conduct or other instruments made or issued under any of the legislation referred to in paragraphs (a), (b), (c) and (d), as amended from time to time.

**Professional Standards Legislation** means the *Professional Standards Act 1994* (NSW) or other equivalent Laws providing for the statutory limitation of liability of certain suppliers.

**Project Plan** has the meaning given to that term in clause 6.5(a).

**Reasonable Steps** means those steps that are reasonable in the circumstances to prevent, identify, mitigate and remedy modern slavery. In assessing whether steps are reasonable, the parties may refer to the Modern Slavery Guidance and related information and resources published by the Office of the NSW Anti-slavery Commissioner.

**Related Body Corporate** has the meaning given to that term in the Corporations Act.

**Remediation Plan** has the meaning given to that term in clause 22.2(a)(vi).

**Renewal Period** means the renewal period specified in Item 9 of the Order Form.

**Schedule** means a Schedule to this Agreement. Those Schedules that are applicable to an Order will be identified in Item 13.

**Security Incident** means any one or more of the following:

- (a) any unauthorised (whether under this Agreement or otherwise) or unlawful use of, loss of, access to, alteration of, or disclosure of Customer Data or Personal Information within the Supplier's or its Personnel's possession or control (including any data and information stored on the Supplier's equipment or in the facilities used by the Supplier to carry out the Supplier's Activities, or any unauthorised or unlawful access to such equipment or facilities);
- (b) any notifiable data breach under the Privacy Laws;
- (c) any Denial of Service Attack, Virus or other incident that compromises or adversely impacts the security, availability or integrity of Customer Data, the systems and technologies holding such data or the Customer Environment (or which has the intent to do so);
- (d) any security breaches, cyber security incidents or similar events relating to, or affecting Customer Data, Personal Information or the Customer Environment which trigger, or are likely to trigger, contractual reporting obligations or legal reporting obligations to an Authority or which would require a response or action under this Agreement, at Law or under any of the Policies, Codes and Standards;
- (e) where there are reasonable grounds to suspect that any breaches or circumstances under paragraphs (a) to (d) have occurred or are likely to have occurred or will occur; or
- (f) any alleged occurrence of any of the above events or circumstances.

**Security Program** has the meaning given to that term in clause 21.2(a).

**Service Levels** means any minimum performance levels, key performance indicators and other service standards with respect to the Supplier's Activities to be achieved by the Supplier as specified, included or incorporated by reference (in accordance with this Agreement) in the Order Documents.

**Services** means:



- (a) the services that the Supplier is required to perform or provide under this Agreement as described in the Order Documents; and
- (b) any related or ancillary services which are required or reasonably incidental for the proper performance of the services, functions, processes and responsibilities referred to in paragraph (a).

**Site** has the meaning given to that term in clause 6.10(a).

**SME Policies** means:

- (a) the New South Wales Government's Small and Medium Enterprises and Regional Procurement Policy, published at <https://buy.nsw.gov.au/policy-library/policies/sme-and-regional-procurement-policy> (or such other link as notified by the Customer);
- (b) the ICT/Digital Sovereign Procurement Commitments, published at <https://buy.nsw.gov.au/resources/ictdigital-sovereign-procurement-commitments> (or such other link as notified by the Customer);
- (c) the Small Business Shorter Payment Terms Policy, published at <https://buy.nsw.gov.au/policy-library/policies/small-business-shorter-payment-terms-policy> (or such other link as notified by the Customer); and
- (d) such other SME policies specified in the NSW Procurement Policy Framework, published at <https://buy.nsw.gov.au/policy-library/policies/procurement-policy-framework> (or such other link as notified by the Customer).

**Specifications** in respect of a Deliverable or Service, means the technical or descriptive specifications of the functional, operational, performance or other characteristics relating to that Deliverable or Service as detailed or referred to in the Order Documents or as otherwise agreed by the parties in writing.

**Stage** means one or more stages or phases of the project as specified in the Order Documents.

**Statement of Work** means a statement of work incorporated within or attached to an Order Form, an illustrative form of which is set out in Schedule 3.

**Step-In Right** has the meaning given to that term in clause 26.

**Step-Out Notice** has the meaning given to that term in clause 26.2(a).

**Supplier** means the entity named as such in Item 4 of the Order Form.

**Supplier's Activities** means all things or tasks which the Supplier is, or may be, required to do to comply with its obligations under this Agreement and includes the supply of the Deliverables and Services and, where applicable, the carrying out of any Transition-In Services and Transition-Out Services.

**Supplier's Documents** means any product specifications, service-specific detail or other terms and conditions of the Supplier which comply with clause 1.5 and which the parties have expressly agreed to incorporate into this Agreement, as set out in Annexure A to the Order Form.

**Supplier's Representative** means the Supplier's employee nominated in Item 5 of the Order Form or as advised in writing by the Supplier from time to time to act on its behalf in connection with this Agreement.

**Tax** means any sales tax, value added tax, duty, withholding tax, levy, impost or other charge or duty levied by any government in Australia or elsewhere, which arises out of or in

connection with the Supplier's performance of its obligations under this Agreement, but excludes GST.

**Term** means the Initial Term of this Agreement and any Renewal Period, unless this Agreement is terminated earlier, in which case the Term ends on the date of termination of this Agreement.

**Test Plan** means the Plan with respect to the conduct of tests pursuant to clause 14, and which is referenced in or annexed to the Statement of Work or other Order Documents or agreed between the parties in writing.

**Transition-In Plan** means a transition-in Plan prepared by the Supplier and approved by the Customer in accordance with clause 7.

**Transition-In Services** means the transition-in Services specified in the Order Documents or in any Transition-In Plan that is approved by the Customer in accordance with clause 7.2.

**Transition-Out Period** means the period specified in the Order Documents or, if no period is specified in the Order Documents, the period commencing on the expiry or termination of this Agreement and continuing for six months.

**Transition-Out Plan** means a transition-out Plan prepared by the Supplier and approved by the Customer in accordance with clause 31.2.

**Transition-Out Services** means any transition-out or disengagement Services provided by the Supplier pursuant to clause 31, including under any Transition-Out Plan.

**Updates** means software which has been produced primarily to overcome Defects in, or to improve the operation of, the relevant part of the Licensed Software without significantly altering the Specifications whether or not that Licensed Software has also been extended, altered or improved by providing additional functionality or performance enhancement.

**User Documentation** means any documentation (such as user manuals, operating manuals, technical manuals, published specifications, security configurations or other documentation) that:

- (a) is specified in the Order Documents; or
- (b) is reasonably required in order for the Customer or Customer Users to use, maintain, secure, operate or otherwise obtain the benefit of any Deliverable or Service.

**Virus** means a computer program, code, device, product or component that is designed to threaten the security or integrity of the Customer's operations or the Deliverables and/or Services, prevent, inhibit or impair the performance of the Customer's operations or the Deliverables and/or Services or pose a threat or hazard to the security or integrity of the Customer's operations, but does not include any code, mechanism or device that is included in software by the Supplier for the purpose of managing the licensed use of software.

**Warranty Period** means the period specified in Item 36 of the Order Form, or where no warranty period is specified:

- (a) 90 days from Acceptance of the relevant Deliverable or Service; or
- (b) if a Deliverable or Service is not subject to Acceptance, 30 days from the provision of the Deliverable or Service to the Customer in accordance with this Agreement.

**WHS Legislation** means legislation relating to health and safety, including the *Work Health and Safety Act 2011* (NSW) and the *Work Health and Safety Regulation 2017* (NSW).

**Wilful Misconduct** means an act or omission of a party, deliberately performed or engaged in, which the relevant party knew (or ought to have known or predicted on due and reasonable consideration), would have a reasonable possibility of damaging, having a materially adverse effect on, or prejudicing, the other party.

## 1.2 Interpretation

In this Agreement, the following rules of interpretation apply unless the contrary intention appears:


- (a) headings are for convenience only and do not affect the interpretation of this Agreement;
- (b) the singular includes the plural and vice versa;
- (c) an obligation or liability assumed by, or a right conferred on, two or more persons binds or benefits them jointly and severally;
- (d) words that are gender neutral or gender specific include each gender;
- (e) where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings;
- (f) the words "such as", "including", "particularly" and similar expressions are not used as, nor are intended to be interpreted as, words of limitation;
- (g) a reference to:
  - (i) a person includes a natural person, partnership, joint venture, government agency, association, corporation or other body corporate;
  - (ii) a thing (including a chose in action or other right) includes a part of that thing;
  - (iii) a party includes its successors and permitted assigns;
  - (iv) a document includes all amendments or supplements to that document;
  - (v) a clause, term, party, schedule or attachment is a reference to a clause or term of, or party, schedule or attachment to the relevant part of this Agreement in which that reference is located;
  - (vi) a reference to a statute or other Law is a reference to that statute or other Law as amended, consolidated or replaced;
  - (vii) a monetary amount is to Australian dollars or such other currency specified in the Order Documents; and
  - (viii) time is to Australian Eastern Standard Time;
- (h) a reference to any Authority, institute, association or body is:
  - (i) if that Authority, institute, association or body is reconstituted, renamed or replaced or if the powers or functions of that Authority, institute, association or body are transferred to another organisation, deemed to refer to the reconstituted, renamed or replaced organisation or the organisation to which the powers or functions are transferred, as the case may be; and

- (ii) if that Authority, institute, association or body ceases to exist, deemed to refer to the organisation which serves substantially the same purposes or object as that Authority, institute, association or body; and
- (i) no rule of construction applies to the disadvantage of a party because that party was responsible for the preparation of any part of this Agreement.

### **1.3 Discretion**

- (a) Subject to any express provision in this Agreement to the contrary:
  - (i) a provision of this Agreement which says that the Customer or the Customer's Representative "may" do or not do something is not to be construed as imposing an obligation on the Customer or the Customer's Representative to do or not do that thing; and
  - (ii) there will be no procedural or substantive limitation upon the manner in which the Customer or the Customer's Representative may exercise any discretion, power or entitlement conferred by this Agreement.
- (b) Without limiting clause 1.3(a) of this Schedule, neither the Customer nor the Customer's Representative will be under any obligation to exercise any such discretion, power or entitlement for the benefit of the Supplier or as required by any other legal doctrine which in any way limits the express words used in the provisions of this Agreement conferring the discretion, power or entitlement.

Schedule 2 - Order Form



**Guidance note:** Where a particular Item number in the Order Form is not applicable, insert "not applicable".

If a particular Item number is addressed in the Statement of Work or another Order Document, reference the relevant document within the last column; for example, "As stated in section X of the Statement of Work".

If the Agreement is being entered into pursuant to a MICTA, certain Items and components of the Order Form may have been pre-agreed as part of the MICTA. If this is this case, the parties only need to complete the remaining Items and components of the Order Form.

PART A: ICTA

Complete this section in relation to parts of this Agreement which reference this Order Form.  
Clause references below are references to clauses in this Agreement.

No	Item	Ref	Description or selection
KEY DETAILS			
1.	Customer	Generally Schedule 1	The Crown in right of the State of New South Wales, acting through the Department of Communities and Justice, ABN 36 433 875 185
2.	Customer's Representative	Generally Schedule 1	Name: Venkatesh Ramamurthi  Position: Manager Technology Operations  Email: venkatesh.ramamurthi@dcj.nsw.gov.au  Phone: 0411 104 155
3.	MICTA	1.4  Generally Schedule 1	Is this Agreement entered into pursuant to a MICTA?  <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No.
4.	Supplier	Generally Schedule 1	Fujitsu Australia Limited ABN 19 001 011 427
5.	Supplier's Representative	Generally Schedule 1	Name: <div></div>  Position: Account Executive  Email: <div></div> @fujitsu.com  Phone: <div></div>
6.	Notices for the Customer	39.13(b)	Customer's address:  Level 10, 6 Parramatta Square 10 Darcy Street, Parramatta NSW 2150  Customer's email: venkatesh.ramamurthi@dcj.nsw.gov.au

No	Item	Ref	Description or selection
	Notices for the Supplier	39.13(b)	<p>Supplier's address: Level 5, 345 George Street, Sydney NSW 2000;</p> <p><b>and</b></p> <p>PO Box Q483, Queen Victoria Building NSW 1230</p> <p>Supplier's email: [REDACTED]@fujitsu.com</p> <p><b>and</b></p> <p>[REDACTED]@fujitsu.com</p>
<b>TERM</b>			
7.	Commencement Date	5.1 Schedule 1	The Commencement Date is 1 April 2025.
8.	Initial Term	5.1 Schedule 1	The Initial Term commences on the Commencement Date and continues for 36 months, ending on 31 March 2028
9.	Renewal Period	5.2 Schedule 1	There are two Renewal Periods and each Renewal Period is twelve months in length
	Notice period for renewals	5.2	60 days prior to the end of the then-current Term.
<b>ORDERING AND PURCHASING</b>			
10.	Additional Orders	3.3 Schedule 1	The Customer may place Additional Orders to alter the scope of the Services under this Agreement subject to the compliance of both parties with Clause 3.3 and Schedule 5.
11.	Additional Conditions	3.5 Schedule 1 Annexure C Annexure D	The Additional Conditions are as set out in Annexures C and D to the Order Form.
12.	Reseller arrangements	3.6	Not applicable – the Supplier is not acting in the capacity of a reseller.

No	Item	Ref	Description or selection
13.	Schedules	Generally  Schedule 1	<input checked="" type="checkbox"/> Schedule 1 - Definitions and interpretation  <input checked="" type="checkbox"/> Schedule 2 - Order Form  Schedule 3 - Statement of Work Template (Note: If a Statement of Work is used, this should be included at Annexure B to Schedule 2 (Order Form). The template in Schedule 3 can be used for this purpose).  <input checked="" type="checkbox"/> Schedule 4 - Payment Schedule  <input checked="" type="checkbox"/> Schedule 5 - Change Request Form (Note: The Change Request Form should be included for all Orders. However, note that, if approved by the Customer, an alternate form to the default provisions in Schedule 5 may be used).  <input checked="" type="checkbox"/> Schedule 6 - Deed of Confidentiality and Privacy  <input type="checkbox"/> Schedule 7 - Escrow Deed  <input type="checkbox"/> Schedule 8 - Performance Guarantee  <input type="checkbox"/> Schedule 9 - Financial Security
	Modules	1.2(c)	[Identify the Module(s) which apply by selecting the relevant box or boxes.]  <input type="checkbox"/> Cloud Module  <input checked="" type="checkbox"/> Services Module  <input type="checkbox"/> Software Module (Non-Cloud)  <input type="checkbox"/> Hardware and Other ICT Deliverables Module
<b>SUPPLIER'S ACTIVITIES</b>			
14.	Scope	Generally	The Supplier must provide the Supplier's Activities in accordance with the Statement of Work.
15.	Requirements - Accessibility requirements	6.3(b)(ii)	The default accessibility requirements apply, unless additional requirements are specified in the Statement of Work (in which case, the default accessibility requirements apply in addition to the requirements specified in the Statement of Work).  In addition to the default accessibility requirements, the Supplier must ensure that any Deliverables or Services comprising software are able to accommodate applications developed which meet the Accessibility Standard AS EN 301 549 or its replacement.
	Requirements - Work health and safety	12.4(f)	The default work health and safety requirements apply, unless additional requirements are specified in the Statement of Work (in which case, the default work health and safety requirements apply in addition to the requirements specified in the Statement of Work).

No	Item	Ref	Description or selection
16.	Site attendance	6.10 Schedule 1 Annexure C	Will the Supplier be required to attend the Site to carry out any aspect of the Supplier's Activities (including the supply of any Deliverables)?  <input checked="" type="checkbox"/> Yes  <input type="checkbox"/> No
	Site location		a) 6 Parramatta Square 10 Darcy St, Parramatta NSW 2150; and/or  b) such other premises or facilities of the Customer as nominated by the Customer from time to time or specified in the Statement of Work.
	Physical delivery		To the extent applicable, the specific delivery area at the Site, the Date for Delivery and the hours for delivery will be nominated by the Customer from time to time.
	Requirements for attendance at the Site		The Supplier and its Personnel are permitted to attend the Site only at the times nominated by the Customer from time to time, and subject to such conditions as may be nominated by the Customer from time to time. Without limitation, the Supplier must comply (and must ensure that its Personnel comply) with the requirements set out in Items 17, 22 and 40 of this Order Form.
17.	Policies, Codes and Standards	12.2 Schedule 1 Annexure C Annexure D Annexure E	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexures C and D.  In addition to the terms of Annexures C and D, the Supplier must comply with the Supplier Code of Conduct published at <a href="https://buy.nsw.gov.au/policy-library/policies/supplier-code-of-conduct">https://buy.nsw.gov.au/policy-library/policies/supplier-code-of-conduct</a> .
	SME Policies	12.2 Schedule 1	The Supplier must comply with the SME and Local Participation Plan as specified in in Annexure A – Supplier's Documents Attachment 1 of this Order Form.  <a href="https://www.info.buy.nsw.gov.au/policy-library/policies/sme- and-regional-procurement-policy">https://www.info.buy.nsw.gov.au/policy-library/policies/sme- and-regional-procurement-policy</a>
	Aboriginal Procurement Policy: Aboriginal participation	12.2(b)	Once the contract value reaches \$7.5m, the Supplier must comply with clause 12.2(b) and the Aboriginal Participation Plan as specified in Annexure A – Supplier's Documents Attachment 1 of this Order Form.  <a href="https://buy.nsw.gov.au/policy-library/policies/aboriginal-procurement-policy">https://buy.nsw.gov.au/policy-library/policies/aboriginal-procurement-policy</a>
18.	Nominated Personnel	11.1 Schedule 1	Not Applicable.



No	Item	Ref	Description or selection
19.	Deed of Confidentiality and Privacy	11.4(a) Schedule 1	If requested by the Customer from time to time, the Supplier must ensure that the Supplier's Personnel (including subcontractors) sign a Deed of Confidentiality and Privacy in the form of Schedule 6.
20.	Permitted subcontractors	11.5(a)	Not Applicable
21.	Subcontractor deed	11.5(j)	If subcontractors are engaged, they must complete Schedule 6 - Deed of Confidentiality and Privacy.
	Additional subcontractor procurement policy requirements	11.5(k)	Not Applicable
22.	Background checks	11.6(b) Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
	Timeframes and time for background checks		The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
<b>PERFORMANCE AND DELIVERY</b>			
23.	Timeframes and requirements for performance	6.1	As set out in the Statement of Work.
	Specifications	6.1 Schedule 1	As set out in the Statement of Work.
24.	Service Levels	15.2 Schedule 1	As set out in the Statement of Work.
25.	Performance reports	15.4(a)(iii)	As set out in the Statement of Work.
	Additional performance reporting requirements	15.4(c)	As set out in the Statement of Work.
	Performance reviews	15.5(a)	Yes, the parties must conduct service and performance reviews in accordance with clause 15.5(a) as and when required by the Customer and in accordance with the requirements of the Customer.

No	Item	Ref	Description or selection
26.	Meetings	15.7(a)	<p>The Supplier's Representative must meet with the Customer's Representative or the Customer's other Personnel at the times and at the locations specified in the Statement of Work or as otherwise requested by the Customer from time to time.</p> <p>Meetings are to be held either in person at the Customer's premises or by video link as required by the Customer.</p>
27.	Project Plans	6.5(b)	As set out in the Statement of Work.
	Other Plans	Schedule 1	<p>The Supplier is required to prepare the following Plans, and any other Plans as set out in the Statement of Work:</p> <p>(a) Business Contingency Plan (clause 25.2);</p> <p>(b) Data Management and Protection Plan (clause 20.2);</p> <p>(c) Test Plan (clause 14.2); and</p> <p>(d) Transition-Out Plan (clause 31.2).</p> <p>in each case in accordance with the terms of the Agreement and the requirements of the Statement of Work.</p>
28.	Stages	6.6(a) Schedule 1	As set out in the Statement of Work. Any reference to 'Phase' (or similar) in a Statement of Work is deemed to be a reference to a Stage.
	Project methodology	6.6(e)	As set out in the Statement of Work.
	Costs of removing any Stage(s)	6.6(d)	No costs apply for the purposes of clause 6.6(d). The Supplier must provide a refund to the Customer for any part of the Price that is pre-paid in respect of any Stage that is removed from the scope of the Supplier's Activities.
29.	Liquidated Damages	16(a)	Not applicable.
		16(b) Schedule 1	
30.	Governance Framework	4.3	Yes, a Governance Framework applies. The Governance Framework must be provided as set out in the Statement of Work.
31.	Customer Supplied Items	6.2 Schedule 1	As set out in the Statement of Work
	Date for provision of CSI		Not applicable, unless otherwise specified in the Statement of Work.
	CSI requirements		Not applicable, unless otherwise specified in the Statement of Work.
	Supplier's costs for CSI and time for payment		Not applicable, unless otherwise specified in the Statement of Work.

No	Item	Ref	Description or selection
32.	Transition-In Plan	7.2 Schedule 1	Not applicable.
	Transition-In Services	7.3 Schedule 1	Not applicable.
33.	Transition-Out Services	31.1 Schedule 1	<p>The Supplier must provide Transition-Out Services upon expiration or termination of this Agreement (regardless of the Stage during which this Agreement terminates or expires).</p> <p>The Prices applicable to the Transition-Out Services will be agreed in writing in advance by the Parties, acting reasonably and in accordance with the rates set out in this Agreement (or if no such rates are set out, in accordance with commercially competitive rates).</p>
	Transition-Out Plan	31.2 Schedule 1	<p>The Supplier must submit the draft Transition-Out Plan to the Customer for its review, comment, and approval within 90 days of the Commencement Date.</p> <p>a) The Supplier must review and update the Transition-Out Plan:</p> <ul style="list-style-type: none"> <li>i. at least annually during the Term;</li> <li>ii. if there is a material change to the Deliverables or the Services; and</li> <li>iii. at least 3 months prior to the expiration of this Agreement, or if this Agreement is terminated earlier, upon receipt of the notice of termination.</li> </ul> <p>The Supplier must promptly submit any proposed amendments to the Transition-Out Plan (either submitted, or reviewed and updated, under paragraphs a) or b) respectively) to the Customer for its review, comment, and approval, and incorporate the reasonable comments or suggestions of the Customer into the draft Transition-Out Plan and resubmit for the Customer approval within the time frame specified by the Customer.</p>
	Transition-Out Period	31.3 Schedule 1	<p>The Transition-Out Period is the period commencing on the expiration or termination of this Agreement, and ending on the date specified in a notice in writing issued by the Customer, provided that such date must be no later than eighteen months following the expiry or termination of this Agreement. For clarity, this Agreement continues to apply during the Transition-Out Period.</p> <p>The Customer may terminate the Transition-out Services, in whole or in part, at any time by giving the Supplier at least 5 Business Days written notice of such termination. Without limiting the maximum end date for the Transition-Out Period, if required by the Customer, the Supplier must commence the provision of Transition-Out Services prior to the expiration or termination of this Agreement (on a date nominated by the Customer).</p>

No	Item	Ref	Description or selection
34.	User Documentation	8.4(a)	Not Applicable.
	Format for the User Documentation	8.4(c)	Yes, the Supplier must provide the User Documentation in electronic format).
35.	Acceptance Testing	14 Schedule 1	<p>All Deliverables (other than Document Deliverables) are subject to Acceptance Testing. Acceptance Testing will be performed in accordance with clause 14. The approval process in clause 8 applies to Document Deliverables.</p> <p>The Supplier must perform the following tests under clause 14.2:</p> <p>(a) updates, fixes, patches and modifications and minor enhancements</p> <p>(b) Documentation</p> <p>(c) any other New Contract Material as agreed.</p> <p>The Customer may perform any such tests as the Customer considers necessary or appropriate to determine that the Services and Deliverables comply with the Acceptance Criteria and the requirements of this Agreement, including the tests set out in the Statement of Work.</p> <p>Additional Acceptance Testing requirements may be agreed by the parties in the Statement of Work.</p>
		14.1	The Acceptance Testing procedures specified in clause 14 apply.
		14.2 Schedule 1	The Acceptance Criteria are as set out in the Statement of Work, or if not set out, are as agreed by the parties in writing from time to time.
36.	Warranty Period	9 Schedule 1	30 Days (One Month) for Base Support Package Warranty as specified in the Statement of Work.
<b>INTELLECTUAL PROPERTY</b>			
37.	Ownership of Existing Materials	17.1	Clause 17.1 applies in all circumstances.
	Licence to use Existing Materials	17.2 17.5	<p>Clause 17.2 applies to the licence granted to the Customer in relation to the Supplier's Existing Materials, and to the licence granted to the Supplier in relation to the Customer's Existing Materials. The licence granted to the Customer in respect of the Supplier's Existing Materials is perpetual and irrevocable and the Customer is permitted to use the Supplier's Existing Materials for the purposes referred to in clause 17.4(b).</p> <p>The licence granted to the Supplier in respect of the Customer's Existing Materials is for the Term only.</p>

No	Item	Ref	Description or selection
	Ownership of New Materials	17.3	All New Materials will be owned by the Customer, and ownership of all Intellectual Property Rights in those New Materials vests in the Customer immediately on creation or is transferred or assigned by the Supplier to the Customer immediately on creation, free of any encumbrances, security interests and third party rights.
	Licence to use New Materials	17.4 17.5	A licence is granted to the Supplier by the Customer in relation to New Materials, but only in accordance with and subject to clause 17.6. Such licence is for the Term only.
	Third party Intellectual Property Rights	17.7	Clause 17.7 applies in relation to third party Intellectual Property Rights.
38.	Escrow	18	Not applicable.
	Escrow Materials	18 Schedule 1	Not applicable.
<b>DATA AND SECURITY</b>			
39.	Location of Personal Information	20.1(a)(iv) Schedule 1 Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
	Data Location Conditions	19.3(b) Schedule 1 Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
40.	Security obligations, standards and Information Security Requirements	19.2 21.2 Annexure C Annexure E	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
	Security certifications	21.2(e) Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
	Security audits	21.3 Schedule 1 Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
41.	Backup of Customer Data	19.4 Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.

No	Item	Ref	Description or selection
	Retention of Customer Data	19.7 Annexure C	The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.
42.	Security Incident	22.1 22.2 Schedule 1 Annexure C	<p>The Supplier must ensure that it and its Subcontractors comply fully with the Customer's Additional Conditions pertaining to this clause, as set out in Annexure C.</p> <p>The definition of Security Incident is deemed to include (in addition to the items specified in the definition of Security Incident) any:</p> <ul style="list-style-type: none"> <li>a) breach of the Information Security Requirements (including the requirements set out in Item 40 above);</li> <li>b) flaw or vulnerability of any kind in the security controls or other measures used to protect the Customer's Confidential Information or Customer Data; and</li> <li>c) misuse or loss of, interference with or unauthorised access to, modification of or disclosure of the Customer's Confidential Information or Customer Data.</li> </ul> <p>Written notification of a security incident must be sent to the Customer representative as well <a href="mailto:InfoSec@dcj.nsw.gov.au">InfoSec@dcj.nsw.gov.au</a>.</p>
<b>FEES AND PAYMENT</b>			
43.	Payment Particulars	24.1(a)	As set out in the Payment Schedule.

105

No	Item	Ref	Description or selection
			<p>c) Without limitation, any electronic invoices must satisfy the criteria below to ensure that they are paid in a timely manner:</p> <ul style="list-style-type: none"> <li>i. all invoices must be sent as PDF attachments;</li> <li>ii. each email must attach only one 'PDF' file, containing only one invoice;</li> <li>iii. any supporting documents must be contained within the same attached 'PDF' file as the invoice, with the invoice being the first page and all supporting documents to follow; and</li> <li>iv. a valid agreement number / purchase order number must be quoted on all invoices.</li> </ul>
	Time for payment	24.5(a) Schedule 1	<p>The Customer will pay any Correctly Rendered Invoice in accordance with the timeframes specified in clause 24.5(a).</p> <p>Notwithstanding the foregoing, to the extent the NSW Government SME Faster Payment Terms policy applies, the Customer will pay any Correctly Rendered Invoice within 5 Business Days of receipt by the Customer of a Correctly Rendered Invoice.</p>
	Purchase order number and Agreement reference number for Correctly Rendered Invoices	Generally	<p>The purchase order number (and, to the extent applicable, the Agreement reference number) must be specified on each Correctly Rendered Invoice. The purchase order number (and, to the extent applicable, the Agreement reference number) to be specified on Correctly Rendered Invoices will be notified by the Customer to the Supplier.</p>
	Supplier's nominated bank account	24.5(a)(i)	<p>The Supplier's bank account details to which payments should be transferred will be as stated in the Correctly Rendered Invoice.</p> <p>Any changes to the Supplier's bank account details during the term of the contract should be communicated in writing to the Customer's Representative (Item 2).</p>
<b>RISK ALLOCATION AND MANAGEMENT</b>			



No	Item	Ref	Description or selection
47.	Business Contingency Plan	25.2(a) 25.2(b)(iii) 25.2(d)	<p>a) A Business Contingency Plan is required and must be provided to the Customer for the Customer's approval by no later than thirty days after the Commencement Date.</p> <p>b) For the purposes of clause 25.2(b)(iii), the Business Contingency Plan must also:</p> <ul style="list-style-type: none"> <li>i. provide for the integration and co-ordination with the Supplier's business continuity arrangements with the Customer and relevant Other Suppliers;</li> <li>ii. be consistent with Best Industry Practice with respect to business continuity; and</li> <li>iii. address any other requirements specified in the Statement of Work or reasonably required by the Customer.</li> </ul> <p>The Supplier must review and test the Business Contingency Plan at least annually and in any event upon the reasonable request of the Customer.</p>
48.	Step-In Rights	26	<p>a) The Customer may exercise Step-In Rights under this Agreement in accordance with clause 26. Without limiting any other right or remedy of the Customer under or in connection with this Agreement (including under clause 29 and including with respect to the events that occurred prior to the exercise of the Customer's Step-In Rights), if the Customer exercises its Step-In Rights for 14 days or more, then the Customer may, at its sole discretion, elect to terminate this Agreement and/or reduce its scope Agreement pursuant to clause 29.1(d).</p> <p>b) The default timeframe of five Business Days applies under clause 26.2(a) for the purposes of the Customer ceasing to exercise its Step-In Rights.</p>
49.	Insurance	27(a)	[REDACTED]
	Cyber security and other insurances	27(a) 27(b)	<p>[REDACTED]</p> <p>[REDACTED]</p>
50.	Performance Guarantee	28.1	Not applicable.
51.	Financial Security	28.2	Not applicable.

No	Item	Ref	Description or selection
52.	Termination for convenience	29.2(b)(ii)B	<p>a) No other costs are payable by the Customer for the purposes of clause 29.2(b)(ii)B.</p> <p>b) If the Customer terminates this Agreement or reduces its scope under clause 29.2(a) and amounts have been pre-paid by the Customer in respect of the period after the termination or reduction (as applicable), the amounts payable by the Customer under clause 29.2(b) will be reduced by such pre-paid amounts. For clarity, if amounts that have been pre-paid by the Customer in respect of the period after the termination or reduction (as applicable) exceed the amounts payable by the Customer under clause 29.2(b), the Supplier must refund the excess amount to the Customer promptly (and in any event within 10 Business Days of the effective date of termination or reduction (as applicable)).</p>
53.	Limitation Amount	34.5(b)	
	Alternate approach to uncapped liability	34.5(c)	Not applicable.
	Non-excluded Losses	34.6(b)(ii)	<p>Where the Customer is the recovering party, the following additional types of Loss will also be treated as Loss of the kind referred to in clause 34.6(b)(i):</p> <p>a) costs arising from the loss of or corruption to data (in whatever format), including the cost and expense of rectifying and reloading the relevant data; and</p> <p>b) expenditure incurred in respect of crisis management and/or public relations.</p>
54.	Alternative dispute resolution	35	Clause 35.3 does not apply, except where the parties mutually agree in writing at the relevant time.
55.	Prolonged Force Majeure Event	36.4	The default position in clauses 36.4 applies.

**PART B: Cloud Module – Not Applicable**

Clause references below are references to clauses in the Cloud Module.

No	Item	Mod ref	Description or selection
<b>SCOPE</b>			
56.	Cloud Services	1.1	Not Applicable.
57.	Services Period	1.3	Not Applicable.
58.	Unilateral Variation	1.4	Not Applicable.
	Form of, and medium for, notice of a Unilateral Variation	1.4(c)	Not Applicable.
59.	Dates for Delivery	2.1(a)	Not Applicable.
	Third Party Components	2.1(a)(iii) Annexure A	Not Applicable.
	Date for provision of access codes	2.1(b)	Not Applicable.
60.	Scope of licence	2.2(b)	Not Applicable.
61.	Permitted Purpose	2.2(b)(v) Annexure A	Not Applicable.
<b>LICENSING MODEL AND TERMS</b>			
62.	Licensing model	2.3(a)	Not Applicable.
	Licensing terms	2.3(b)  2.3(c)	Not Applicable.
63.	Permitted Users	2.3(b) Annexure A	Not Applicable.
64.	Data backups by the Customer	2.5(a)	Not Applicable.
	Data backups by the Supplier	2.5(b)	Not Applicable.
65.	Records of usage and audits	2.6	Not Applicable.
66.	Additional Conditions - Cloud Services terms	2.7	Not Applicable.
67.	Restrictions	3(a)	Not Applicable.

No	Item	Mod ref	Description or selection
68.	Primary and Secondary Data Centres	4.3(a) 4.4(a)	Not Applicable.
69.	Remote access to Customer Data	4.3(b)	Not Applicable.
70.	Notice of change to location of data centres	4.4(a)	Not Applicable.
71.	Excluded locations	4.4(b)	Not Applicable.
72.	Media decommissioning	4.5(a)(ii)	Not Applicable.
<b>SUPPORT AND TRAINING SERVICES</b>			
73.	Support Services	5.1 5.3	Not Applicable.
74.	Support Period	5.2 Annexure A	Not Applicable.
75.	Help desk	5.4	Not Applicable.
76.	Training Services	6.1	Not Applicable.
77.	Training Reports	6.2	Not Applicable.
<b>GENERAL</b>			
78.	Additional/ancillary Deliverables and Services	7.1	Not Applicable.
79.	Records	8	Not Applicable.
80.	Operating procedures	9(a)(iv)	Not Applicable.

**PART C: Services Module**

Clause references below are references to clauses in the Services Module.

No	Item	Mod ref	Description or selection
<b>SCOPE</b>			
81.	Services	1.1	The Services and associated Deliverables that the Supplier must provide are as set out in the Statement of Work.
82.	Non-ICT Services	Generally	Not Applicable
83.	Services Period	1.3 Annexure A	The Services must be provided for the duration of the Term, in accordance with the Statement of Work.
<b>SUPPORT SERVICES</b>			
84.	Support Services	2.1 2.3	The Supplier must provide Support Services in accordance with the Statement of Work.
	Support Period	2.2 Annexure A	The Support Period is the full Term.
85.	Help desk	2.4	The Supplier must provide help desk Services in accordance with the Statement of Work.
86.	Software Support Services	3.1 3.2(b) Annexure A	The Supplier must provide Software Support Services in accordance with the Statement of Work, and such Software Support Services must include the provision of both Updates and New Releases
	Updates	3.2	The default requirements apply.
	New Releases	3.2	The default requirements apply.
	Security Corrections	3.2(f)	The default requirements apply.
87.	Period to maintain the Software after provision of Updates and New Releases	3.2(g)	The Supplier must maintain any versions of the Software in use by the Customer for the full Support Period, regardless of whether the Customer has rejected any Update or New Release.
88.	Support Services for Hardware and Other ICT Deliverables	4.1 4.2 Annexure A	Not applicable.

No	Item	Mod ref	Description or selection
89.	Preventative Maintenance	4.3 Annexure A	The Supplier must provide Preventative Maintenance in accordance with clause 4.3 of the Services Module.
90.	Engineering changes	4.4	The default position applies - the Supplier must make available to the Customer all engineering changes. The Supplier must give the Customer at least ninety days advance written notice of all proposed engineering changes.
91.	Remedial Maintenance	4.5 Annexure A	The Supplier must provide Remedial Maintenance in accordance with clause 4.5 of the Services Module.
<b>DEVELOPMENT SERVICES</b>			
92.	Development Services	5.1 Annexure A	The Supplier must provide Development Services in accordance with the Statement of Work.
93.	Software Solution	5.2 Annexure A	The Application has already been deployed into production hence Not Applicable
94.	Design Specification	5.3(a) 5.3(b)	Not Applicable
95.	Service Levels or criteria that apply to the Development Services	5.4(d)	The Supplier must comply with the Service Levels set out in the Statement of Work in the provision of the Development Services.
96.	Alternative project delivery methodology	5.5	Not Applicable
<b>SYSTEM INTEGRATION SERVICES</b>			
97.	Systems Integration Services	6.1 Annexure A	The Supplier must provide System Integration Services in accordance with the Statement of Work
	Scope of Systems Integration Services	6.2	Not Applicable
	SI Plan and SI Specifications	6.3	Not Applicable

No	Item	Mod ref	Description or selection
<b>DATA SERVICES</b>			
98.	Data Services	7.1 7.2(a) Annexure A	Not Applicable
99.	Backup	7.4	Not Applicable
100.	Data cleansing	7.5	Supplier to use reasonable efforts to provide Data Cleansing using contracted Supplier resources if requested by the Customer. [REDACTED]
101.	Data analysis	7.6	Supplier to use reasonable efforts to provide Data analysis using contracted Supplier resources if requested by the Customer. [REDACTED]
102.	Data migration	7.7	Supplier to use reasonable efforts to provide Data migration using contracted Supplier resources if requested by the Customer. [REDACTED]
103.	Data Migration Plan	7.7	Supplier to use reasonable efforts to provide Data Migration planning using contracted Supplier resources if requested by the Customer. [REDACTED]
<b>OTHER PROFESSIONAL SERVICES</b>			
104.	Professional Services	8.1 Annexure A	The Supplier must provide Professional Services in accordance with the Statement of Work.
	Specifications and standards	8.2	The Supplier must provide the Professional Services in accordance with the Specifications and standards specified in the Statement of Work.
105.	Dates for Delivery and timeframes	8.2 8.3	Not applicable.
<b>MANAGED SERVICES</b>			
106.	Managed Services	9.1 9.2 Annexure A	Not applicable.
	Transition-In Services	9.3	Not applicable.
107.	Procedures Manual	9.4	Not applicable.

No	Item	Mod ref	Description or selection
108.	Managed Third Party Contracts	9.5 Annexure A	Not applicable.
109.	Assets	9.6 Annexure A	Not applicable.
110.	Transition-Out Services	9.7	Not applicable.
<b>TRAINING SERVICES</b>			
111.	Training Services	10.1	Not applicable.
	Training Reports	10.2	Not applicable.
<b>GENERAL</b>			
112.	Additional/ancillary Deliverables and Services	11.1 11.2	The Supplier must provide any additional or related Deliverables and Services specified in the Statement of Work.
113.	Records	12	Clause 12(b) of the Services Module applies.  The Supplier must at its sole cost, provide copies of the records (Application codes) required to be maintained and kept under clause 12 of the Services Module to the Customer's Representative at least every 30 days and when reasonably required by the Customer.
114.	Operating procedures	13(a)(v)	No operating procedures apply (and clause 13(a)(v) of the Services Module therefore does not apply).



**PART D: Software Module (Non-Cloud) – Not Applicable**

Clause references below are references to clauses in the Software Module (Non-Cloud).

No	Item	Mod ref	Description or selection
<b>SCOPE</b>			
115.	Scope	1.1 2.1(a) 9.1	Not Applicable.
	Licensed Software and Software Support Services	1.1 2.1(a) 9.3(a) Annexure A	Not Applicable.
<b>SUPPLY OF LICENSED SOFTWARE</b>			
116.	Dates for Delivery	2.1(b)	Not Applicable.
	Installation	2.1(c) 2.2	Not Applicable.
	Download of Licensed Software	2.1(d)	Not Applicable.
117.	Data backups by the Customer	2.3(a)	Not Applicable.
	Data backups by the Supplier	2.3(b)	Not Applicable.
118.	Licence Period	3.1 Annexure A	Not Applicable.
	Licensing model	3.2	Not Applicable.
	Permitted Users	3.2 Annexure A	Not Applicable.
	Permitted Purposes	3.3 Annexure A	Not Applicable.
	Scope of licence	3.3	Not Applicable.
119.	Updates and New Releases - General	4.1(a)	Not Applicable.
	Updates	4.2(a) 4.2(c)	Not Applicable.
	New Releases	4.2(a) 4.2(c)	Not Applicable.

No	Item	Mod ref	Description or selection
	Security Corrections	4.2(e)	Not Applicable.
	Period to maintain the Licensed Software after provision of Updates and New Releases	4.2(f)	Not Applicable.
120.	Transfer rights	5.1	Not Applicable.
121.	Restrictions	6.1(a)	Not Applicable.
122.	End of Licence Period	6.2(a)	Not Applicable.
123.	Third Party Components	7.1(b) Annexure A	Not Applicable.
	Third party warranties	7.2	Not Applicable.
124.	Record keeping	8.1	Not Applicable.
125.	Software Audits	8.2(b) 8.2(c)	Not Applicable.
	Results and consequences of Software Audit	8.3(b)	Not Applicable.
<b>SOFTWARE SUPPORT SERVICES</b>			
126.	Support Period	9.2	Not Applicable.
	Software Support Services	9.3(b)	Not Applicable.
127.	Help desk	10	Not Applicable.
<b>TRAINING</b>			
128.	Training Services	11.1	Not Applicable.
	Training Reports	11.2	Not Applicable.
<b>GENERAL</b>			
129.	Additional/ancillary Deliverables and Services	12	Not Applicable.
130.	Export Laws	13(a)(ii) Annexure A	Not Applicable.

No	Item	Mod ref	Description or selection
131.	Records	14	Not Applicable.
132.	Operating procedures	15(a)(iv)	Not Applicable.

**PART E: Hardware and Other ICT Deliverables Module – Not Applicable**

Clause references below are references to clauses in the Hardware and Other ICT Deliverables Module.

No	Item	Mod ref	Description or selection
<b>SCOPE</b>			
133.	Scope	1.1 7.1	Not Applicable.
	Hardware, Other ICT Deliverables and Support Services	1.1 2.3(a)(ii) 7.3 Annexure A	Not Applicable.
<b>SUPPLY OF HARDWARE AND OTHER ICT DELIVERABLES</b>			
134.	Status of Deliverables	2.1(a)	Not Applicable.
135.	Supply and delivery	2.3	Not Applicable.
136.	Availability Period	2.5 Annexure A	Not Applicable.
137.	Passing of title	3.1(a)	Not Applicable.
138.	Risk	3.2(b)	Not Applicable.
139.	Installation	4.1	Not Applicable.
140.	Data backups by the Customer	4.2(a)	Not Applicable.
	Data backups by the Supplier	4.2(b)	Not Applicable.
141.	Machine Code	5.1(b) Annexure A	Not Applicable.
142.	Licensed Software	5.2	Not Applicable.
<b>TRAINING</b>			
143.	Demonstration	6.1	Not Applicable.
	Training Services	6.2	Not Applicable.
	Training Reports	6.3	Not Applicable.
<b>SUPPORT SERVICES</b>			
144.	Support Period	7.2 Annexure A	Not Applicable.
145.	Preventative	7.4	Not Applicable.


No	Item	Mod ref	Description or selection
	Maintenance	Annexure A	
146.	Engineering changes	7.5	Not Applicable.
147.	Remedial Maintenance	7.6 Annexure A	Not Applicable.
148.	Help desk	8	Not Applicable.
<b>GENERAL</b>			
149.	Records	9	Not Applicable.
150.	Optional Features	11.1	Not Applicable.
151.	Additional/ancillary Deliverables and Services	11.3	Not Applicable.
152.	Site access	12	Not Applicable.
153.	Export Laws	13 Annexure A	Not Applicable.
154.	Compatibility	14.1	Not Applicable.
155.	Third party warranties	14.2	Not Applicable.
156.	Operating procedures	15(a)(v)	Not Applicable.
157.	Movement of Deliverables by Supplier	16(a)	Not Applicable.
	Movement of Deliverables by Customer	16(b)	Not Applicable.

Annexure A to Order Form – Supplier's Documents

The Supplier's Documents are:


Supplier's Documents	
No.	Title
1.	JusticeLink Support & Maintenance Aboriginal, SME and Local Participation Plan v.1
2.	JusticeLink FY25 Pricing Proposal 2025 V4.1

Annexure B to Order Form – Statement of Work



**Guidance note:** A template for the Statement of Work is included in Schedule 3. Parties may evolve it appropriately as required, or adopt their own form (subject to consistency with the other Agreement documents).

Statement of Work – Software Support Services and Other Professional Services



**Guidance note:** The Statement of Work forms part of the Order Form. Details in relation to the Supplier's Activities (including Services and Deliverables to be provided) should be inserted below. The Statement of Work should be consistent with any requirements in the other parts of the Order Form. Where necessary, relevant Items in the Order Form can refer to this Statement of Work.

This is a template only and not all parts below will be applicable for all procurements. Delete and amend as necessary.

1. Statement of Work Details

- (a)

Statement of Work Name: Software Support Services and Other Professional Services
- (b)

Statement of Work Number: S&M-SOW-001
- (c)

Purchase Order Number and Agreement reference (where available): Insert.

2. Revision History

Version	Status	Date	Prepared By	Comments
V.1	Draft	16/10/2024	Venkatesh Ramamurthi	

3. Introduction and overview of the Supplier's Activities

- The Supplier's Activities are:
- Level 2 Support and Level 3 Support
  - Project management and service delivery management
  - Platform support related to the Fujitsu managed infrastructure
  - Test support
  - Patches
  - Updates required to the test environment
  - 3rd party interfaces and integration
  - Ad-hoc support eg for extraordinary events such as major legislation change or business peak periods
  - Subject Matter Experts to attend meetings, comment on business requirements and generate change request documentation.

4. Software Support Services, Other Professional Services and Deliverables

**Applications covered:**

Software Support Services will be applicable to the JusticeLink Software as below.

- (i) JusticeLink Core Application
- (ii) JusticeLink Admin
- (iii) JusticeLink Scheduler
- (iv) JusticeLink Web Services
- (v) JusticeLink eServices and Legacy eServices

(the above applications include

- admin-webapp
- cicero-webapp
- cicero-ws
- eservices-webapp
- scheduler-webapp
- config-tools
- scheduler-tools)

- (vi) and, for the purposes of this Agreement, "JusticeLink Software" also includes the following applications ("Middleware"), which are the Intellectual Property of the Customer:

- JUJ Interface Outgoings
- JUJ Interface Scheduler
- JUJ Message Rejections or Interface Rejections System (IRS)
- JUJ eCAN or XMLCANS
- JUJ eCAN Support or Support Application

**Supported JusticeLink Hosting Environments**

(a) Supplier will support the development and testing infrastructure environments for the JusticeLink Software that it provides.

(b) The Supplier's development environment must be consistent with the Designated Operating Environment and include a Supplier operating system for support including peripherals (printers, scanners) that replicates that of the Customer.

(c) The Customer will continue to supply the two personal computers that it currently makes available to the Supplier at the Supplier's offices, plus existing VPN access and Defect ticketing software licences, to enable the Supplier to provide the Base Support Package.

**Management of Base Support Package**

(a) The Software Support Services for which the annual instalment of the Support Services Price for the Base Support Package is payable is the Base Support Package. The Customer may manage the allocation of its Base Support Package hours in any twelve-month period in accordance with this clause.

**(b) Unused Support Hours**

Unused Support Hours can be rolled over monthly for up to one year and be allocated at the Customer's discretion for Additional Activities. The Customer will decide its allocation of Unused Support Hours at the monthly meetings of the JusticeLink Support Governance Committee.

**(c) Support Hours more than Base Support Package**

(i) If additional Level 2 or 3 Support (within Business Hours) is required by the Customer in any one month of this Agreement beyond the Base Support Package hours allocation for that month then the Customer may elect to obtain this additional support by:

- (A) using any available Unused Support Hours;
- (B) deducting the additional hours from its Base Support Package allocation for the following month/s, for up to twelve months; or
- (C) purchasing the additional support as a Professional Service, charged at the blended rate on a Time and Materials Basis.



(ii) The Customer will notify the Supplier of any proposed deduction from a future Base Support Package monthly hours allocation and wherever possible will decide such deductions at the monthly meetings of the Justice link Support Governance Committee.

(d) Timesheets

The Supplier is to ensure personnel keep timesheets that fully document time spent on provision of services under this Agreement. The timesheets will detail the member of staff, time spent and tasks to which the time has been allocated (separately identifying Software Support Services and Additional Activities and Professional Services undertaken). The Supplier will supply these timesheets to the Customer monthly and otherwise at any time upon request. These timesheets will be deemed to be accepted by the Customer unless they are challenged by the Customer within five (5) business days of them being supplied to the Customer.

### Software Support Services

(a) The Software Support Services cover the JusticeLink Software and do not include the infrastructure, which is supported by the Customer. Support includes remediation of system performance issues relating to core application and reporting environments as implemented in the Actual Operating Environment if they have been registered as a Defect.

(b) Software Support Services to be provided by the Supplier under this Agreement only cover Level 2 Support and Level 3 Support.

(c) Level 1 Support will be the sole responsibility of the Customer and the Supplier will have no responsibility for Level 1 Support.

### Level 2 Support

(a) The Customer will be responsible for Level 2 Support for the JusticeLink Software. It may also request the Supplier to assist with Level 2 Support as part of the Base Support Package.

(b) The Supplier's obligation in relation to Level 2 Support is limited to providing suitably qualified resources to provide Level 2 Support if requested to by the Customer from time to time.

The Supplier will:

(i) ensure that, subject to normal business practices, until the particular issue is resolved the resources are available on a full-time basis during Business Hours (at the Supplier's premises, with the actual hours of attendance at the Customer's site to be negotiated between the Customer and the Supplier's Manager Technology Operations.

(ii) continue to be responsible for all wages, and employment benefits payable or due to the resources and will manage the employment of the resources which will include providing opportunities for learning and development and ensuring that their knowledge of the JusticeLink Software is current; and

(iii) for whatever reason, as the need arises, propose new resources for consideration by the Customer's representative to ensure that the required number of resources are always available to the Customer.

(c) The Supplier will ensure that

(i) resources provided for Level 2 Support are technically competent and have good knowledge of the JusticeLink Software. If the Customer is not satisfied with any of the resources provided the Customer will advise the Supplier in writing and the Supplier will replace the resources as soon as possible and within a thirty (30) day period; and

(ii) all time spent by its resources on Level 2 Support will be recorded in timesheets in an accurate and timely manner

(d) The Customer will:

(i) manage the day-to-day work and attendance of the provided resources when they are working at the Customer's site.

(ii) as possible, allow the resources suitable time to liaise with other qualified Supplier staff to ensure currency of skills and transfer of knowledge to and from other Supplier resources; and

(iii) ensure that Level 2 Support provided by the Supplier does not exceed the Base Support Package hours allocation for any twelve (12) month period.

### Level 3 Support

Level 3 Support will be provided by the Supplier during Business Hours and will generally be carried out on the Supplier's premises. If requested by the Customer, the Supplier will provide emergency Level 3 Support for the JusticeLink Software outside the Business Hours.

---

## 5. Specifications

The Specifications for software support and other professional services include:

### Updates, fixes, patches, modifications, and enhancements for the JusticeLink Software

(a) No additional Support Services Price beyond the price for the Base Services Support Package is payable by the Customer for any updates, fixes, patches, modifications, and enhancements developed as part of the Base Support Package (including as Additional Activities). Nor shall there be any charge to the Customer for the demonstration of the functionality and/or performance of any of these, whether developed as part of the Base Support Package or pursuant to a Customer request for Professional Services.

(b) The Parties will work together to determine the delivery dates and the design and nature of the features, functionalities and enhancements which should be incorporated in any updates, fixes, patches, modifications, and enhancements.

(c) Any updates, fixes, patches, modifications and enhancements will deliver software and documentation to facilitate installation by the Customer which will include source code as specified, release notes where applicable (including test cases) in format as mutually agreed and database scripts, if necessary, validated prior to deployment. The changes in each update, fix, patch, modification, and enhancement will be tested by the Supplier before being passed to the Customer. The release notes will include a list of the changes since the last relevant update, fix, patch, modification and enhancement and a description of how they were tested.

(d) To avoid doubt, the Supplier acknowledges that the Customer may edit and amend the software, including the source code, of any update, fix, patch, modification and enhancement if required to maintain, modify, correct or enhance the current production version of the JusticeLink Software.

(e) Unless otherwise required by the Customer, at least fifteen (15) days prior to the scheduled date for delivery of an update, fix, patch, modification or enhancement, the Supplier must advise the Customer of each Defect being resolved by the update, fix, patch, modification or enhancement, and any known limitation to the resolution of a defect.

(f) Unless otherwise agreed between the Customer and the Supplier:

(i) an update, fix, patch, modification or enhancement must not cause any loss of functionality or performance in the JusticeLink Software or in any customisation previously developed by the Supplier for the Customer; and

(ii) any changes made to the JusticeLink Software code by the Customer without involvement of the Supplier will operate as an automatic release for the Supplier from the requirement of Additional Condition (f)(i) until such time as the Customer replaces the modified code with the then current release of the Supplier provided code.

(g) As part of Software Support Services, the Supplier must supply the Customer at the time it delivers the relevant update, fix, patch, modification or enhancement to the Customer for Customer testing, with the following information concerning the relevant update, fix, patch, modification or enhancement:

- (i) certification that the software has been developed, tested and released to the Supplier's software quality standards.
- (ii) a statement of the functions and modules of the JusticeLink Software that are affected by the update, fix, patch, modification or enhancement and a description of the effects on these functions and modules.
- (iii) a statement describing any database structural changes caused by installation of the update, fix, patch, modification or enhancement.
- (iv) a statement of possible effects on the performance of the JusticeLink Software.
- (v) a statement of any possible increase or decrease to the computing and communications infrastructure resources required to operate the JusticeLink Software.
- (vi) documentation of, and executable instructions for, the rollback of the update, fix, patch, modification, or enhancement.

(h) To avoid doubt, unless otherwise agreed, the Supplier is not obliged to develop any updates and new releases for the JusticeLink Software apart from the obligations described within this Agreement with respect to updates, fixes, patches, modifications and enhancements as part of the Base Support Package.

### **Third party software**

(a) The Customer is responsible for procuring, including applicable licences, and maintaining any third party software required to support the operation of the JusticeLink Software but which is not delivered by the Supplier under Official Order No. 1 or this Agreement. A list of the third party software which is the responsibility of the Customer and the versions supported by the Supplier in operation of the JusticeLink Software are set out in Third party software. The third party software, and / or the versions of the software will be updated from time to time by the Customer, and the Supplier will support that new version in line with the product Roadmap developed by the Customer in consultation with the Supplier through the support governance process.

(b) The Supplier is responsible for any third party software, tools, object libraries and materials ("Software Materials") that are incorporated in the supplied version of the JusticeLink Software and are not licensed separately by the Customer and the Supplier must ensure that the JusticeLink Software is supported and maintained in line with the life cycle of these Software Materials.

### **Access to Source Code and Supporting Materials**

(a) The Supplier must, within 10 Business Days of the Commencement Date or such other date as may be agreed, provide the Customer with a copy of the Source Code and Supporting Material for the current production version of the JusticeLink Software.

(b) The Supplier will, at the time when it delivers any updates, fixes, patches, modifications and enhancements under this Official Order for Customer testing, also deliver to the Customer in a usable format as requested), all the Source Code and Supporting Materials required for the Customer to understand, operate, maintain, modify, correct and enhance the same (including, to avoid doubt, by reverse engineering the source code).

(c) Within 5 Business Days of termination or expiry of this Agreement, the Supplier must, to the extent that it has not already done so, deliver to the Customer a copy of the Source Code and Supporting Material for all New Material created under this Agreement.

### **Work Location, Network, Communications and Access Requirements**

(a) The Supplier's Software Support Services will be primarily provided from the Supplier's offices in Sydney, NSW and other remote Supplier approved 'working from home office' sites in NSW. No Services under this Agreement may be provided from Supplier's offices located outside NSW without the prior agreement of the Customer.

(b) The parties agree that, if the Customer requests it in writing, Supplier support personnel with appropriate skillsets may be co-located with the Customer at the Customer site within the Sydney metropolitan area as required by the Customer from time to time to address Level 2 Support and Level 3 Support issues that the Customer needs assistance with.

To avoid doubt, the Customer does not require:

- (i) any Supplier personnel to be permanently located at the Customer's offices to provide the Base Support Package (or any other Services unless otherwise agreed);
- or
- (ii) any fixed level of resources to provide the Base Support Package, provided the Customer is entitled to obtain Base Support Package, including the undertaking of Additional Activities using Unused Support Hours.

(c) Supplier support personnel will also be available to attend the PJP site or other Customer sites within the metropolitan area as required based on the required support tasks, to be agreed from time to time.

(d) The Supplier must establish and maintain such network facilities at its premises as are necessary to supply Level 3 Support and to connect to the Customer's network connection point (the "Customer's NCP"). The Supplier must also ensure that the network created for Level 3 Support is logically separated, in a manner approved by the Customer in writing, from any other network of the Supplier.

(e) In order to enable the Supplier to connect to the Customer's network for the purposes of providing Level 3 Support, the Customer will, at its cost, provide the Supplier with appropriate access to the Customer's NCP within the Sydney metropolitan area. If the Supplier requires connection to the Customer's NCP from outside the Sydney metropolitan area, the Customer will provide the same at the Supplier's cost.

(f) Without altering the Parties' other rights and obligations under this Agreement, the Customer will:

- (i) provide the Supplier's Level 3 Support personnel operating from the Supplier's premises with access to the Customer's Help Desk System. Subject to Additional Conditions (d) & (e) and (Help Desk System), such access shall be provided at no cost to the Supplier;
- (ii) allow the Supplier to use the Customer's JusticeLink Project development and test environments for the purpose of providing Level 3 Support, provided that the Supplier ensures that such use does not negatively impact work on the JusticeLink Project or other work of the Customer;
- (iii) at the Customer's discretion, for the purposes of investigating Problems, provide access to the Customer's production code and data: and (iv) provide timely advice to the Supplier's Level 3 Support personnel of any proposed outages or other disruptions to services and prompt advice of the availability of facilities following an outage.

### Document Maintenance

(a) As part of Software Support Services, the Supplier is responsible for updating and maintaining all Documentation provided by the Supplier to ensure that such Documentation accurately describes the operation of the JusticeLink Software following any changes to the JusticeLink Software, or to the way it operates, carried out by the Supplier.

(b) To the extent that the relevant Documentation has not already been supplied under Additional Condition (Access to Source Code and Supporting Materials), The Contractor will provide soft copies of the required documentation (Operation Guides, Upgrade Guides, Installation Checklists, and various other supporting documentation) with each release.

### Defect Support (including Support notice periods)

(a) Without prejudice to any other right or remedy of the Customer (whether arising by statute or otherwise), the Supplier as part of Software Support Services at no additional cost and expense to the Customer save the Support Service Price for the Base Support Package shall, during Business Hours, respond to and remedy a Defect in accordance with the Severity Classification of the Defect and the Defect Response Times and Defect Target Resolution Times. Any unreasonable delay in response by the Customer to a reasonable request by the Supplier will be considered when determining actual defect resolution Times.

(b) All Problems, faults and Defects reported by users to the Customer's Level 1 Support Help Desk will be assigned a Severity Classification. Severity Classifications are assigned by the Customer's Help Desk Representative after consultation with the users impacted. Defects shall be notified to the Supplier by assigning the Defect to the Supplier through the Customer's Help Desk System, provided however, Severity 1 and Severity 2 Defects shall also be notified to the Supplier by telephone.

(c) If the Help Desk system is unavailable Severity 1 and Severity 2 Defects reported via the telephone shall have the same effect as if allocated to the Supplier via the Help Desk System.

(d) The Supplier will maintain current a telephone service to be used by the Customer when reporting Severity 1 and Severity 2 incidents.

(e) If the initial Severity Classification is disputed, or the Defect cannot be re-created in the Supplier's environment (in circumstances where the Supplier has sought, and Customer endeavoured to provide the Supplier with, sufficient information to verify the Defect and both parties are reasonably satisfied that the Supplier's inability to reproduce the Defect is not due to differences in the Supplier's environment), the Supplier's representative and the Customer's representative will be called to review the Severity Classification for the Defect. Notwithstanding any dispute regarding the Severity Classification, the Supplier will respond to the Defect according to the Severity Classification assigned by the Help Desk Representative until such time as the Severity Classification is changed under this Additional Condition (Defect Support - including Support notice periods) or Additional Condition (Changes to Severity Classification).

(f) The time at which the Supplier is deemed to have received notice of a Defect shall be the time at which the Defect is assigned to the Supplier in the Customer's Help Desk System.

(g) If the Supplier determines that it is unable to provide a software repair or resolve the Defect within the Defect Target Resolution Time, the Supplier may provide the Customer with or recommend an Emergency Short Term Solution, having regard to the Severity Classification of the Defect in question. The Customer shall be the sole judge of whether the solution provided is a Viable Emergency Short Term Solution.

(h) Where the Supplier has provided or made a recommendation and the Customer has accepted that the solution is a Viable Emergency Short Term Solution, the Customer will reclassify the relevant Defect and assign a lower Severity Classification for the Defect. The Supplier shall respond in accordance with the new Severity Classification to fully resolve the Defect.

(i) The Supplier shall primarily liaise with the Customer's Information Technology Services Division regarding issues relating to the correction of Defects, JusticeLink Software usage and functionality.

(j) The Supplier must ensure that Problem fixes are of a high quality and that robust testing is undertaken prior to release to the Customer. The Supplier shall demonstrate to the Customer's reasonable satisfaction that the Defect has been successfully rectified.

(k) The Supplier shall not be liable under this Additional Condition (Defect Support) to the extent that a Defect is caused by the failure of the Customer or the Customer's employees or agents or any independent third parties (unconnected with Fujitsu) to maintain the Customer's system or operate the JusticeLink Software in accordance with the supplied Supplier specifications or Documentation. To the extent that there are no Unused Support Hours available to undertake the work, the Supplier will be permitted to charge the Customer for time it spends working on Defects caused by the circumstances referred to in this clause with this time being charged on a Time and Material Basis at the blended rate.

(l) The Supplier shall not be liable under this Additional Condition (Defect Support) for any Defect that is caused by changes that the Customer has made to the Configuration Files that are outside the scope of the Configuration Specifications. However, the Supplier is liable where any party, including the Customer, changes the Configuration Files within the scope of the Configuration Specifications and this causes a Defect in the JusticeLink Software to become apparent. To the extent that there are no Unused Support Hours available to undertake the work, the Supplier will be permitted to charge the Customer for time it spends working on Defects caused by changes that the Customer has made to the Configuration Files that are outside the scope of the Configuration Specifications, with this time being charged on a Time and Material Basis at the blended rate.

(m) The Supplier is responsible for addressing defects in the Configuration Files as follows:



- (i) All Defects associated with Configuration Files supplied by the Supplier under Official Order No. 1, if these Configuration Files are unchanged by the Customer;
  - (ii) Defects associated with Configuration Files scripted by the Supplier under this Customer Contract - for clarification this does not include Defects in Configuration Files scripted by the Customer after the implementation in production of Part Five of the JusticeLink Software.
- (n) Any Defect in the JusticeLink Software revealed by the use of Configuration Files scripted by either the Customer or the Supplier will be the responsibility of the Supplier.
- (o) Support notice periods
- (i) For Software Support Services (other than Additional Activities) under the Base Support Package, the Customer:
    - (A) is not required to give any notice (beyond notification through the Help Desk System or under cl.7.6(c)) of required support under the Base Support Package that is to be undertaken at:
      - ( 1) the Supplier's Sydney offices: or
      - (2) the Customer's offices if the required support is to fix Severity Level 1-3 Defects.
    - (B) will give 48 hours' notice of support required to be undertaken at the Customer's offices to fix Severity Level 4 Defects (however agreed service levels for these Defects will still apply from the time of notification of the Defect).
    - (C) will give two (2) weeks' notice of support required to be undertaken at the Customer's offices to fix Severity Level 5 Defects (however agreed service levels for these Defects will still apply from the time of notification of the Defect).
  - (ii) For Additional Activities the Customer:
    - (A) will give two (2) weeks' notice of required Additional Activities if it requires these to be carried out at the Customer's offices.
    - (B) will give one (1) week's notice of required Additional Activities if it requires theses to be carried out at the Supplier's offices.

## Help Desk System

- (a) The Customer will provide the Supplier with sufficient access to the Help Desk System to allow the Supplier to run up to two concurrent sessions of the computerised part of the Help Desk System.
- (b) The Customer's Help Desk Representatives and the Supplier's Level 3 Support personnel shall use the Help Desk System to manage the Defect resolution process. The Supplier must ensure that its Level 3 Support personnel promptly enter, update and/or provide such information as may be necessary to track and maintain the currency and accuracy of the Defect resolution status information in the Help Desk System.
- (c) If the computerised part of the Help Desk System is not available the Customer may report Problems via telephone, email or facsimile and such reported problems shall be treated as reported via the Help Desk System.
- (d) Problems reported and recorded outside of the computerised part of the Help Desk System will be recorded on the computerised system as soon as it is available.

## Data Correction

- (a) The correction of data corruption when caused by the Customer is not part of Software Support Services. When data corruption is caused by the Customer, the Supplier may, upon request from the Customer, assist the Customer in Data Correction. In these cases, to the extent that there are no Base Support Package hours, including Unused Support Hours, available to undertake the work, the Supplier will undertake the Data Correction as a Professional Service on request by the Customer, charged at the blended rate on a Time and Materials basis.
- (b) The correction of data corruption caused by the Supplier is part of Software Support Services. Where data corruption is caused by the Supplier, **no additional fees are** payable for the Data Correction and the

Supplier will (using the Supplier's methodology to correct the data, if required by the Supplier), at the Supplier's expense (calculated at rates equivalent to those that the Supplier would charge if the work was carried out by the Supplier's personnel), develop the procedures necessary to carry out the Data Correction unless otherwise agreed.

(c) The Customer may, at its discretion, either agree to the Supplier's Personnel (who have undergone a satisfactory police check and who have executed the required confidentiality deed) undertaking the execution of the procedures to complete the Data Correction in production at the Customer's offices and under the Customer's supervision or execute these procedures itself with assistance from the Supplier as requested.

## **Warranties**

(a) The Supplier warrants that all work performed under this Agreement will be performed to a high professional standard, undertaken by suitably trained staff and delivered in a timely manner.

(b) The Supplier warrants that no virus will be introduced into the Supported Software through the supply of products containing a virus as a result of any negligent, wilful or wrongful act or omission by the Supplier, its employees, sub-contractors and agents, in providing the Software Support Services.

(c) The Supplier hereby assigns to the Customer the benefit of all warranties which it receives or has received from the supplier or suppliers of the products and/or services forming part of the Software Support Services to be provided to the Customer under this Customer Contract, provided however, if the benefit of any such warranty is not assignable to the Customer, the Supplier will do all things necessary to ensure that the Customer otherwise receives the benefit of any such warranty. In addition, the Supplier shall provide to the Customer any reasonable assistance and co-ordination services it requires to receive the benefit of such warranties.

(d) Base Support Package Warranty items

(i) The Supplier will provide a 1 month (30 day) warranty commencing from release into the Customer's production environment in respect of each update, fix, patch, modification and enhancement supplied by the Supplier under this Agreement as part of the Base Support Package (in this Additional Condition 7 referred to as "Base Support Package Warranty").

(ii) Response and target resolution times for Base Support Package Warranty items will be the same as response and target resolution times for defects arising under this Agreement.

(iii) The Supplier must track Base Support Package Warranty items separately to support items for reporting purposes. Warranty repair work does not draw down hours paid for as Software Support Services under this Agreement.

(e) The parties will negotiate any warranty for deliverables requested under any purchase order for Professional Services as part of the agreed terms of any such order.

## **Performance Targets**

(a) The Supplier is responsible for ensuring that the JusticeLink Software will operate within the Performance Targets provided that:

(i) the Actual Operating Environment has the equivalent or greater capacity than the Designated Operating Environment; and

(ii) the actual workload is not greater than the Projected Total Workload.

(b) Any failure of the JusticeLink Software to operate within the Performance Targets will be treated as a Defect subject to Severity Classification and rectified as such under this Official Order.

## **Changes to Severity Classification**

(a) Appropriate Customer and Supplier personnel, as agreed, will, on a regular basis, review all Problems raised and, where appropriate, assess or re-assess the priorities of work to be undertaken as well as review and propose amending the classification of Severity 1 and Severity 2 calls logged if necessary.

- (b) The Supplier's representative may at any time approach the Customer's representative to seek a change to the Severity Classification assigned to a Defect.
- (c) If a Severity Classification remains in dispute following the application of Additional Conditions and/or the Severity Classification will be referred to the Customer CIO for final determination, provided however, where the Supplier reasonably considers that:
- (i) higher Severity Classifications than reasonably warranted were consistently being assigned to Defects;
  - (ii) a pattern of Severity Classifications disputes has arisen: or
  - (iii) the Customer had acted unreasonably in rejecting an Emergency Short Term Solution provided or recommended by the Supplier as a viable solution, the Supplier may refer the matter to the Management Committee for resolution.

**Third-party software required for the operation of the JusticeLink Software**

- I. Operating System: Windows Server 2012 R2
- II. Application Server: IBM WebSphere Application Server v8.5.5.9
- III. Database management System: Oracle 11g DBMS
- IV. Internet Browser: Chrome Version 124.0.6367.201, Edge Version 124.0.2478.97
- V. Microsoft 365
- VI. Identity Management: Oracle Access Manager 10 & 11/OKTA/Identity Hub/ LDAP Server.
- VII. Testing workstations: Windows 10

Future upgrades will be determined by the Customer in consultation with the Supplier through the support and governance forum and will be included in any product Roadmap, and agreed in a variation

---

**6. Customer Supplied Items (CSI)**

- (a) The Customer will provide the CSI as set out in the table below:

Item No.	CSI
1.	The Customer will continue to supply the two laptop computers that it currently makes available to the Supplier at the Supplier's offices, plus existing VPN access and Defect ticketing software licences, to enable the Supplier to provide the Base Support Package.
2.	The customer will continue to provide access to the contractor to a nominated customer office location and desks within the location.

---

**7. Timeframes and Dates for Delivery**

Not Applicable

---

**8. Key Milestones**

Not Applicable



---

**9. Transition-In Services**

Not Applicable

---

**10. Transition-Out Services**

See Annexure D Part B. Transition-Out Services is not funded under this Contract.

---

**11. Roles and responsibilities**

The Supplier's Project Director will submit a Monthly Status Report to the JSG Committee, with content that includes:

- (i) summary of Support issues during last period
- (ii) unused Support Hours and Additional Activities update
- (iii) approved/proposed continuous improvement tasks
- (iv) budget spent - fixed price, timesheets and issuing of monthly invoices
- (v) work planned for next period
- (vi) strategic product roadmap status.

The JSG Committee will meet monthly. Its terms of reference will include:

- (i) review Monthly Status report
- (ii) review issues arising
- (iii) workload
- (iv) performance against service levels and service level credits
- (v) effort used

---

**12. Business Contingency Plan**

A Business Contingency Plan is required and must be provided to the Customer for the Customer's approval by no later than thirty days after the Commencement Date.

For the purposes of clause 25.2 of the ICTA, the Business Contingency Plan must also:

- provide for the integration and co-ordination with the Supplier's business continuity arrangements with the Customer and relevant Other Suppliers.
- be consistent with Best Industry Practice with respect to business continuity; and
- address any other requirements specified in the Statement of Work or reasonably required by the Customer.

The Supplier must review and test the Business Contingency Plan at least annually and in any event upon the reasonable request of the Customer.

---

**13. Project Plan and management**

Not Applicable

---

**14. Stages and methodology**

*Not Applicable.*

---

## 15. Acceptance Testing

Acceptance Test Notification Period : 2 Business Days for Defect remediation acceptance

Acceptance Test Data: As agreed by the parties in each case

Acceptance Test Period: As agreed by the parties in each case (and not less than 15 Business Days unless otherwise agreed).

Acceptance: Deliverables to undergo Acceptance Testing are

- (a) updates, fixes, patches and modifications and minor enhancements
- (b) Documentation
- (c) any other New Contract Material as agreed.

### Conducting Acceptance Tests:

The Customer to determine the requirements to its UAT in each case.

To avoid doubt, Customer acceptance testing does not affect any Supplier obligations under this Agreement and under the general law with regard to delivery of Deliverables that are fit for purpose and, in the case of updates, fixes, patches, modifications and enhancements.

Prior to delivery of Deliverables requiring acceptance testing to the Customer, the Supplier will complete functionality, performance, system unit and other tests as may be necessary to verify that the Deliverables meet the functionality, compatibility, resilience, reliability and performance specified or agreed in or under the Contract.

The Supplier will carry out tests to ensure updates/fixes/patches will rectify the Defect they are intended to address without creating additional faults or Defects prior to delivery to the Customer and as agreed with the Customer.

The Customer shall conduct acceptance tests for Defects rectified.

The Supplier can make test cases and results available to the Customer and the Customer can provide regression test scripts to the Supplier where applicable.

The Customer will notify the Supplier that it has accepted or rejected Deliverables in accordance with the Contract's timeframes for notification of results of acceptance tests, and if the Customer fails to so notify within the timeframe then the Deliverable is deemed to have been Accepted by the Customer.

---

## 16. Governance arrangements

- (a) There shall be a JusticeLink Support Governance Committee ("JSG Committee")
- (b) Membership of the JSG Committee will be:

### Customer:

- (i) Director, Frontline Divisional Services (or nominee) as Chair
- (ii) Director, Portfolio Management and Planning (or nominee)
- (iii) Manager, Business Information Systems (or nominee)

- (iv) Manager, Digital Portfolio Systems and Delivery (or nominee)
- (v) Manager Technology Operations (or nominee)
- (vi) Application Support Lead (or nominee)

**Supplier:**

- (i) Project Director
- (ii) Manager/Lead Application Specialist (or nominee)
- (iii) Other nominees and/or guests

**The Supplier's Project Director will submit a Monthly Status Report to the JSG Committee, with content that includes:**

- (i) summary of Support issues during last period
  - (ii) unused Support Hours and Additional Activities update
  - (iii) approved/proposed continuous improvement tasks
  - (iv) budget spent - fixed price, timesheets and issuing of monthly invoices
  - (v) work planned for next period
  - (vi) strategic product roadmap status.
- (c) The JSG Committee will meet monthly. Its terms of reference will include:
- (i) review Monthly Status report
  - (ii) review issues arising
  - (iii) workload
  - (iv) performance against service levels and service level credits
  - (v) effort used

---

## 17. Assumptions and dependencies

- Access to Systems –Supplier's support staff will have the required access to DCJ's environments, tools, and necessary documentation to provide timely support.
- Defined Scope – Support is limited to agreed services (e.g., bug fixes and system maintenance) and excludes upgrades or new feature development unless otherwise agreed.
- Timely Response from DCJ – DCJ will provide timely responses to queries, approvals, and access requests needed to resolve support issues within SLA timeframes.
- User Responsibilities – DCJ users will follow agreed processes (e.g., logging issues through a designated service desk and providing necessary details for troubleshooting).
- Software Licenses – DCJ will provide the Supplier with the necessary software licenses to operate Justice Link in the Supplier's Test Environment.

[Exhaustively describe any assumptions or dependencies which apply to the provision of the Services or the supply of the Deliverables. All assumptions and dependencies are subject to the Customer's approval and must be clearly described.]

18. Service Level Agreement

<b>SERVICE PERFORMANCE</b>
<b>SEVERITY CLASSIFICATION OF PROBLEM TABLE</b>
<b>Severity 1 - Severe Impact Problem</b> <ul style="list-style-type: none"><li>• One or more critical application modules have a full or partial failure.</li><li>• The failure has a severe business impact.</li><li>• The failure must be addressed immediately.</li><li>• No Viable Emergency Short Term Solution is available.</li></ul> <p>Severity 1 will generally be used only when:</p> <ul style="list-style-type: none"><li>• applications are not available; or</li><li>• errors are so gross that the effect is the same as if the applications were not available;</li></ul> <p>and</p> <p>it is vital that all necessary resources of both Parties apply maximum effort to a resolution immediately.</p> <b>Severity 2- High Impact Problem</b> <ul style="list-style-type: none"><li>• One or more critical application modules have a full or partial failure.</li><li>• The failure has a major business impact.</li><li>• A Viable Emergency Short Term Solution is available.</li><li>• The resolution process should start as soon as possible as the business needs the failure repaired with 20 Business Hours.</li></ul>
<b>Severity 3 - Medium Impact Problem</b> <ul style="list-style-type: none"><li>• One or more application modules have a full or partial failure.</li><li>• The failure has a medium business impact.</li><li>• The business needs the failure repaired within 10 Normal Working Days.</li></ul> <p>Severity 3 should be used for failures that might be Severity 2, but the business is able to proceed with a Viable Emergency Short Term Solution for up to 10 Normal Working Days</p> <b>Severity 4- Low Impact Problem</b> <ul style="list-style-type: none"><li>• One or more facilities or application modules have a full or partial failure.</li><li>• The failure has a minor business impact.</li><li>• The business can live with the problem for up to 3 months.</li></ul> <b>Severity 5- Minor problem</b> <ul style="list-style-type: none"><li>• The business can live with the problem for up to 6 months or as otherwise agreed by the Customer.</li></ul>

DEFECT RESPONSE AND RESOLUTION COMMITMENT TABLE		
Classification Of Defect	Response Time	Target Resolution Time
Severity 1	30 minutes (Business Hours)	Four (4) hours (Business Hours)
Severity 2	4 hours (Business Hours)	Twenty (20) hours (Business Hours)
Severity 3	2 Working Days	Ten (10) Working Days
Severity 4	14 Days	Three (3) months
Severity 5	2 months	Six (6) months or as otherwise agreed by the Customer)

---

**19. Pricing**

Please refer to the Schedule 4 - Payment Schedule.

[REDACTED]

---

**20. Interpretation**

- (a) Terms in this Statement of Work which are not otherwise defined in this document have the meaning given to them in the ICTA.

Annexure C to Order Form – Supplementary Customer Requirements

1. General Security Conditions

1.1. Impacted Personnel

- 1.1.1 The Supplementary Customer Requirements contained in the sections of this Annexure C shall apply to the Supplier’s and its Subcontractors’ Personnel who have a need to access Customer Data for whatever reason (**Relevant Service Personnel**) and not to all of the Supplier’s or Subcontractor’s Personnel
- 1.1.2 References to **Authorised Relevant Service Personnel** in this Annexure C are to be interpreted as **Relevant Service Personnel** who have undergone and passed the background checks specified in this Annexure C.
- 1.1.3 Only **Authorised Relevant Service Personnel** are permitted to access Customer Data apart from the exceptional circumstance covered in section 1.1.4 below.
- 1.1.4 The only exception is if there is a need for urgent intervention to ensure the operational continuity or integrity of the Services. In such an event, **Relevant Service Personnel** may access Customer Data on a purely temporary basis following receipt of the Customer’s express approval in writing and will be considered to be **Authorised Relevant Service Personnel** on a temporary basis under the provisions of this Annexure C.

1.2. Compliance with Policies, Codes and Standards including SME and Aboriginal Procurement Policies (Item 17)

- 1.2.1. The Supplier must ensure its **Relevant Service Personnel** comply at all times with the following when
  - i) accessing the Customer’s facilities, computer systems, networks or information (including Customer Data) and
  - ii) providing ICT goods and services:

Customer’s Policies	
No.	Title
1	The Supplier Code of Conduct <a href="https://buy.nsw.gov.au/policy-library/policies/supplier-code-of-conduct;">https://buy.nsw.gov.au/policy-library/policies/supplier-code-of-conduct;</a>
2.	The Worst Forms of Child Labour Convention,1999 (ILO Convention 182) <a href="https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182">https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182</a>

1.3. Compliance with security obligations, standards and Information Security Requirements (Item 40, Box 1)

- 1.3.1. The Supplier must ensure its **Relevant Service Personnel** comply at all times with the legislation and policies in the following table (as applicable) when accessing the Customer’s facilities, computer systems, networks or information (including Customer Data):

NSW Privacy Legislation		
No.	Title	
1	Privacy Act 1988 (Cth) <a href="https://www.legislation.gov.au/C2004A03712/latest/text">https://www.legislation.gov.au/C2004A03712/latest/text</a>	
2	Privacy and Personal Information Protection Act 1988 (including applicable Regulations and Codes or Public Interest Directions) <a href="https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133">https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133</a>	
3	Health Record and Information Privacy Act 2002 (including applicable Regulations and Code or Public Interest Directions) <a href="https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071">https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071</a>	
NSW ICT Security Policies		
No.	Title	
1	the NSW Government Cyber Security Policy published at <a href="https://www.digital.nsw.gov.au/policy/cyber-security-policy">https://www.digital.nsw.gov.au/policy/cyber-security-policy</a> in so far as it relates to the Supplier's Activities and the Supplier is directed by the Customer to assist the Customer's compliance with that policy;	
2.	the NSW Government Internet of Things (IoT) Policy published at <a href="https://www.digital.nsw.gov.au/policy/internet-things-iot">https://www.digital.nsw.gov.au/policy/internet-things-iot</a> in so far as it relates to the Supplier's Activities	
Customer's ICT Security and other Policies		
No.	Title	Date
1	Access Control Policy Related Documents: <ul style="list-style-type: none"><li>Access Control Standards</li></ul>	28/09/2023 28/09/2023
2	Cloud Security Policy	28/09/2023
3	Data Protection and Privacy Policy Related Documents: <ul style="list-style-type: none"><li>Data Privacy and Protection Standards</li></ul>	28/09/2023 28/09/2023
4	IT Acceptable Use Policy	28/09/2023
5	IT Security Policy Related Documents: <ul style="list-style-type: none"><li>IT Security Standards</li><li>Cryptographic Controls Standards</li><li>Data Backup and Retention Standards</li></ul>	28/09/2023 28/09/2023 28/09/2023
6	Information Security Policy	28/09/2023
7	Patch Management Policy	29/03/2021
8	Privacy Policy	December 2017
9	Records and Management Policy	14/6/2023
10	Secure Software Development Standard	28/09/2023

11	Statement of Business Ethics	1/01/2021
----	------------------------------	-----------

- such other Customer policies and legislative obligations advised to the Supplier from time to time;
- all other reasonable requirements and directions of the Customer in regard to conduct, behaviour, protection of privacy, use of systems, safety and security (including submitting to security checks as required and complying with any obligation imposed on any person by law) as notified to the Supplier by the Customer from time to time.

1.3.2. Without limiting any obligation of the Supplier under this Agreement, if any of the **Authorised Relevant Service Personnel** breach the conditions under this Agreement, including but not limited to any of the above policies, the Customer may, for good cause, at any time and for any period, revoke that **Authorised Relevant Service Personnel's** access to (and require the Supplier to ensure that the **Authorised Relevant Service Personnel** does not access) the Customer's facilities, computer systems, networks and information (including the Customer Data).

1.3.3. Where it is practicable to do so following such a breach, the Customer will give the Supplier prior written notice of the withdrawal of **Authorised Relevant Service Personnel** access to the Customer's facilities, computer systems, networks and information.

1.3.4. Where such a breach occurs when the **Authorised Relevant Service Personnel** is on the Customer's facilities, the Customer reserves the right to immediately require the person that has performed the breach to leave the facilities.

1.3.5. Without limiting any obligation of the Supplier under this Agreement, the Supplier must replace any of the **Authorised Relevant Service Personnel** whose access has been withdrawn due to such a breach without interruption, inconvenience or cost to the Customer.

1.3.6. For all Suppliers and Subcontractors, who have a need to access Customer Data or the Customer's network, the Supplier must ensure they first complete a risk assessment provided by the Customer's Cyber Security team and then obtain the Customer's approval for such access.

#### 1.4. Requirements for attendance at the Site (Item 16, Box 4)

1.4.1. The Supplier and its Personnel are permitted to attend the Site only at the times nominated by the Customer from time to time, and subject to such conditions as may be nominated by the Customer from time to time. Without limitation, the Supplier must comply (and must ensure that its Personnel comply) with the requirements set out in Items 17, 22 and 40 of this Order Form.

#### 1.5. Security certifications (Item 40, Box 2)

1.5.1. In terms of clause 21.2(e) of the ICTA Terms and Conditions, the Supplier must, within 10 Business Days of the Commencement Date, provide a copy of its ISO/IEC 27001:2022 certification to the Customer and maintain controls aligned with the scope of the ISO/IEC27001:2022 controls that are relevant to the Services for the Term of the ICTA. .

#### 1.6. Security audits and compliance (Item 40, Box 3)

1.6.1. In addition to the requirements in clause 21.3, the Supplier must provide to the Customer all information reasonably requested by the Customer related to the Supplier's security audits and compliances, including any request for the completion of the Customer's Third Party Cyber Risk Assessment (TPCRA) document.

#### 1.7. Reporting of Security Incidents (Item 42)

1.7.1. Clause 22.2 of the ICTA Terms and Conditions shall apply. Both parties agree that the timeframe for



actions to be undertaken under clause 22.2(b)(i) of the ICTA Terms and Conditions shall be within 48 hours after the Supplier's initial awareness or notification of the Security Incident (clause 22.1(a)).

## 2. Background Checks

### 2.1 Conduct of background checks on Relevant Service Personnel (Item 22)

2.1.1 For the **Relevant Service Personnel** normally domiciled within Australia, the Supplier must:

- procure a Nationally Coordinated Criminal History Check (NCCHC) for those personnel from an Australian Criminal Intelligence Commission (ACIC) Accredited Body (or such other branch or office of the Australian Federal Police or law enforcement agency performing the functions of the ACIC from time to time); and
- ensure that any persons whose Result shown in the NCCHC Check Results Report is other than 'no Disclosable Court Outcomes' (DCOs) will never have access to any Customer Data.

2.1.2 For the **Relevant Service Personnel** normally domiciled outside Australia; the Supplier must:

- use reasonable endeavours to perform or procure a criminal record search of that person from the relevant police force of the jurisdiction where the Supplier Personnel resides; and
- must confirm the outcome of the check and the date the check was completed, but must not provide the results of the check to the Customer.

2.1.3 For any **Relevant Service Personnel** wherever normally domiciled who have a need to access the Customer Data containing Personal Information, the Supplier must:

- provide sufficient personal details of those **Relevant Service Personnel** to the Customer to allow it to conduct a security check against the Customer's vulnerable persons' register.

2.1.4 For any **Relevant Service Personnel** who fail the clearance against the Customer's vulnerable persons register, the Supplier will ensure they never have access to any Customer Data.

2.1.5 For any **Relevant Service Personnel** who refuse to give their consent to enable any of the above background checks to be conducted, the Supplier will ensure they never have access to any Customer Data.

2.1.6 For any **Relevant Service Personnel** whose results from any of the above background checks prove to be in any way negative, the Supplier will ensure they never have access to any Customer Data.

2.1.7 For any **Relevant Service Personnel** whose results from any of the above checks have proved to be clear but the Supplier later becomes aware of information to the contrary, the Supplier will ensure their access to Customer Data (if any) is immediately removed and also that they never subsequently have access to Customer Data.

2.1.8 Any Relevant Service Personnel who have passed the specified background checks in the sections above will be classified as **Authorised Relevant Service Personnel** above.

2.1.9 The Customer may reasonably request the Supplier to provide details of **Authorised Relevant Service Personnel** to the extent permissible by law in the country of their normal domicile. The Supplier must then provide the Customer with a list identifying each of the **Authorised Relevant Service Personnel** by name; their qualifications; and, their actual or proposed access to any of the Customer's facilities, computer systems, networks or information (including Customer Data).

2.1.10 If the Customer is of the reasonable opinion that any of the **Authorised Relevant Service Personnel** are unsuitable to undertake work in respect of this Agreement, then the Customer may request the Supplier to remove that person from the performance of the ICTA Terms and Conditions by providing written reasons for the person's removal and give the Supplier the ability to address the issues raised

by the Customer. If the Customer makes such a request, then, without limiting any obligation of the Supplier under this Agreement, the Supplier must provide a replacement reasonably acceptable to the Customer within 20 Business Days of the Customer's request and without inconvenience or cost to the Customer. The Customer undertakes not to rely on this clause more than 4 times in any Calendar year.

- 2.1.11 For any **Relevant Service Personnel** normally domiciled within Australia requiring access to Customer Data classified as Protected or higher, as specified in the Australian Government's Protective Security Policy Framework at the following link:

<https://www.protectivesecurity.gov.au/>

the Supplier must additionally:

- comply with all of the provisions contained therein as they pertain to Customer Data classified as Protected or higher;
- procure the correct level of security clearance associated with the applicable level of data classification; and,
- provide the Customer with evidence of appropriately cleared Supplier Personnel in order they can be tracked by the Customer's and/or the Australian Government's security Personnel.

### 3. Data Protection Provisions

#### 3.1 Location of personal information (Item 39, Box 1)

- 3.1.1 Clause 20.1(a)(iv) of the ICTA Terms and Conditions shall apply but is amended to allow **Authorised Relevant Service Personnel** who are normally domiciled within the whole of Australia to access the Customer Data Personal Information with the written consent of the Customer, instead of just those located within the State of New South Wales.

#### 3.2 Data Location Conditions (Item 39, Box 2)

- 3.2.1 Unless otherwise agreed in writing in advance by the Customer, the Supplier must ensure that none of its **Authorised Relevant Service Personnel** transfer Customer Data to, or access Customer Data from, outside Australia or allow Customer Data to be transferred to or accessed from outside of Australia.
- 3.2.2 If the Supplier has a need to access Customer Data from, or transfer Customer Data to, outside of Australia in order to meet its obligations under this Agreement, it must submit a request to the Customer citing the specific reasons and any such request **must** undergo a risk assessment by the Customer to determine the suitability for this to occur.
- 3.2.3 The Customer may refuse the above request at its sole discretion or may agree to the request subject to the Supplier complying with the Customer's conditions.

#### 3.3 Backup of Customer Data (Item 41, Box 1)

Where Item 13 of an Order identifies that the Supplier is providing services under the Cloud Module of this Agreement:

- 3.3.1 The Supplier will complete regular backups of Customer Data in accordance with clause 19.4 of the ICTA Terms and Conditions. The frequency of such backups will be daily, unless otherwise notified by the Customer to the Supplier. All backups must be stored in a secure, fireproof location that is separated from the primary data centre in Australia.

### 3.4 Retention of Customer Data (Item 41, Box 2)

Where Item 13 of an Order identifies that the Supplier is providing services under the Cloud Module of this Agreement:

- 3.4.1 The Supplier is required to establish, keep and maintain complete, accurate and up-to- date copies of Customer Data in accordance with clause 19.7 and provide them to the Customer on request.
- 3.4.2 In respect of the destruction of any records and backups of the Customer Data the Supplier must ensure that prior to final disposal, any storage media used to store Customer Data will be securely degaussed, erased, purged, physically destroyed, or otherwise sanitised in accordance with the requirements of the Australian Government Information Security Manual and the Customer's Policies, Codes and Standards.
- 3.4.3 Clause 19.7(b)(ii)B is amended as follows: *"securely return all records of Customer Data to the Customer in accordance with the timeframes under the Agreement and in a format notified by the Customer."*

### 3.5 Data Backups by the Supplier (Item 64, Box 2)

Where Item 13 of an Order identifies that the Supplier is providing services under the Cloud Module of this Agreement:

- 3.5.1 Section 3.3 of this Annexure C shall apply.

### 3.6 Media Decommissioning (Item 72)

- 3.6.1 The Supplier must ensure all Deliverables under the ICTA that include or comprise any electronic storage media have the capability for all Customer Data to be erased upon termination of the ICTA or upon written request of the Customer.
- 3.6.2 For Supplier-owned storage devices used to deliver the Services under this Agreement that are located on the Customer's premises, the Supplier must erase all Customer Data within 10 Business Days of either of the two instances referred to in section 3.6.1 above using up-to-date software (that has a 3 pass erasure process which is fully compliant to the DOD 5220.22-M standard) and provide a completion report detailing the certificate reference and storage device serial number for each unit wiped within a further 5 Business Days. The Supplier must then remove those storage devices from the Customer's premises at no charge to the Customer within 5 Business Days from the Supplier's receipt of that certificate. Should any storage devices fail the erasure process, the Supplier must notify the Customer immediately for the Customer to notify the Supplier of an alternative approach.
- 3.6.3 For all storage devices used to deliver the Services under this Agreement that are not located on the Customer's premises, the Supplier must erase all Customer Data within 10 Business Days of either of the two instances referred to in section 3.6.1 above using up-to-date software (that has a 3 pass erasure process which is fully compliant to the DOD 5220.22-M standard) and provide a completion report detailing the certificate reference and storage device serial number for each unit wiped within a further 5 Business Days. Should any storage devices fail the erasure process, the Supplier must notify the Customer immediately for the Customer to notify the Supplier of an alternative approach.

### 3.7 Primary and Secondary Data Centre (Item 68)

Where Item 13 of an Order identifies that the Supplier is providing services under the Cloud Module of this Agreement:

3.7.1 With reference to clause 4.3(a) of the Cloud Module, the Supplier's primary data centre must be located in New South Wales and the Supplier's secondary data centre must be located within Australia and at least 20 kilometres from the primary data centre.

### **3.8 Remote Access to Customer Data (Item 69)**

Where Item 13 of an Order identifies that the Supplier is providing services under the Cloud Module of this Agreement:

3.8.1 With reference to clause 4.3(b) of the Cloud Module, the Supplier is not permitted to remotely access Customer Data from outside Australia unless agreed in writing by the Customer and only following an approved risk assessment conducted by the Customer.

### **3.9 Excluded locations (Item 71)**

3.9.1 By exception but only where this Agreement is for Services involving less sensitive Customer Data, the Customer may at its sole discretion provide its consent to a Supplier's proposal to use a data centre located outside Australia. Following receipt of such a proposal, the Customer will determine its risk profile and will have the sole discretion whether to accept the proposal or not. The Supplier must obtain the Customer's prior written consent before proceeding with any such proposal and all costs of such a change will be borne solely by the Supplier.

3.9.2 The Customer may accept a change of data centres between locations within Australia subject to prior written notification by the Supplier and approval in writing by the Customer and all costs of such a change will be borne solely by the Supplier.

### **3.10 Cloud Services**

Where Item 13 of an Order identifies that the Supplier is providing services under the Cloud Module of this Agreement:

3.10.1 With respect to clause 19.1(d)(v) of the ICTA Terms and Conditions, all Customer Data must be encrypted in transit and at rest.

### **3.11 Protection and use of Personal Information**

3.11.1 Without limiting clause 20.1(a)(v) of the Agreement, the Supplier must:

- run initial and annual mandatory privacy training for all of the Supplier's Personnel involved in carrying out the Supplier's Activities under this Agreement and ensure that those Personnel have completed the initial training prior to carrying out the Supplier's Activities;
- audit annually (random sample audit) Supplier's Personnel access, use, disclosure of Customer's Data to ensure compliance with privacy laws;
- report annually on privacy complaints received and actioned and data breaches (suspected, alleged or actual) involving Customer Data Personal Information:
  - which must contain (at a minimum) full and complete details of the complaint / incident
  - steps taken to remediate and prevent reoccurrence.

3.11.2 Without limiting clause 20.1(a)(vi) of the Agreement, the Supplier must:

*ICTA | Department of Customer Service*

- If requested by the Customer, provide to the Customer within a reasonable timeframe the Customer's Data impacted by the incident;
- If requested by the Customer assist with the investigation and remediation activities arising from the incident.

Annexure D to Order Form – Additional Conditions

Part A – Amendments to the Agreement

1. No deemed Acceptance

- 1.1 Clause 8.1(e) of the Core Terms is amended by deleting the words ‘, except where clause 8.2(f) applies’.
- 1.2 Clause 8.2(f) of the Core Terms is amended by deleting the sentence ‘If the Customer does not approve or reject the relevant Document Deliverable or otherwise communicate with the Supplier in relation to that reminder notice within 10 Business Days of its receipt, then the relevant Document Deliverable will be deemed to have been approved by the Customer.’ and replacing it with the sentence ‘Under no circumstances will a Document Deliverable be deemed to have been Accepted by the Customer.’
- 1.3 Clause 14.3(f) of the Core Terms is amended by deleting the sentence ‘If the Customer does not take one of the actions referred to in clause 14.3(c) or otherwise communicate with the Supplier in relation to that reminder notice within 15 Business Days of its receipt, then the relevant Deliverable will be deemed to have been Accepted by the Customer.’ and replacing it with the sentence ‘Under no circumstances will a Deliverable be deemed to have been Accepted by the Customer.’

2. Policies, Codes and Standards

- 2.1 Clause 12.2(a) of the Core Terms is amended by inserting the following words at the end of the clause ‘(to the same extent as if those Policies, Codes and Standards applied to the Supplier and as if references to the Customer (or similar) were references to the Supplier), and must do all things necessary in the performance of the Supplier’s Activities to ensure that the Customer complies with all Policies, Codes and Standards’.

3. Intellectual Property Rights

- 3.1 A new clause 17.14 of the Core Terms is inserted as follows:

17.14 Scope of licence rights

The Supplier represents, warrants and undertakes that the Customer’s use of the Services and Deliverables will not under any circumstance, or at any time, be subject to any terms and conditions other than those terms and conditions expressly set out in this Agreement, with the exception of third party owned Intellectual Property Rights acquired by the Customer related to the Services and/or Deliverables (as applicable) disclosed in the Statement of Work.

4. Liability - the Professional Standards Legislation

Part B – Additional Terms and Conditions

5. Transition Out

- 5.1 The parties acknowledge and agree that:
  - (a) this Additional Condition 5 supplements and applies in addition to the requirements of this Agreement (including clause 31 of the Core Terms);

- (b) the main objectives of the Transition-Out Services are to ensure the smooth and orderly transition of the Supplier's Activities from the Supplier to the Customer or its nominee/s;
- (c) the successful performance of the Transition-Out Services by the Supplier is critically important to the Customer, including to minimise the risk and impact on the Customer and the Customer's operations, Personnel, end users and/or other stakeholders; and
- (d) the Customer may require the Supplier to perform Transition-Out Services in relation to all or part of the Supplier's Activities.

5.2 The Supplier must:

- (a) except to the extent otherwise requested by the Customer in writing, continue to provide the Supplier's Activities (including any associated reporting and other related services required under this Agreement) during the Transition-Out Period in accordance with the terms of this Agreement (for clarity, to the extent that the Customer requires the Supplier to continue to provide the Supplier's Activities, the Customer must continue to pay for such Supplier's Activities, in accordance with, and to the extent set out in, the Payment Particulars);
- (b) ensure that there is no disruption to, or degradation in the quality of such Supplier's Activities during the Transition-Out Period;
- (c) perform the Services (including the Transition-Out Services), deliver the Deliverables, and meet the requirements specified in this Additional Condition 5 and do everything else required of it under the Transition-Out Plan; and
- (d) where required by the Customer, provide for the orderly hand over of such Supplier's Activities to the Customer or the relevant Other Supplier/s nominated by Customer.

5.3 The Transition-Out Services that the Customer may require the Supplier to perform include:

- (a) assisting the Customer in discussions with any Other Suppliers;
- (b) providing such information on hardware, software, processes and procedures as reasonably required by the Customer to enable discussions with any Other Supplier to take place;
- (c) providing such cooperation as is reasonably necessary to enable any Other Supplier to perform a technical joint verification or due diligence exercise in relation to the Supplier's Activities;
- (d) without limiting the Supplier's obligations under this Agreement, converting any data into a common and generally accepted non-proprietary format (as nominated by the Customer);
- (e) undertaking or assisting with the un-encryption of any encrypted data to allow data migration or translation to other system;
- (f) providing all relevant encryption 'keys' and tools sufficient to allow the Other Supplier to access any encrypted data;
- (g) providing any Other Supplier with all necessary documentation, configuration details, specifications and assistance to ascertain the status of any outstanding Supplier's and the input required to provide and complete the Services and to operate, support and maintain the Deliverables;

- (h) ensuring the attendance of relevant Personnel at such meetings as may reasonably be required by the Customer;
  - (i) doing all things necessary to ensure the smooth and orderly transition to the Other Supplier/s;
  - (j) transferring and/or returning all records, data, information, equipment and/or assets of the Customer to the Customer or the Other Supplier/s; and
  - (k) continuing to provide relevant Supplier's Activities to the Customer.
- 5.4 The fees for the Transition-Out Services must not exceed the rates specified in this Agreement, or if no such rates are specified, will be chargeable in accordance with commercially competitive rates, and in any event will be agreed between the parties in writing and in advance of the Transition-Out Period.
- 5.5 The Parties acknowledges and agree that:
  - (a) fees for Transition Out Services are only payable for any resources (based on total full-time-equivalent count) required in addition to the resources used to deliver the Supplier's Activities prior to commencement of the Transition-Out Period;
  - (b) no fees are payable if additional resources are not utilised; and
  - (c) the Supplier must use reasonable endeavours to use existing resources where possible and without risking a degradation to the provision of Supplier's Activities to the Customer.
- 5.6 At the end of the Transition-Out Period (and earlier, if determined necessary by the Customer in its sole direction):
  - (a) the Supplier must and must ensure that its Personnel:
    - (i) cease access the Customer's premises, facilities, data, information, systems or other materials; and
    - (ii) return all data, information, equipment and other materials of the Customer to the Customer; and
  - (b) the Supplier's security and access rights to Customer's premises, facilities, data, information, systems and other materials will be terminated.
- 5.7 Upon request of the Customer, the Supplier must provide a statutory declaration to the Customer confirming that the Supplier has complied with its obligations under Additional Condition 5.6.
- 5.8 All Transition-Out Services must be provided by the Supplier in accordance with the terms and conditions of this Agreement. The Supplier must perform the Transition-Out Services with at least the same degree of accuracy, quality, completeness, timeliness, responsiveness and resource efficiency as it provided and was required to provide the same or similar services prior to the start of the Transition-Out Period.
- 5.9 The Customer may terminate the Transition-Out Services (or reduce their scope), in whole or in part, at any time by giving the Supplier five (5) Business Days written notice of such termination, in which case the Supplier must promptly provide a refund to the Customer of any fees, charges or other similar amounts that have been paid by the Customer in advance in respect of the period following termination of the Transition-Out Services, or for Services and Deliverables that have not been provided by the Supplier.



- 5.10 The Supplier must act reasonably and in good faith in the performance of the Transition-Out Services and must provide all information and materials to the Customer as reasonably requested by the Customer.
- 5.11 The Supplier must provide Transition-Out Services to the Customer regardless of the reason for the expiration or termination of this Agreement.

## 6. Tender Response

- 6.1 If directed by the Customer, the Supplier must comply with the Tender Response to the extent that any matter or thing addressed in the Tender Response is not provided for in this Agreement.
- 6.2 Where the Tender or the Tender Response is capable of assisting in ascertaining the meaning of a particular provision of this Agreement, the Customer may rely on the Tender and/or the Tender Response to:
  - (a) confirm that the meaning of the provision is the ordinary meaning conveyed by the text of the provision taking into account its context in this Agreement and the purpose or object underlying this Agreement; or
  - (b) determine the meaning of a provision of this Agreement when the provision is ambiguous or obscure.
- 6.3 To the extent that there is any conflict between this Agreement and the Tender or the Tender Response, the conflict will be resolved by giving priority to this Agreement.
- 6.4 To the extent that there is any conflict between the Tender and Tender Response, the conflict will be resolved by giving priority to the Tender, except to the extent that the Tender Response expressly provides otherwise in relation to particular section of the Tender (for clarity, any wording in the Tender Response which provides that the entire Tender Response or a substantial part of the Tender Response prevails over the Tender will not apply to this Agreement).
- 6.5 For the purposes of Additional Conditions 6.1 to 6.4:
  - (a) **Tender** means the 'Rfx\_1190 JusticeLink Support and Maintenance Agreement and Professional Services' released by DCJ issued by the Customer on or about 03/03/2025 including any all conditions, annexures, schedules, attachments, addenda, clarifications and other similar things; and
  - (b) **Tender Response** means:
    - (i) the Supplier's response to the Tender dated 07/03/2025;
    - (ii) any written response by or on behalf of the Supplier to a request from the Customer for clarification or further information given before the Commencement Date; and
    - (iii) any written statement made by or on behalf of the Supplier to the Customer before the Commencement Date in relation to its proposed provision of the Supplier's Activities.

**Annexure E to Order Form - Customer Policies**

**Guide Note: To keep only the relevant DCJ Specific Policies in the ICTA**

No.	Title	Date
	<b>Department of Communities and Justice (DCJ) Specific Policies</b>	
	<u>DCJ Policy Suite</u>	
1	Access Control Policy Related Documents: • Access Control Standards	28/09/2023 28/09/2023
2	Cloud Security Policy	28/09/2023
3	Data Privacy and Protection Policy Related Documents: • Data Privacy and Protection Standards	28/09/2023 28/09/2023
4	IT Acceptable Use Policy	28/09/2023
5	IT Security Policy Related Documents: • IT Security Standards • Cryptographic Controls Standards • Data Backup and Retention Standards	28/09/2023 28/09/2023 28/09/2023
6	Information Security Policy	28/09/2023
7	Patch Management Policy	29/03/2021
8	Privacy Policy	December 2017
9	Records Management Policy	14/06/2023
10	Secure Software Development Standards	28/09/2023
11	Statement of Business Ethics	1/01/2021
	<b>Other Policies</b>	
12	Supplier Code of Conduct <a href="https://buy.nsw.gov.au/policy-library/policies/supplier-code-of-conduct">https://buy.nsw.gov.au/policy-library/policies/supplier-code-of-conduct</a>	11/2019
13	The Worst Forms of Child Labour Convention, 1999 (ILO Convention 182) <a href="https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182">https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182</a>	19/11/2000
	<b>NSW Whole of Government ICT Security Policies</b>	
14	NSW Government Cyber Security Policy <a href="https://www.digital.nsw.gov.au/policy/cyber-security-policy">https://www.digital.nsw.gov.au/policy/cyber-security-policy</a> (in so far as it relates to the Supplier's Activities and the Supplier is directed by the Customer to assist the Customer's compliance with that policy.	01/2022
15	the NSW Government Internet of Things (IoT) Policy <a href="https://www.digital.nsw.gov.au/policy/internet-things-iot">https://www.digital.nsw.gov.au/policy/internet-things-iot</a> (in so far as it relates to the Supplier's Activities)	10/2019



\_\_\_\_\_

[REDACTED]

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**Schedule 5 - Change Request Form**

<b>Change Request number</b>	<i>[Number the Change Request to assist with tracking Change Requests and administrating the Agreement.]</i>
<b>Purchase Order Number and Agreement reference</b>	<i>[Where available, insert a reference to the applicable Purchase Order number and the Agreement reference number to which the Change Request relates.]</i>
<b>Effective date for Change Request</b>	<i>[Insert the date on which the parties agree the Change Request will become effective.]</i>
<b>Details of Change Request</b>	<i>[Insert a sufficiently detailed description of the Change Request, including which sections of the Statement of Work will be changed by the Change Request. Please attach a more detailed scope document to this Change Request, if required.]</i>
<b>Specifications</b>	<i>[Insert any changes to the Specifications, including any additional Specifications.]</i>
<b>Plans</b>	<i>[If applicable, outline the effect the Change Request will have on any Plans, such as the Project Plan. To the extent that it is appropriate to replace any Plans with new Plans, please attach those to this Change Request.]</i>
<b>Date for Delivery and Key Milestones</b>	<i>[List any new or amended Dates for Delivery and identify whether any of these dates constitute Key Milestones.]</i>
<b>Effect on Price</b>	<i>[If applicable, specify how the Change Request will affect the Price.]</i>
<b>Nominated Personnel</b>	<i>[Specify any changes to the Nominated Personnel.]</i>
<b>Implementation</b>	<i>[Outline in sufficient detail how the Change Request will be implemented.]</i>
<b>Effect on Customer Users</b>	<i>[Outline the effect, if any, of the change to the Customer Users.]</i>
<b>Other matters</b>	<i>[List any other matters that are relevant to the Change Request or that the Customer has requested are covered by this Change Request.]</i>
<b>List documents that form part of this Change Request</b>	<i>[Insert list.]</i>

<b>Customer</b>  Name (Print):  Signature:  Date:	<b>Supplier</b>  Name (Print):  Signature:  Date:
---	---



**Guidance note:** Only persons with the necessary authorisation or delegation may execute Change Request Forms.

Schedule 6 - Deed of Confidentiality and Privacy

Given by: [Insert full name of Recipient (insert ABN, if applicable)] of [Insert address of Recipient] (Recipient)

In favour of: [Insert full name of Customer (insert ABN)] (Customer)

Made: on the date the Recipient executes this Deed (Date of this Deed).

Background

- A The [Insert name of the Supplier] and the Customer have entered into an ICT Agreement dated on or about the date of this Deed (Agreement) pursuant to which the Supplier must carry out certain activities (Supplier's Activities).
- B The Recipient has been engaged, contracted or may provide works or services in connection with the Agreement.
- C The Customer has agreed that the Recipient may access or receive certain Confidential Information and/or Personal Information on the terms and conditions of this Deed and for the Permitted Use.

1. Definitions and Interpretation

1.1 Definitions

In this Deed:

Confidential Information means information that:

- (a) is by its nature confidential;
- (b) is communicated by the Customer as being confidential;
- (c) the Recipient knows or ought to know is confidential; or
- (d) relates to or comprises the:
  - (i) financial, corporate and commercial information of the Customer;
  - (ii) affairs of a third party; or
  - (iii) strategies, practices and procedures of the State of New South Wales and any information in the Recipient's possession relating to a Government Agency,

but excludes information:

- (e) in the public domain, unless it came into the public domain due to a breach of confidentiality;
- (f) independently developed by the Recipient; or
- (g) in the possession of the Recipient without breach of confidentiality by the Recipient or other person.

Customer Data means all data (including metadata) and information relating to the Customer or any Government Agency and the operations, facilities, customers, clients, personnel, assets and programs of the Customer and any Government Agency, including Personal Information, in whatever form that information may exist and whether created, captured, collected, entered

into, stored in, generated by, controlled, managed, retrieved, transferred, transmitted, printed, processed or produced as part of carrying out the Supplier's Activities, but excluding any Performance Data.

**Deed** means this deed poll.

**Government Agency** means any of the following:

- (a) a government sector agency (within the meaning of the *Government Sector Employment Act 2013* (NSW));
- (b) a New South Wales Government agency;
- (c) any other public authority that is constituted by or under an Act or that exercises public functions for or on behalf of the State of New South Wales (other than a State owned corporation); or
- (d) any State owned corporation prescribed by regulations under the *Public Works and Procurement Act 1912* (NSW).

**Performance Data** means automatically generated metadata, not including any Personal Information or Confidential Information of the Customer or a Government Agency that:

- (e) is incidentally generated by a computer system in the course of its normal operation;
- (f) relates to the performance or operation of that computer system; and
- (g) arises in the course of the performance of the Supplier's Activities.

**Permitted Use** has the meaning given to that term in clause 3(a) of this Deed.

**Personal Information** means information or an opinion about an identified individual (that is, a natural person) or an individual who is reasonably identifiable whether the information or opinion is:

- (a) true or not; and
- (b) recorded in a material form or not.

**Privacy Laws** means:

- (a) the *Privacy Act 1988* (Cth);
- (b) the *Privacy and Personal Information Protection Act 1998* (NSW);
- (c) the *Health Records and Information Privacy Act 2002* (NSW);
- (d) any legislation (to the extent that such legislation applies to the Customer, the Recipient or the Supplier) from time to time in force in:
  - (i) any Australian jurisdiction (which includes the Commonwealth of Australia and any State or Territory of Australia); and
  - (ii) any other jurisdiction (to the extent that the Customer or any Personal Information or the Supplier or the Recipient is subject to the laws of that jurisdiction),

affecting privacy or Personal Information, provided that the Recipient ensures that it complies at all times with the Privacy Laws applicable in New South Wales to the extent relevant to the Recipient's activities; and

- (e) any ancillary rules, guidelines, orders, directions, directives, codes of conduct or other instruments made or issued under any of the legislation referred to in paragraphs (a), (b), (c) and (d), as amended from time to time.

## 1.2 Interpretation

In this Deed:

- (a) headings are for convenience only and do not affect interpretation;
- (b) an obligation or liability assumed by, or a right conferred on, two or more persons binds or benefits them jointly and severally;
- (c) a reference to a "person" includes an individual, the estate of an individual, a corporation, an authority, an association or a joint venture (whether incorporated or unincorporated), a partnership and a trust;
- (d) a reference to a party includes that party's executors, administrators, successors and permitted assigns, including persons taking by way of novation and, in the case of a trustee, includes a substituted or an additional trustee;
- (e) a reference to a document (including this Deed) is to that document as varied, novated, ratified or replaced from time to time;
- (f) a reference to a statute or statutory provision includes a statutory modification or re-enactment of it or a statutory provision substituted for it, and each ordinance, by-law, regulation, rule and statutory instrument (however described) issued under it;
- (g) a word importing the singular includes the plural (and vice versa), and a word indicating a gender includes every other gender;
- (h) a reference to a clause is a reference to a clause of this Deed;
- (i) if a word or phrase is given a defined meaning, any other part of speech or grammatical form of that word or phrase has a corresponding meaning; and
- (j) "including", "in particular" and words of equivalent expression are not words of limitation.

---

## 2. Access and non-disclosure

- (a) The Recipient acknowledges and agrees that:
  - (i) in the course of performing duties under the Agreement, it may receive or have access to Confidential Information and/or Personal Information;
  - (ii) compliance with this Deed and the protection of Confidential Information and Personal Information are of paramount importance to the Customer; and
  - (iii) the obligations in this Deed are for the benefit of the Customer and the Customer may enforce the obligations under this Deed.
- (b) The Recipient must not disclose any Confidential Information or Personal Information that it receives or obtains in connection with the Agreement or the Supplier's Activities except with the consent of the Customer or as otherwise authorised under the Agreement or this Deed.
- (c) If the Customer grants its consent for the Recipient to disclose Confidential Information or Personal Information, it may impose conditions on that consent. In



particular, the Customer may require that the Recipient obtain the execution of a deed in these terms by the person to whom the Recipient proposes to disclose the Personal Information or Confidential Information.

- (d) The Recipient's obligations under this Deed will not be taken to have been breached to the extent it is required by law to disclose the Confidential Information or Personal Information. However, if the Recipient is required by law to disclose any Confidential Information or Personal Information, the Recipient must, before doing so, immediately notify the Customer and comply with any reasonable directions or requirements given by the Customer.

---

### 3. Recipient's obligations

- (a) The Recipient must only use Confidential Information and Personal Information that it receives or obtains in connection with the Agreement or the Supplier's Activities for the sole purpose of carrying out duties under the Agreement (**Permitted Use**).
- (b) The Recipient must:
  - (i) safeguard and protect all Confidential Information and Personal Information;
  - (ii) not copy or reproduce Confidential Information or Personal Information for purposes other than the Permitted Use;
  - (iii) not sell, let for hire, assign rights in or otherwise commercially dispose of any Confidential Information or Personal Information;
  - (iv) not commercialise or otherwise exploit any Confidential Information or Personal Information; and
  - (v) take all necessary precautions to prevent the loss; unauthorised use, disclosure or other misuse of Confidential Information and Personal Information in its possession or control.

#### 3.2 Comply with Privacy Laws

Where the Recipient receives or obtains access to any Personal Information in connection with the Agreement or the Supplier's Activities, the Recipient must comply with all applicable Privacy Laws, including the *Personal Information Protection Act 1998* (NSW) in respect of that Personal Information, regardless of whether the Recipient is legally bound to comply with those Privacy Laws.

#### 3.3 Security measures

Without limiting any other obligation under this Deed or at law, the Recipient must ensure that any Confidential Information or Personal Information in its possession or control is kept secure at all times, including by:

- (a) where the Recipient has access to Confidential Information or Personal Information by password or other secure means, not disclosing that password or means of access to any other person unless it has been authorised in writing to do so by the Customer; and
- (b) complying with the security requirements under the Agreement or as notified by the Customer to the Recipient.

### 3.4 Breach of obligations

If the Recipient becomes aware of any actual, threatened or suspected breach of this Deed, including by any of the Recipient's personnel, the Recipient must:

- (a) immediately notify the Customer in writing and take all steps necessary to remedy, prevent or stop the actual, threatened or suspected breach of this Deed and comply with any reasonable directions issued by the Customer regarding any unauthorised use or disclosure of the Confidential Information or Personal Information; and
- (b) provide such other assistance as may be reasonably required by the Customer, including in relation to any claim or proceedings that the Customer may bring against any third party for unauthorised use or disclosure of the Confidential Information or Personal Information.

### 3.5 Return of Confidential Information and Personal Information

If requested by the Customer, the Recipient must:

- (a) promptly and securely return to the Customer all documents and other physical records of Confidential Information or Personal Information in its or its personnel's possession, custody or control;
- (b) securely delete the Confidential Information and Personal Information from any computer system or other device operated or controlled by, or which may be accessed by, the Recipient;
- (c) where applicable, comply with any Customer policies and procedures in respect of the destruction or return of any Confidential Information and Personal Information; and
- (d) comply with any reasonable directions issued by the Customer in respect of the Confidential Information and Personal Information.

---

## 4. Remedies

The Recipient acknowledges that:

- (a) damages may not be an adequate remedy for the Customer for any breach of this Deed by the Recipient; and
- (b) the Customer is entitled to seek injunctive relief as a remedy for any breach or threatened breach of this Deed by the Recipient, in addition to any other remedies available at law or in equity under, or independently of, this Deed.

---

## 5. General

### 5.1 No exclusion of law or equity

This Deed must not be construed to exclude the operation of any principle of law or equity, including in relation to the protection and preservation of the confidentiality of Confidential Information.

5.2      **Waiver**

The Recipient acknowledges and agrees that:

- (a)      no waiver by the Customer of one breach of any obligation or provision under this Deed will operate as a waiver of another breach of the same or of any other obligation or provision; and
- (b)      none of the provisions under this Deed will be taken either at law or in equity to have been varied, waived, discharged or released by the Customer unless by its express consent in writing.

5.3      **Governing Law**

This Deed will be governed by, and construed in accordance with, the laws in force in the State of New South Wales, Australia. The Recipient submits to the exclusive jurisdiction of the courts of New South Wales, Australia and the courts competent to determine appeals from those courts.

5.4      **Continuing obligations**

The obligations of the Recipient under this Deed continue after the completion or termination of any employment, engagement or assignment in respect of the Permitted Use.

5.5      **Revocation or amendment**

This Deed may not be revoked or otherwise modified or amended without the prior written consent of the Customer.

**Executed** as a deed poll:

[Note: Delete the execution block that is not applicable.]

[If the Recipient is an individual]

Signed, sealed and delivered by *[insert full legal name of Recipient]* in the presence of:

\_\_\_\_\_  
Signature of witness

\_\_\_\_\_  
Signature of Recipient

\_\_\_\_\_  
Full name and position of witness

\_\_\_\_\_  
Full name and position of Recipient

\_\_\_\_\_

\_\_\_\_\_  
Date

[If the Recipient is a company]

Executed by [Insert] **ABN** [Insert ABN] in  
accordance with section 127 of the  
*Corporations Act 2001* (Cth):

\_\_\_\_\_  
Signature of director

\_\_\_\_\_  
Signature of director/company secretary

\_\_\_\_\_  
Full name of director

\_\_\_\_\_  
Full name of director/company secretary

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

**Schedule 7 - Escrow Deed – Not Applicable**

**Schedule 8 - Performance Guarantee – Not applicable**

**Schedule 9 - Financial Security – Not applicable**

## Aboriginal, SME and Local Participation Plan Template

The Aboriginal Procurement Policy (2021) requires that suppliers submit an Aboriginal Participation Plan for all projects valued at \$7.5m or above with their tender documents.

The SME and Regional Procurement Policy (2021) requires that suppliers submit an SME & Local Participation Plan which references SME and NSW specific content for all goods and services contracts valued at \$3m or above.

This plan is the supplier's commitment to APP, SME and Local content on the project. Plans will be finalised with the agency contract manager upon contract award and suppliers will be required to report progress against the plan quarterly.

NOTE: this is a template only and indicates the required information. Agencies may allow suppliers to use other formats, and may amend as appropriate to meet the objective of the procurement.

Contracting agency	Department of Communities and Justice (DCJ) NSW
Project Name & ID	JusticeLink Support and Maintenance Agreement (PRJ_5302)
Project Location	Sydney, NSW
Project start date	1 <sup>st</sup> April 2025
Expected project end date	31 <sup>st</sup> March 2028
Supplier name and contact details	Fujitsu Australia Ltd Level 5, 345 George Street, Sydney NSW 2000
Supplier ABN	19 0010 114 27
Are you an Aboriginal business?	NO
Is your business recognised as an Aboriginal business by:	Please tick appropriate response: <input type="checkbox"/> Supply Nation <input type="checkbox"/> NSW Indigenous Chamber of Commerce <input checked="" type="checkbox"/> None of the above

## 1. SME Content Commitments

SME Content Commitments	
SME status	<p>Are you an SME (Australian or New Zealand based enterprises with fewer than 200 full-time equivalent employees)?</p> <p><input type="checkbox"/> Yes</p> <p><input checked="" type="checkbox"/> No</p> <p>If you are an SME, you are not required to complete or report on the three fields below, however, you can complete as much as possible of the three fields below.</p>
SME Subcontracting (Subcontracting with an Australian or New Zealand based enterprises with fewer than 200 full-time equivalent employees)	<p>Number of SME subcontractors: <u>  0  </u></p>
SME participation commitment	<p>Estimated value of products/goods procured from SMEs: \$ <u>  0  </u> <u>  </u></p> <p><i>Non labour components of contract</i></p> <p>Estimated value of services/labour procured from SMEs: \$ <u>  0  </u> <u>  </u></p> <p><i>All costs related to time spent by an employee or subcontractor in contract delivery</i></p>
SME participation percentage	<p>Percentage of contract spend estimated to be with SMEs: <u>  0  </u> %</p>

2. SUSTAINABILITY COMMITMENTS

a) Sustainability outcomes (Optional)

Sustainability Commitments (Optional)	
Support of the government’s economic, ethical, environment and social priorities	<ul style="list-style-type: none"><li>• Creation of jobs in NSW (where possible)</li><li>• Developing and sustaining NSW industry capabilities, including through supporting people to gain in-demand or relevant skills, providing relevant skills and training opportunities and employing trainees or apprentices in NSW</li><li>• Supporting remote and regional communities, such as through employment opportunities, upskilling and training</li><li>• Supplier commitments to prevent or minimise the risk of modern slavery in their supply chain</li><li>• Participation of social enterprises or disability employment organisations in the supply chain and/or using goods and services from a business that provides services of persons with a disability</li></ul>



**b) Local Participation**

<b>Local Participation Commitments (where possible)</b> Note: For the purpose of the SME and Local Participation Plan, local content is defined as: goods produced, services provided, and labour supplied by the NSW industry	
NSW jobs	<b>Number of FTEs in NSW (where possible): _5-6_</b> <b>Note:</b> Fujitsu will report actuals for the applicable reporting period.
NSW content value	<b>Total estimated value of products/goods procured in NSW (where possible): \$ Not applicable as this is a services contract</b> <i>Non labour components of contract (detailed above)</i>  <b>Total estimated value of services/labour procured in NSW (where possible): [REDACTED] million /year approximately</b> <i>All costs related to time spent by an employee in contract delivery</i>  <b>Note:</b> Fujitsu will report actuals for the applicable reporting period.
NSW Capital Expenditure	<b>Estimated value of capital expenditure in NSW (where possible): [REDACTED] million (approximate till FY 23)</b> <i>This figure is separate from your tender value. It is the total value of capital investment (spend by your business), for example building, leasing or procuring infrastructure that benefit NSW communities. Either purchased in NSW or to be retained in the state and to be used as part of the contract delivery. Previously purchased assets are to be calculated at a depreciated value.</i>  <b>Note:</b> Fujitsu will report actuals for the applicable reporting period.

**c) Aboriginal Participation Commitments**

**Note:** Aboriginal Participation is applicable only when the contract value reaches \$7.5 million AUD (ex-GST)

Aboriginal Participation requirements	
Estimated contract value	
Exclusions	Not applicable
Project value	
Aboriginal participation percentage	1.5% of the project value or project workforce. Note: applicable only when the contract value reaches 7.5 million AUD (ex-GST)
Value of Aboriginal participation	1.5% of the project value Note: applicable only when the contract value reaches 7.5 million AUD (ex-GST)
<p><b>Plan to meet Aboriginal participation requirements</b> (if you are an Aboriginal business, you do not have to proceed further on this form). Aboriginal participation requirements may be met in the following ways:</p> <ul style="list-style-type: none"> <li>• A minimum 1.5% of project value directed toward Aboriginal businesses through sub-contracting</li> <li>• A minimum 1.5% of the project workforce to be Aboriginal people across the life of the project</li> <li>• A minimum 1.5% of the project value directed toward capability and capacity building of Aboriginal people or businesses</li> <li>• Or, a combination of these options.</li> </ul>	
Subcontracting	
Employment	
Education, training or capability building for Aboriginal staff or businesses	<p>Fujitsu will direct 1.5% of the Project Value to existing education, training or capability building programs for Aboriginal staff or businesses. Which will include but not limited to:</p> <ul style="list-style-type: none"> <li>• Mentoring or professional development support.</li> <li>• Explore traineeships and education pathways to promote Aboriginal peoples participation in IT.</li> <li>• Building cultural capability within the workplace.</li> <li>• Continuation in the execution of our Innovate Reconciliation Action Plan.</li> </ul>
Past Aboriginal participation compliance history	
Please indicate whether your business is currently, or has previously been, subject to Aboriginal participation requirements on a NSW Government project and if so, please indicate how it has performed against its commitments.	<p>If your business is currently or has previously been subject to Aboriginal participation requirements, please advise the project, contracting agency, participation requirements and the businesses performance against the requirements (were the commitments met? If not, why not etc).</p> <p>If your business has no experience with Aboriginal participation requirements, evidence can be provided of your businesses commitment to Aboriginal employment or use of Aboriginal suppliers through:</p>

- Previous track record of Aboriginal employment and use of Aboriginal suppliers, including by providing examples or case studies.
- A Reconciliation Action Plan (RAP) or similar that provides a business commitment to Aboriginal employment and Aboriginal supplier targets.

**Fujitsu Response:**

Fujitsu has not been subject to prior Aboriginal participation requirements on an NSW Government Project.

Fujitsu is committed to actively contributing to the reconciliation process in Australia including New South Wales. Our vision is to achieve a more equitable, just, and prosperous future for Aboriginal and Torres Strait Islander peoples by building trust with First Nations communities and peoples through innovative and ethical partnerships.

**First Nations supplier spend and engagement**

In line with Fujitsu’s Indigenous Procurement Policy, we actively procure products and services from suppliers that are Aboriginal and/or Torres Strait Islander owned, managed, and controlled. Fujitsu has two partnerships in place to assist in the achievement of our policy aims and wider reconciliation goals.

[REDACTED]

For the previous financial year (FY) (1 April 2023 – 31 March 2024), Fujitsu achieved a total spend of [REDACTED] with First Nations businesses. Over [REDACTED] of this spend was spent with First Nations businesses in New South Wales. For the current FY, the YTD spend with Indigenous businesses is [REDACTED] approximately in NSW.

To track spend of Indigenous suppliers and create an easy way for employees to engage with suppliers, Fujitsu launched an internal marketplace (online guided buying portal in SAP). The portal allows employees to purchase from businesses and suppliers through the [REDACTED] in Aotearoa New Zealand. Fujitsu worked with [REDACTED] on the development of the guided buying portal in SAP and was awarded the Chris O’Brien Award in the SAP Best Run awards for 2023.

**Fujitsu’s rate of First Nations employment**

Fujitsu commenced collecting the demographic data of its permanent employees – which includes whether the employee identifies as being Aboriginal and/or Torres Strait Islander – in mid-2021. The completion of this statistical demographic data is voluntary, and, to date, we have

had just over [REDACTED] permanent workforce complete this information. For the available data, Fujitsu's known rate of Aboriginal employment is [REDACTED]. The actual number of employees who identify as being First Nations may be much higher, but due to the voluntary nature of discourse and low disclosure rate, this cannot be substantiated at present.

Fujitsu is working to improve both completion of demographic information and rates of First Nation employment by ensuring that workplaces are culturally safe. We do this through:

- Manager and team training, education and celebrating important cultural events, such as NAIDOC and National Reconciliation Week.
- Working with the [REDACTED] to recruit Aboriginal and Torres Strait Islander people directly to the business, and/or by subcontracting to First Nations-owned businesses.
- Partnering to expand the talent pipeline, including through internships, traineeships, and apprenticeships. For example, Fujitsu has partnered with the CSIRO Young Indigenous Women's STEM program, providing workshops to First Nation high school students mainly across western NSW.

### **Digital inclusion partnerships and projects**

As an ICT and DX company, Fujitsu is uniquely placed to help bridge the digital divide in our region and to consider digital inclusion in our products and services. We believe that everyone should have equal access to technology and are committed to creating positive social impact through digital inclusion. Fujitsu continues to contribute to the empowerment of First Nations people and communities both internally and externally, including the following initiatives:

### **Indigenous Precision Services and 'WildAI'**

Fujitsu partners with many different stakeholders to develop innovative technology solutions that help to solve business and sustainability challenges. We call this 'digital co-creation'.

In 2023, Fujitsu started co-developed 'Wild-AI' - a system involving 'ecology-AI' and the use of long-range drones for surveying kangaroo species, as well as other native and introduced fauna. In partnership with Sci-eye, an interdisciplinary team of experienced scientists, and Indigenous Precision Services (IPS), a 100% Indigenous-owned and New South Wales-based company committed to delivering high-quality animal welfare for species endemic to Australia, aligned with the values and aspirations of Aboriginal and Torres Strait Islander people, we can converge traditional knowledge, modern-day science and technology for improved environmental outcomes.

The objective of 'Wild-AI' is to explore how an integrated SaaS (Software-as-a-Service) platform with highly accurate and detailed ecological AI-derived data might assist with research, conservation and population control efforts. In recent times, this work has been expanded to include many native (e.g. red kangaroo, emu, wallaroo, swamp wallaby) livestock (e.g. cow, sheep, horse, alpaca) and feral species (e.g. red fox, fallow deer, hare).

The intent is to provide efficient real-world survey applications, with the aim of providing detection and identification of multiple species, at the species-level. We are also developing post-AI output workflows, to provide abundance/density/population estimates over large areas.

	<p><b>Cherbourg Digital Service Centre</b></p> <p>In April 2022 Fujitsu, together with the Cherbourg Aboriginal Shire Council and community; Queensland Department of Innovation, Tourism and Sport (Deadly Innovations Strategy); TAFE Queensland; and our customer, Australia Post, opened a First Nations IT Service Centre to support the digital transformation of the Cherbourg community.</p> <p>Located on Wakka Wakka Country in Cherbourg (an Aboriginal community town 260km north-west of Brisbane), the Service Centre is part of a 3-year pilot program designed to boost the economic development of Queensland First Nations communities through digital skills training and employment opportunities.</p> <p>In addition to supplying the equipment and training for the facility, Fujitsu had its first customer (Australia Post) opting to have their support calls attended by staff from the Cherbourg Service Centre. Agents at the Service Centre are also working towards obtaining certification (Certificate III) from TAFE Queensland.</p> <p>In August 2024, 7 more agents joined the Fujitsu account at the Cherbourg Digital Service Centre following successful completion of a digital pre-employment course with TAFE Queensland. As per previous cohorts, the team is also working towards obtaining a Certificate III qualification with TAFE Queensland whilst employed by the Centre. The Fujitsu Service Desk team continues to provide training and best practice support to agents at the Centre and we are now also planning the next stages of our support following the completion of the 3-year pilot in 2025.</p> <p><b>Innovate Reconciliation Action Plan</b></p> <p>Fujitsu has been part of the Reconciliation Action Plan (RAP) program since 2018, our most recent RAP was an Innovate RAP for the 2021-23 period. Our next Innovate RAP for 2025-28 is expected to be published by April-May 2025.</p>
--	--



# **Department of Communities and Justice NSW**

**Justice Link Support Contract**

**Pricing Proposal**



**10<sup>th</sup> October 2024**





In the spirit of reconciliation, Fujitsu acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Artist: Jasmin Sarin

# Our Story

**We use technology to make happier lives.**

**We are a global leader in technology and business solutions that transform organisations and the world around us. We have a long heritage of bringing innovation and expertise, continuously working to contribute to the growth of society and our customers.**

## Our purpose

Make the world more sustainable by building trust in society through innovation. We have reconsidered what role Fujitsu should play in this changing world. Our purpose drives every action of every person at Fujitsu.

## What we do

Building new possibilities by connecting people, technology, and ideas, creating a more sustainable world where anyone can advance their dreams. By bringing together our integration capabilities and cutting-edge technologies, we drive your success, moving forward for a more sustainable world. We call this 'Fujitsu Uvance'. It is the business focus we are bringing to technology and cross-industry functions. Through Fujitsu Uvance, we are committed to transforming the world into a place where people can live their lives, enjoying prosperity and peace of mind.

## How we work with you

We put people first. We believe in the power of diversity. Our values of empathy, trust and aspiration drive everything we do.

## Better together

Together, anything is possible. We dream big so you can dream bigger. Empowering each other to make the world more sustainable.







DCJ – Justice Link Support Contract

Version History			
Date	Issue Version	Comments	Author
28/05/24	1.0	Finalised for Customer Submission	████
18/06/24	2.0	Added a reduced days option, on DCJ request	████
10/10/24	3.0	Removed 83 days option and converted to Fixed Price construct	████
28/10/24	4.0	Updated Pricing Proposal based on discussions with DCJ	████
06/11/24	4.1	Corrected rounding-up impacts on Blended Rate	████

**DCJ – Justice Link Support Contract**

## Proposal for Justice Link Renewal (April 2025 to March 2030)

## Background and Context:

The current Justice Link (“JL”) Support Contract, executed on 26.05.2017 and which is in force between Fujitsu Australia Limited (“Fujitsu”) and Department of Communities and Justice NSW (“DCJ”) (“Current Contract”) expires on 31<sup>st</sup> March 2025. This proposal outlines Fujitsu’s pricing for the JL Support Services to ensure their timely extension till March 2030 for the following two options that have been requested by DCJ:

1. A 5-year contract term till March 2030
2. A 3-year contract term till March 2028 followed by a 1+1 annual extension option

DCJ has also indicated that the Current Contract which is based on the NSW Procure IT framework will be superseded with a new contract based on the NSW ICTA/MICTA framework (“New Contract”) for the period for which this proposal is sought.

Please note the following important assumptions that apply to this Pricing Proposal:

- a) Scope: The scope of the Support Services and Professional Services (for which Pricing is provided) is defined in Annexures 1,3,4,5 and 6 of the Current Contract, except for the following modifications

Annexure 1	<p>Page 37 - “Searchable Court List” is deleted from the application support list</p> <p>Page 44- The following lines</p> <p>“To the extent that the relevant Documentation has not already been supplied under Additional Condition 3.4 (Access to Source Code and Supporting Materials), within thirty (30) days of the general availability of an Update or a New Release, the Contractor must supply the Customer with two (2) free hard copies and one (1) free soft copy (in CD-ROM) of the updated Documentation.”</p> <p>are replaced with</p> <p>“To the extent that the relevant Documentation has not already been supplied under Additional Condition 3.4 (Access to Source Code and Supporting Materials), The Contractor will provide soft copies of the required documentation (Operation Guides, Upgrade Guides, Installation Checklists, and various other supporting documentation) with each release”</p>
Annexure 5	<p>The content following the line “Third party software required for the operation of the JusticeLink Software includes:” is replaced with:</p>

	<p>“Current State:</p> <ol style="list-style-type: none"> <li>1. Operating System: Windows Server 2012 R2</li> <li>2. Application Server: IBM WebSphere Application Server v8.5.5.9</li> <li>3. Database management System: Oracle 11g DBMS</li> <li>4. Internet Browser: Chrome Version 124.0.6367.201, Edge Version 124.0.2478.97</li> <li>5. Microsoft 365</li> <li>6. Identity Management: Oracle Access Manager 10 &amp; 11/OKTA/Identity Hub/ LDAP Server.</li> <li>7. Testing workstations: Windows 10</li> </ol> <p>Future State:</p> <p>Future upgrades will be determined by the Customer in consultation with the Contractor through the support and governance forum and will be included in the product Roadmap”</p>
Annexure 6	<p>The content following the line “Designated Operating Environment” is replaced with:</p> <p>“Current State:</p> <ol style="list-style-type: none"> <li>1. Operating System: Windows Server 2012 R2</li> <li>2. Application Server: IBM WebSphere Application Server v8.5.5.9</li> <li>3. Database management System: Oracle 11g DBMS</li> <li>4. Internet Browser: Chrome Version 124.0.6367.201, Edge Version 124.0.2478.97</li> <li>5. Microsoft 365</li> <li>6. Identity Management: Oracle Access Manager 10 &amp; 11/OKTA/Identity Hub/ LDAP Server.</li> <li>7. Testing workstations: Windows 10</li> </ol> <p>Future State:</p> <p>Future upgrades will be determined by the Customer in consultation with the Contractor through the support and governance forum and will be included in the product Roadmap.”</p>

- b) Terms and Conditions: The pricing is submitted on the assumption that the terms and conditions of New Contract will be no more onerous to Fujitsu than the terms and conditions in the Current Contract .

c) CPI clause : The New Contract will have a CPI clause that is equivalent to the CPI clause in the Current Contract (specifically, the CPI clause as per Annexure 2 Clause 1.4 of the Current Contract)

- d) Impact of Justice Link technology stack upgrade: Fujitsu is aware that there is an initiative underway by DCJ to upgrade the JL technology stack and migrate the JL ecosystem to the cloud. At this stage Fujitsu has no visibility of the planned target state or its implementation pathway. Fujitsu should be provided visibility of the target state and its implementation pathway at the earliest opportunity so that we can advise DCJ of any JL application compatibility issues associated with this initiative. It will be important to incorporate Fujitsu JL architects early in the planning stage of the JL upgrade project so that we can provide appropriate inputs and advice to minimise application compatibility issues.



DCJ – Justice Link Support Contract

DCJ acknowledges that any upgrade pathway is likely to impact JL application compatibility and supportability. On DCJ’s request, Fujitsu can execute an initial “Application Compatibility & Supportability Assessment” and subsequent “Application Recertification Project” to help quantify the associated JL remediation costs. Fujitsu will provide a Professional Services quotation to DCJ for these assignments using the Time and Material Rates for Professional Services that are applicable in the Contract period to which these assignments pertain.

1. Option 1: 5-year contract term till March 2030

a) Support Services Price for Base Support Package

The Pricing for Years 1 to 5 (starting month of Year 1 being April 2025) is proposed to be:  
Selected option: 78 days per month

Period	Total Pricing (AUD, ex GST)	Blended Rate (AUD, ex-GST)
Year 1	\$ 1,476,072	\$ 1,577
Year 2	\$ 1,535,040	\$ 1,640
Year 3	\$ 1,595,880	\$ 1,705
Year 4		\$ 1,791
Year 5		\$ 1,881



DCJ – Justice Link Support Contract

2. Option 2: 3-year contract term till March 2028, followed by a 1+1 annual extension option

a) Support Services Price for Base Support Package

The Pricing for Years 1 to 3 (starting month of Year 1 being April 2025) is proposed to be:

Selected option: 78 days per month

Period	Total Pricing (AUD, ex GST)	Blended Rate (AUD, ex-GST)
Year 1	\$ 1,476,072	\$ 1,577
Year 2	\$ 1,535,040	\$ 1,640
Year 3	\$ 1,595,880	\$ 1,705

For the subsequent years (post Year 3), actual CPI will continue to apply as per the CPI clause in the New Contract

i. For the purposes of estimation only, the following indicative pricing has been projected for each subsequent year assuming a CPI2/CPI1 ratio of 1.05. Fujitsu will submit a pricing proposal using actual CPI indices prior to the annual anniversary of the contract for each subsequent year to confirm pricing.

Period	Indicative Pricing (AUD, ex GST) – for estimation purposes only
Year 4	\$ 1,676,345
Year 5	\$ 1,760,163

ii. Prior to the end of Year 3, should DCJ wish to exercise the 1+1 extension option and provides Fujitsu with adequate notice, Fujitsu will provide a pricing proposal to address this request prior to the end of the contract term.

## Important Notice

The information contained in this document is confidential and is submitted by Fujitsu on the basis that it will be used solely for the purposes of evaluating Fujitsu's proposal. Its content must not be made public and/or communicated, in whole or in part, to any third party, by any means and for any purpose without Fujitsu's prior written consent. Provided that this does not prevent disclosure required by law including in the case of government to a relevant parliament or committee. The pricing in this proposal is indicative only for your evaluation purposes and does not constitute an offer capable of acceptance. This proposal is subject to contract.

Fujitsu endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

This document is the property of Fujitsu and can only be used for the purpose it was intended. It cannot be considered or interpreted as granting a license or transferring property rights (including intellectual property rights) to its recipient.

© Copyright Fujitsu 2024. All rights reserved. Other than for the purpose of evaluation, no part of this document may be reproduced in any form without the prior written permission of Fujitsu.

©2024 Fujitsu Australia Limited. All rights reserved. FUJITSU and FUJITSU logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.

FUJITSU-RESTRICTED Uncontrolled if printed



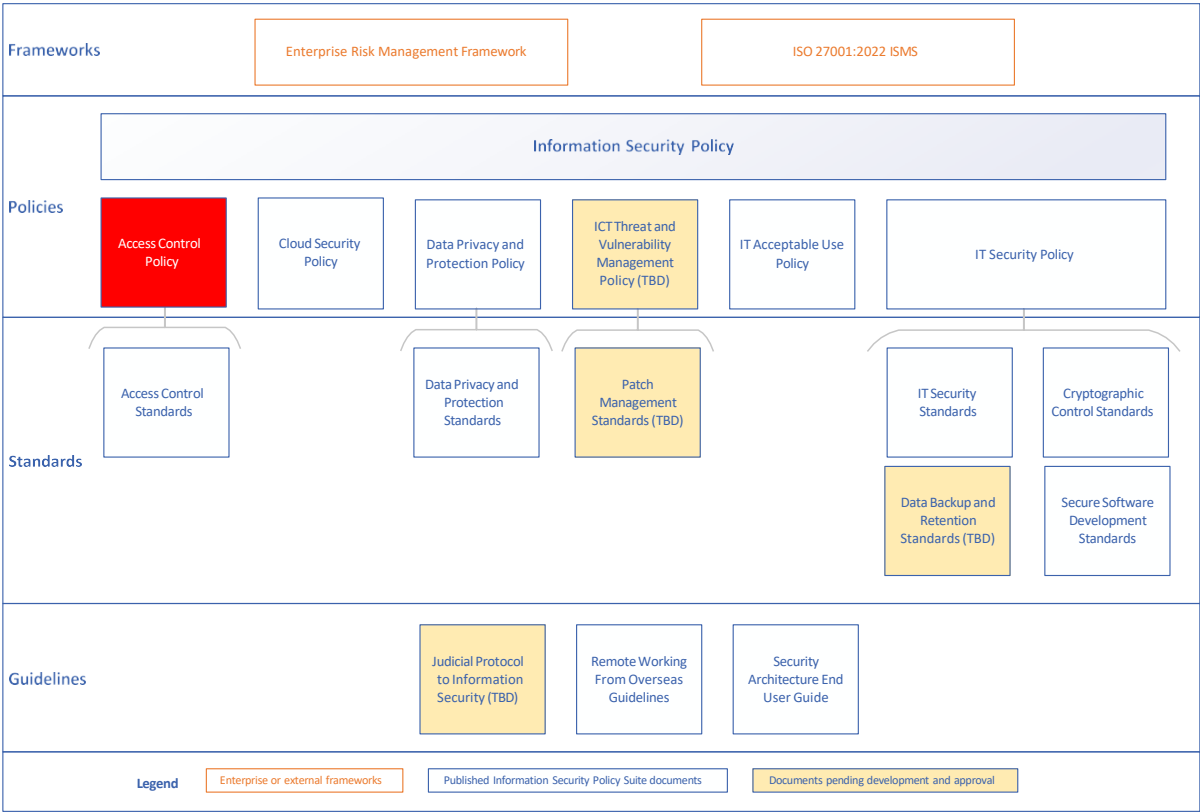
# Access Control Policy

---

## Table of contents

1	Purpose .....	2
1.1	Related policies .....	2
2	Definitions.....	3
3	Scope.....	3
4	Policy statement .....	4
5	Policy.....	4
5.1	Access control .....	4
5.2	Access to networks and network services .....	4
5.3	User access management.....	4
5.4	System and application access control.....	8
5.5	Mobile devices and teleworking .....	10
7	Related legislation, regulation and other documents.....	10
8	Document information .....	11
9	Support and advice .....	11
10	Version and review details .....	11
11	Appendix – Engaging information security .....	12





The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

This policy is designed to articulate the high-level access requirements that the Department of Communities and Justice (DCJ) expects from its ICT systems to ensure information is being protected appropriately.

1.1 Related policies

This document is related to the following policies:

- [IT Security Policy](#)
- [Data Privacy and Protection Policy](#)
- [Information Security Policy](#)
- [IT Acceptable Use Policy](#)
- [Employment Screening Policy](#)
- [End User Computing Policy](#)
- [Cloud Security Policy](#)
- [NSW Cyber Security Policy](#) 2020 v3.0

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met

## 3 Scope

The requirements and expectations outlined in this policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

It should be noted, this policy will be implemented by system and service support/development staff.

This policy does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

## **4 Policy statement**

DCJ information assets need to be protected appropriately throughout their lifecycle to ensure the confidentiality, integrity and availability of DCJ ICT systems and information. Appropriately controlling and restricting access to information and systems ensures individuals are provided the right access at the right time for their role.

## **5 Policy**

### **5.1 Access control**

Access to information assets, both digitally and physically, must be driven by information management requirements. These requirements must be translated into controls which deliver appropriate and enforceable access management.

Access to information and resources must be granted in a controlled manner. Appropriate approval from the information asset owner, delegate, or where acceptable the line manager, must be sourced prior to the delivery of access. Where possible, the principle of least privilege should be applied to ensure the right person has the right access to only the information they need.

Applicable legislation or regulatory restrictions (such as privacy and records management) must be considered when creating or issuing access to DCJ information or systems. Any system covered under legislation must abide by the legislative restrictions within the access process.

### **5.2 Access to networks and network services**

Provision and de-provision of access to networks must be in line with this policy. Access to a network does not infer or assume access to a system or service, specific and unique authorisations must be obtained for each.

### **5.3 User access management**

### 5.3.1 User registration and de-registration

Accounts must be registered in such a way that they uniquely identify the owner/user.

User registration and de-registration procedures must be implemented and documented when granting or revoking access rights.

These procedures must be documented and include:

- recorded authorisation from appropriate management to perform the registration or de-registration
- verification that the registration or de-registration action performed is correct.

These documents must be kept for appropriate amounts of time, commensurate with legislative requirements. If no specific timeframes are articulated by legislation, this history must be kept for a reasonable amount of time to support an investigation, if required.

Where an account is required to be created for a specific business need and is not associated to an individual, a system account or a generic account can be created to perform the required functions.

#### 5.3.1.1 System accounts

System accounts (also known as service accounts) are accounts which are primarily used by an application and are only used by humans in the event of an emergency situation. Where possible, system accounts must be made non-interactive to prevent human interaction. System accounts should be registered and tracked by the information asset owner or delegate of the identity store that the account resides on.

#### 5.3.1.2 Generic accounts

Generic accounts (also known as shared network accounts) are accounts that are not associated to an individual and are created to satisfy a specific business need. Multiple users can login to a single generic account to authenticate to DCJ's network, application or other resources.

Generic accounts must not be allocated an email address or given access to sensitive information such as employee or client's details. Where possible, generic accounts should follow the principle of least privileges required to do the job they are intended for.

Generic or shared network accounts must have a defined owner who is responsible for managing access to the account, password resets etc. Requests for generic or shared accounts must undergo a formal review process with

approval obtained from the Cyber Risk, Audit and Compliance team (CRAC) via [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au).

#### **5.3.1.3 Robot (BOT) accounts**

Robot accounts (aka BOT accounts) are accounts that were created with certain privileges to automate tasks of a repetitive nature, freeing people to focus more on other business priorities.

BOT accounts should follow the principle of least privileges required to do the job they are intended for and should follow the DCJ password management policy.

BOT accounts should be registered, tracked and maintained by the information asset owner or delegate of the identity store that the account resides on.

Requests for BOT accounts must undergo a formal risk assessment by the Cyber Risk, Audit and Compliance team via [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au).

#### **5.3.2 User access provisioning**

Access to DCJ information resources must be authorised by the information asset owner or delegate prior to access being provisioned. It is the responsibility of the information asset owner to ensure that access privileges are aligned with the needs of the business, meet the information management requirements, are assigned on a need-to-know basis and are communicated to custodians.

Temporary login accounts provided to individual non-DCJ personnel (e.g. auditors, consultants, work experience students, vendors, and contractors engaged by Strategic Sourcing) must be approved by the Chief Information Security Officer (CISO) or delegate.

Procedures for access provisioning must be documented and must ensure that access requests and approvals are documented. Furthermore, segregation of duties should be applied to ensure the requester is not provisioning their own access.

#### **5.3.3 Management of privileged access rights**

Privileged access rights are access rights provided to an identity, a role or a process that allows the performance of activities that typical users or processes cannot perform. System administrator roles typically require privileged access rights.

Where technically feasible, privileged access permissions should be applied to a secondary user account in order to prevent a user operating with heightened access privileges when they are not required. Privileged user accounts must not be used for general purposes such as browsing the Internet.

Privileged access rights must follow the principle of least privileges required to do the job they are intended for and, where technically feasible, should be applied on a temporary basis unless a business need exists justifying their persistence.

All requests for privileged access rights must be approved by the information asset owner or delegate and documented following an approved procedure. The provision of elevated access must only be actioned after approval is obtained and cannot be actioned by the requester.

Login credentials for privileged access accounts must be supplied and handled in a secure manner, and the access source must be controlled and positively attributable.

Privileged access accounts must be registered, tracked and maintained by the relevant information asset owner or delegate and user access reviews carried out quarterly.

All privileged access accounts must use multifactor authentication to verify their credentials when they are accessing the system to which they have privileged access.

Generic privileged access accounts must not be used unless a technical preclusion exists.

Asset owners are responsible for implementing controls which restrict privileged access only to approved users.

#### **5.3.4 Management of secret authentication information of users**

User ID's must be unique and not easily associated with a DCJ position or role etc. Should an 'as a Service' (aaS) model be utilised within DCJ which requires the use of email addresses as usernames, only unique individual email addresses should be used, not shared mailboxes.

Passwords must meet the following password construction, use and change requirements:

- Passwords must not be associated with DCJ or the user such as user's name, date of birth and cannot comprise solely of a word found in a dictionary, movie, geography, etc.
- Passwords must be of appropriate complexity and length and commensurate with the level of risk associated to the system being accessed or the permissions being provided.
- Where technically feasible and appropriate, complexity and length controls should be enforced by systems.
- Users must be forced to change their initial password.

- Custodians must ensure the identity of the user prior to releasing the initial password or password changes.
- Users must protect their password/s from compromise and must not disclose or share their password with others.
- Users must be forced to change their passwords at regular intervals.
- Users must not use cyclical passwords which see an integer at the end of a password increment or decrement at each password change.
- Users must avoid reuse passwords across different accounts
- Users must avoid common password/passphrase words, sayings & patterns (e.g. 'Password1234' or 'LetMeIn')
- Where technically feasible, systems must use password history techniques to maintain a password history of users.
- Passwords must never be stored in clear text.

#### **5.3.5 Password manager tools**

If a user utilises a password manager tool for any of their DCJ accounts, they should use DCJ approved password managers which must be used with Multi- factor Authentication (MFA).

#### **5.3.6 Review of user access rights**

Managers are responsible for ensuring their staff's access entitlements are appropriate for the staff member's role and position.

Custodians are responsible for ensuring user access reviews are conducted at regular intervals to ensure the right people are provided the right access at the right time.

Actions arising from a user access review must be in line with *Section 5.3.77 Removal or adjustment of access rights*.

#### **5.3.7 Removal or adjustment of access rights**

Removal of a user's access rights must follow an approved process and should secure appropriate approvals.

Adjustment of a user's access rights must be approved by the information asset owner or delegate.

Adjustments and removals of access rights must be documented and verification that the rights were removed or adjusted as appropriate should occur.

### **5.4 System and application access control**

### 5.4.1 Information access restriction

All information should have controls applied to ensure the integrity of data.

All information of value which has been classified must have appropriate access restrictions applied to ensure the right person, has the right access, at the right time.

### 5.4.2 Secure logon procedures

Before being given the opportunity to log onto a computer facility, intended users must be presented with an approved login banner.

System administrator connections to information systems must be secured with appropriate cryptographic techniques to prevent exposure of credentials or eavesdropping.

Identification of network, location, system criticality, service supported or host should not appear prior to a successful login.

Systems must be configured not to give any information on an unsuccessful login. This includes identifying which portion of a login sequence (user ID or password) was incorrect. User account management controls must be established to lock user accounts after a defined number of failed authentication attempts.

Where DCJ leverages an external service (e.g. cloud) and requires the ability to manage numerous identities and credentials, the DCJ enterprise federation capability should be used. The creation of disparate user accounts on the external platform or integration via less secure mechanisms (e.g. two way active directory trust) presents elevated risk and is discouraged.

### 5.4.3 Password management system

Systems which manage passwords must implement techniques which ensure the quality of passwords but also ensure the stored passwords are suitably protected.

Password management systems should:

- ensure passwords are changed at scheduled intervals
- keep a password history
- provide uniqueness of user accounts to ensure accountability
- ensure temporary passwords are unique to an individual and selected at random
- store passwords in a non-reconstitute-able form (i.e. one way hash). This means the password is encrypted and if the password file is compromised, the password will not display as clear text



- ensure password entry is secure.

#### **5.4.4 Use of privileged utility programs**

The use of privileged utility programs must be provided only to a limited number of staff that has a genuine need to use the utilities. Techniques must be implemented to prevent general users from gaining access to these utilities.

Actions performed whilst using these utilities should be logged.

An inventory of privileged utility programs should be kept, monitored and reviewed regularly

#### **5.4.5 Access control to program source code**

Strict, auditable, and controlled access to source code must be implemented.

### **5.5 Mobile devices and teleworking**

#### **5.5.1 Mobile devices**

Additional security measures must be implemented to protect data held on or accessed via mobile devices. All corporate data must be encrypted and where technically feasible corporate data and applications should be segregated to avoid inappropriate use or disclosure. Device configurations must abide by the technical requirements identified by the access control standard and IT security standard.

Mobile devices must be password protected by a minimum four-digit passcodes. Simple passcodes that are common and easily guessed are not to be used.

#### **5.5.2 Teleworking**

All remote connections to the DCJ network must implement appropriate controls including encryption to mitigate the risks posed by being external to the protected facilities and computing equipment of the organisation by utilising two-factor authentication. Cloud based systems that hold highly sensitive information and provide direct access should leverage two-factor authentication.

## **6 Monitoring, evaluation and review**

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## **7 Related legislation, regulation and other documents**

This policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *State Records Act 1998*
- *Government Information (Public Access) Act 2009*

## 8 Document information

Document name	Access Control Policy
Document reference	D22/1831836
Replaces	Access Control Policy v2.2
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/23

## 9 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

If you need assistance identifying when you need to engage information security, please see **Appendix – Engaging information security**.

## 10 Version and review details

Version	Effective date	Reason for amendment	Due for review
2.2	29/06/2022	Annual review due	29/06/2023
3.0	28/09/2023	Annual review Transferred to new DCJ Document Template and minor edits	28/09/2024

## 11 Appendix – Engaging information security

The following questionnaire can be used to help you determine when you need to engage Cyber Risk Audit and Compliance team.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party?

If you answer yes to any of the above or related legal advice, please email:

- **CRAC:** [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au)
- **Legal:** [infoandprivacy@justice.nsw.gov.au](mailto:infoandprivacy@justice.nsw.gov.au)

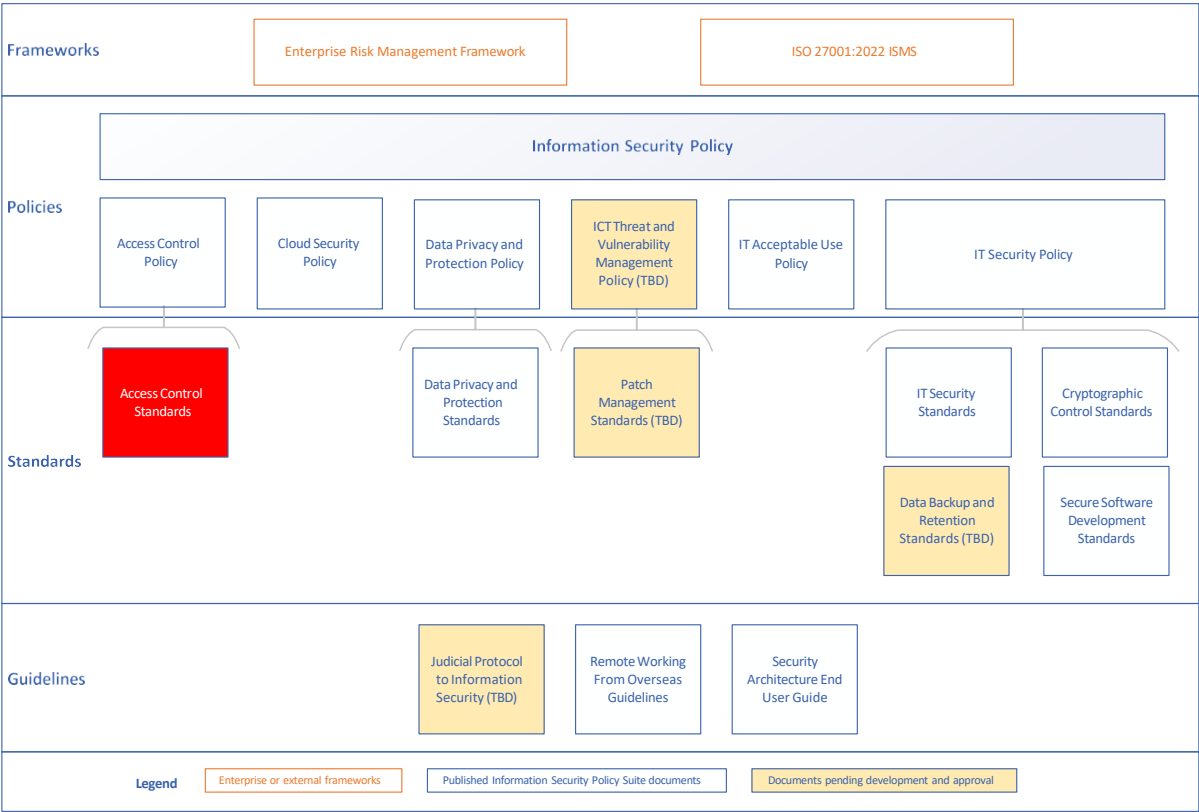


# Access Control Standards

---

## Table of contents

1	Purpose .....	2
2	Definitions.....	2
3	Scope.....	3
4	Access Control Standards .....	4
4.1	Principles .....	4
4.2	User Access Management .....	4
4.3	System and application access controls .....	9
4.4	Mobile devices and teleworking .....	10
5	Monitoring, evaluation and review .....	11
6	Related legislation, regulation and other documents.....	11
7	Document information .....	11
8	Support and advice .....	11
9	Version and review details .....	11
10	Appendix – Acceptable IDs for 3 points identity check .....	13



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

The following standard articulates the Department of Communities and Justice’s (DCJ’s) access control standards in regard to the Access Control Policy.

2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Computing systems	Covers Personal computer, Desktop, laptop, netbook, Personal Digital Assistant (PDA), smart phones, tablets, workstation, server mainframe, super-computer, wearable computer.
Information Asset	Any information, infrastructure, application or ICT Configuration items (CI) which stores, transmits, creates or uses DCJ information.
MAC	Mandatory access control

Term	Definition
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
RBAC	Role based access control
Should	Valid reasons to deviate from the item may exist in particular circumstances; but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances; but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.
System account (also known as “service accounts”)	An account whose primary purpose is for use by an application or system as opposed to humans.

### 3 Scope

The requirements and expectations outlined in this document applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This standard will be used by staff who are responsible for the design, administration, support and hosting of DCJ information systems.

This standard does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges’ tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

## 4 Access Control Standards

### 4.1 Principles

Ref	Directive
PRI-001	Access and permissions <b>SHOULD</b> be provided following the principle of least privilege and only provided to those who have a business need.
PRI-002	Wherever feasible and appropriate, RBAC or MAC <b>SHOULD</b> be used to deliver access.
PRI-003	It is the responsibility of the information asset owner, delegate, or where applicable the line manager, to check if MAC or RBAC is feasible and apply it where appropriate.
PRI-004	Access to an information system or information asset does not subvert the need to follow defined procedures and processes.
PRI-005	Segregation of duties, where technically possible, <b>MUST</b> be enforced to ensure controls are not circumvented.

### 4.2 User Access Management

#### 4.2.1 User registration and deregistration

Ref	Directive
REG-001	User account ID's <b>MUST</b> be unique, identify a specific unique owner and <b>MUST NOT</b> easily be associated with a DCJ position or title etc.
REG-002	Registration of accounts <b>MUST</b> be recorded in a register and approved by appropriate management.
REG-003	Deregistration of accounts <b>MUST</b> be recorded in a register and approved by appropriate management.
REG-004	The registration or deregistration action <b>MUST</b> be verified to ensure that it has been performed correctly.
REG-005	Third party providers <b>MUST</b> use federation solutions which leverage SAML, Oauth and OpenID. Read Write Domain Controllers (or Read Only Domain Controller's with cached credentials) <b>MUST NOT</b> be provided to the third party. DCJ authentication secrets (i.e. Active Directory passwords) <b>SHOULD NOT</b> traverse the Internet to a third party.

#### 4.2.2 General user access provisioning

Ref	Directive
PRO-001	User accounts <b>MUST</b> be authorised by the Line Manager, Director or approved delegate prior to being provisioned. The authorisation <b>MUST</b> be recorded and reviewed for accuracy.
PRO-002	In the case where email addresses are required as the username, only unique individual email addresses <b>SHOULD</b> be used rather than shared mailboxes.
PRO-003	Procedures for access provisioning <b>MUST</b> be documented and approved by management.
PRO-004	The requestor <b>MUST NOT</b> provision their own access request.
PRO-005	The account user <b>MUST</b> change their initial password upon first logon.
PRO-006	Requests for non-DCJ user accounts <b>MUST</b> be approved by the Chief Information Security Officer or delegate

PRO-007	The maximum term of a temporary account for individual non-DCJ user <b>MUST NOT</b> extend beyond 12 months. A new form is required to extend this period.
---------	--

#### 4.2.3 System accounts

Ref	Directive
SYS-001	System accounts <b>MUST</b> only be created where a technical justification is evident. The technical team responsible for the identity store where the proposed account will be created is accountable for verifying the justification.
SYS-002	System account registration <b>MUST</b> be endorsed by the Security Operations team and by the appropriate Director.
SYS-003	System account registration and de-registration <b>MUST</b> be recorded by the technical team responsible for the identity store where the proposed account will be created. The record <b>MUST</b> identify the date provisioned, requester, owner, justification, validation by technical team, endorsement by Security Operations, approval by the identity store owner, renewal/review period (depending on application lifecycle), deregistration date and deregistration approval (client).
SYS-004	System accounts which are non-interactive (i.e. a shell, command prompt or GUI session cannot be established with the account) are exempt from the 60 day password rotation policy requirement (PAS-001). They <b>MUST</b> be changed on an annual basis or more frequently, and the process auditable and documented.
SYS-005	System accounts which are interactive are bound by the 60-day password rotation and complexity requirement as per <a href="#">Section 4.3.2 Password Management System</a> below. However, when a staff member with knowledge of the password exits the organisation or changes roles, the technical team responsible for the identity store <b>MUST</b> refresh the password immediately after authorisation is granted by appropriate management.

#### 4.2.4 Generic accounts

Ref	Directive
GEN-001	<p>Generic administrative accounts <b>MUST NOT</b> be used unless a technical preclusion exists and <b>SHOULD</b> follow the principle of least privileges required to do the job they are intended for. To request for a generic account:</p> <ul style="list-style-type: none"> <li>• Users <b>SHOULD</b> contact their Business Partners (BP) who will explore options.</li> <li>• If there is no viable option, BP to request for a generic account to be created by contacting the Cyber Risk, Audit and Compliance (CRAC) team via <a href="mailto:securityarchitecture@facs.nsw.gov.au">securityarchitecture@facs.nsw.gov.au</a></li> <li>• Request <b>MUST</b> be endorsed by the Security Architects and by the appropriate Director prior to this type of account being provisioned.</li> </ul>



Ref	Directive
GEN-002	Internal generic or shared accounts <sup>1</sup> <b>MUST</b> undergo an initial formal review process and then be continually revalidated with approval obtained from the Security Architect via <a href="mailto:securityarchitecture@facs.nsw.gov.au">securityarchitecture@facs.nsw.gov.au</a> . An electronic list of individuals accessing accounts <b>MUST</b> be kept current and discussed during the access review. The electronic list shall include an account owner, expiry date, revalidation period etc.
GEN-003	The account <b>MUST</b> have an owner which is responsible for any issues relating to security breaches etc.
GEN-004	The account password <b>MUST</b> be changed immediately after individuals accessing the account leave the organisation or are transferred to a role that does not require the access.
GEN-005	Generic accounts <b>MUST</b> conform to the requirements and safeguards set out in this standard, such as a password change every 60 days.
GEN-006	Changes in the <b>password MUST</b> be communicated privately to generic account holders, such as in an office meeting room. Passwords <b>MUST</b> never be written down.

#### 4.2.5 Robot (BOT) accounts

Ref	Directive
BOT-001	BOT accounts <sup>2</sup> <b>MUST</b> only be created where a business justification for automation is evident. The technical team responsible for the identity store where the proposed account will be created is accountable for verifying the justification.
BOT-002	Requests for BOT accounts <b>MUST</b> undergo a formal risk assessment by the Cyber Risk, Audit and Compliance (CRAC) team via <a href="mailto:securityarchitecture@facs.nsw.gov.au">securityarchitecture@facs.nsw.gov.au</a>
BOT-003	BOT account registration <b>MUST</b> be endorsed by the Security Architect via <a href="mailto:securityarchitecture@facs.nsw.gov.au">securityarchitecture@facs.nsw.gov.au</a> and by the appropriate Director.
BOT-004	BOT account registration and de-registration <b>MUST</b> be recorded by the technical team responsible for the identity store where the proposed account will be created. The record <b>MUST</b> identify the date provisioned, requester, owner, justification, validation by technical team, endorsement by Security Architect via <a href="mailto:securityarchitecture@facs.nsw.gov.au">securityarchitecture@facs.nsw.gov.au</a> , approval by the identity store owner, renewal/review period (depending on application lifecycle), deregistration date and deregistration approval (client).
BOT-005	BOT accounts are bound by the 60-day password rotation and complexity requirement as per <i>Section 4.3.2 Password Management System</i> below. However, when a staff member with knowledge of the password exits the organisation or changes roles, the technical team responsible for the identity store <b>MUST</b> refresh the password.
BOT-006	Each robot/thread <b>MUST</b> have its own robotic account.

<sup>1</sup> Generic accounts – Accounts whose primary purpose is to allow a human user to interact with an application or service. E.g. this includes wallboards and training accounts

<sup>2</sup> BOT accounts - Accounts whose primary purpose is to carry out repetitive and mundane tasks enabling the employees to focus on other priority work.

Ref	Directive
BOT-007	BOT accounts <b>SHOULD</b> have restricted access to only perform the role of that robot.
BOT-008	Logging/auditing <b>SHOULD</b> be available to track all actions performed by the robot

#### 4.2.6 Management of privileged access rights

Ref	Directive
RIG-001	<p>The use of privileged accounts <b>MUST</b> be granted only to:</p> <ul style="list-style-type: none"> <li>• an administrator account,</li> <li>• to those that require it for a job function (e.g. system administrator, developer etc.),</li> <li>• to those who have completed the required training and background checks.</li> </ul> <p>Access to privileged accounts <b>MUST NOT</b> be granted to general staff or executive managers. The granting of privileged access <b>MUST</b> be justified and endorsed by the applicable Director and approved by the applicable application/system owner.</p>
RIG-002	Where technically feasible, administrative permissions <b>SHOULD</b> be applied on a temporary basis unless a business need exists to justify their persistence. An account expiry date <b>SHOULD</b> be set for a maximum of 120 days.
RIG-003	Administrative access rights <b>MUST</b> be allocated to a users' administrative (ADM) account and <b>MUST</b> follow least privilege
RIG-004	Administrators <b>MUST</b> use their regular user accounts for non-administrative activities and switch to their administrator accounts only when needed.
RIG-005	ADM accounts <b>MUST NOT</b> have access to email or internet facilities, if not needed for that specific admin function.
RIG-006	Remote administration access <b>SHOULD</b> be restricted to a static IP or similarly limited and prescribed IP range
RIG-007	Privileged user access reviews <b>MUST</b> be carried out on a quarterly basis if not more frequently to ensure that privileges are appropriate and that accounts for departed staff are disabled and deleted.
RIG-008	Procedures for privileged user access provisioning and revocation of privileged user access (e.g. role changes, off-boarding, expired accounts and others) <b>MUST</b> be documented and it <b>MUST</b> be approved by the business owner)
RIG-009	The IT manager or a designated authority <b>MUST</b> ensure that all administrator accounts are deactivated or deleted promptly.
RIG-010	All administrative access <b>MUST</b> use MFA that <b>SHOULD</b> verify credentials back to a DCJ central Identity Provider (i.e., OKTA, AD) or to an IdP that does integrate with DCJ IdP.
RIG-011	Only strong MFA factors <b>SHOULD</b> be used for administrator access e.g. OKTA Verify, strong biometric, etc

RIG-012	Administrators <b>MUST</b> safeguard their credentials and devices, and follow the best practices for secure administration, such as using strong passwords, multi-factor authentication, encryption, VPNs.
RIG-013	ADM account password settings <b>MUST</b> be compliant with <i>Section 4.3.2 Password management system: PAS-001</i>
RIG-014	Administrators <b>MUST</b> provide a valid reason for each use of their administrator accounts and document their actions. The IT manager or a designated authority <b>MUST</b> review the administrator logs periodically and investigate any anomalies or violations.
RIG-015	All administrator access and activity <b>MUST</b> be logged and monitored for any unusual or unauthorized activities, and any incidents or violations <b>MUST</b> be reported and investigated promptly. Such admin access logs <b>MUST</b> be preserved for a minimum of 90 days.
RIG-016	All admin access traffic <b>MUST</b> be properly encrypted, and, when not using a central authentication, the various admin credentials <b>MUST</b> be stored in a secure encrypted facility (like a password manager).
RIG-017	Admin credentials <b>MUST</b> be stored (in memory or in a disk saved configuration) only in a reliable encrypted fashion. Admin credentials <b>MUST NOT</b> be stored in clear text or reversible decryption fashion in any piece of code.
RIG-018	All administrative access traffic flows <b>MUST</b> come from restricted and formally allowed sources, and a non-repudiation access chain <b>MUST</b> be established. Direct admin access to the managed resource originating from Internet or any large network segments <b>SHOULD NOT</b> be allowed.
RIG-019	The use of Jump Servers, Bastion Hosts and similar technologies <b>SHOULD</b> be employed when the admin traffic source destination cannot be restricted securely enough.

#### 4.2.7 User access reviews

Ref	Directive
REV-001	Staff access entitlements <b>MUST</b> be appropriate for the staff member's role and position.
REV-002	User access reviews <b>MUST</b> be carried out on a quarterly basis if not more frequently to ensure that accounts are appropriate and accounts for departed staff are disabled and deleted. This <b>SHOULD</b> be managed via the policy exception process.
REV-003	The access review process <b>MUST</b> enforce the segregation of duties i.e. the person gathering attestation information cannot conduct the access review itself.
REV-004	Follow-up actions arising from an access review <b>MUST</b> be recorded and in line with <a href="#">Removal of access rights</a> .

#### 4.2.8 Removal of access rights

Ref	Directive
-----	-----------

REM-001	Removal or adjustment of a user's access rights <b>MUST</b> be recorded and endorsed by the line manager or delegate and approved by the information asset owner or the information custodian
---------	---

### 4.3 System and application access controls

#### 4.3.1 Secure logon procedure

Ref	Directive
LOG-001	Intended users of DCJ corporate devices and BYO devices <b>MUST</b> be presented with an approved business use notice/login banner which identifies: <ul style="list-style-type: none"> <li>• The information asset owner (DCJ)</li> <li>• Legislation such as the Crime Act</li> <li>• Legal action if the asset is misused</li> <li>• Who can access the information asset</li> </ul>
LOG-002	User accounts <b>MUST</b> be locked-out after <b>five (5) consecutive</b> invalid password attempts.
LOG-003	Details of the reason for an unsuccessful authentication attempt <b>MUST NOT</b> be presented to the user.
LOG-004	Passwords <b>MUST NOT</b> appear as clear text.
LOG-005	System administrator connections to information systems <b>MUST</b> be secured with contemporary protocols which encrypt the data payload to prevent exposure of credentials or eavesdropping.
LOG-006	The system <b>MUST NOT</b> provide help messages during the log-on procedure that would aid an unauthorised user.
LOG-007	DCJ OKTA Identity Management Service (OKTA) <b>MUST</b> be used whenever technically possible for information access.

#### 4.3.2 Password Management System

Ref	Directive
PAS-001	<p>Passwords <b>MUST</b>:</p> <ul style="list-style-type: none"> <li>• Be a minimum of 10 characters in length</li> <li>• Contain 3 out the following 4 categories for complexity - <ul style="list-style-type: none"> <li>○ At least one number (0-9)</li> <li>○ At least one uppercase character (A – Z)</li> <li>○ At least one lowercase character (a – z)</li> <li>○ At least one special character (e.g. !@#\$%^&amp;* _-+=`  \(){}[]:;'"&lt;&gt;.,?/)</li> </ul> </li> <li>• Not contain the user's account name or parts of the user's full name</li> <li>• Have a maximum lifetime of 90 days</li> <li>• Have a minimum lifetime of 1 day</li> <li>• Enforce a history requirement of 12</li> <li>• Be stored in a non-reconstitute-able form (i.e. one way hash with salt/random data applied)</li> </ul> <p>Privileged access accounts <b>MUST</b> adhere to above controls with the exception that the password maximum lifetime is decreased to 60 days.</p>
PAS-002	<p>Password management systems <b>SHOULD</b>:</p> <ul style="list-style-type: none"> <li>• Ensure passwords are changed at scheduled intervals</li> <li>• Provide uniqueness of user accounts to ensure accountability</li> </ul>

	<ul style="list-style-type: none"> <li>• Ensure temporary passwords are unique to an individual and are selected at random</li> <li>• Ensure passwords are secure in transit and at rest</li> <li>• Ensure password complexity requirements as above</li> </ul>
PAS-003	Accounts <b>MUST</b> enforce an account lockout duration of 1 hour or until an administrator specifically unlocks it.
PAS-004	The password reset procedure <b>MUST</b> be documented and it <b>MUST</b> be approved by Management. The reset procedure <b>MUST</b> cover both online and call-up. If the latter, the owner of the account <b>MUST</b> be verified prior to reset (refer to the <b>Appendix – Acceptable IDs for 3 points identity check</b> )
PAS-005	<p>For call-up password reset, ensure the new password is provided via a secure means</p> <ul style="list-style-type: none"> <li>• Provide the password over the phone after conducting the 3 points identity checks.</li> </ul> <p><i>*DO NOT reset password via Live chat</i></p> <p><i>*DO NOT send one time password to external email</i></p> <p><i>*DO NOT provide one time password in Service Now</i></p>

### 4.3.3 Use of privileged utility programs

Ref	Directive
UTI-001	The use of privileged utility programs such as Wireshark, Ethereal, CyberArk, Qualys Guard, PHP-SYSLG-NG etc. <b>MUST</b> only be provided to system administrators after a written approval from the security operations team for either a single use or ongoing use of the tools.
UTI-002	The use of privileged utility programs <b>MUST</b> be recorded and reviewed regularly.

### 4.3.4 Access control to program source code

Ref	Directive
COD-001	Read only access <b>SHOULD</b> be provisioned to code reviewers to ensure segregation of duties.
COD-002	<p>'Gold' or final SOE image <b>SHOULD</b> include:</p> <ul style="list-style-type: none"> <li>• Checksum collection and comparison for integrity checking</li> <li>• Version control for any changes to the code</li> </ul>

## 4.4 Mobile devices and teleworking

### 4.4.1 Mobile devices

Ref	Directive
MOB-001	DCJ developed corporate applications <b>SHOULD</b> support Intune libraries.
MOB-002	The mobile device management solution <b>SHOULD</b> support a containerisation approach, whereby third-party applications are unable to

	communicate with DCJ applications, data and resources. For further information, please consult the IT Security Standards <i>Section 4.1 Mobile devices and teleworking</i> .
--	--

#### 4.4.2 Teleworking

Ref	Directive
TEL-001	All remote connections to the DCJ network <b>MUST</b> utilise ICT approved remote access solutions

## 5 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 6 Related legislation, regulation and other documents

This document is related to the Access Control Policy in that it is an implementation of the policy.

## 7 Document information

Document name	Access Control Standards
Document reference	D22/1832011
Replaces	Access Control Standards V1.2
Applies to	All staff excluding the Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Chief Digital Information Officer
Approved date	28/09/2023

## 8 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance team Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

## 9 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.2	29/06/2022	Annual review due	29/06/2023
2.0	28/09/2023	Annual review due Transferred to new DCJ Document Template and minor edits	28/09/2024

## 10 Appendix – Acceptable IDs for 3 points identity check

The following are acceptable IDs for conducting 3 points identity check:

- What is the Client's Employee Number?
- What is the Client's Date of Birth?
- What is the Client's Home Address, Suburb and Postcode?
- What is the Client's Personal Telephone Number or Mobile Contact Number?
- What is the Client's Current Position?

If there is insufficient data from people's records in SAP for conducting identity checks using the above 5 methods, direct the request to their current manager to validate is acceptable. Alternatively, their manager can log a ticket on their behalf.

For Corrective Services (CS) staff, the following are acceptable IDs for conducting 3-points identity check:

- Date of Birth
- CS Number
- Full Name

For staff walk-in to do password reset requests, a driver licence or any photo ID displaying the username is acceptable as a form of identify check. If no Photo ID is provided, then perform 3-point security check (see above).



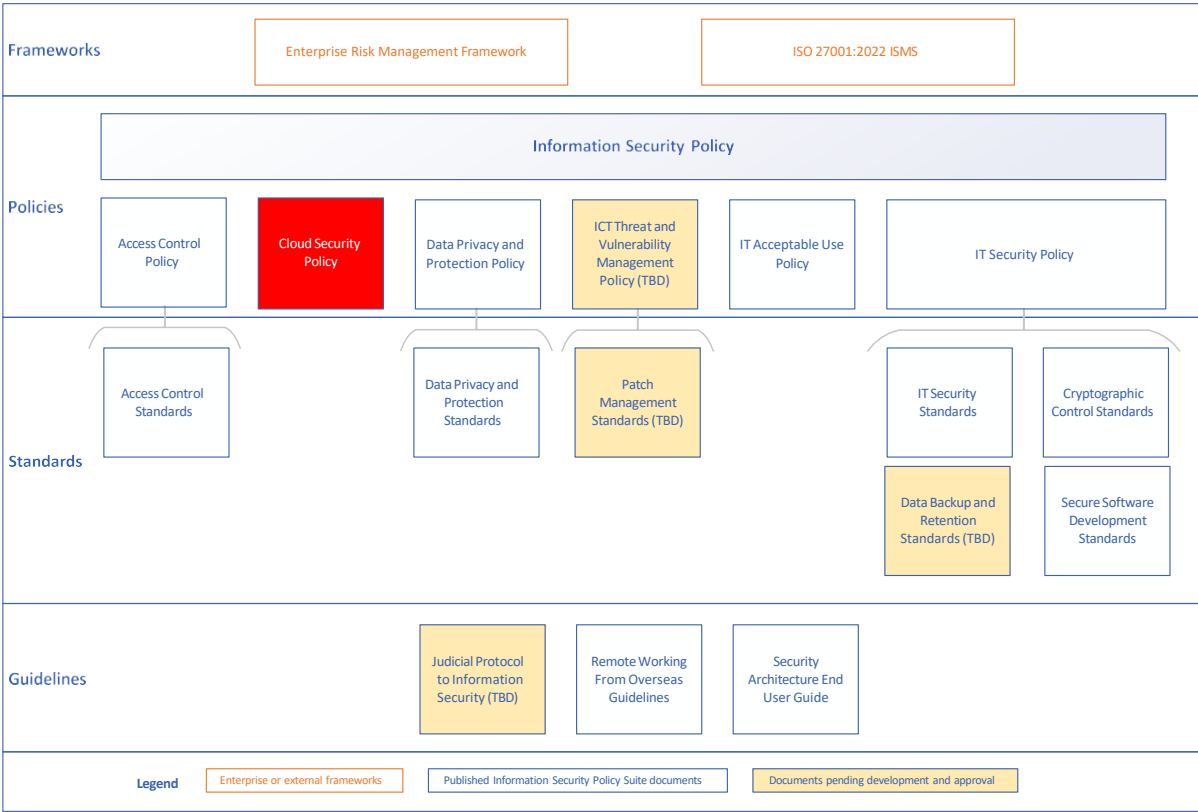


# Cloud Security Policy

---

## Table of contents

1	Purpose .....	2
1.1	Related policies .....	3
2	Definitions.....	3
3	Scope.....	5
4	Policy statement .....	5
5	Policy.....	5
5.1	Prior to consuming cloud services .....	5
5.2	Contracting with cloud service providers.....	7
5.3	During the cloud services .....	8
5.4	Availability of the cloud services .....	9
5.5	Exception .....	10
6	Roles and responsibilities.....	10
6.1	Business/information owner/delegated information owner (as per information asset register).....	10
6.2	Information custodian (as per information asset register) .....	10
6.3	Contract operator or relationship manager .....	10
6.4	Chief Information Security Officer .....	11
6.5	Chief Information Officer .....	11
8	Related legislation, regulation and other documents.....	11
9	Document information .....	11
10	Support and advice .....	12
11	Version and review details .....	12
12	Appendix – Engaging information security .....	13



The red highlighted box shows where this document sits within the Information Security Policy Suite.

# 1 Purpose

This policy is designed to articulate the high-level security requirements the Department of Communities and Justice (DCJ) expects, with the exception of the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members, all its employees and approved users (including Cloud Service Providers (CSP) and their subcontractors) to comply with when procuring and managing cloud-based services.

A cloud-based service is where DCJ pays to use, rather than own, the resources that are delivered over the network such as the internet by the CSP. “Cloud” refers to where the solution is provided.

As DCJ adopts more cloud-based services in alignment with Digital NSW strategies to streamline our services and operations, it is imperative that DCJ data being processed, stored and transmitted by cloud-based services remain secure at all times.

This policy is developed based on the following guiding principles:

- **Standardise architecture** to reduce complexity and deliver a common user experience across disparate systems.
- **Appropriate security and control** to better protect DCJ’ information.

- **Alignment to DCJ's ICT strategy** to reduce architecture/strategic debt and increase agility.

## 1.1 Related policies

This document is related to the following policies:

- [IT Security Policy](#)
- [Data Privacy and Protection Policy](#)
- [Information Security Policy](#)
- [Access Control Policy](#)
- [End User Computing Policy](#)
- Code of Ethics and Conduct
- Enterprise Risk Management Policy
- [IT Acceptable Use Policy](#)
- NSW Government Information Classification, Labelling and Handling Guidelines
- DCJ Business Classification Scheme
- [NSW Government Cloud Policy](#)
- [NSW Cyber Security Policy](#) 2020 v3.0

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Cloud-based service	Any service made available to DCJ users on demand via the Internet from a Cloud Service Provider's servers instead of from DCJ' own on-premises servers.
Cloud service provider (CSP)	Any company that provides applications, services or storage made available to users on demand via the Internet, for a fee.
Computing device	Any electronic device which facilitates the storage, capture, transfer, use or creation of information.

Term	Definition
CSP subcontractors	A person or organisation providing a component of the cloud service under contract to the CSP.
Device return merchandise authorisation (RMA)	Returning a device to receive a refund, replacement, or repair.
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
ISO 27001	A specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
ISO 27017	Provides enhanced controls for cloud service providers and cloud service customers. It clarifies both party's roles and responsibilities to help make cloud services as safe and secure as the rest of the data included in a certified information management system.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a "must" must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a "must not" must follow the procedures for requesting exceptions.
Should	Valid reasons to deviate from the item may exist in particular circumstances; but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met
Should not	Valid reasons to implement the item may exist in particular circumstances; but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met

### 3 Scope

The requirements and expectations outlined in this policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This policy does not apply to the Judiciary and NCAT board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

### 4 Policy statement

DCJ is committed to ensuring the confidentiality, integrity and availability of its client's data and the data of the organisation as a whole. The implementation of cloud solutions by DCJ provides staff the flexibility to work from any location, sharing real time data and collaborate to complete their tasks anytime, anywhere.

As the custodians of information that is politically, commercially, and personally sensitive it is imperative that DCJ information residing in the cloud remains with DCJ. This includes knowing exactly where the information will be stored geographically, particularly if it includes sensitive or personal information.

DCJ is committed to ensuring that the CSP maintain their information security management system (ISMS) which should be current and compliant with a globally recognised standard. An ISMS is a set of policies and procedures that allows the CSP to thoroughly handle confidential and potentially critical data.

Appropriately controlling and monitoring of security controls and reporting by the CSP and its subcontractors ensures DCJ information is protected. It also ensures the CSP's compliance with regulations about where certain data can be stored and who can access the data.

### 5 Policy

#### 5.1 Prior to consuming cloud services

### 5.1.1 Perform a security risk assessment

A risk assessment must be performed to identify the necessary security controls that must be established to manage risks to an acceptable level. This risk assessment must:

- include a gap analysis between DCJ's Information Security Policy and the security controls implemented by the CSP, identifying the threats to DCJ's information.
- gain adequate assurance that the identified risks have been addressed, and that the appropriate controls are in place prior to transfer of sensitive information to the cloud-based service
- where a multi-tenanted cloud platform is being considered (e.g. a single instance of a software application serving multiple customers) ensure appropriate controls are implemented and a procedure must be in place to implement suitable physical and logical segregation of DCJ information from other clients of the CSP
- be accepted by DCJ information owner or data custodian.

### 5.1.2 Maintenance of CSP ISMS

The CSP and its subcontractors should maintain an ISMS which covers the scope of services offered to DCJ. The ISMS must be aligned with ISO 27001 and leverage cloud controls as identified in ISO 27017. On an annual basis the vendor must:

- provide evidence of current audit or certification of the ISMS
- confirm its ISMS is currently compliant with ISO27001 and ISO27017
- confirm the ISMS is supported by vendor's executive management.

However, there may be a case where compliance cannot be achieved for a variety of reasons.

In such cases, all requests for exception must follow the exception process as defined by this policy (as per *Section 5.5 Exception*)

### 5.1.3 Single sign on and authentication

- The service offered must support federation and multi factor authentication (MFA) capabilities via Okta
- DCJ OKTA (or a reliable and monitored Identity Provider) should be used for service accounts (as used for API calls). Identity providers can be chained if the used service accounts are originating on the internal DCJ AD.
- Federation — Authentication must be delivered by SAML2.0 or other industry standard federation protocol (OIDC, OAuth2.0)

- Where appropriate authorisation should also be delivered via 'claims'. The solution should support single sign on (SSO)
- MFA — The service must support DCJ's MFA capability.

## **5.2 Contracting with cloud service providers**

### **5.2.1 Background checks**

The CSP should ensure its staff and contractors working on the DCJ account with access to DCJ networks, systems or data have undergone a criminal background check including Police, service suitability check and where applicable, undergo and maintain a Working With Children Checks (WWCC).

### **5.2.2 Data sanitisation**

Data sanitisation must be conducted across all storage devices upon DCJ exit/termination of the contract with the CSP, device return merchandised authorisation or device decommission. The CSP should issue a destruction certificate as evidence that DCJ data has indeed been sanitised.

### **5.2.3 Information custody and ownership**

The contractual arrangements or service level with the CSP must specify:

- that the ownership of data remains with DCJ at all time
- data residency. The geographical location(s) where DCJ information will be stored and accessed by the vendor and their sub-contractors
- the provisions for the safe return/transfer of data/disposal as appropriate back to DCJ in the event the service is terminated or when DCJ wishes to transition out of the service
- that DCJ retains an immediate and ongoing right of access to all of its data held by the CSP. The service provider must provide the links to connect to its service

DCJ information must not be stored outside Australia without a security risk assessment being performed and written consent from DCJ for all new solutions.

### **5.2.4 Controlling disclosure of DCJ data/information**

The CSP and its subcontractors must not share or disclose DCJ data and information obtained in a professional capacity without the prior written consent of the DCJ information owner supported by an appropriate confidentiality agreement or NDA, unless required by law.

### 5.2.5 Controlling privacy disclosure of DCJ services

The CSP and its subcontractors must abide by the NSW *Privacy and Personal Information Protection Act 1998* (and any subsequent amendment thereto) and any other applicable privacy laws.

The CSP and its subcontractors must not make privacy disclosures regarding DCJ data without DCJ's consent.

## 5.3 During the cloud services

### 5.3.1 Audit of security program

The CSP and its subcontractors must provide evidence of an annual external audit of the security program against globally recognised standards. Such evidence should be in the form of a certificate or report.

### 5.3.2 Security incident response plan

The CSP and its subcontractors must maintain a current and annually tested security incident response plan to ensure timely corrective action is taken during information security events, incidents, near misses and weaknesses. The incident response plan must consider threat identification, containment, remediation and root cause analysis.

Relevant contacts and escalation points between DCJ and the CSP must be maintained to appropriately manage interruptions to business activities and ensure that DCJ IT systems support the recovery of critical business processes.

### 5.3.3 Logging user access

The CSP and its subcontractors must deliver a capability to monitor and log user access (i.e. read, write, modify, execute) to the system and/or services. The monitoring solution should be able to proactively identify suspect behaviour and raise alerts where appropriate.

The logging facilities and log information must be protected against tampering and unauthorised access.

User activities, exceptions, faults and information security events must be recorded. Logs should provide at least 92 days of online access which is readily available to DCJ.

Logs should detail date, time, source, account name, action, result. Where possible, all logs should be processable by DCJ's centralised logging systems.



### 5.3.4 Auditing of data centres

Data centres hosting DCJ data must be externally audited and certified against a globally recognised standard for physical security including but not limited to ISO 27001.

No less than annually, the CSP must provide evidence that audits have been carried out. Such evidence should be in the form of a certificate or compliance report. Physical controls must include:

- 24/7 guards
- video recording
- security access devices
- perimeter fencing.

### 5.3.5 Proactive management of vulnerabilities

The CSP must maintain a vulnerability management program covering the services offered to DCJ. This should include regular vulnerability scans and a vulnerability management plan.

The vendor must undertake annual penetration tests which verify the services offered to DCJ are secure and be able to provide these reports to DCJ upon request for assurance purposes.

Should the vendor undertake software development associated with the services offered to DCJ, the vendor must maintain a secure code development program which mandates appropriate security testing of code releases.

### 5.3.6 Logging vendor access

The CSP and its subcontractors must deliver a capability to monitor vendor (administrator) actions (i.e. read, write, modify, execute) to supporting infrastructure.

Logs should provide at least 92 days of online access which is readily available to DCJ.

The logging facilities and log information must be protected against tampering and unauthorised access. Logs should detail date, time, source, account name, action, result.

### 5.3.7 Reporting of cyber security incidents

CSPs must ensure that DCJ is notified within 48 hours of identification of any cyber security incident or near-miss involving DCJ information assets.

## 5.4 Availability of the cloud services

Scheduled outages and service level agreements to avoid disruptions of DCJ's services must be included in the contractual agreement with the CSP. Notification processes for outages and the process for minimisation of disruption must be clearly defined.

The CSP must have the resilience capability to meet DCJ uptime objectives.

## 5.5 Exception

Only the relevant Deputy Secretary of the agency can authorise a deviation from this policy.

To apply for a policy exception please refer to *Section 7.4 Procedures for requesting exceptions* in the Information Security Policy.

## 6 Roles and responsibilities

The following roles and responsibilities are in regard to the acquisition and use of DCJ data within a cloud service.

For a full list of information security roles and their responsibilities please refer to the Information Security Policy *Section 7.6 Allocation of information security responsibilities*.

### 6.1 Business/information owner/delegated information owner (as per information asset register)

- Accountable for the data placed into the cloud service.
- Ultimate responsibility and ownership of the procured cloud service.
- Accountable for ensuring acquisition of cloud service complies with legal and policy requirements and is within organisation risk tolerance levels.
- Responsible for identifying the correct data classification and impact level.

### 6.2 Information custodian (as per information asset register)

- Responsible for advising the information owner of the data classification and impact levels.
- Responsible for identifying business specific requirements regarding the use, storage, access, security etc. of the data set.
- Responsible for monitoring the cloud service requirements and reporting to the contract manager/relationship manager on the service meeting the service level requirements.

### 6.3 Contract operator or relationship manager

- Responsible for the development and customisation of a service management plan which tracks the cloud service provider’s delivery of service through regular engagements and collection of appropriate metrics.
- Acts as an SME for the service and provides advice to the Information owner and custodian. Seeks support from appropriate internal parties to verify metrics and assurances.
- Responsible for ensuring the cloud service is meeting requirements and service levels.

6.4 Chief Information Security Officer

- Responsible for conducting vendor risk assessments on behalf of the information owner prior to acquisition of services.
- Provides advice and support regarding security requirements, and contract inclusions (including security metrics).
- Provides incident response support and vendor engagement during a cyber- security event involving the cloud service.

6.5 Chief Information Officer

- Approves the acquisition of all cloud services as appropriate.

7 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

8 Related legislation, regulation and other documents

This policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*
- *State Records Act 1998*
- *Government Information (Public Access) Act 2009*

9 Document information

Document name	Cloud Security Policy
Document reference	D22/1832022

Replaces	Cloud Security Policy V2.2
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/2023

## 10 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

If you need assistance identifying when you need to engage information security, please see

**Appendix – Engaging information security.**

**11 Version and review details**

Version	Effective date	Reason for amendment	Due for review
2.2	29/06/2022	Annual review due	29/06/2023
3.0	28/09/23	Annual review Transferred to new DCJ Document Template and minor edits	28/09/24

## 12 Appendix – Engaging information security

The following questionnaire can be used to help you determine when you need to engage the Cyber Risk Audit and Compliance team.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party?

If you answer yes to any of the above or related legal advice, please email:

- **CRAC:** [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au)
- **Legal:** [infoandprivacy@justice.nsw.gov.au](mailto:infoandprivacy@justice.nsw.gov.au)

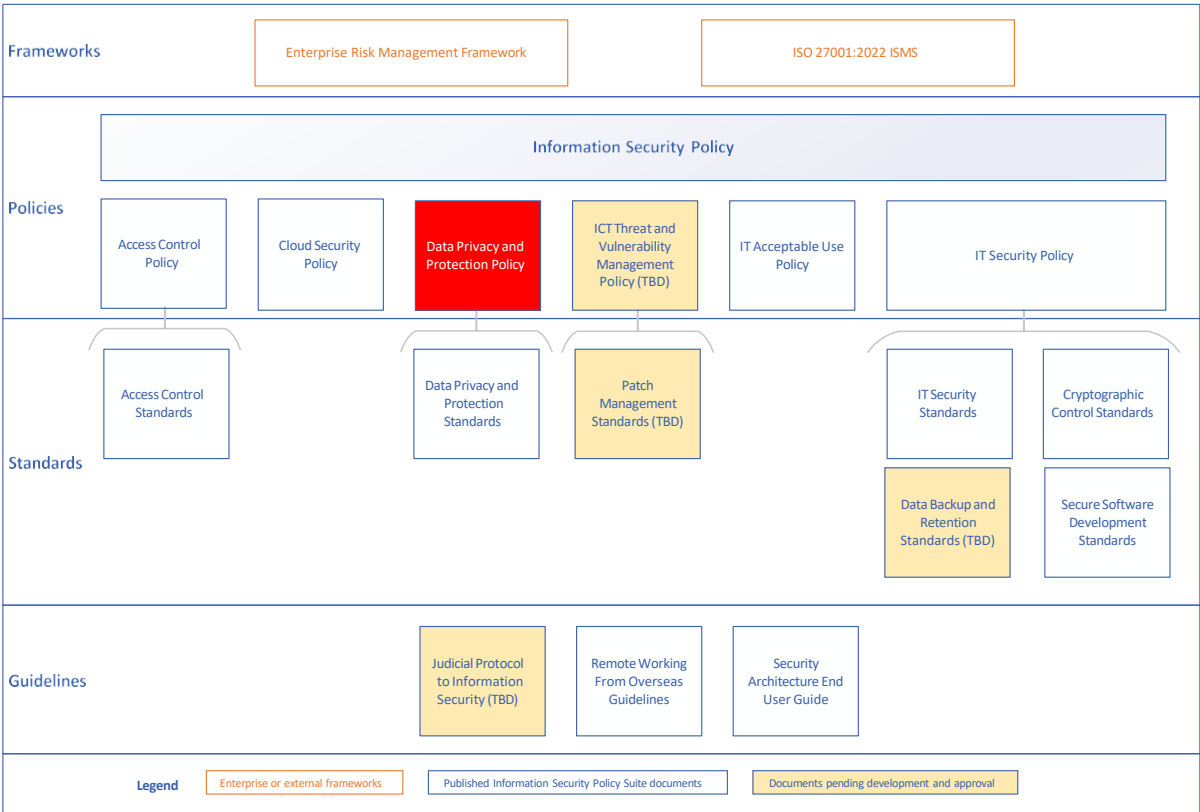


# Data Privacy and Protection Policy

---

## Table of contents

1	Purpose.....	2
1.1	Related policies .....	2
2	Definitions.....	3
3	Scope.....	5
4	Policy statement .....	5
5	Policy.....	6
5.1	Access to information .....	6
5.2	Protective markings.....	6
5.3	Classification of information .....	9
5.4	Secure information use .....	10
5.5	Sharing information.....	12
5.6	Outsourcing information.....	12
5.7	Protection of data and information .....	13
5.8	Protection of records .....	13
7	Related legislation, regulation and other documents.....	14
8	Document information .....	14
9	Support and advice .....	14
10	Version and review details .....	15
11	Appendix A – Engaging information security.....	16
12	Appendix B – How to assess sensitive and classified information .....	17
13	Appendix C – Business Impacts Levels (BILs) tool .....	18
14	Appendix D – Management of sensitive and classified information .....	22
15	Appendix E – Application of Dissemination Limiting Markers (DLMs).....	29



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

This Policy is designed to state the way the Department of Communities and Justice (DCJ) information is to be categorised, secured, managed and used. Applying a classification to information then informs the way it needs to be secured, managed and specific restrictions regarding how it can be used.

1.1 Related policies

This document is related to the following policies:

- [IT Security Policy](#)
- [IT Acceptable Use Policy](#)
- [Information Security Policy](#)
- [Access Control Policy](#)
- [Cloud Security Policy](#)
- [End User Computing Policy](#)
- Code of Ethics and Conduct



- Enterprise Risk Management Policy
- Information Management Policy
- Privacy Management Plan
- [NSW Cyber Security Policy](#) 2020 v3.0
- [NSW Government Information Classification, Labelling and Handling Guidelines](#)
- [NSW Government Cloud Policy](#)
- [Commonwealth Protective Security Policy Framework](#)

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information
CIA	<p>The following principles are a guide for information security:</p> <ul style="list-style-type: none"> <li>• <b>Confidentiality</b> – Access to information is limited to authorised persons for approved purposes.</li> <li>• <b>Integrity</b> – Information is maintained and assured throughout its lifecycle to maintain its authenticity, accuracy, validity and trustworthiness.</li> <li>• <b>Availability</b> – Information is available to authorised personnel for authorised purposes at the time they need it.</li> </ul>
Data Leakage Prevention	<p>Methods used to prevent data flowing out of DCJ to an inappropriate party.</p> <p>Causes of a data leakage can include deliberate or accidental exposure of DCJ data in a public place such as leaving a paper file or removable media device on a train or in a café, emailing data to an internal or external entity who is not authorised to see it, and attacks on DCJ infrastructure with the intention of stealing data.</p> <p>Data leakage prevention methods include but are not limited to identifying sensitive data through data classification processes, educating DCJ staff in data classification, security and privacy and how that data must be safeguarded, enforcing data privacy and protection policies.</p>

Term	Definition
Data Loss Prevention	<p>Methods used to prevent data being lost or inaccessible to DCJ. Causes of data loss can include hardware failures, power outages, natural disasters, deliberate or accidental deletion of the data, and malware or virus attacks.</p> <p>Data Loss Prevention methods include but are not limited to anti-malware, anti-virus, data backup processes, disaster recovery plans (DRPs), business continuity plans (BCPs)</p>
Information asset	<p>Any information (both physical and digital) in any format, including audio and visual;</p> <p>Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.</p>
Information Asset Owner	<p>An information asset owner is the originator of an information asset. This individual is responsible for applying the relevant sensitive or security classification, based on an assessment of the Business Impact Level (BIL) which considers the likely damage if the information's confidentiality was compromised. The information asset owner remains responsible for controlling the sanitisation, reclassification or declassification of the information asset.</p> <p>Includes all DCJ staff, third parties, or consultants.</p>
Information sharing	<p>Information sharing specifically refers to a situation in which DCJ furnishes an external party with specific information as the result of a legally permissible information request. This scenario is normally authorised under a research agreement or other approved agreement.</p> <p>It should be noted this does not include the FOI (<i>Freedom of Information Act 1982</i>), GIPA (<i>Government Information (Public Access) Act 2009</i>) and information required to be produced in response to a court order. These types of requests should be responded to in compliance with legislation.</p>
May / May not	<p>The item is not mandatory.</p> <p>Recommended as best practice for consideration. No policy exception required if condition is not met.</p>
Must	<p>The item is mandatory.</p> <p>Any request for deviation from a "must" must follow the procedures for requesting exceptions.</p>

Term	Definition
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Outsourcing	Outsourcing includes any commercial arrangement where an external party stores, transfers, uses or creates DCJ information and data. This is however separate from an information sharing venture.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met

### 3 Scope

The requirements and expectations outlined in this policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information (including personal information and de- identified information)
- any other body authorised to host DCJ information, administer, develop, manage and support DCJ information systems and assets.

This policy does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges’ tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This policy also applies to tribunal staff who are DCJ employees.

### 4 Policy statement

Information is an asset, physical (hardcopy) or electronic (softcopy), which needs to be protected appropriately to ensure its confidentiality, integrity and availability. The DCJ handles information across a range of classifications including OFFICIAL: Sensitive, as well as some security classified information.

As the custodians of information that is politically, commercially or personally sensitive, or classified; DCJ has a responsibility to protect information from accidental or malicious modification, unauthorised access or use, loss or disclosure. DCJ must ensure that information is stored, transferred, and disposed of appropriately.

Documents that commit or oblige the DCJ in its business activities should be checked and countersigned (manually or electronically) to confirm their validity and integrity.

## 5 Policy

### 5.1 Access to information

DCJ must ensure that

- any access to sensitive and security classified information is limited to people with **a need-to-know**. This will mitigate the risk of deliberate or inadvertent disclosure or information sharing with unauthorised parties.
- Any user with ongoing access to sensitive and security classified information must have **a need-to-know and maintain the necessary security clearance** where applicable. The user should not be entitled to access information because it is convenient for them to know due to their position, rank, or authorised level of access.

The table below provides a brief overview of information classifications where access must be considered:

Classification	Must have a need to know	Required Security Clearance
OFFICIAL	Yes	No security clearance required
OFFICIAL: Sensitive - XX	Yes	No security clearance required
PROTECTED	Yes	Baseline or above
SECRET	Yes	Negative Vetting Level 1 or above

### 5.2 Protective markings

It is the responsibility of the information asset owner to ensure appropriate classification and labelling of the information they create.

Material that is not work related should be labelled UNOFFICIAL.

Material that may contain OFFICIAL, sensitive or security classified information needs to be labelled and managed according to the level/type of sensitivity as per the [NSW Government's Information Classification, Labelling and Handling Guidelines](#).

5.2.1 OFFICIAL

OFFICIAL information is related to the DCJ's business but does not have security or sensitivity issues. This information does not need to be labelled but DCJ may choose to do so. This should be the default position for newly created material unless there is a specific need to protect the confidentiality or integrity of the information.

5.2.2 DLM, OFFICIAL: Sensitive – XX and security classified

If OFFICIAL material requires specific handling or where disclosure may be limited or prohibited by legislation, the DLM must be applied to the document.

There are three protective marking paradigms which can be applied to a document:

- DLM
- security classification
- caveat (not used in NSW)

Paradigm	Description
DLM	<ul style="list-style-type: none"><li>• Sensitive information, if compromised, may cause damage to individuals, organisations or government. NSW uses six DLMs to describe the type of sensitivity of the information. DLM's adopted by DCJ as part of the NSW Government's system include:</li><li>• OFFICIAL: Sensitive - NSW Cabinet</li><li>• OFFICIAL: Sensitive - Legal</li><li>• OFFICIAL: Sensitive - Law enforcement</li><li>• OFFICIAL: Sensitive - Health information</li><li>• OFFICIAL: Sensitive - Personal</li><li>• OFFICIAL: Sensitive - NSW Government</li></ul> <p>Examples of sensitive information are an individual's personal details, credit information, tax file numbers, medical records, drivers licence information, criminal records, biometric information and other personal details.</p>
Security Classification	<p>Used to protect the most sensitive government information. The security classifications include:</p> <ul style="list-style-type: none"><li>• PROTECTED</li></ul>

	<ul style="list-style-type: none"> <li>• SECRET</li> <li>• TOP SECRET</li> </ul> <p>Each level of classification reflects the consequences of unauthorised disclosure and has strict handling and security clearance requirements. NSW agencies that handle information requiring security classification must manage this information in accordance with Commonwealth requirements as prescribed in the Commonwealth Protective Security Policy Framework (PSPF) and as directed by the NSW Government Information Classification, Labelling and Handling Guidelines.</p> <p>Security classifications PROTECTED, SECRET and TOP SECRET are to be regarded as national security classifications under these guidelines.</p>
Caveat	<p>The caveat is a warning that the information has special protections in addition to those indicated by the security classification. Caveats are not classifications and must appear with an appropriate security classification marked as text. The caveat is a warning that the information has special non- disclosure requirements in addition to those indicated by the protective marking. Caveats should not be used extensively in NSW. People who need to know will be cleared and briefed about the significance of information bearing caveats; other people are not to have access to this information.</p> <p>Caveats include:</p> <ul style="list-style-type: none"> <li>• codewords (sensitive compartment information)</li> <li>• foreign government markings</li> <li>• special handling instructions</li> <li>• releasability caveats</li> </ul>

Application of classification and labelling must be in compliance with the DCJ Data Privacy and Protection Standard. This standard provides further information on which protective markings should be used in different circumstances and provides information on how to apply those protective markings.

Information with a DLM or security classification:

- may only be transferred across networks or copied to other media where the confidentiality and availability of the information can be reasonably assured.
- may only be disclosed outside the DCJ with the appropriate authorisation.
- may only be provided to third parties (consultants, researchers etc) following the completion of a third-party risk assessment checklist to identify privacy or security risks associated with providing access to the information. Legal

advice should be sought from Legal prior to disclosing personal information of clients or employees to a third party at [infoandprivacy@justice.nsw.gov.au](mailto:infoandprivacy@justice.nsw.gov.au)

Use of information that is deemed to be judicial in nature should be handled according to the current judicial procedure.

### 5.3 Classification of information

All material in any format (e.g. hand-written, Word, JPG format) medium (online publishing platform e.g. Twitter) or resource (digital or physical materials) should be assessed to determine its classification as per the NSW Government's Information Classification, Labelling and Handling Guidelines.

Information asset owners must apply the lowest level of classification practicable to systems that are under their control. An information asset owner can determine the level of classification by assessing the value, importance or sensitivity of the information considering the potential damage to DCJ if that information was compromised.

The abbreviated table below provides an overview of the classification criteria for DCJ's most commonly used levels of information, based on the business impact and damage to DCJ that would occur if information is compromised.

Protective Marking	Business Impact	Damage
<b>OFFICIAL: Sensitive – XX</b>	Low to medium business impact	Limited damage to an individual, organisations or the government generally
<b>PROTECTED</b>	High business impact	Damage to the national interest, organisations or individuals
<b>SECRET</b>	Extreme business impact	Serious damage to the national interest, organisations or individuals

Note: The historical classification CONFIDENTIAL does not have an equivalent level of classification under the current PSPF. Information that was classified as CONFIDENTIAL before October 2020, has a Business Impact Level of very high. This means the compromise of CONFIDENTIAL information would be expected to cause significant damage to individuals, organisations, or the national interest. Most CONFIDENTIAL information will generally be re-assessed and re-classified or treated as Secret.

- Appendix B provides a guide for assessing if information is sensitive or classified.

- Appendix C provides the Business Impact Levels tool to assist with assessing the business impact levels of information compromise.
- Appendix E provides a guide for the application of dissemination limiting markers.

### 5.3.1 Over classification

Information asset owners should balance the needs and expectations of DCJ, the wider government and community to protect information and ensure appropriate access. Over classification of information can result in access to information being unnecessarily limited or delayed, increased administrative time and costs, and classifications being devalued or ignored. Security classifications must also not be applied as an effort to restrain competition, hide violations or inefficiencies of legal or administrative processes, or prevent or delay the release of information that does not need protection.

### 5.3.2 Changing sensitivity or classification

The information asset owner is the only person permitted to change the sensitivity or security classification applied to information. If a classification is considered inappropriate, the information asset owner should be queried and review their classification.

Information should not be downgraded to a lower classification without undergoing a formal declassification effort sponsored by the information asset's delegated owner. The owner of the information must determine whether the information can be moved to a lower classification based upon the definitions of the classifications.

## 5.4 Secure information use

Information must be managed according to the requirements of its classification, as per *Appendix D – Management of Sensitive and Classified Information* and additionally supported by the Data Privacy & Protection Standard. This includes use, storage, carriage, transfer and disposal for classifications of OFFICIAL up to sensitive and security classified information.

DCJ subscribes to a clear desk and clear screen principle, by which all information of a sensitive nature must not be left unattended whether working from home or in any other location.

### 5.4.1 Use

An approved user should not discuss or view highly sensitive information in public locations susceptible to eavesdropping



### 5.4.2 Storage

An approved user should:

- follow a clear desk and clear screen principle, by which all information of a sensitive nature must not be left unattended whether working from home or in any other location.
- store all sensitive physical information in locked cabinets or within document filing rooms when not in use — if the information is no longer required, the documents must be destroyed by placing in secure disposal bins or by shredding
- lock IT devices when not in use

### 5.4.3 Carriage (including off-site and remote working)

Information with a DLM or security classification can only be removed from DCJ premises (including for offsite and remote working) on the following conditions:

- if the information is in a physical form (e.g. hardcopy document) prior written approval must be obtained from the appropriate manager
- if the information is in electronic form (e.g. data file) it can only be downloaded to external media / devices using approved technologies, otherwise prior written approval must be obtained from the appropriate manager.

An approved user working off-site/remotely should:

- refrain from taking physical information off-site wherever possible
- protect devices from unauthorised access by storing them securely when not in use (in line with storage requirements stated above and within Appendix D).
- consider their location and who else may be watching
- not share devices or logins and password information with others (including people in their household).
- physical information should be brought back to the office for appropriate destruction (in line with the disposal requirements stated below and within Appendix D). Do not dispose of DCJ physical information in domestic garbage or recycling bins.

### 5.4.4 Transfer

Information with a DLM or security classification can only be removed from DCJ premises with the appropriate authorisation and where the confidentiality, integrity, and availability of the information can be reasonably assured.

### 5.4.5 Disposal

Destruction of media must be in compliance with the *State Records Act 1998* and the relevant disposal authority relating to the information. A link to the various

State Archives & Records disposal authorities as they relate to DCJ information can be found at the following link:

<https://www.records.nsw.gov.au/recordkeeping/rules/retention-disposal-authorities>.

Personnel must also comply with the directives identified within the DCJ Data Privacy and Protection Standard.

## 5.5 Sharing information

The NSW Government establishes that government information is to be open to the public. Information that must be released to the public is classified as 'open access information' in accordance with the obligations of the GIPA Act which mandates the publication of open access information unless there is an overriding public interest against disclosure. These include DCJ policy documents, register of government contracts and agency information guide.

All documents that are considered to be open access information must be first approved by a director or above.

When sharing or disclosing information with an external entity, contracted non-government organisation, or other NSW Government agency as mandated by law such as a subpoena or search warrant, or there are reasonable grounds to believe the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person, appropriate privacy and security consideration should be given to the disclosure. The requirements for ensuring the security of the information to be disclosed must be directly proportional to the sensitivity of the information and level of risk imposed by the sharing arrangement. Advice should be sought from Legal where there are any concerns about the lawfulness of a disclosure of information at [infoandprivacy@dcj.nsw.gov.au](mailto:infoandprivacy@dcj.nsw.gov.au).

## 5.6 Outsourcing information

The outsourcing of DCJ information systems must undergo a vendor risk assessment to appropriately ensure risks are managed prior to the information system being outsourced and the classification of the data residing in the outsourced solution. To conduct a vendor risk assessment, the user should contact the CRAC team ([securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au))

All outsourcing or sharing contracts/agreements:

- must contain clauses that indicate the relevant entity will take all steps necessary to comply with State and Commonwealth privacy legislation as appropriate
- must have contemporary non-disclosure clauses which protect the privacy and confidentiality of DCJ information.

- must contain clause that require the entity and its subcontractors to work with DCJ collaboratively in the investigation, management and resolution (including reporting where required to the Information Commissioner and impacted individuals).
- the clause must clearly state that a copy of any exfiltrated data is to be provided to DCJ within a reasonable time frame.
- should be monitored regularly to ensure requirements are being met.

Where an external party is engaged to manage the transmission or storage of DCJ information, the arrangement for the collection, storage, access, use and disclosure of information must be in compliance with the *Privacy and Personal Information Protection Act 1998*, the *Government Information (Public Access) Act 2009* and the *State Records Act 1998* and procedures identified within the DCJ Data Privacy and Protection Standard.

DCJ information must not be stored outside Australia without a security risk assessment being performed, including consideration as to appropriate contractual clauses being in place and written consent from DCJ for all new solutions.

## 5.7 Artificial Intelligence

AI (Artificial Intelligence) is intelligent technology, programs and the use of advanced computing algorithms that can augment decision making by identifying meaningful patterns in data. The user should be mindful when utilising tools with natural language processing capabilities, such as OpenAI's ChatGPT. While these tools can provide assistance and improvement to tasks such as technical or conversational writing, or answering general enquiries, considerable human involvement is necessary to ensure the accuracy and reliability of responses. User should also be mindful of the data classification and associated restrictions on any DCJ data they intend to upload into these tools. Personal information should not be included in these tools.

Any user of an AI-based technology must be aware of its limitations and risks, and always consider potential implications to the security and privacy of data and systems

## 5.8 Protection of data and information

Data Breach Leakage and Data Leakage Prevention measures must be included to ensure that DCJ data and information is appropriately protected from unauthorised distribution or accidental or malicious loss.

## 5.9 Protection of records

Standards for record retention, storage, handling, and disposal must comply with the *State Records Act 1998* for applicable information. The relevant disposal authority for this type of information must be defined and disseminated.

Should DCJ enter into a contract with an external entity which results in the transfer of devices to the external party, DCJ must:

- ensure all information as appropriate is stored in a records management repository prior to being wiped
- wipe the devices in line with the requirements from the data privacy and protection standard to ensure configuration files and information are not inadvertently provided to the external party.

## 6 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 7 Related legislation, regulation and other documents

This policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *State Records Act 1998*

## 8 Document information

Document name	Data Privacy and Protection Policy
Document reference	D22/1832020
Replaces	Data Privacy and Protection Policy V2.2
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/2023

## 9 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

If you need assistance identifying when you need to engage information security, please see [Appendix – Engaging information security](#).

10 Version and review details

Version	Effective date	Reason for amendment	Due for review
2.2	29/06/2022	Annual review due	29/06/2023
3.0	28/09/2023	Annual review Transferred to new DCJ Document Template and minor edits	28/09/2024

## 11 Appendix A – Engaging information security

The following questionnaire can be used to help you determine when you need to engage Cyber Risk Audit and Compliance team

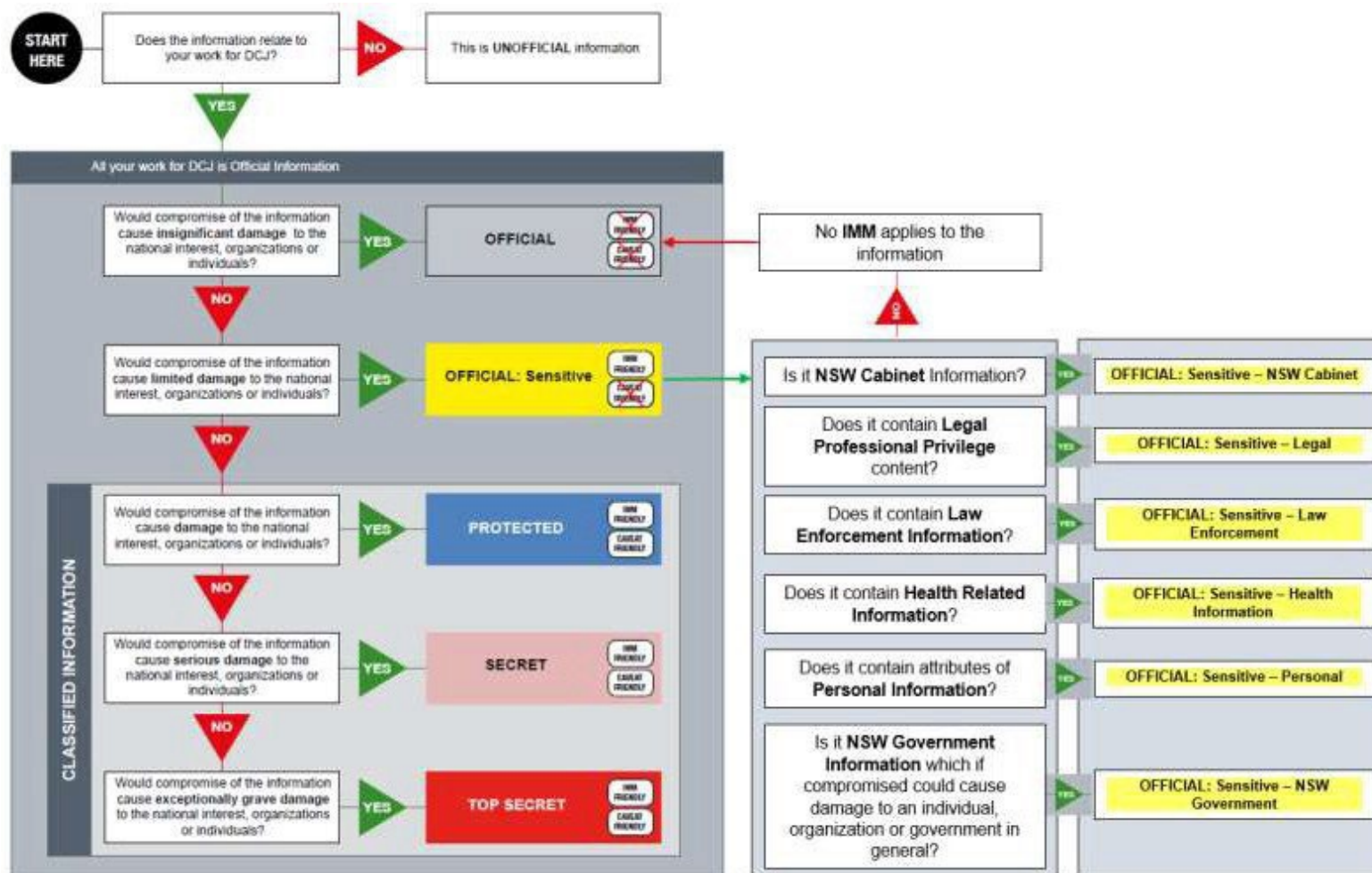
- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Have you become aware of a data breach and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party and require advice about whether this is lawful or require advice about an ICT risk assessment?
- If you answer yes to any of the above or related legal advice, please email:
- **CRAC:** [Securityarchitecture@fac.s.nsw.gov.au](mailto:Securityarchitecture@fac.s.nsw.gov.au)
- **Legal:** [Infoandprivacy@justice.nsw.gov.au](mailto:Infoandprivacy@justice.nsw.gov.au)

## 12 Appendix B – How to assess sensitive and classified information



## 13 Appendix C – Business Impacts Levels (BILs) tool

Impact Category	OFFICIAL	Sensitive information	Security classified information		
		DLM with prefix: OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
Business Impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Description	Most official information created or processed by the public sector. This includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would result in no or insignificant damage to individuals, organisations or government.	OFFICIAL information that due to its sensitive nature requires limited dissemination. Information with a prefix of OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM), indicating compromise of the information would result in limited damage to an individual, organisation or government.	Valuable, important and sensitive information. Compromise of PROTECTED information would be expected to cause damage to the national interest, organisations or individuals.	Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the national interest, organisations or individuals.	The most valuable, important and sensitive information. Compromise of TOP SECRET information would be expected to cause exceptionally grave damage to the national interest, organisations or individuals.
Potential impact on individuals from compromise of the information					



Impact Category	OFFICIAL	Sensitive information	Security classified information		
		DLM with prefix: OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
<b>Dignity or safety of an individual (or those associated with the individual)</b>	<p>Information from routine business operations and services.</p> <p>Can include personal information but excludes sensitive information as defined under the <i>Privacy Act</i> (Cth).</p> <p>Note: NSW privacy legislation (HRIPA and PPIPA) do not have a definition for sensitive information.</p>	<p>Limited damage to an individual is:</p> <ul style="list-style-type: none"> <li>a. potential harm, for example injuries that are not serious or life threatening or</li> <li>b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is not life threatening.</li> </ul>	<p>Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially <b>significant harm or potentially life-threatening injury</b>.</p>	<p>Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to <b>directly threaten or lead to the loss of life of an individual or small group</b>.</p>	<p>Exceptionally grave damage is:</p> <ul style="list-style-type: none"> <li>a. widespread loss of life</li> <li>b. discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.</li> </ul>
<b>Potential impact on organisations from compromise of the information</b>					
<b>Entity operations, capability and service delivery</b>	<p>Information from routine business operations and services.</p>	<p>Limited damage to entity operations is:</p> <ul style="list-style-type: none"> <li>a. a degradation in organisational capability to an extent and duration that, while the <b>entity can perform its primary functions</b>, the effectiveness of the</li> </ul>	<p>Damage to entity operations is:</p> <ul style="list-style-type: none"> <li>a. a degradation in, or loss of, organisational capability to an extent and duration that the <b>entity cannot perform one or more of its primary functions</b></li> </ul>	<p>Serious damage to entity operations is:</p> <ul style="list-style-type: none"> <li>a. a severe degradation in, or loss of, organisational capability to an extent and duration that the <b>entity cannot perform any of its functions</b></li> </ul>	<p>Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.</p>

Impact Category	OFFICIAL	Sensitive information	Security classified information		
		DLM with prefix: OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
		functions is noticeably reduced b. minor loss of confidence in government.	b. major loss of confidence in government.	b. directly threatening the internal stability of Australia.	
<b>Entity assets and finances, e.g. operating budget</b>	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to <b>\$10 million to \$100 million.</b>	Damage is: a. substantial financial loss to an entity b. <b>\$100 million to \$10 billion</b> damage to entity assets.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.
<b>Legal compliance, e.g. information compromise would cause non-compliance with legislation, commercial confidentiality or legal professional privilege</b>	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal professional privilege for communications between legal practitioners and their clients b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation	Damage is: a. failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.

Impact Category	OFFICIAL	Sensitive information	Security classified information		
		DLM with prefix: OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
		resulting in less than two years' imprisonment.			
Compiled data	A compilation of routine business information.	A significant compiled holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	A significant compiled holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant compiled holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant compiled holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.
<b>Potential impact on government or the national interest from compromise of the information</b>					
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a. impeding the development or operation of major policies	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.

## 14 Appendix D – Management of sensitive and classified information

Category		DCJ Requirements
<b>UNOFFICIAL</b>		
Protective Marking	Nil	
Access & Clearance Requirement	Nil	
Use	Nil	
Storage	Nil	
Carriage	Nil	
Transfer	Nil	
Disposal	Nil	
<b>OFFICIAL</b>		

Category	DCJ Requirements
Protective Marking	<b>No specific requirement</b> to apply text-based or colour-based markings. If protective markings are applied should be marked in accordance with recommendations outlined in Appendix B (i.e. <b>OFFICIAL</b> ) located at the centre top and bottom of each page.
Access & Clearance Requirement	Need to know and no security clearance requirements.
Use	For regular or occasional ongoing home-based or off-site work (e.g. other offices, café etc), apply storage and carriage requirements and exercise judgement to assess risk.
Storage	<ul style="list-style-type: none"> <li>• Can be left unattended at DCJ facilities if in a secured state and subject to DCJ clear desk procedure.</li> <li>• Store in a lockable container when unattended.</li> <li>• For regular ongoing home-based work, <b>it is recommended</b> to install a Class C container or higher.</li> <li>• For occasional home-based work, store in a lockable container and apply carriage requirements.</li> </ul>
Carriage	<ul style="list-style-type: none"> <li>• Inside DCJ facilities <b>it is recommended</b> to carry in an opaque envelope or folder that avoids unnecessary disclosure or visibility.</li> <li>• Outside DCJ facilities carry in an opaque or sealed envelope, container, pouch or satchel.</li> </ul>
Transfer	<ul style="list-style-type: none"> <li>• Inside DCJ facilities transfer by hand, safe hand or internal mail and apply carriage requirements.</li> <li>• Outside DCJ facilities transfer by hand, safe hand, external mail or courier and apply carriage requirements.</li> </ul>
Disposal	<ul style="list-style-type: none"> <li>• Dispose using any class of shredder or secure disposal bin.</li> </ul>
<b>OFFICIAL: SENSITIVE</b>	

Category	DCJ Requirements
Protective Marking	<b>No specific requirement</b> to apply text-based or colour-based markings. If protective markings are applied should be marked in accordance with recommendations outlined at Appendix B (i.e. <b>OFFICIAL: Sensitive</b> ) located at the centre top and bottom of each page.
Access Clearance Requirement	Need to know and no security clearance requirements.
Use	For regular or occasional ongoing home-based or off-site work (e.g. other offices, café etc), apply storage and carriage requirements and exercise judgement to assess risk.
Storage	<ul style="list-style-type: none"> <li>• Can be left unattended at DCJ facilities if in a secured state and subject to DCJ clear desk procedure.</li> <li>• Store in a lockable container when unattended.</li> <li>• For regular ongoing home-based work, <b>it is recommended</b> to install a Class C container or higher.</li> <li>• For occasional home-based work, store in a lockable container and apply carriage requirements.</li> </ul>
Carriage	<ul style="list-style-type: none"> <li>• Inside DCJ facilities <b>it is recommended</b> to carry in an opaque envelope or folder that avoids unnecessary disclosure or visibility.</li> <li>• Outside DCJ facilities carry in an opaque or sealed envelope, container, pouch or satchel.</li> </ul>
Transfer	<ul style="list-style-type: none"> <li>• Inside DCJ facilities transfer by hand, safe hand or internal mail and apply carriage requirements.</li> <li>• Outside DCJ facilities transfer by hand, safe hand, external mail or courier and apply carriage requirements.</li> </ul>
Disposal	<ul style="list-style-type: none"> <li>• Dispose using any class of shredder or secure disposal bin.</li> </ul>
PROTECTED	

Category	DCJ Requirements
Protective Marking	Apply text-based or colour-based markings in accordance with recommendations outlined at Appendix B (i.e. <b>PROTECTED</b> ) located at the centre top and bottom of each page.
Access & Clearance Requirement	Need to know and Baseline security clearance required
Use	<ul style="list-style-type: none"> <li>• Can only be used in DCJ facilities.</li> <li>• For regular ongoing home-based work, apply storage and carriage requirements and conduct a risk assessment of proposed work environment.</li> <li>• For occasional home-based work, apply storage and carriage requirements and exercise judgement to assess risk.</li> <li>• <b>It is not recommended</b> to use for other off-site work (e.g. other offices, café etc). If required, apply storage and carriage requirements and exercise judgement to assess risk.</li> </ul>
Storage	<ul style="list-style-type: none"> <li>• Can be left unattended at DCJ facilities if in a secured state and subject to DCJ clear desk procedure.</li> <li>• Store in a Class C container or higher when unattended.</li> <li>• For regular ongoing home-based work, storage is permitted if Class C container or higher is installed.</li> <li>• For occasional home-based work, store in a lockable container, apply carriage requirements and exercise judgement to assess risk.</li> </ul>
Carriage	<ul style="list-style-type: none"> <li>• Always retain in personal custody.</li> <li>• Inside DCJ facilities carry in an opaque envelope or folder that indicates classification.</li> <li>• Outside DCJ facilities carry in a security briefcase, pouch or satchel and <b>it is recommended</b> to place in tamper-evident packaging.</li> </ul>
Transfer	<ul style="list-style-type: none"> <li>• Inside DCJ facilities transfer by hand or safe hand and apply carriage requirements.</li> </ul>

Category	DCJ Requirements
	<ul style="list-style-type: none"> <li>Outside DCJ facilities apply carriage requirements and transfer by hand, safe hand or safe hand courier and apply carriage requirements.</li> <li>Transfer requires a receipt.</li> </ul>
Disposal	Dispose using a Class B shredder.
<b>SECRET</b>	
Protective Marking	Apply text-based or colour-based markings in accordance with recommendations outlined at <i>6.4 Application of Disseminating Limiting Markers</i> (i.e. <b>SECRET</b> ) located at the centre top and bottom of each page.
Access & Clearance Requirement	Need to know & Negative Vetting Level 1 security clearance required.
Use	<ul style="list-style-type: none"> <li>Can only be used in restricted access areas within DCJ facilities (i.e. Zones 3-5).</li> <li><b>It is not recommended</b> to use outside DCJ facilities. If required, obtain written approval from Corporate Security, conduct a security risk assessment and exercise judgement in use.</li> </ul>
Storage	<ul style="list-style-type: none"> <li>Can be left unattended at DCJ facilities if in a secured state and subject to DCJ clear desk procedure.</li> <li>Store in a Class B container or higher when unattended.</li> <li><b>It is not recommended</b> to store outside DCJ facilities. If required, apply carriage requirements, retain in personal custody or store in Class B container or higher and return to DCJ facility as soon as practicable.</li> </ul>
Carriage	<ul style="list-style-type: none"> <li><b>Always retain</b> in personal custody.</li> <li>Inside DCJ facilities carry in an opaque envelope or folder that indicates classification.</li> </ul>



Category	DCJ Requirements
	<ul style="list-style-type: none"> <li>Outside DCJ facilities carry in a security briefcase, pouch or satchel and <b>it is recommended</b> to place in tamper-evident packaging.</li> </ul>
Transfer	<ul style="list-style-type: none"> <li>Inside DCJ facilities transfer by hand or safe hand and apply carriage requirements.</li> <li>Outside DCJ facilities apply carriage requirements and transfer by safe hand, safe hand courier or DFAT courier.</li> <li>Transfer requires a receipt.</li> </ul>
Disposal	Dispose using a Class A shredder.
<b>TOP SECRET</b>	
Protective Marking	Apply text-based or colour-based markings in accordance with recommendations outlined at Appendix B (i.e. <b>TOP SECRET</b> ) located at the centre top and bottom of each page.
Access & Clearance Requirement	Need to know and Negative Vetting Level 2 or Positive Vetting security clearance required.
Use	<ul style="list-style-type: none"> <li>Can only be used in restricted access areas within DCJ facilities (i.e. Zones 3-5).</li> <li><b>Do not</b> use outside DCJ facilities.</li> </ul>
Storage	<ul style="list-style-type: none"> <li>Can be left unattended at DCJ facilities if in a secured state and subject to DCJ clear desk procedure.</li> <li>Store in a Class B container or higher when unattended.</li> <li><b>Do not</b> store outside DCJ facilities.</li> </ul>
Carriage	<ul style="list-style-type: none"> <li><b>Always retain</b> in personal custody.</li> <li>Inside DCJ facilities carry in an opaque envelope or folder that indicates classification.</li> </ul>

Category	DCJ Requirements
	<ul style="list-style-type: none"><li>• <b>It is not recommended</b> to carry outside DCJ facilities. If required, obtain written approval from Corporate Security and carry in an opaque envelope or folder that indicates classification.</li></ul>
Transfer	<ul style="list-style-type: none"><li>• Inside DCJ facilities transfer by hand or safe hand and apply carriage requirements.</li><li>• Outside DCJ facilities apply, obtain written approval from CRAC Team and apply carriage requirements.</li><li>• Transfer requires a receipt.</li></ul>
Disposal	<ul style="list-style-type: none"><li>• Dispose using a Class A shredder.</li><li>• Destruction must be supervised and documented in Auditable register.</li></ul>

## 15 Appendix E – Application of Dissemination Limiting Markers (DLMs)

Once information has been classified, the appropriate Disseminating Limiting Marker (DLM) should be applied to the information through text-based or colour-based protective markings.

### Text-Based Protective Markings

It is preferable for text-based protective markings to be applied to easily identify sensitive and security classified information. To achieve this, it is recommended that text-based protective markings:

- are in capital letters with bold text. These should be in a large font with a distinctive colour, ideally red (e.g. **PROTECTED**).
- are at the centre top and bottom of each page.
- have a double forward slash between separate markings to help clearly differentiate each marking.

### Other Applications of Protective Markings

If text-based markings cannot be used, the following colour based markings must be used to indicate a documents security classification.

Protective Marking	Colour Based Marking
<b>UNOFFICIAL</b>	None required
<b>OFFICIAL</b>	None Required
<b>OFFICIAL: Sensitive</b>	Yellow
<b>PROTECTED</b>	Blue
<b>SECRET</b>	Pink
<b>TOP SECRET</b>	Red

Appendix B provides practical guidance on the application of protective markings to information in accordance with its sensitivity or security classification.

DCJ must apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process, or communicate sensitive or security classified information.



# Data Privacy and Protection Standards

---

## Table of contents

1	Purpose.....	2
2	Definitions.....	2
3	Scope.....	3
4	Privacy and protection standards .....	3
4.1	Principles .....	3
4.2	DLM .....	4
4.3	Security classification .....	5
4.4	Applying labels .....	6
4.5	Storage protection mechanisms .....	7
4.6	Secure information use and transfer .....	8
4.7	Information sharing and sourcing .....	10
4.8	Protection of data and information .....	11
4.9	Secure destruction .....	12
5	Monitoring, evaluation and review .....	13
6	Related legislation, regulation and other documents.....	13
7	Document information .....	13
8	Support and advice .....	13
9	Version and review details .....	13
10	Appendix 1 - Decision making tool for NSW DLMs.....	14

[OBJ]

The red highlighted box shows where this document sits within the Information Security Policy Suite.

## 1 Purpose

The following standard articulates the Department of Communities and Justice’s (DCJ’s) data privacy and protection standards in regard to the Data Privacy and Protection Policy.

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Classified information / security classification	Classified information refers to information that aligns to the Federal Government classification system. The Australian Government uses three security classifications: PROTECTED, SECRET and TOP SECRET. The relevant security classification is based on t`he likely damage resulting from compromise of the information's confidentiality. Where compromise of the information's confidentiality would cause limited damage but does not warrant a security classification, that information is considered sensitive, and a DLM would apply (a DLM is not a classification).
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.

Term	Definition
Outsourcing	Outsourcing includes any commercial arrangement where an external party stores, transfers, uses or creates DCJ information and data. This is however separate from an information sharing venture.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.

### 3 Scope

The requirements and expectations outlined in this document applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information (including personal information and de-identified information)
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This standard will be used by staff who are responsible for the design, administration, support and hosting of DCJ information systems.

This standard does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

## 4 Privacy and protection standards

### 4.1 Principles

Ref	Directive
PRI-001	All information which is not work related is considered UNOFFICIAL and <b>MUST</b> be labelled UNOFFICIAL

Ref	Directive
PRI-002	Information which is work related but does not have security or sensitivity issues is considered OFFICIAL with no applicable dissemination limiting marker (DLM). Official information <b>MAY</b> have the 'OFFICIAL' label applied, however this is not required.
PRI-003	OFFICIAL: Sensitive – X where 'X' is a NSW DLM <b>SHOULD</b> be used when its compromise may cause limited damage to individuals, organisations or the government. Information with this label <b>SHOULD</b> only be provided to people who have a need to know.
PRI-004	Material that may contain sensitive information needs to be labelled and managed according to the level/type of sensitivity. Sensitive material includes information that: <ul style="list-style-type: none"> <li>• identifying a person</li> <li>• is health information</li> <li>• is legally sensitive</li> <li>• is law enforcement sensitive</li> <li>• relates to NSW Cabinet</li> <li>• if released publicly could have an adverse effect</li> </ul>
PRI-005	Information that does not meet the criteria for security classification, but which requires some level of protection can be labelled with DLM to indicate the level/type of sensitivity.

## 4.2 DLM

The following six DLMs may be used as appropriate within DCJ to describe the type of sensitivity of the information. Please note Appendix 1 provides a decision chart to help you appropriately apply DLM's.

Ref	Directive
DLM-001	<b>OFFICIAL: Sensitive – NSW Cabinet SHOULD</b> be applied to sensitive NSW Government Cabinet documents, including: <ul style="list-style-type: none"> <li>• all official records of the NSW Government Cabinet including Cabinet agendas, Cabinet submissions, Cabinet Minutes, advice on Cabinet Minutes and Cabinet decisions</li> <li>• any other information that would reveal or prejudice: <ul style="list-style-type: none"> <li>• the deliberations or decisions of the NSW Government Cabinet</li> <li>• the position that a particular Minister has taken or may take on a matter in the NSW Cabinet</li> <li>• drafts, copies or extracts of the above documents.</li> </ul> </li> </ul>

Ref	Directive
DLM-002	<p><b>OFFICIAL: Sensitive – Legal SHOULD</b> be used for any information that may be subject to legal professional privilege or:</p> <ul style="list-style-type: none"> <li>• <i>Legal Professional Act 2004</i></li> <li>• <i>Legal Professional Regulation 2005</i></li> <li>• <i>Evidence Act 1995</i></li> <li>• <i>Criminal Procedure Act 1986</i></li> <li>• NSW Barristers Rules.</li> </ul>
DLM-003	<p><b>OFFICIAL: Sensitive – Law Enforcement SHOULD</b> be applied by law enforcement agencies and is to be used for law enforcement activities. It denotes that the information was compiled for law enforcement purposes and <b>SHOULD</b> be afforded appropriate security in order to protect certain legitimate government interest, including enforcement proceedings, the right of a person to a fair trial, policing and community safety practices, proprietary information or to protect a confidential source.</p>
DLM-004	<p><b>OFFICIAL: Sensitive – Health Information SHOULD</b> be applied to health information as defined by the <i>Health Records and Information Privacy Act 2002</i> Section 6 definition of “health information”.</p>
DLM-005	<p><b>OFFICIAL: Sensitive – Personal SHOULD</b> be used with security classified or unclassified information that contains attributes of personal information as defined in the <i>Privacy and Personal Information Protection Act 1998</i>.</p>
DLM-006	<p><b>OFFICIAL: Sensitive – NSW Government SHOULD</b> be used when the compromise of the information could cause limited damage or damage to the NSW Government, commercial entities or members of the public.</p> <p>For instance, where compromise could:</p> <ul style="list-style-type: none"> <li>• endanger individuals and/or private entities</li> <li>• work substantially against state or national finances or economic and commercial interests</li> <li>• substantially undermine the financial viability of major organisations</li> <li>• impede the investigation or facilitate the commission of serious crime</li> <li>• seriously impede the development or operation of major government policies.</li> </ul>

### 4.3 Security classification

Before applying a security classification, [recordsmanagementcompliance@facs.nsw.gov.au](mailto:recordsmanagementcompliance@facs.nsw.gov.au) must be contacted to discuss the information and the required security controls.

Ref	Directive
SEC-001	PROTECTED security classification <b>SHOULD</b> be applied and labelled.



	Personnel who access information that is classified at a level of PROTECTED or above <b>SHOULD</b> be security-vetted. Information <b>SHOULD</b> be labelled PROTECTED when compromise of the confidentiality of information could be expected to cause damage to national interest, organisations or individuals.
SEC-002	Information <b>SHOULD</b> be labelled SECRET when compromise of the confidentiality of information could be expected to cause serious damage to corresponding national interest, organisations, or individuals.
SEC-003	Information <b>SHOULD</b> be labelled TOP SECRET when compromise of the confidentiality of information could be expected to cause exceptionally grave damage.

#### 4.4 Applying labels

Ref	Directive
LAB-001	Label sensitive or security classified information at the time of collection or creation.
LAB-002	<p>Where a document has multiple types of information, or information that fits more than one DLM or security classification, the document <b>MUST</b> be labelled and/or classified as per the information of the highest level of sensitivity within that document.</p> <p>E.g. most health information contains information about health as well as personal information and this <b>SHOULD</b> be labelled as OFFICIAL: Sensitive – Health Information.</p> <p>Refer to:</p> <ul style="list-style-type: none"> <li>The <b>NSW Government Information Classification Labelling and Handling Guidelines</b> for more information <a href="https://data.nsw.gov.au/nsw-government-information-classification-labelling-and-handling-guidelines/sensitive-information">https://data.nsw.gov.au/nsw-government-information-classification-labelling-and-handling-guidelines/sensitive-information</a></li> <li><b>Appendix 1 - Decision making tool for NSW DLMs</b> to help determine which label to use</li> </ul>
LAB-003	<p>When composing an email, the subject <b>SHOULD</b> be prefixed with a label (if appropriate) e.g. OFFICIAL: Sensitive - Personal, to indicate the protective requirements of the email body and or attachments.</p> <p>Note: 'Sensitive' can only be used in conjunction with a NSW DLM – not by itself.</p>
LAB-004	Within a document, labels <b>SHOULD</b> be applied at the centre of the top and bottom of each page. The label <b>SHOULD</b> be in bold text and a minimum of 5mm high, preferably in red.
LAB-005	The label applied to a file cover/container/binder <b>MUST</b> be at least equal to the label of the most sensitive item within the collection.

Ref	Directive
LAB-006	Electronic and other documents <b>SHOULD</b> include their sensitivity label in their metadata as appropriate.
LAB-007	The delegated owner or custodian <b>MUST</b> periodically review the information assets classification to determine whether the information classification should be changed. If required, the delegated owner <b>SHOULD</b> advise of any changes that need to be made.

#### 4.5 Storage protection mechanisms

Ref	Directive
SPM-001	<p>All users <b>SHOULD</b>:</p> <ul style="list-style-type: none"> <li>• follow a clear desk and clear screen principle, by which all information of a sensitive nature must not be left unattended whether working from home or in any other location.</li> <li>• store all sensitive physical information in locked cabinets or within document filing rooms when not in use — if the information is no longer required, the documents must be destroyed by placing in secure disposal bins or by shredding</li> <li>• lock IT devices when not in use</li> <li>• not download or save DCJ data on personal devices unless it is on an approved BYO service such as DCJ Citrix portal or Office Web Access.</li> </ul>
SPM-002	<p>Minimum controls for Sensitive and above information include:</p> <ul style="list-style-type: none"> <li>• <b>MUST</b> be provided only to authorised staff with a genuine need to know.</li> <li>• <b>MUST</b> be protected by physical controls which limit access to documents and or hardware.</li> <li>• Digital audit trails <b>SHOULD</b> be available to identify access, creation, deletion and modification of information.</li> <li>• Multifactor authentication to external digital information repositories <b>SHOULD</b> be considered.</li> <li>• Digital repositories <b>SHOULD</b> not be directly connected to external networks, perimeter controls <b>MUST</b> be in place to mediate connections and access.</li> <li>• Encryption at rest <b>MUST</b> be considered for external digital information repositories or whenever dealing with sensitive information or where the threat of confidentiality breach is elevated.</li> </ul>
SPM-003	OFFICIAL: Sensitive – NSW Cabinet documents <b>SHOULD</b> be stored and managed within the eCabinet online portal.
SPM-004	Handling of OFFICIAL: Sensitive – NSW Cabinet documents <b>MUST</b> be compliant with the NSW Ministerial Handbook.

Ref	Directive
SPM-005	Non-disclosure of OFFICIAL: Sensitive – Legal documents <b>MUST</b> be observed to preserve client privilege.
SPM-006	Sharing of OFFICIAL: Sensitive – Law Enforcement documents is prohibited unless approval from the Law Enforcement information owner is obtained and recorded as this may impact upon an investigation or legal matter.
SPM-007	User access reviews and or access monitoring <b>MUST</b> be conducted on pertinent sensitive information.
SPM-008	Corporate mobile computing devices (tablets, smart phones, laptops etc.) <b>MUST</b> be encrypted.

#### 4.6 Secure information use and transfer

Ref	Directive
SIU-001	Approved users should not discuss or view sensitive information in public locations susceptible to eavesdropping
SIU-002	Information with a DLM or security classification <b>MUST</b> only be removed from DCJ premises on the following conditions: <ul style="list-style-type: none"> <li>if the information is in a physical form (e.g. hardcopy document) prior written approval must be obtained from the appropriate manager</li> <li>if the information is in electronic form (e.g. data file) it can only be downloaded to external media / devices using approved technologies, otherwise prior written approval must be obtained from the appropriate manager.</li> </ul>
SIU-003	Minimum controls for sensitive and above information include: <ul style="list-style-type: none"> <li>Dissemination and use of information <b>MUST</b> be for authorised purposes.</li> <li>Sensitive information <b>SHOULD NOT</b> be given over the phone unless the caller's identity has been confirmed and the caller has a right to know.</li> <li>Physical transfer of records externally <b>MUST</b> be executed by DCJ staff or reputable couriers. The information <b>MUST</b> be stored within a sealed opaque envelope or similar. No classification or DLM markings are to be displayed on the envelope.</li> <li>Storage of digital information on USBs <b>SHOULD</b> be encrypted: <ul style="list-style-type: none"> <li>where the USB device is used for an appropriate business process and remains within the confines of a DCJ premises the data may be unencrypted unless the information has a security classification of Protected or above or other reasons to be protected from unauthorised access, for example where the information is personal or health information.</li> </ul> </li> </ul>

Ref	Directive
	<ul style="list-style-type: none"> <li>where digital information is stored on a USB device and transferred outside the confines of a DCJ premise, the data <b>MUST</b> be encrypted.</li> <li>Electronic transfer of digital information may be transferred without encryption, unless the information has a security classification of Protected or above or other reasons to be protected from unauthorised access, for example if the information does not contain personal or health information.</li> <li>Electronic transfer of large quantities of digital information or on transfers on a consistent basis or information that contains personal or health information <b>MUST</b> be encrypted in transit.</li> <li>Use of the information <b>MUST</b> be confined to the purpose for which it was provided. Any further or separate use of the information <b>MUST</b> be subject to the data owner's approval.</li> </ul>
SIU-004	OFFICIAL: Sensitive – Personal information <b>MUST</b> only be used for purposes compliant with the <i>Privacy and Personal Information Protection Act 1998</i> .
SIU-005	Copying of OFFICIAL: Sensitive – Personal information <b>MUST</b> be kept to a minimum and all copies are to be afforded the same protections as the original
SIU-006	<p>OFFICIAL: Sensitive - NSW Cabinet information <b>MUST</b> only be shared with persons who have a need to know and, where required, the recipient has explicitly acknowledged their responsibility for securing the data.</p> <p>Refer to the Premier's Memorandum for more information  <a href="https://arp.nsw.gov.au/m2006-08-maintaining-confidentiality-cabinet-documents-and-other-cabinet-conventions">https://arp.nsw.gov.au/m2006-08-maintaining-confidentiality-cabinet-documents-and-other-cabinet-conventions</a>.</p>
SIU-007	OFFICIAL: Sensitive – NSW Cabinet information <b>MUST</b> not be copied to a local hard disk or stored on removable media once it has been submitted in the eCabinet system.
SIU-008	Access to OFFICIAL: Sensitive – NSW Cabinet submissions may only be granted by the NSW Cabinet secretariat and is non-transferable.
SIU-009	All non-required records used in drafting an OFFICIAL: Sensitive – NSW Cabinet submission <b>MUST</b> be destroyed after the submission is made.
SIU-010	OFFICIAL: Sensitive – Legal Information includes privileged and/or confidential legal communications and records that <b>SHOULD</b> not be forwarded, sent or distributed, in whole or in part, including any attachments, internally or to any agency or organisation outside of DCJ without the express written permission and further advice from DCJ Legal at <a href="mailto:allocationsDCJLegal@fac.nsw.gov.au">allocationsDCJLegal@fac.nsw.gov.au</a>
SIU-011	Classified information (i.e. Protected, Secret, Top Secret) <b>MUST</b> only be transferred across networks or copied to other media where the

Ref	Directive
	confidentiality and availability of the information can be reasonably assured.
SIU-012	Classified information (i.e. Protected, Secret, Top Secret) <b>MUST</b> only be disclosed outside DCJ with appropriate authorisation.
SIU-013	Classified information (i.e. Protected, Secret, Top Secret) that commit or oblige DCJ in its business activities <b>SHOULD</b> be checked and countersigned (manually or electronically) to confirm their validity and integrity.
SIU-014	Classified information (i.e. Protected, Secret, Top Secret), including files and electronic media, <b>MUST NOT</b> be removed from DCJ premises, unless prior written approval has been granted by the appropriate manager.
SIU-015	Classified information (i.e. Protected, Secret, Top Secret) <b>MUST</b> align to requirements as specified in the Australian Government Protective Security Policy Framework.
SIU-016	Classified information (i.e. Protected, Secret, Top Secret) <b>SHOULD</b> be transferred according to the information's legal basis for sharing, classification, and the inherent handling requirements.
SIU-017	Classified information (i.e. Protected, Secret, Top Secret) <b>MUST</b> be transferred in a manner consistent with the highest classification's protective controls.
SIU-018	Bulk transfers of sensitive unique records which convey information covered by the <i>Health Records and Information Privacy Act 2002</i> or <i>Privacy and Personal Information Protection Act 1998</i> <b>MUST</b> be encrypted in transit. Intermittent transfers of singular or a limited numbers of these types of records <b>SHOULD</b> be encrypted but can be transferred without encryption as long as appropriate precautions are taken.

## 4.7 Information sharing and sourcing

Ref	Directive
ISO-001	A risk assessment <b>MUST</b> be completed prior to any third party sharing or outsourcing of information unless the sharing is mandated by law (Chapter 16A in the <i>Children and Young Persons (Care and Protection) Act 1998</i> . Contact <a href="mailto:FACSSecurityGovernance@facs.nsw.gov.au">FACSSecurityGovernance@facs.nsw.gov.au</a> to organise a risk assessment. Contact <a href="mailto:infoandprivacy@justice.nsw.gov.au">infoandprivacy@justice.nsw.gov.au</a> for advice or to conduct a privacy risk assessment on the sharing of information that contains personal or health information.
ISO-002	The risk assessment report of the third party's security controls and any identified privacy risks <b>SHOULD</b> be considered by the information owner prior to leveraging the third party's service or the transfer of information.

Ref	Directive
ISO-003	The information owner <b>MUST</b> approve of the information sharing or outsourcing prior to execution.
ISO-004	<p>When consuming cloud services, the information owner <b>MUST</b> ensure that the service provider and its subcontractors will contractually comply with the <i>NSW State Records Act 1998</i>, <i>Privacy and Personal Information Protection Act 1998</i> and any other applicable privacy laws. Additional contractual measures in relation to notification and action to be taken in response to suspected or actual data breaches concerning DCJ information will require specific contractual provisions to be inserted where relevant.</p> <p>For further information, please consult <i>Section 5.2 Contracting with cloud service providers</i> in the Cloud Security Policy.</p>
ISO-005	All DCJ documents for public release (e.g. DCJ internet pages, annual report and general awareness / information sheets etc.) <b>MUST</b> first be approved by a Director or above.
ISO-006	DCJ information <b>MUST</b> not be stored outside Australia without a security risk assessment being performed and written consent from DCJ for all new solutions.

#### 4.8 Protection of data and information

Ref	Directive
DLP-001	Data Leakage Prevention and Data Loss Prevention measures <b>MUST</b> be considered in the development of new solutions that will contain DCJ data
DLP-002	These measures <b>SHOULD</b> be reviewed regularly for all applications and systems that hold DCJ data
DLP-003	<p>The following aspects <b>MUST</b> be considered in the initial establishment and subsequent periodic reviews of these measures:</p> <ul style="list-style-type: none"> <li>• Identification and classification of data (DLM, security classification, caveat)</li> <li>• Identification of the Owner and Custodian of the data or information</li> <li>• Who is authorised to access the data, what level of access, and how they access the data</li> <li>• How is the data used, accessed, and shared between internal and external users? Will the prevention measures adversely impact DCJ business functions and cause users to find ways to circumvent them?</li> <li>• Is data encryption necessary? What type of encryption / how will it be encrypted?</li> </ul>

Ref	Directive
	<ul style="list-style-type: none"> <li>Are there any touchpoints to where the data resides that are not adequately protected? E.g. can the data be laterally accessed from a less protected server within the network</li> <li>Alerts and notifications that report on anomalies</li> <li>Consider data leakage prevention and data loss prevention when engaging contracts involving access to or sharing of DCJ data</li> </ul>

#### 4.9 Secure destruction

Ref	Directive
SED-001	All records <b>MUST</b> be retained in line with the <i>State Records Act 1998</i> and where relevant returned by any third party / vendor engaged by DCJ to DCJ in a format agreed to by DCJ at the conclusions of the engagement.
SED-002	All original records <b>MUST</b> be destroyed in line with the relevant disposal authority as defined by the <i>State Records Act 1998</i> .
SED-003	Sensitive information in physical form (paper) <b>SHOULD</b> be destroyed by shredding or via secure destruction bins or authorised destruction providers.
SED-004	Destruction of paper records <b>SHOULD</b> have the approval of the Principal Records Manager or be approved via authorised records management procedure.
SED-005	Destruction of records within Content Manager/EDRMS can only be done by the Content Manager/EDRMS Administrators.
SED-006	Digital records are to undergo sanitisation whereby the media in its entirety is overwritten at least once with a random pattern followed by a read back for verification upon disposal.
SED-007	Where digital records cannot be sanitised due to a technical preclusion of the media it is stored on, the media <b>MUST</b> be destroyed by either breaking up the media, heating the media until it has either burnt to ash or melted, or degauss the media.
SED-008	A destruction certificate <b>MUST</b> be provided if a third party vendor is destroying records on DCJ's behalf.
SED-009	Where DCJ enters into a contract with an external entity which results in the transfer of devices to the external party, ensure that: <ul style="list-style-type: none"> <li>all information as appropriate is stored in a DCJ's records management repository</li> <li>devices are wiped so that configuration files and information are not inadvertently provided to the external party.</li> </ul>

Ref	Directive
SED-010	Hard-copy classified material that requires destruction <b>MUST</b> be placed in secure (locked) destruction bins for secure disposal by approved contractors who hold a government security clearance.

## 5 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when significant new information, legislative or organisational change warrants amendments to this document.

## 6 Related legislation, regulation and other documents

This document is related to the Data Privacy and Protection Policy in that it is an implementation of the policy.

## 7 Document information

Document name	Data Privacy and Protection Standards
Document reference	D22/1832009
Replaces	Data Privacy and Protection Standards v1.2
Applies to	All staff excluding the Judiciary and NCAT Board members.
Policy administrator	Chief Information Security Officer
Approval	Chief Digital Information Officer
Approved date	28/09/2023

## 8 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

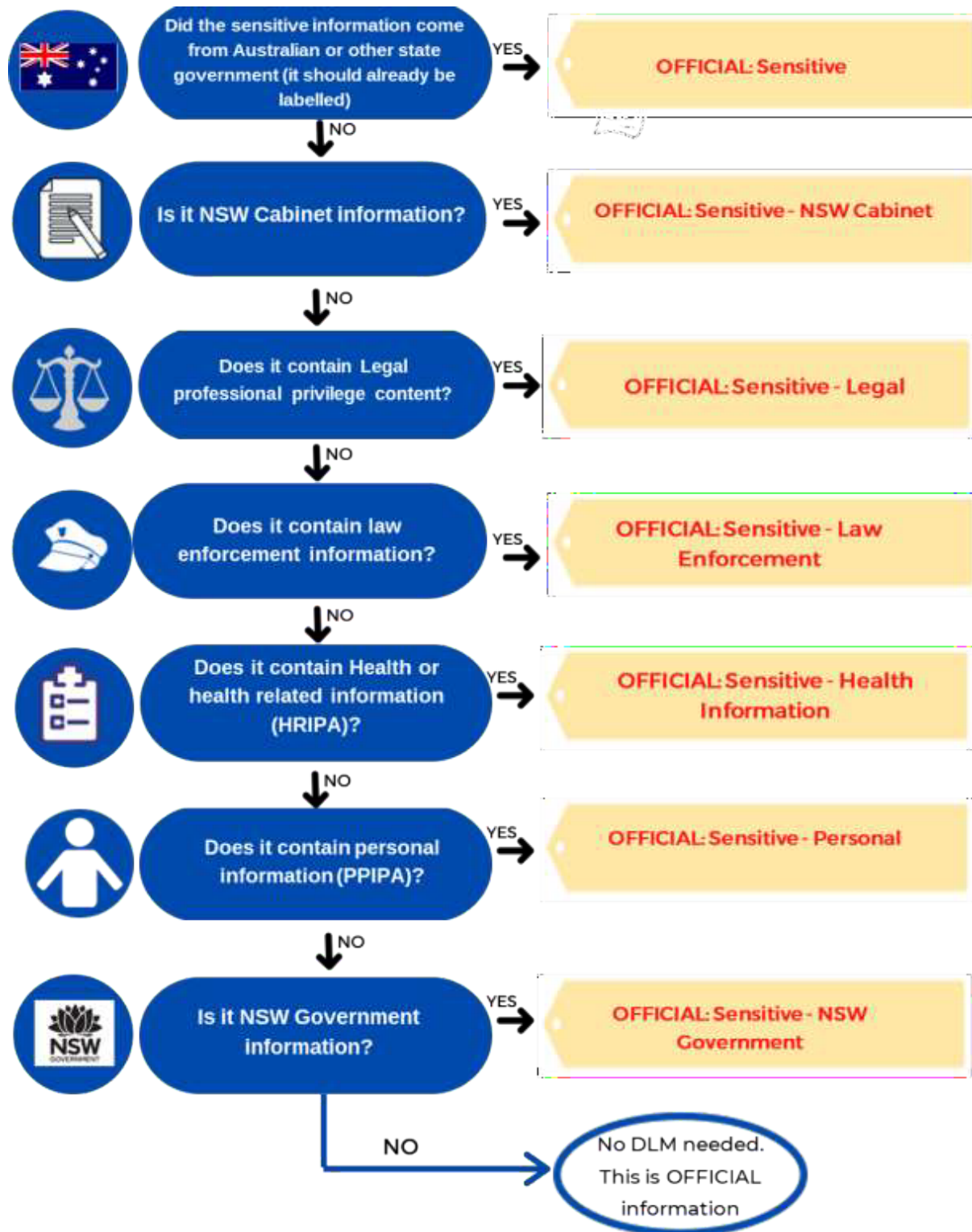
## 9 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.2	29/06/2022	Annual review due	29/06/2023
2.0	28/09/2023	Annual review	28/09/2024



## 10 Appendix 1 - Decision making tool for NSW DLMs

The flowchart below is taken from the NSW information Classification, Labelling and Handling Guidelines 2020 (<https://data.nsw.gov.au/sites/default/files/inline-images/Figure 5.JPG>)



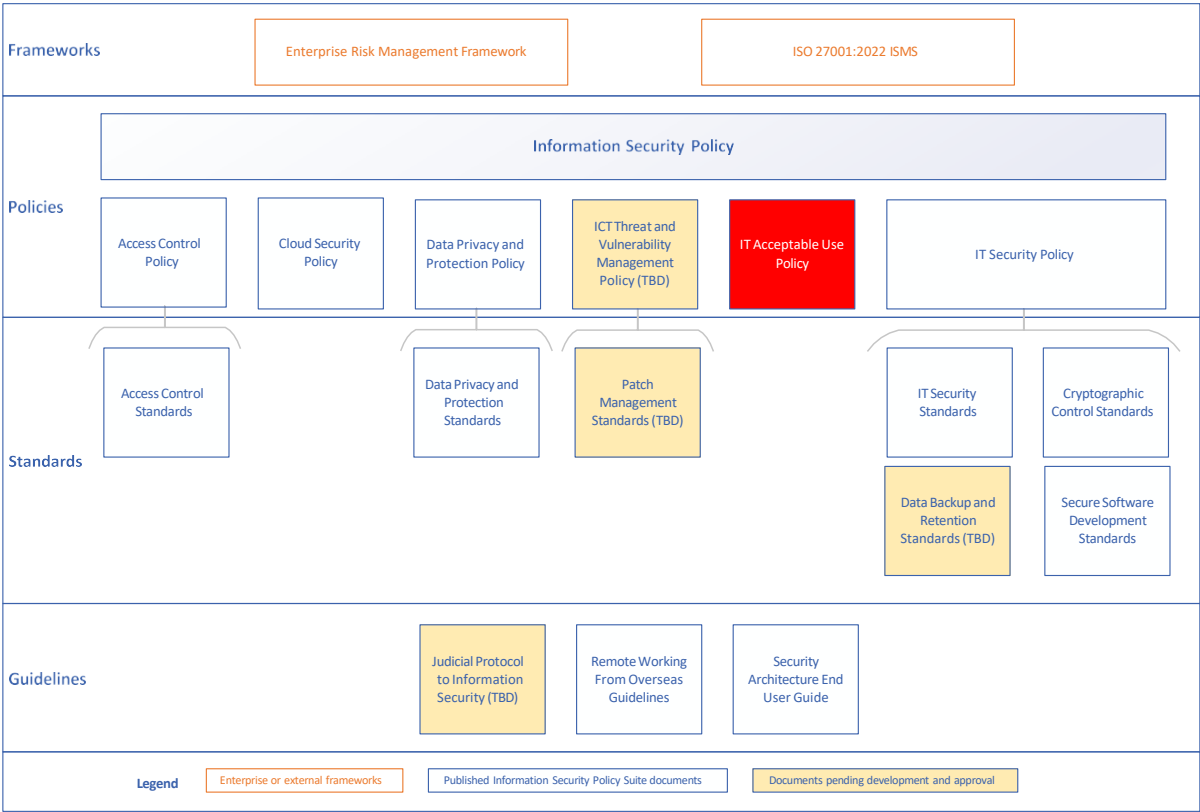


# IT Acceptable Use Policy

---

## Table of contents

1	Purpose .....	2
1.1	Related policies .....	2
2	Definitions.....	3
3	Scope.....	3
4	Policy statement .....	4
5	Policy.....	4
5.1	General use and ownership .....	4
5.2	Internet usage .....	5
5.3	Email system usage .....	6
5.4	Remote working from overseas .....	6
5.5	Monitoring and auditing .....	6
5.6	Secure use .....	7
5.7	Unacceptable use of DCJ information assets .....	9
7	Related legislation, regulation and other documents.....	10
8	Document information .....	10
9	Support and advice .....	10
10	Version and review details .....	11
11	Appendix.....	12
11.1	Engaging information security .....	12
11.2	References.....	12



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

This policy is designed to articulate the appropriate use of Department of Communities and Justice (DCJ) information and systems (information assets). It is expected that all employees, third parties, consultants and any other individual or body authorised to use DCJ information and or systems will do so in a manner which is lawful and in-line with the objectives and values of DCJ.

1.1 Related policies

This document is related to the following policies:

- [IT Security Policy](#)
- [Data Privacy and Protection Policy](#)
- [Information Security Policy](#)
- [Access Control Policy](#)
- [Cloud Security Policy](#)
- [End User Computing Policy](#)
- Code of Ethical Conduct

- DCJ Records Management Policy
- Enterprise Risk Management Policy

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information
Computing device	Any electronic device which facilitates the storage, capture, transfer, use or creation of information.
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.

## 3 Scope

The requirements and expectations outlined in the policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.

- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This policy does not apply to the Judiciary and NCAT board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

## 4 Policy statement

As the custodians of information that is politically, commercially or personally sensitive, DCJ has a duty to protect information from accidental or malicious modification, unauthorised access, use, loss or disclosure. DCJ employees and any individual or body authorised to use DCJ information and or systems, must not engage in unlawful or any other actions that contravene this policy or any other DCJ policy, either knowingly or unknowingly.

Information assets provided for or by DCJ, including but not limited to: computer equipment, software, operating systems, storage media, network accounts, IT devices, data and information are the property of DCJ. They are provided to DCJ employees and other authorised individuals and bodies in relation to the discharge of activities directly related to their responsibilities.

Use of DCJ information assets (including the use of a personal device to access DCJ networks) are subject to monitoring to ensure this use of DCJ information assets does not interfere with the DCJ mission and does not violate standards of ethical conduct or pose a risk to DCJ infrastructure, assets, reputation or business.

Limited non-work use of these computing devices and services is acceptable assuming it does not interrupt the discharge of duties or adversely impact the discharge of others' responsibilities.

Effective security is a team effort involving the participation and support of every DCJ employee and approved user who deals with information and/or information systems. It is everyone's responsibility to be aware of this policy and to conduct their activities accordingly.

## 5 Policy

### 5.1 General use and ownership

DCJ Information stored on any device irrespective of the owner of the device remains the property of DCJ.

Non-DCJ information which is either created, collected, stored or transmitted using a DCJ Information Asset will be considered as DCJ information and subject to standard retention, monitoring, auditing, logging, destruction processes and security protocols. This information is considered to be 'held' by DCJ and may be subject to a request for access by any individual under the *Government Information (Public Access) Act 2009* or the *Privacy and Personal Information Protection Act 1998*.

You may access, use or share DCJ information assets only to the extent it is authorised, compliant with the Data Privacy and Protection Policy and necessary to fulfil your assigned role. You have a responsibility to promptly report to management the theft/loss/unauthorised disclosure of DCJ information or DCJ assets and observed or suspected information security weaknesses in systems or services.

All employees are responsible for exercising good judgment regarding the reasonableness of personal use. Personal use should not interrupt the discharge of duties or those of others. Furthermore, the use should not be in relation to other employment or any other unauthorised use.

Information assets no longer required or at the termination of your employment or permission to use, must be promptly returned to the DCJ.

## 5.2 Internet usage

Internet access is to be used primarily for departmental business including the performance of work-related or other approved users authorised by DCJ and endorsed professional development activities. However, limited personal use of the internet access is permitted provided that it meets the following characteristics:

- it is infrequent and brief
- does not adversely impact productivity or service delivery
- does not demonstrate illegal, unacceptable or prohibited behaviour (refer to DCJ's Code of Ethical Conduct)
- does not negatively impact on the performance or security of the DCJ's information systems or services
- it is not in relation to other employment

Users should avoid using the same password across different services or websites so that in the event the password of one service/website is compromised, the damage is limited to that site only.

### 5.3 Email system usage

The DCJ's email system is provided to employees and other approved users primarily for work related use. However, limited personal use of the DCJ's email system is permitted provided that it meets the following characteristics:

- it is infrequent and brief
- does not adversely impact productivity or service delivery
- does not demonstrate illegal, unacceptable, inappropriate or prohibited behaviour (refer to DCJ's Code of Ethical conduct)
- does not negatively impact on the performance or security of the DCJ's information systems or services
- it is not in relation to other employment or approved DCJ use.

Using the DCJ's email facility from computing workstations located in public and community spaces such as at internet cafes and digital kiosks should be avoided unless it is a work or approved use related to an emergency. Should this occur such use should be immediately reported to your supervisor.

### 5.4 Remote working from overseas

Users intending to access DCJ digital systems (including emails) from overseas must comply with the [DCJ Remote Working from Overseas Guidelines](#) which align to the Circular [DCS-2022-03 Accessing NSW Government digital systems while overseas](#).

### 5.5 Monitoring and auditing

DCJ will implement processes to appropriately monitor and audit the use of DCJ resources. DCJ employees and approved users should not have an expectation of privacy when conducting business or personal activities using DCJ resources.

Your use of the Department's computer resources and network may be monitored continuously or intermittently throughout the term of your employment to validate compliance with the Department's policies and procedures.

Monitoring can include, but is not limited to, the use of automated and manual review of electronic content, emails, internet usage and files stored on IT resources.

The NSW Workplace Surveillance Act 2005 requires that employees be notified of surveillance arrangements in their workplaces. DCJ ensures this by displaying an appropriate notice whenever a user logs on to a corporate device.

DCJ reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Policy and to take any other reasonable steps to

protect the security of DCJ networks and systems by using and disclosing the information to address any identified risks, take preventative action to minimise concerns and for reporting purposes.

## 5.6 Secure use

All corporate end user computing devices must be protected by a password and self-locking mechanism which is compliant with the Access Control Policy. All users must lock the screen or log off when leaving the computing device unattended. Users must also cover laptop webcams and unplug desktop webcams when not in use.<sup>1</sup> Any non-corporate devices which are used for remote access should also have password and self-locking mechanisms applied.

Authentication information should never be physically written down and must not be stored in clear text. Regardless of the secret authentication information (password, token etc.), it must not be shared with anyone other than the owner or user. In the case of a generic account, authentication information should be shared no further than required and the authentication information should be refreshed regularly.

DCJ provided email addresses must not be used to subscribe to non-work- related services or websites. Similarly, users must not use corporate credentials to sign up to non-work-related services or websites.

Users must never use unsecured public Wi-Fi, particularly for work-related activities<sup>2</sup>.

All users must only use USB's and external hard drives where the source is known, trusted and the control of the USB and external hard drive can be guaranteed. Never plug in devices from unknown sources including USBs or external hard drives given as gifts or found lying around.<sup>3</sup>

Users should not handle a USB containing an inmate's legal/personal data except for transferring the data to/from a laptop.

All users must use extreme caution when opening email attachments received from unsolicited or unknown senders. Users must report violations of cyber security policies, cyber security incidents, suspicious activity and any suspected security risk (e.g. malware) using the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)

---

<sup>1</sup> See Section 11.2 References

<sup>2</sup> See Section 11.2 References

<sup>3</sup> See Section 11.2 References



- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

User permissions shall be removed on cessation of employment or authorised use. User permissions may also be removed or modified during change of role unless a prior arrangement is approved by the present and future managers or an authorised approver.

Approved users should wear their DCJ security pass when within the perimeter of a DCJ corporate facility.

Staff should be mindful when utilising tools with natural language processing capabilities, such as OpenAI's ChatGPT. While these tools can provide assistance and improvement to tasks such as technical or conversational writing, or answering general enquiries, considerable human involvement is necessary to ensure the accuracy and reliability of responses. Staff should also be mindful of the data classification and associated restrictions on any DCJ data they intend to upload into these tools.

Users of AI-based technology should be aware of its limitations and risks, and always consider potential implications to the security and privacy of data and systems.

#### **5.6.1 Special considerations for BYO devices**

All non-corporate devices must not be connected to the production corporate network. Where appropriate, non-corporate devices may be connected to specific 'bring your own device (BYOD)' ready networks.

The following security considerations also apply to BYO Devices when used for the purposes of conducting DCJ employed work:

- Employees must never use public Wi-Fi, particularly for work-related activities, as per Cyber Security NSW directive DCS-2020-05.
- Employees should ensure the safe handling and transport of BYO devices if used for the purposes of conducting work.
- Any compromise/theft/loss of BYO devices that are used for the purposes of conducting work must be reported to the DCJ cyber security team.
- BYO devices must not be used to store DCJ data locally or outside of the provided Citrix work environment.
- Employees should report to the DCJ cyber security team before reaching out to third parties for repair/service/clean of the personal device, should they believe that any DCJ data may be present on the device.
- BYO devices used for work purposes should adhere to the password complexity requirements from the Information Security Policy.

- BYO devices that have unauthorised modifications to the operating system, also known as “jailbreaking” or “rooting”, must not be used for accessing DCJ data

For additional information concerning the appropriate use of BYO devices and DCJ’s secure remote network, refer to the End User Computing Policy.

## **5.7 Unacceptable use of DCJ information assets**

Under no circumstances is an employee or authorised user authorised to engage in any activity that is illegal under local, state, federal or international law while using DCJ owned resources and systems.

The following activities are also prohibited:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Knowingly introducing of malicious programs (malware) into the network or computing devices.
- Use of DCJ resources (including internet access) to gain unauthorised access to data in another system or computer.
- Use of a computing device or information to actively engage in functions which are contradictory to any DCJ policy.
- Effecting security breaches or disruptions of network communication.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Cyber Security ([information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)) is approved. Port scanning is a method for determining which connections on the network are open (holes). For an intruder, these ‘holes’ represent opportunities to gain access for an attack.
- Executing any form of network monitoring which will intercept data not intended for the designated host, unless this activity is a part of the DCJ employee’s (including contractors and authorised users) normal job/duty/authorised use.
- Circumventing user authentication or security of any host, network or account.
- Providing lists or personal information of DCJ employees/contractors/authorised users or organisational structure charts to external parties without appropriate approval or authority from executive management.

- Publishing the DCJ's employee and approved email addresses on public facing websites without the approval of the Director, Communications, Ministerial and Communication Services.
- Using the email system as a records management and archiving database.
- Auto-forwarding corporate emails to non-governmental mailboxes.

## 6 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 7 Related legislation, regulation and other documents

This policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*
- *Commonwealth Criminal Code*
- *Crimes Act 1900*
- *Government Sector Employment Act 2013*
- *Workplace Surveillance Act 2005*
- *State Records Act 1998*
- *Government Information (Public Access) Act 2009*

## 8 Document information

Document name	IT Acceptable Use Policy
Document reference	D22/1832017
Replaces	IT Acceptable Use Policy V2.2
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/2023

## 9 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

If you need assistance identifying when you need to engage information security, please see

**Appendix**

**Engaging information** security.

**10    Version and review details**

Version	Effective date	Reason for amendment	Due for review
2.2	29/06/2022	Annual review	29/06/2023
3.0	28/09/2023	Annual review	28/09/2024

## 11 Appendix

### 11.1 Engaging information security

The following questionnaire can be used to help you determine when you need to engage Cyber Risk Audit and Compliance team.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov](mailto:information.security@justice.nsw.gov)
- Are you running or involved with a project which is implementing, updating or removing an ICT component?

- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party?

If you answer yes to any of the above or related legal advice, please email:

- 
- CRAC: [Securityarchitecture@facss.nsw.gov.au](mailto:Securityarchitecture@facss.nsw.gov.au)
- Legal: [infoandprivacy@justice.nsw.gov.au](mailto:infoandprivacy@justice.nsw.gov.au)

### 11.2 References

Ref #	Reference doc	Title	Version

1,2,3	Cyber Security NSW Directives	DCS-2020-05 Cyber Security NSW directive – Practice Requirements for NSW Government	Oct 16, 2020
-------	-------------------------------	--	--------------



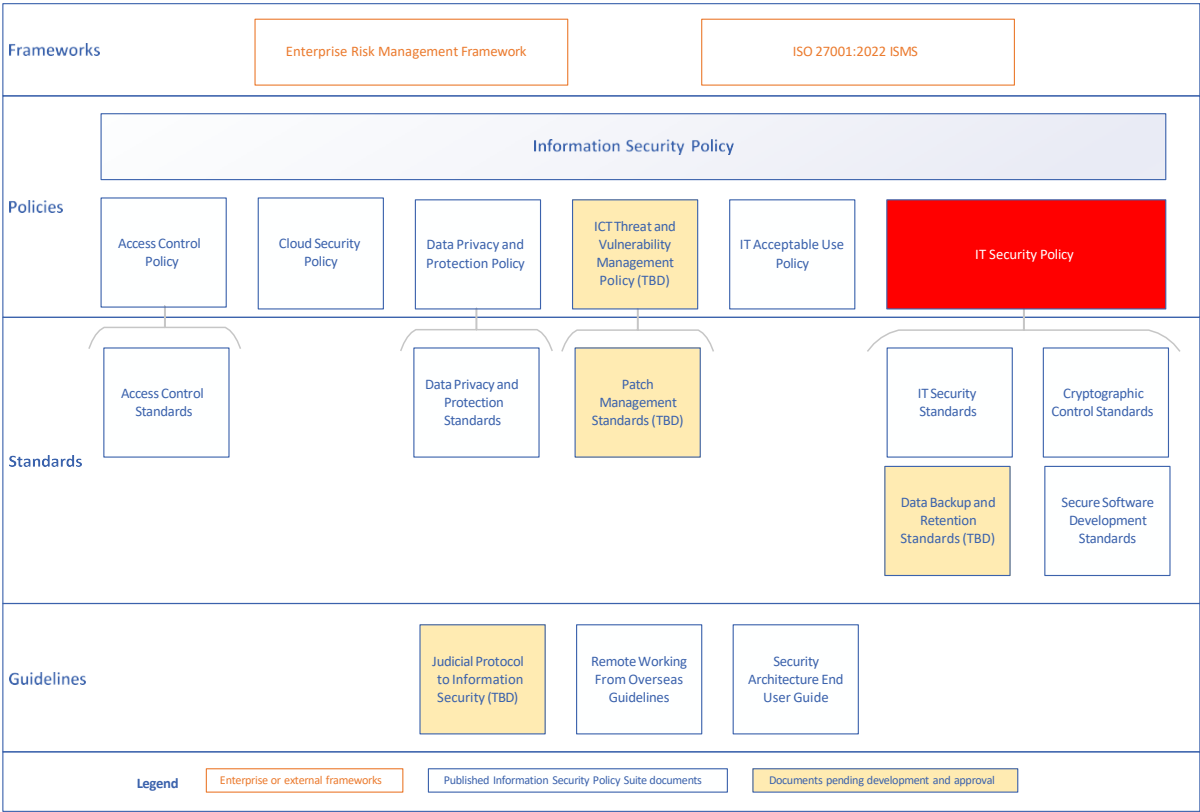
# IT Security Policy

---

## Table of contents

1	Purpose .....	2
1.1	Related policies .....	2
2	Definitions.....	3
3	Scope.....	4
4	Policy statement .....	4
5	Policy.....	5
5.1	Mobile devices .....	5
5.2	Teleworking / remote working.....	6
5.3	Asset management.....	6
5.4	Cryptographic controls .....	8
5.5	Physical and environmental security.....	8
5.6	Operations security .....	12
5.7	Communications strategy .....	17
5.8	System acquisition, development and maintenance .....	19
5.9	Supplier relationships .....	22
5.10	Information security incident management .....	24
7	Related legislation, regulation and other documents.....	26
8	Document information .....	26
9	Support and advice .....	26
10	Version and review details .....	27
11	Appendix – Engaging information security .....	28





The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

This policy is designed to articulate the high-level requirements the Department of Communities and Justice (DCJ) expects from its information technology (IT) systems to ensure information is being protected appropriately.

1.1 Related policies

This document is related to the following policies:

- [Access Control Policy](#)
- [IT Acceptable Use Policy](#)
- [Data Privacy and Protection Policy](#)
- [Information Security Policy](#)
- [Cloud Security Policy](#)
- [Employment Screening Policy](#)
- [End User Computing Policy](#)
- [NSW Cyber Security Policy 2020 v3.0](#)

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Information asset	Any information (both physical and digital in any format, including audio and visual). Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.
System importance	<p><b>External:</b> DCJ systems that are on internet accessible infrastructure – either publicly accessible, or via a proxy. Includes “untrusted” and “semi-trusted” sites.</p> <p><b>Internal:</b> DCJ systems that sit on an infrastructure that is only available from inside the DCJ ICT network.</p> <p><b>Critical system, external:</b></p> <ul style="list-style-type: none"> <li>• DCJ systems that are public/internet facing.</li> <li>• Systems that have been identified as DCJ’s crown jewels and are public/internet facing.</li> </ul> <p><b>Critical system, internal:</b></p> <ul style="list-style-type: none"> <li>• Internal DCJ systems.</li> </ul>

	<ul style="list-style-type: none"><li>• Systems that have been identified as DCJ’s crown jewels and are internal to DCJ only.</li></ul> <p><b>Non-critical system, internal:</b></p> <ul style="list-style-type: none"><li>• Other systems that do not hold critical data themselves, but are required in order to perform certain business services e.g. ServiceNow.</li></ul> <p><b>Other systems:</b></p> <p>Systems not in any of the previous categories and do not directly impact business functions e.g. personal endpoint devices such as employee workstations and laptops.</p>
--	---

3 Scope

The requirements and expectations outlined in this policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ Information systems and assets.

This policy does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges’ tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

4 Policy statement

DCJ information assets need to be protected appropriately throughout their lifecycle to ensure the confidentiality, integrity and availability of DCJ IT systems and information. This policy provides a framework for the appropriate administration, operation and implementation of controls to secure our information assets.

## 5 Policy

### 5.1 Mobile devices

#### 5.1.1 Enterprise mobility

Devices must use standard operating systems which are not 'jail broken'. This means that the smartphones or other electronic devices are not modified to remove restrictions imposed by the manufacturer or operator e.g. to allow the installation of unauthorised software.

Mobile operating systems and software must be kept up to date by the end user.

All corporate mobile devices which store DCJ information must be configured with disk encryption, access passwords and auto locking features.

Corporate mobile devices which are intended to store, create, use or transmit DCJ information should be connected to a Mobile Device Manager which has remote disable/enable, erasure and lockout capabilities.

Restrictions must be in place to ensure only DCJ owned and managed mobile devices are connected to the internal corporate network. Software which is designed to circumvent security controls is not to be installed.

Should a corporate device be lost, the user must advise the Information and Digital Services (IDS) Service Desk by calling 02 9765 3999 (former FACS) or 02 8688 1111 (former Justice) as soon as practicable.

#### 5.1.2 BYO devices

Bring your own (BYO) devices must not be connected to the internal corporate network, they may only interact with DCJ information and systems via approved remote access solutions or application services. If a BYO device is connected to a DCJ endpoint computing device (e.g. connect BYO mobile phone to a corporate desktop for the purpose of re-charging), it should be fitted with a locally sourced data blocker<sup>1</sup> that will prevent the possibility of transferring malicious files onto the DCJ network or device.

The device should be enrolled in the DCJ mobile device management solution, which will enforce limited controls to safeguard DCJ information. If the device is unenrolled, or breaches defined requirements (e.g. phone passcode is removed or the device is 'jail broken'), all DCJ apps and data may be removed.

---

<sup>1</sup> USB data blocker – a device that allows you to plug into USB charging ports to charge your devices while preventing any accidental exchange of data any time you connect your device into a charging station or foreign computers via a USB cable.

Should a user lose their BYO device which is utilising Enterprise Application Software (EAS) and/or DCJ apps, the user is required to advise IDS service desk by calling 02 9765 3999 (former FACS) or 02 8688 1111 (former Justice).

Staff utilising BYO devices are responsible for ensuring their mobile operating system and applications are kept up to date and are responsible for device maintenance and support.

## **5.2 Teleworking / remote working**

Remote access to the corporate network from any device must leverage and trigger DCJ's standard multi-factor authentication solution (MFA), which is OKTA, using a user bound strong MFA factor (e.g., one-time password, OKTA

Verify Push application) in addition to a username and password. Only approved remote access solutions may be used to remotely access internal systems and services.

Remote access solutions for non-corporate (BYO devices) or unverifiable devices should enforce restrictions to protect the corporate environment.

Users intending to access DCJ digital systems (including emails) from overseas must comply with the [DCJ Remote Working from Overseas Guidelines](#) which align to the Circular [DCS-2022-03 Accessing NSW Government digital systems while overseas](#).

Any vendor, contractor, or third-party supplier using BYO devices (including mobiles, laptops, and desktop computers) must use the DCJ Citrix portal and an approved VPN with Australia IP to access DCJ applications and networks.

## **5.3 Asset management**

### **5.3.1 Inventory of assets**

Information asset owners must maintain an inventory of all assets and classify them as per the Data Privacy and Protection Policy. Information asset owners should communicate changes and additions of the inventory to the relevant custodian/s and the [Information Strategy and Architecture team](#) who manage the Information Asset Register.

### **5.3.2 Ownership of assets**

Owners and custodians shall be assigned to all important assets identified and recorded in the asset register.

Where a service is provided by a cloud service provider (CSP), the ownership of Information Assets must remain with DCJ at all times. This must be specified in the contractual agreement between DCJ and the CSP.

DCJ must retain an immediate and ongoing right of access to all of its data held by the CSP who shall provide mechanisms to connect to its service.

The owners of information assets must ensure the safe return/transfer of readable/reusable data format back to DCJ in the event the service may be interrupted, terminated, or when DCJ wishes to transition out of the service, to ensure business continuity.

### **5.3.3 Handling of assets**

Assets holding information must be handled in a manner consistent with the standards driven by the DCJ Data Privacy and Protection Policy based upon the information assets classification.

DCJ assets which are provided to staff must be recorded and the asset secured in line with the classification of the data it is intended to store.

DCJ information assets stored in the cloud that are accessed, processed, communicated to, or managed by the CSP must be controlled so that the CSP and its subcontractors must not share or disclose DCJ data and information obtained in a professional capacity without the prior written consent of the DCJ information owner supported by an appropriate confidentiality agreement or non-disclosure agreement (NDA), unless required by law.

### **5.3.4 Management of removable media**

The management of removable computer media should be controlled. All media must be stored in a safe and secure state in accordance with the highest-level classification of the data stored on the media. Any removable media used to store classified information must be encrypted.

### **5.3.5 Disposal of media**

Data sanitisation/disposal must be conducted across all storage devices upon DCJ's exit from the cloud-based service, device repair or device decommission. All staff must use proper destruction methods and ensure compliance with the *State Records Act 1998* when disposing of media containing DCJ records and or classified information.

All media must be disposed of in a manner commensurate with the information classification stored within. In general, records need to be disposed of in such a manner that they cannot be reconstituted. The controls and procedures to achieve this vary as identified in the [Data Privacy and Protection Policy](#).

### **5.3.6 Physical media transfer**

All physical media containing DCJ data must be protected against unauthorised access, misuse or corruption during transportation. This includes DCJ-configured laptops and portable devices.

Any physical media containing sensitive data must be shipped by a reputable/approved carrier with tracking provided and must require a recipient signature. Where the physical media contains encrypted data, the encryption key should only be released after the package has arrived and been signed for.

## 5.4 Cryptographic controls

### 5.4.1 Policy on the use of cryptographic controls

The use of cryptographic algorithms and key sizes by cryptographic implementations is subject to the conditions specified in *Section 5.4.3. Regulation of cryptographic controls* must be in compliance with the DCJ Cryptographic Control Standards. This standard provides guidance on the use of cryptography and it is heavily based on the related Australian Cyber Security Centre (ACSC) recommendations and best industry best practices.

Implementations of data encryption must be addressing a risk and must be reviewed by Cyber, Risk, Audit and Compliance team via [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au).

### 5.4.2 Key management

Access to cryptographic keys and the ability to generate new cryptographic keys from a trusted publishing authority must be restricted and controlled.

Where a hardware security module cannot be used to store private key data, appropriate access controls should be applied to the private certificate store to ensure least privilege is enforced and confidentiality preserved.

Engagements with external service providers who encrypt DCJ data must consider key escrow arrangements, especially when related to OFFICIAL: Sensitive and above.

Key storage for PROTECTED and above classified data should be managed within the DCJ infrastructure

All keys must be crypto-shredded (destroyed) upon contract termination

Cryptographic key lifetimes should be indicative of the risk posed to the entity. All certificates must specifically reference an entity or group of entities via the use of a subject alternate name. Wildcard certificates are not acceptable.

### 5.4.3 Regulation of cryptographic controls

Only Australian Cyber Security Centre approved cryptographic controls should be used. Deviation from these must only occur after approval from Information Security Management.

## 5.5 Physical and environmental security

### 5.5.1 Physical security perimeter

All DCJ facilities must implement a security perimeter commensurate with the information housed or accessible from within the facility. Each physical security implementation must at a minimum consider:

- a clear definition of the area to be secured (e.g. specified zone for protective facilities)
- physically sound perimeter components (walls, doors, windows, etc.)
- appropriate controls to facility entrances
- alarmed fire control doors as per local safety requirements
- compliance with all applicable occupational health and safety regulations.

### 5.5.2 Physical entry controls

All DCJ secure areas must implement physical entry controls which are commensurate with the information housed within the facility. At a minimum:

- all staff should wear a form of visible identification
- all visitors must be escorted<sup>2</sup> at all times
- the identity of staff, third parties and visitors must be confirmed prior to the issue of a visitors pass or access token (key or swipe pass)
- physical barriers must be implemented requiring staff to 'authorise' themselves before accessing. Controls should be applied to prevent tailgating
- record successful and failed access attempts
- restrict access to staff with a genuine need, or provide temporary access when required
- regularly review access control lists.

### 5.5.3 Secure offices, rooms and facilities

DCJ offices, rooms and facilities must implement physical controls which are commensurate with the information housed or accessible.

Rooms and facilities within these offices should also implement auxiliary controls should the level of risk or sensitivity be increased.

Staff are to report unknown or unauthorised persons to building security immediately if the person is identified within a secured area.

---

<sup>2</sup> Escorted visitors should enter and exit the building under the purview of a staff member. Their actions when within the perimeter of a DCJ facility must be observed.



### **5.5.4 Protecting against external and environmental threats**

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. Consideration should be given to any security threats presented by neighbouring premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion.

#### **5.5.5 Working in secure areas**

Any person working or having access to a secure area must be informed of the enhanced security requirements of the secure area, the details of the security perimeter of that area and the associated responsibilities for the area.

Recording equipment (e.g. photo, video or audio) must not be used in a secure area unless specifically authorised by the staff member's manager, information security management or as required by law.

Any third-party access granted to a secure area must be strictly controlled and monitored. All parties with access to the area must be authorised and logged, including support services such as cleaning or waste removal.

Any area deemed a secure area must be locked when unoccupied and physically checked periodically.

#### **5.5.6 Delivery and loading areas**

Delivery and loading areas must be adequately separated from information processing facilities. Access via the delivery and loading areas must be monitored and secured by:

- supervising any delivery personnel
- controlling access to the area
- registering all visitors, delivery personnel and incoming material
- securing physical access points to the area.

#### **5.5.7 Equipment siting and protection**

All DCJ equipment must be sited in a manner to minimise exposure or threat. This includes:

- threats of theft or vandalism
- risk of fire, explosion, smoke, chemical agents
- loss of services such as power, communication or water.

### **5.5.8 Supporting utilities**

Key information assets and equipment shall be protected from power failures and surges and other electrical anomalies. To avoid power failures, a suitable electrical power supply must be provided to computer rooms in such way that single points of failure can be avoided.

Uninterruptible power supplies (UPS) must be used for equipment supporting critical information systems to allow an orderly close down or to allow the systems to continue running. Service owners should ensure UPS equipment is checked on a regular basis to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.

### **5.5.9 Cabling security**

All power and telecommunications equipment and cabling must be protected against deliberate or accidental interruption of service. This includes protecting control boxes, cables, wiring hubs and other equipment from fire, vandalism, interception of communications or disruption of service.

All DCJ network connections must be removed and/or deactivated when a site is being vacated. Network operations staff must ensure this has been completed appropriately before the site is vacated.

### **5.5.10 Equipment maintenance**

All equipment must be correctly maintained to provide availability and protect the integrity and confidentiality of information. Equipment should be monitored and inspected in accordance with manufacturer's specifications. Only authorised maintenance personnel are allowed to perform repairs and all repairs or service work must be recorded. If equipment must be sent offsite for repairs, the confidentiality and integrity of any information must be ensured. Any damage to the equipment should be reported to the IDS Service Desk. If the equipment is lost or stolen, staff must report to the IDS Service Desk as soon as practicable.

An equipment refresh plan must be maintained to track the periodic replacement of equipment before they reach end of life. Considerations for a refresh must include the equipment's age, the warranty date and service history. The equipment must be thoroughly examined on regular basis for an up-to-date vendor support to ensure continuing reliability of equipment.

### **5.5.11 Removal of property**

Equipment, information or software must not be taken off-site without prior approval from the information asset owner or delegate. Where necessary, an equipment tracking log should be maintained.

### **5.5.12 Security of equipment and assets off-premise**

The information asset owner or delegate must authorise any equipment used to process DCJ information at non DCJ premises.

Equipment and information taken off premise, or outside of DCJ premises may be under increased threat and must have appropriate controls in place to secure the device and the information.

### **5.5.13 Secure disposal or re-use of equipment**

Information shall be removed from any information systems equipment that has been used for DCJ business before disposal, donation or re-use. This sanitisation process must take place before releasing such equipment for disposal in accordance with the Data Privacy and Protection Policy.

### **5.5.14 Clear desk and clear screen policy**

All users must keep a clear desk and screen. This requires all information, whether it be on paper or screen is properly locked away or disposed of when a workstation is not in use or unattended. The clear desk and clear screen policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

Screensavers/session locks on all PCs/laptops and servers must be implemented. The lock must require the user to re-authenticate before system access is granted.

All printers and fax machines should be cleared of papers as soon as they are printed to ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Sensitive physical documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.

## **5.6 Operations security**

### **5.6.1 Documented operating procedures**

Appropriately documented operating procedures must be maintained to enable the proficient commission and decommission of information systems along with the proficient administration and support of key information assets and processes.

If a service or application involves any external parties, all contact information for operational or technical difficulties must be included in the documentation.

### 5.6.2 Change management

All changes to DCJ information assets must be performed in a controlled and managed fashion consistent with the DCJ Change Management Procedure. All changes must be:

- formally documented
- peer reviewed
- tested prior to implementation
- reviewed and approved by an appropriately authorised audience.

Post verification testing (PVT) should occur as soon as possible after a change to ensure the requirements are met and to reduce opportunities for unauthorised modification of DCJ information resources.

In addition, there must be a post implementation review of all changes to record the outcomes on the change request.

Where changes to the information resources do not come under the province of change management (e.g. new-user registrations), suitable audit trails and authorisation procedures should be established.

### 5.6.3 Capacity management

All information resources must meet anticipated capacity requirements. It is the responsibility of the system's development team to determine anticipated hardware and capacity requirements. Furthermore, it is the operational team's responsibility to monitor system capacity performance requirements are being met. Consumption of aaS (as a Service) may remove DCJ's responsibility to determine the anticipated capacity requirements, however the monitoring of system capacity performance should be a service requirement.

### 5.6.4 Separation of development, testing and operational environments

Separate (this may be physical or logical separation) and controlled environments should exist for development, test and production where business requirements support their necessity.

Compilers, where possible, should only be installed on development servers to prevent unmanaged change being implemented during testing or production phases.

Appropriate access controls should be applied to the development and testing environments to ensure the confidentiality and integrity of development activities and data.

Naming conventions should be applied to delineate production and non- production servers.

### 5.6.5 Controls against malware

To prevent the introduction of malicious software, approved malware protection software must be installed where technologically possible on DCJ resources including servers, user workstations, standalone workstations, mobile computing devices and laptops.

Malicious software controls must be regularly updated to ensure malicious software can appropriately be identified.

Instances of detected malicious code software outbreaks must be handled in accordance with the DCJ Security Incident Management Procedures.

All users must report malicious software by contacting CRAC (Cyber Security) using the contacts listed in *Section 11 Appendix – Engaging information security* if it is identified on their machine. The user should also physically disconnect their computer from the network as soon as possible to prevent spreading the infection.

### 5.6.6 Information backup and retention

Information asset owners must ensure that appropriate backup and recovery procedures exist for all information assets that have backup requirements.

These procedures must consider the information security requirements of confidentiality, integrity and availability as well as the Recovery Point Objective (RPO), Recovery Time Objective (RTO), and Maximum Acceptable Outage (MAO).

To maximise protection to DCJ and minimise risk of data loss, DCJ's ICT systems and software assets should aim to achieve ASD's highest maturity level of mitigation strategy for backups and retention, namely regular backups which are retained in a coordinated and resilient manner that is only accessible to approved backup administrators and tested regularly.

The types of backups and their minimum frequencies should be determined by the information asset owner and in line with the Data Backup Standards (TBA) following a risk-based assessment regarding the system criticality, data classification, data type and frequency of changes to the data. Custodians must develop backup rotation and retention schedules based on these requirements. Backups must occur after patching, when a new solution is implemented, and after major system changes or upgrades.

Where possible, if the risk assessment allows, backups should be stored in the cloud as it adds redundancy to the infrastructure and improves cost and scalability for DCJ. They can also be stored on different types of media such as external hard drives, tapes, and WORM to reduce the risk of failure related to a specific medium or technology.

The backup strategy should follow the "3-2-1" best practise method:

- 3 copies of data (not including the original data)
- 2 copies on different storage media
- 1 copy stored off-site in a location that is at a distance that would protect it from damage from any incident at the main site, such as a site wide failure or geographical disaster.

Backups must be provided the same level of confidentiality, integrity, and physical and environmental protection as the source data<sup>3</sup>. The backup data must be read-only and encrypted whether onsite or offsite and only accessible by authorised staff.

Critical business information and critical software backups must be tested at appropriate intervals to provide assurance that backups can facilitate recovery of data.

Data backup and retention must be considered during new solution design.

At the end of the retention period all media must be disposed of in accordance with *Section 5.2.5 Disposal of media*.

#### **5.6.7 Event logging**

Systems which facilitate access to, store, transfer or create DCJ information must, where technically feasible, have logging capabilities enabled which identify at a minimum:

- who performed an action
- what action was performed
- when the event occurred
- where the event was initiated from.

Where possible and appropriate, this event log data should be centralised to support security intelligence.

All event logs should be kept for periods in line with legislative requirements. If no legal requirements are identified, the event logs should be kept for time periods that support an investigation.

#### **5.6.8 Protection of log information**

All system and application logs must be maintained in a secure manner that cannot be readily viewed by unauthorised personnel. Access to view logs should only be given to users with a genuine need for the access.

---

<sup>3</sup> The minimum protections for storage are identified in the NSW Government Information, Classification, Labelling and Handling Guidelines

### 5.6.9 Administrator and operator logs

Where supported, actions performed by users of authority (administrators or operators) should be logged.

Mechanisms should be in place to evidence when administrative tasks are performed which are outside of the bounds of normal application or system processes (i.e. clearing or flushing logs).

### 5.6.10 Clock synchronisation

System clocks must be synchronised using a reliable time source to ensure the accuracy of audit logs and potential forensic evidence.

### 5.6.11 Installation of software on operational systems

The updating or installation of software and program libraries on servers must only be performed by authorised personnel and be in accordance to *Section 5.6.2 Change management*. The updating or installation of software and program libraries on desktops and laptops must be restricted and controlled.

### 5.6.12 Management of technical vulnerabilities

A risk-based vulnerability management process must be documented and implemented. Vulnerability management must be a continuous process which validates Information assets before go live and during the course of their lifetime.

This process should ensure that pertinent systems are regularly scanned and identified vulnerabilities escalated to custodians for mitigation.

### 5.6.13 Restriction on software installation

Only approved pieces of software should be installed on systems by an authorised individual. Controls should be implemented to control the installation of software by unauthorised individuals.

### 5.6.14 Information systems audit controls

Information system audits need to be documented and approved prior to being conducted. The timing, scope and depth of testing must be defined. Furthermore, they must be carried out in a fashion that does not impact service delivery.

### 5.6.14 Alerting and Monitoring Systems

All critical servers (refer to 'System Importance' in *Section 2 Definitions* for definition of critical system) must be set up to alert technical support teams of changes to operating parameters that can lead to a failure event. The alerts

should be configured to provide notifications when indicators reach certain thresholds that suggests imminent failures (red flags).

## **5.7 Communications strategy**

### **5.7.1 Network controls**

Network solutions must be implemented and managed in such a way that preserves the confidentiality and integrity of the data being transferred, stored or used. Network solutions must ensure appropriate logging and auditing is available. Core network infrastructure must be designed in a redundant fashion to ensure the availability of the data and or systems.

New network segments must consider the impact upon security (e.g. implementation of wireless networks) and appropriate controls put in place to ensure the segment does not negatively impact upon the existing network or allow unauthorised connections.

Roles and responsibilities for the management of network operations must be documented, furthermore these roles and responsibilities should be segregated from the operators of computer systems. Changes performed by this identified group must be bound by the DCJ change management process.

### **5.7.2 Security of network services**

A clear description of the security attributes, service levels and management requirements of all network services used by DCJ should be provided, including service level agreements and monitoring for services provided in-house or outsourced.

Critical and/or core network infrastructure and network security assets must be proven to be secure via accreditation to globally recognised standards or identified on the Australian Cyber Security Centre Evaluated Product List.

### **5.7.3 Segregation in networks**

Unmanaged connections between networks boundaries must not be permitted. Whilst unmanaged networks may be leveraged, controls must be implemented to ensure the confidentiality, integrity and availability of the networks and data flows.

Network connections or segments which present an increased level of risk must employ controls which allow for the preservation of the greater network security posture. High risk networks where technically feasible must be physically segregated from corporate networks.

Systems of similar risk profiles must be segmented from those with increased risk profiles. Information flows should always initiate from most secure to least secure zones.



Where technically feasible, strict routing architectures must be used to limit remote access to specific points in the network.

#### **5.7.4 Information transfer policies and procedures**

Procedures and controls must be developed and implemented in accordance with the Data Privacy and Protection Policy to protect the exchange, confidentiality and integrity of information.

All information exchanged must be logged and details regarding the sender, recipient, dispatch date and receipt of information should be recorded.

#### **5.7.5 Agreements on information transfer**

Agreements and controls must be established for exchange of information and software between DCJ and other organisations in accordance with the Data Privacy and Protection Policy to protect the, confidentiality, availability and integrity of information. These agreements should consider the:

- type of information is being exchanged
- purpose for information exchange
- non-disclosure agreements
- confidentiality agreements
- period
- acknowledgement of receipt
- record of destruction
- controls securing the data shared.

All such exchanges must be approved by information owners.

#### **5.7.6 Electronic messaging**

Information being sent over email or any other messaging/collaboration platform is subject to the DCJ Data Privacy and Protection Policy. As such these correspondences must be labelled in alignment with this policy and must follow the classifications handling requirements.

The use of internet-based messaging/collaboration tools should not be used to ferry 'Sensitive' information unless an appropriate risk assessment has been conducted to validate its use and Chief Digital Information Officer's approval has been obtained to procure the service.

### 5.7.7 Confidentiality or non-disclosure agreements

All employees, contractors, third parties, services providers and external entities<sup>4</sup> must be bound by a non-disclosure agreement or policy. This agreement or policy must explain the information covered and the purpose of its use.

Non-disclosure or confidentiality agreements and policies must be reviewed at regular intervals and kept current to ensure compliance with relevant legislation and to uphold the confidentiality of DCJ information.

## 5.8 System acquisition, development and maintenance

### 5.8.1 Information security in project management

All projects must consider information security throughout the project lifecycle and recognise security requirements in their project objectives by:

- addressing security specifications in project plan
- performing risk assessments addressing information security
- ensuring security is included in all steps of the project
- performing tests to verify if the project deliverables are compliant with security specifications.

Where applicable, information security requirements and objectives should be captured as early inputs to the project. Where a project has the potential to impact the security posture of DCJ, a risk assessment must be completed. All identified risks need to be managed appropriately by the project and any risks transitioned to the service owner during go live, unless other risk management arrangements have been formalised

Asset owners in conjunction with project delivery resources must ensure that Information management requirements are adequately addressed during all phases include plan, organise, design, development, implementation, operation, support and decommission phases.

Cyber, Risk, Audit and Compliance team (CRAC) [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au) must be involved throughout the project lifecycle and controls should be finalised prior to the application development phase.

---

<sup>4</sup> External entities in this context are defined as any non DCJ individual, department, organization, entity etc. that DCJ share information and or data with.

### 5.8.2 Securing application services on public networks

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification. Prior to leveraging an online application service, a risk assessment must be completed to ensure the service meets the information security and classification and labelling expectations of DCJ.

Where possible cryptographic techniques should be used to verify the identity of the online service and secure the data flows between the service and DCJ.

### 5.8.3 Protecting application services transactions

Where the risk of a transaction is heightened or the classification level of the information requires it, appropriate cryptographic techniques must be implemented to ensure the confidentiality and integrity of transactions.

Where DCJ leverages an external trusted authority for the creation of digital certificates, reputable providers must be used where assurance of secure management is available.

### 5.8.4 Secure development policy<sup>5</sup>

Development of systems and applications must be performed securely in a way that does not expose the internal network, production systems or production information to unmanaged risk.

Modifications applied to code, systems or applications must be documented and where possible previous code versions should be securely maintained.

Internally facing systems and applications should undergo vulnerability assessment prior to production release. Systems and applications which are externally facing must undergo vulnerability assessment before release. High risk solutions should leverage external vulnerability assessment services.

Development practices must be in line with the Secure Software Development Standard which align with this policy.

### 5.8.5 System change control procedures

All changes to production systems are bound by change management as articulated in *Section 5.6.2 Change management*. Changes to development and test environments should be documented and approved prior to implementation into production.

---

### 5.8.6 Technical review of applications after operating system changes

The change implementer must ensure all operating system and application releases are checked for functionality and security. Implementations must include back-out planning and should identify success criteria.

### 5.8.7 Restrictions on changes to software packages

Modifications to software packages should be discouraged and essential changes strictly controlled. Where possible the vendor should be leveraged to make these changes. Modifications to copyrighted material should be first verified with the copyright owner. Any applied changes must follow DCJ change management processes.

### 5.8.8 Secure system engineering principles

Principles for engineering secure systems should be maintained, documented and align to the intentions of the Information Security Policy.

### 5.8.9 Secure development environment

Development environments must comply with *Section 5.6.4 Separation of development, testing and operational environments* and should not be internet facing.

Projects/deployments/applications must not use Production data in Non- Production environments unless a policy exception has been approved.

All sensitive data (either live production data or a testing copy) should not be used in NON-PROD environment without:

- the NON-PROD environment has the same security and access controls as production and/or
  - applying appropriate irreversible masking/scrambling to de-identify the data, or
  - removing the sensitive data, or
  - restricting access to the data as appropriate

Security controls applied to the production environment should be documented and should ensure an acceptable level of control over the environments.

### 5.8.10 Outsourced development environment

Outsourced development environments must be closely supervised and the providers bound by a contract ensuring confidentiality and confirming their alignment to DCJ policies and standards. Such engagements should ensure appropriate documentation is maintained providing evidence of compliance and

testing. Providers/third party vendors (i.e. developers) should not have access to any Production data if not expressly permitted by the business data owner.

All outsourced development environments must be reviewed by the Security Architect via [securityarchitecture@facs.nsw.gov.au](mailto:securityarchitecture@facs.nsw.gov.au) prior to use.

#### **5.8.11 System security testing**

Security testing aims to determine whether or not the system is secure against incursion (i.e. cannot be breached) and that there are no weaknesses either in the design or construction of the system that can be exploited to breach it.

Security testing comprises:

- penetration testing – test cases to see whether or not the system can be breached. In many cases, penetration testing is combined with vulnerability assessments to identify candidate weaknesses in the system which must be tested.
- vulnerability assessment – assesses whether the design / construction of the system is robust enough to prevent any penetration. This is a risk- based assessment. The discovery of potential vulnerabilities in the system can provide a scope for penetration testing.

Security testing (particularly vulnerability assessment) should be carried out during development to aid in the reduction of vulnerabilities discovered late in the development life cycle, which may impact on project timelines. New applications and systems should undergo vulnerability assessment.

Where the system is classified as a Crown Jewel, is external facing, or is a cloud service provision, it must undertake independent external penetration testing on an annual basis, and after major modification. All other systems should have periodic penetration tests conducted at least every 3 years, and after major modification.

#### **5.8.12 System acceptance testing**

Information security requirements should be included within acceptance testing processes. Where appropriate, vulnerability assessments can facilitate this test process.

#### **5.8.13 Protection of test data**

The use of unmasked production data in a test environment must comply with *Section 5.8.9 Secure development environment* and an approval from the information asset owner must be obtained before the data is loaded into the development environment.

### **5.9 Supplier relationships**

### **5.9.1 Information security policy for supplier relationships**

Whilst we can outsource a service or deliverable, we cannot however outsource our risk or contract out of our legislative obligations under privacy legislation.

All suppliers, third parties, managed service providers etc. must act in a fashion compliant with our Information Security policies and standards. Where DCJ shares information with a supplier, appropriate assurances must be obtained which ensures the supplier will act in a manner which preserves our risk posture. Furthermore, the method in which they technically integrate with DCJ must undergo a risk assessment. In addition, a Third Party Cyber Risk Assessment must be successfully completed by all suppliers/vendors prior to their being granted access to DCJ's data for the purpose of being stored, used, collected, transferred or destroyed. This applies specifically to all data that is classified OFFICIAL: Sensitive, or above.

Before leveraging a supplier, an appropriate contract must be entered into. This contract must bind the supplier to obligations ensuring the security of our data and provision of service. A documented process should be followed to manage these contracts on an ongoing basis.

### **5.9.2 Addressing security within supplier agreements**

Where possible, a standardised procurement contract should be used (NSW Procurement Procure IT) for all agreements regarding a supplier that may access, process, store, communicate, or provide IT infrastructure components for the organisation. Appropriate clauses need to be added which ensure the security of DCJ, hold the supplier accountable for the proper use of DCJ data, explicitly detail required obligations, identify security reporting metrics and ensure compliance with relevant legislation.

### **5.9.3 Information and communication technology supply chain**

Contracts with suppliers must place obligations on the contracted party to ensure the security requirements and intentions of the agreement are upheld by other parties which are components of the supply chain. Monitoring and verification techniques should be included in the contract to ensure delivered components are meeting requirements.

### **5.9.4 Monitoring and review of supplier services**

The services, reports and records provided by the third party must be regularly monitored against the service level agreements and audits shall be carried out as required. Information security incidents or events must be reported to Cyber, Risk, Audit and Compliance (Cyber Security team) via [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)

### **5.9.5 Managing changes to supplier services**

Changes to the provision of services, including maintaining and improving of existing information security policies, procedures and controls, must be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

## **5.10 Information security incident management**

### **5.10.1 Responsibilities and procedures**

All users are responsible for reporting all information security incidents to CRAC (Cyber Security) using the contacts listed in *Section 11 Appendix – Engaging information security*.

Cyber Security staff are responsible for addressing all information security incidents and breaches in a timely manner following the processes identified in the Information Security Incident Management Standard.

Management are responsible for approving remediation activities and assisting in potential disciplinary processes.

### **5.10.2 Reporting information security events/suspicious**

Events which clearly are a breach of the law must be referred to the appropriate authorities. All information security incidents will be reported to management and may be shared with the Senior Responsible Officer (SRO) where applicable.

Where there is a security incident involving DCJ data, the information on security threat and intelligence shall also be shared with Cyber Security NSW.

An actual or suspected security breach must be reported to Cyber Security at the earliest opportunity.

### **5.10.3 Reporting information security weaknesses**

All staff must report security weaknesses to the Cyber Security team in a timely manner to ensure the weakness is addressed before an incident occurs. Staff must not attempt to prove the validity or impact of the identified weakness.

### **5.10.4 Assessment of and decision on information security events**

The Cyber Security team is responsible for the triage of information security events based upon a documented and agreed procedure. A priority/severity will be applied to the incident based upon the impact or the pervasiveness which affects the way the CRAC (Cyber Security team) handle the incident.

### **5.10.5 Response to information security incidents**

Processes to respond to Information security incidents must be documented and approved by management. This process must ensure that activities regarding addressing the incident are documented and appropriate audit trails and logs maintained. Appropriate escalation paths must be identified to ensure management are informed and engaged when appropriate.

DCJ's incident response plan should integrate with the NSW Government Cyber Incident Response Plan and DCJ's Disaster Recovery Plan.

### **5.10.6 Learning from information security incidents**

The Information Security Incident Management Process must articulate how security incidents will be used to inform future processes and actions in an attempt to prevent repeat incidents.

### **5.10.7 Collection of evidence**

All forensic investigations must be outsourced to reputable providers. Information security may collect devices and store them in a secure room but must not do anything which may affect the integrity of the data.

CRAC (Cyber Security team) may conduct general investigations and collect evidence to support business activities under the assumption it is not part of a forensic investigation into an illegal activity.

### **5.10.8 Planning information security continuity**

There should be a managed process regarding information security requirements in place for developing and maintaining business continuity throughout DCJ.

### **5.10.9 Implement information security continuity**

Procedures and controls should be defined and implemented to ensure required information security controls are available and maintainable during a disruption. Consideration should be given to Information security when constructing continuity or disaster recovery plans for systems and services.

### **5.10.10 Verify, review and evaluate information security continuity**

Disaster recovery and continuity processes should be tested at regular intervals to ensure they are valid and meet information security requirements. Disaster recovery and continuity plans should be reviewed regularly or after major changes which may impact their implementation.



### 5.10.11 Availability of information processing facilities

Information processing facilities should be implemented with appropriate redundancies to meet the prescribed availability requirements.

## 6 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 7 Related legislation, regulation and other documents

This policy supports adherence to:

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *Government Sector Employment Act 2013*
- *Workplace Surveillance Act 2005*
- *State Records Act 1998*
- *Government Information (Public Access) Act 2009.*

## 8 Document information

Document name	IT Security Policy
Document reference	D22/1832016
Replaces	IT Security Policy V2.3
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/2023

## 9 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
---------------	---

Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>
-------	--

If you need assistance identifying when you need to engage information security, please see **Appendix – Engaging information security**.

10 Version and review details

Version	Effective date	Reason for amendment	Due for review
2.3	11/11/2022	Annual review	29/06/2023
3.0	28/09/2023	Annual review	28/09/2024

## 11 Appendix – Engaging information security

The following questionnaire can be used to help you determine when you need to engage Cyber Risk Audit and Compliance team.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party?

If you answer yes to any of the above or related legal advice, please email:

- **CRAC:** [Securityarchitecture@facs.nsw.gov.au](mailto:Securityarchitecture@facs.nsw.gov.au)
- **Legal:** [infoandprivacy@justice.nsw.gov.au](mailto:infoandprivacy@justice.nsw.gov.au)

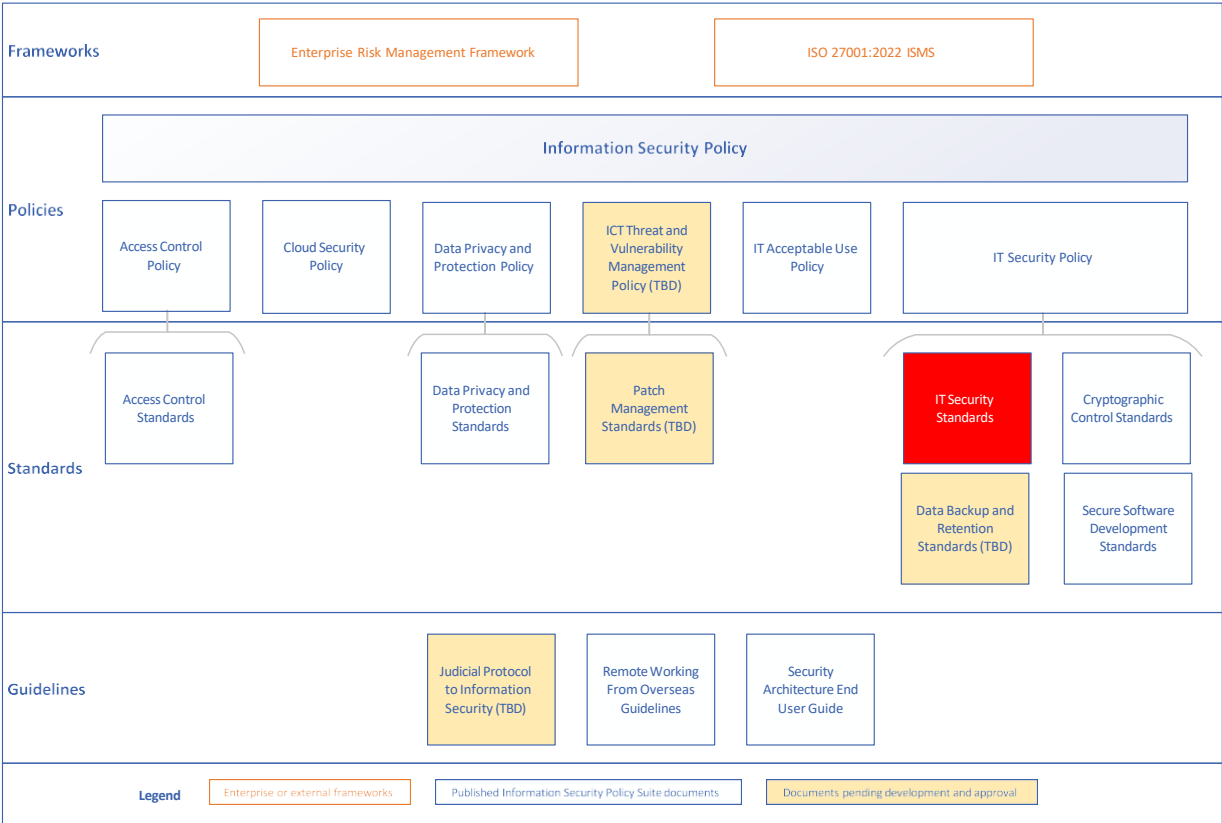


# IT Security Standards

---

## Table of contents

1	Purpose .....	2
2	Definitions.....	2
3	Scope.....	4
4	IT Security Standards .....	4
4.1	Mobile devices and teleworking.....	4
4.2	Asset management.....	6
4.3	Cryptography.....	6
4.4	Physical and environmental security.....	7
4.5	Operational procedures and responsibilities .....	8
4.6	Controls against malware.....	9
4.7	Data backup controls.....	9
4.8	Logging and monitoring.....	9
4.9	Vulnerability management .....	14
4.10	Communications security .....	14
4.11	Application security.....	16
4.12	Systems acquisition and development.....	17
4.13	Supplier relationship .....	18
4.14	Security incident management .....	19
4.15	Information security in service continuity.....	19
5	Monitoring, evaluation and review.....	20
6	Related legislation, regulation and other documents .....	20
7	Document information .....	20
8	Support and advice .....	20
9	Version and review details.....	20



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

The following standard articulates the Department of Communities and Justice’s (DCJ’s) IT security standards in regard to the IT Security Policy.

2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
BYO devices	Bring your own devices are personally owned devices (laptops, tablets, and smart phones) that employees are permitted to bring to their workplace, and to use those devices to access the organisation’s ICT systems.
Cloud service provider (CSP)	Any company that provides applications, services or storage made available to users on demand via the internet, for a fee. Typically this will be an ‘as a Service (aaS)’ offering.
CMDB	Configuration Management Database

Term	Definition
Computing systems	Covers personal computer, desktop, laptop, netbook, personal digital assistant (PDA), smart phones, tablets, workstation, server mainframe, super computer and wearable computer.
Conditional access (CA)	Conditional access is an authority in a network that issues and manages security credentials.
CRAC	Cyber Risk, Audit and Compliance
CSP subcontractors or subprocessors	A person or organisation providing a component of the cloud service under contract to the CSP.
Exchange ActiveSync (EAS)	Exchange ActiveSync is a technology that allows for the synchronisation of email, contacts, calendar, tasks and notes across mobile devices.
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Outsourcing	Outsourcing includes any commercial arrangement where an external party stores, transfers, uses or creates DCJ information and data. This is, however, separate from an information sharing venture.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.

### 3 Scope

The requirements and expectations outlined in this document applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This standard will be used by staff who are responsible for the design, administration, support and hosting of DCJ information systems.

This standard does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges’ tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

### 4 IT Security Standards

#### 4.1 Mobile devices and teleworking

Ref	Directive
MDT-001	Mobile devices <b>MUST</b> be password protected by a minimum four-digit passcode, simple passcodes such as ‘0000’ or ‘1234’ are not to be used. Remembered passcode history and passcode expiration for the device may be left unconfigured.
MDT-002	Mobile devices <b>MUST</b> employ device locking techniques to prevent brute force attempts.
MDT-003	Mobile devices which store sensitive DCJ data <b>MUST</b> employ disk/data encryption to protect the content.
MDT-004	Mobile devices <b>MUST</b> employ automated screen locking techniques which require a password to unlock. Time out for screen locking <b>SHOULD</b> be no greater than 15 minutes of inactivity.

Ref	Directive
MDT-005	<p>Mobile devices which store sensitive DCJ data <b>MUST</b> be enrolled with the department's mobile device management solution, which:</p> <ul style="list-style-type: none"> <li>• monitors application installation and can prevent undesirable application installs</li> <li>• forces desirable application/configuration controls</li> <li>• is capable of wiping the device</li> <li>• is capable of locking or disabling the device</li> <li>• is capable of enforcing Mdt-01, Mdt-02, Mdt-03, Mdt-04.</li> </ul>
MDT-006	Mobile devices on the corporate network may be tethered to non- corporate or bring your own (BYO) devices for internet access purposes.
MDT-007	Mobile devices may be connected to other corporate mobile devices and laptops to share their 4G data connection.
MDT-008	Remote access to the corporate network from any device <b>MUST</b> leverage and trigger DCJ's standard multi-factor authentication solution (MFA), which is OKTA, using a user bound strong MFA factor (e.g., one-time password, OKTA Verify Push application) in addition to a username and password.
MDT-009	Only approved remote access solutions may be used to remotely access internal systems and services.
MDT-010	Any vendor, contractor, or third-party supplier using BYO devices <b>MUST</b> use the DCJ Citrix portal, or an approved DCJ VPN with Australia IP to access DCJ applications and networks.
MDT-011	Users intending to access DCJ digital systems (including emails) from overseas <b>MUST</b> comply with the DCJ Remote Working from Overseas Guidelines which align to the Circular <a href="#">DCS-2022-03 Accessing NSW Government digital systems while overseas</a> .
MDT-012	<p>Remote access solutions for non-corporate (BYO devices) or unverifiable devices <b>SHOULD</b> enforce restrictions to protect the corporate environment:</p> <ul style="list-style-type: none"> <li>• Local drives must not be mapped.</li> <li>• Remote drives must not be mapped locally.</li> </ul> <p>Files and folders <b>MUST NOT</b> be moved or copied in and out of the organisation without using an approved mechanism (e.g. email, Kiteworks).</p>
MDT-013	Corporate applications <b>MUST</b> be containerised to ensure application data is encrypted and cannot be transferred outside of the 'container' to non- corporate applications.



Ref	Directive
MDT-014	Loss of corporate or BYO mobile devices that utilise EAS and/or DCJ 'apps' <b>MUST</b> be reported to the IDS Service Desk.
MDT-015	BYO devices may be connected to DCJ end point computing devices with the use of a locally sourced data blocker to prevent malicious file transfer when connected for the purposes of charging.
MDT-016	Downloading or saving DCJ data on personal devices <b>SHOULD NOT</b> be done unless it is on approved BYO services such as DCJ Citrix portal or Office Web Access, as per <i>Data Privacy and Protection Standards SPM-001</i>

## 4.2 Asset management

Ref	Directive
ASM-001	All DCJ owned information assets and information system assets <b>SHOULD</b> be recorded in an asset database or a register. All assets outside of this database <b>SHOULD</b> have a technical preclusion or plan to migrate in.
ASM-002	The asset owner or custodian of all DCJ owned infrastructure (information systems) <b>SHOULD</b> be recorded in the asset database or register. If undefined, the cost centre owner against the asset will be declared the owner.
ASM-003	All DCJ owned information system assets recorded in a CMDB if unlabelled will be considered 'OFFICIAL' as per the Data Privacy and Protection Policy. All entries should however be labelled appropriately.
ASM-004	Information systems which hold sensitive information <b>SHOULD NOT</b> be removed from secure premises without first encrypting or removing the sensitive information.
ASM-005	DCJ is the owner of its Information assets stored in the cloud. The ownership <b>MUST</b> be clearly stipulated in the contract with the cloud service provider (CSP). For further information, please consult <i>Section 5.3.2 Ownership of Assets</i> in the IT Security Policy and <i>Section 5.2 Contracting with Cloud Service Providers</i> in the Cloud Security Policy.

## 4.3 Cryptography

Ref	Directive
CRY-001	<p>Wild card certificates can only be used for approved SSL inspection devices to inspect encrypted data flows. In all other scenarios wild card certificates are not permissible, they <b>MUST NOT</b> be used. Instead, a subject alternate name or similar <b>SHOULD</b> be used.</p> <p>Where appropriate, a separate signing certificate authority <b>SHOULD</b> be used to produce these wildcard certificates.</p>

CRY-002	The root conditional access (CA) <b>SHOULD</b> be kept 'offline' when not in use.
CRY-003	End point entity certificate lifetimes are dependent upon the risk level posed by the entity. <ul style="list-style-type: none"> <li>High risk entities certificate lifetimes <b>SHOULD</b> be no more than 1 year.</li> <li>Low risk entity certificates <b>SHOULD</b> be no more than 2 years.</li> <li>Issuing and root certificates <b>MUST NOT</b> exceed 20 years.</li> </ul>
CRY-004	Encryption <b>SHOULD</b> only be implemented in order to address or reduce a risk. The strength and type must be proportionate to the risk.
CRY-005	Access to generate certificates, modify or create certificate templates <b>MUST</b> be strictly controlled with user access reviews implemented.
CRY-006	All certificates issued to a person or corporate devices in their possession <b>SHOULD</b> be terminated at the cessation of their service.
CRY-007	Application of cryptographic algorithms <b>MUST</b> be in compliance with the DCJ Cryptographic Control Standards
CRY-008	Cryptographic keys <b>SHOULD</b> be stored in a Hardware Security Module (HSM)
CRY-009	For PROTECTED and above classified data, all encryption keys <b>SHOULD</b> be stored and managed by DCJ.
CRY-010	Upon contract termination of the cloud service provider, all cryptographic keys <b>SHOULD</b> be crypto-shredded in the HSM to ensure data cannot be recovered.

#### 4.4 Physical and environmental security

Note: Information processing facilities are offices in which sensitive information is processed.

Computer rooms are facilities which house centralised computing resources such as servers i.e. a data centre.

Ref	Directive
PHY-001	DCJ data centres must be protected by a 24/7 security guard, other computer room locations <b>MUST</b> utilise swipe cards on an as needed basis and have sign in procedures for visitors.
PHY-002	Premises in which DCJ computer rooms reside <b>MUST</b> have ISO 27001 certification.
PHY-003	Computer room access <b>MUST</b> be provided in a least privilege principle and in a temporary fashion where possible.

Ref	Directive
PHY-004	Computer room and record management/information processing facilities access doors <b>MUST</b> automatically close. Doors which are left open should sound an alarm.
PHY-005	Record management/Information processing facilities access <b>SHOULD</b> be controlled on a least privilege principle.
PHY-006	Computer rooms <b>SHOULD NOT</b> have public facing signage that identifies the premises as being used by DCJ.
PHY-007	Chemicals, combustible materials or any abundance of materials which present a fire hazard <b>MUST</b> be appropriately stored at a safe distance from both computer rooms and information processing facilities.
PHY-008	All DCJ information systems (servers and end points) <b>MUST</b> have an automatic screen lock capability which requires a password to unlock. Screen lock <b>MUST</b> occur after no more than 15 minutes of inactivity.
PHY-009	Documents which are sensitive in nature <b>MUST NOT</b> be left unattended, they <b>MUST</b> be stored in lockable cabinets or secured filing rooms.
PHY-010	Access tokens (key or swipe cards) <b>SHOULD</b> provide least privilege access.
PHY-011	Where identification badges are provided, the badges <b>MUST</b> be visibly displayed whilst in DCJ premises.
PHY-012	Where guests are present at a DCJ premise, a visitor's pass <b>MUST</b> be visibly displayed.
PHY-013	Rooms which store or provide access to heightened sensitivity information assets <b>MUST</b> require an access token provided based upon requirement.
PHY-014	Physical security requirements that are specific for protective facilities (e.g. correctional centres) are specified in the <a href="#">Australian Government Protective Security Policy Framework</a> (PSPF). <sup>1</sup> The framework addresses the security requirements for the four areas below: <ul style="list-style-type: none"> <li>• hardware: (PSPF Requirement 3)</li> <li>• security alarm systems (PSPF Requirement 4)</li> <li>• access control (PSPF Requirement 5)</li> <li>• ICT facilities (PSPF Requirement 9).</li> </ul>

## 4.5 Operational procedures and responsibilities

<sup>1</sup>Additional information relating to physical security requirements for entity resources and access to information (data cards, biometrics, tokens etc.) can be found at: [https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-16-entity-facilities\\_0.pdf](https://www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-16-entity-facilities_0.pdf) v2018.2 and <https://www.protectivesecurity.gov.au/system/files/2021-11/PSPF%20Policy%2009%20-%20Access%20to%20information.pdf> v2018.5 (November 2021)

Ref	Directive
OPE-001	Standard operating procedures (SOP) <b>SHOULD</b> be updated/reviewed when a process is modified or if a software/hardware version is changed. Document <b>SHOULD</b> however be reviewed at least annually.
OPE-002	SOPs <b>MUST</b> be approved by the manager (or higher seniority) of the team implementing the procedure
OPE-003	All information system changes <b>MUST</b> be recorded in an approved change management repository.
OPE-004	Changes with the potential to cause adverse impact <b>SHOULD</b> be scheduled outside of business hours.
OPE-005	Standard changes <b>MUST</b> be approved by the Change Advisory Board. Implementation of a standard change must still be documented.
OPE-006	The change implementer <b>MUST</b> not be the approver.

#### 4.6 Controls against malware

Ref	Directive
CON-001	Malware protection software <b>SHOULD NOT</b> just rely upon signature based identification. Heuristics and other advanced techniques <b>SHOULD</b> be enabled.
CON-002	Antivirus protection software <b>MUST</b> report all infections back to a central alerting facility.
CON-003	Malware protection software <b>MUST</b> be reputable and certified by Av- Test.org or similar.
CON-004	Devices which are infected with malware and are at risk of spreading the infection <b>MUST</b> be removed or quarantined from the network as soon as possible.
CON-005	The ability to install local applications <b>SHOULD</b> be limited to approved staff.
CON-006	Network permissions (i.e. Active Directory-based) <b>SHOULD</b> be applied on a least privilege principle to restrict the potential spread and or impact of malware.

#### 4.7 Data backup controls

Data backup controls are set out in the Data Backup and Retention Standards.

#### 4.8 Logging and monitoring

#### 4.8.1 Application/infrastructure

The following standards apply to application servers and infrastructure servers. This could be an email server, a database or an application. Whilst these devices capture 'security events', their purpose is not specifically the implementation or control of security.

Ref	Directive
LMA-001	All audit logs <b>MUST</b> identify the user identification (user id) which instigated an action or event.
LMA-002	System logs <b>MUST</b> identify all key events on the system (e.g. shutdown, start up, purge log).
LMA-003	All audit logs <b>MUST</b> identify the action that occurred with sufficient detail (e.g. process name, file/record name)
LMA-004	All audit logs <b>MUST</b> identify where the action was initiated (i.e. the IP address or location).
LMA-005	All logs <b>MUST</b> be appropriately time stamped in Australian Eastern Standard Time (AEST), Australian Eastern Daylight Time (AEDT) or Greenwich Mean Time (GMT).

Ref	Directive																								
LMA-006	<p>Where possible, all application and infrastructure systems logging configuration <b>SHOULD</b> abide by the below unless a technical ramification prevents compliance. If this is the case, Security Architect securityarchitecture@facs.nsw.gov.au <b>SHOULD</b> be engaged to ensure the most appropriate logging configuration for the system is maintained.</p> <p>The below is the DCJ standard, if however your system needs to abide by a legal requirement, the legal requirement must be complied with first and foremost.</p> <table><tr><th>Characteristic\ system type</th><th>Low impact system</th><th>Moderate impact system</th><th>High/critical impact system or crown jewel</th></tr><tr><td>How long should the logs be kept?</td><td>1-2 weeks</td><td>1-3 months</td><td>3months +</td></tr><tr><td>Do logs need to be centralised?</td><td>No</td><td>Yes, should</td><td>Yes*</td></tr><tr><td>At what frequency should logs be centralised?</td><td>NA</td><td>≤24hours</td><td>≤10 minutes</td></tr><tr><td>Encrypted transfer to log centralisation?</td><td>NA</td><td>No</td><td>If feasible and appropriate</td></tr><tr><td>Restrict access to logs * Logs <b>MUST</b> be centralised to prevent reading or deleting logs by:<ul style="list-style-type: none"><li>• deleting servers/systems comprise this service</li><li>• unauthorised staff</li><li>• the system/service does not provide alerting capabilities</li><li>• centralisation provides a benefit above what is currently offered natively.</li></ul></td><td>Yes</td><td>Yes Yes feasible when:  • deleting servers/systems comprise this service • unauthorised staff • the system/service does not provide alerting capabilities • centralisation provides a benefit above what is currently offered natively.</td><td>Yes</td></tr></table>	Characteristic\ system type	Low impact system	Moderate impact system	High/critical impact system or crown jewel	How long should the logs be kept?	1-2 weeks	1-3 months	3months +	Do logs need to be centralised?	No	Yes, should	Yes*	At what frequency should logs be centralised?	NA	≤24hours	≤10 minutes	Encrypted transfer to log centralisation?	NA	No	If feasible and appropriate	Restrict access to logs * Logs <b>MUST</b> be centralised to prevent reading or deleting logs by: <ul style="list-style-type: none"><li>• deleting servers/systems comprise this service</li><li>• unauthorised staff</li><li>• the system/service does not provide alerting capabilities</li><li>• centralisation provides a benefit above what is currently offered natively.</li></ul>	Yes	Yes Yes feasible when:  • deleting servers/systems comprise this service • unauthorised staff • the system/service does not provide alerting capabilities • centralisation provides a benefit above what is currently offered natively.	Yes
Characteristic\ system type	Low impact system	Moderate impact system	High/critical impact system or crown jewel																						
How long should the logs be kept?	1-2 weeks	1-3 months	3months +																						
Do logs need to be centralised?	No	Yes, should	Yes*																						
At what frequency should logs be centralised?	NA	≤24hours	≤10 minutes																						
Encrypted transfer to log centralisation?	NA	No	If feasible and appropriate																						
Restrict access to logs * Logs <b>MUST</b> be centralised to prevent reading or deleting logs by: <ul style="list-style-type: none"><li>• deleting servers/systems comprise this service</li><li>• unauthorised staff</li><li>• the system/service does not provide alerting capabilities</li><li>• centralisation provides a benefit above what is currently offered natively.</li></ul>	Yes	Yes Yes feasible when:  • deleting servers/systems comprise this service • unauthorised staff • the system/service does not provide alerting capabilities • centralisation provides a benefit above what is currently offered natively.	Yes																						
LMA-007	Logs <b>MUST</b> capture administrative changes either within the application, or on the operating system housing the application.																								
LMA-008	Logs <b>MUST</b> indicate the identity of the person who ‘purged’ the log.																								
LMA-009	All logging systems <b>MUST</b> be time synchronised to a single trustworthy source.																								

Ref	Directive
LMA-010	Logs <b>SHOULD</b> capture the following events for web applications: <ul style="list-style-type: none"><li>• attempted access that is denied</li><li>• crashes and any error messages</li><li>• search queries initiated by users.</li></ul>
LMA-011	Logs <b>SHOULD</b> capture the following events for databases: <ul style="list-style-type: none"><li>• access to particularly important data</li><li>• addition of new users, especially privileged users</li><li>• any query containing comments</li><li>• any query containing multiple embedded queries</li><li>• any query or database alerts or failures</li><li>• attempts to elevate privileges</li><li>• attempted access that is successful or unsuccessful</li><li>• changes to the database structure</li><li>• changes to user roles or database permissions</li><li>• database administrator actions</li><li>• database logons and logoffs</li><li>• modifications to data</li></ul>

#### 4.8.2 Security

The following standards apply directly to systems which provide security control, protection or monitoring. This could include networking equipment (firewalls and core network), intrusion detection systems, AV consoles etc.

Ref	Directive
LMS-001	All audit logs <b>MUST</b> identify the user id an action or event occurred under.
LMS-002	System logs <b>MUST</b> identify all key events on the system (e.g. shutdown, start up, flush log).
LMS-003	All event logs <b>MUST</b> identify the action that occurred with sufficient detail (e.g. process name, file/record name, packet source and destination).
LMS-004	All audit logs <b>MUST</b> identify where the action was initiated (i.e. the IP address or location).
LMS-005	All logs <b>MUST</b> be appropriately time stamped in AEST, AEDT or GMT.

Ref	Directive																		
LMS-006	<p>Where possible, all security systems <b>SHOULD</b> abide by the below unless a technical ramification prevents compliance. If this is the case, Security Architect securityarchitecture@facs.nsw.gov.au <b>SHOULD</b> be engaged to ensure the most appropriate logging configuration for the system is maintained.</p> <p>The below is the standard recommendation, if, however, your system needs to abide by a legal requirement, the legal requirement <b>MUST</b> be complied with first and foremost.</p> <table><tr><th>Characteristic\ system type</th><th>Internal security system</th><th>Border security system</th></tr><tr><td>How long should the logs be kept?</td><td>1-3 months</td><td>3months +</td></tr><tr><td>Do logs need to be centralised?</td><td>Yes*</td><td>Yes*</td></tr><tr><td>At what frequency should logs be centralised?</td><td>≤1hours</td><td>≤10 minutes</td></tr><tr><td>Encrypted transfer to log centralisation?</td><td>No</td><td>If feasible and appropriate</td></tr><tr><td>*Logs <b>MUST</b> be centralised if:<ul style="list-style-type: none"><li>• prevent reading or deleting by unauthorised staff?</li><li>• the system/service does not provide alerting capabilities</li><li>• provides a benefit above what is currently offered natively.</li></ul></td><td>Yes</td><td>Yes</td></tr></table>	Characteristic\ system type	Internal security system	Border security system	How long should the logs be kept?	1-3 months	3months +	Do logs need to be centralised?	Yes*	Yes*	At what frequency should logs be centralised?	≤1hours	≤10 minutes	Encrypted transfer to log centralisation?	No	If feasible and appropriate	*Logs <b>MUST</b> be centralised if: <ul style="list-style-type: none"><li>• prevent reading or deleting by unauthorised staff?</li><li>• the system/service does not provide alerting capabilities</li><li>• provides a benefit above what is currently offered natively.</li></ul>	Yes	Yes
Characteristic\ system type	Internal security system	Border security system																	
How long should the logs be kept?	1-3 months	3months +																	
Do logs need to be centralised?	Yes*	Yes*																	
At what frequency should logs be centralised?	≤1hours	≤10 minutes																	
Encrypted transfer to log centralisation?	No	If feasible and appropriate																	
*Logs <b>MUST</b> be centralised if: <ul style="list-style-type: none"><li>• prevent reading or deleting by unauthorised staff?</li><li>• the system/service does not provide alerting capabilities</li><li>• provides a benefit above what is currently offered natively.</li></ul>	Yes	Yes																	
LMS-007	Logs <b>MUST</b> capture administrative changes either within the application, or on the operating system housing the application.																		
LMS-008	Logs <b>MUST</b> indicate the identity of the person who ‘purged’ the log.																		
LMS-009	All logging systems <b>MUST</b> be time synchronised to a single trustworthy source.																		



Ref	Directive
LMS-010	<p>Logs <b>SHOULD</b> capture the following events for operating systems:</p> <ul style="list-style-type: none"><li>• access to important data and processes</li><li>• application crashes and any error messages</li><li>• attempts to use special privileges</li><li>• changes to accounts</li><li>• changes to security policy</li><li>• changes to system configurations</li><li>• Domain Name System (DNS) and Hypertext Transfer Protocol requests</li><li>• failed attempts to access data and system resources</li><li>• service failures and restarts</li><li>• system startup and shutdown</li><li>• transfer of data to and from external media</li><li>• user or group management</li><li>• use of special privileges.</li></ul>

## 4.9 Vulnerability management

Ref	Directive
VUL-001	All vulnerabilities identified with a highly rated vulnerability or risk <b>MUST</b> be assessed immediately by the Cyber Security team <a href="mailto:security.incident@justice.nsw.gov.au">security.incident@justice.nsw.gov.au</a> and escalated to asset custodian for remediation according to timelines that are stated in vulnerability management procedure document.
VUL-002	An equipment refresh plan <b>MUST</b> be maintained to track the periodic replacement of equipment before they reach end of life (equipment's age, the warranty date and service history), The equipment <b>MUST</b> be thoroughly examined on regular basis for an up-to-date vendor support to ensure continuing reliability of equipment.

## 4.10 Communications security

Ref	Directive
COM-001	Network connections <b>SHOULD</b> always initiate from most secure to least secure network zones. Connections which do not follow this practice <b>SHOULD</b> be intercepted by a reverse proxy or similar which breaks the connection stream and repackages it. This intermediary device <b>SHOULD</b> inspect the traffic and ensure it is free from malware or illegal actions.

Ref	Directive
COM-002	Critical network infrastructure <b>MUST</b> have logging enabled. This logging <b>MUST</b> identify administrative changes along with traffic logging. Where possible these logs should be centralised into a security information and event management (SIEM) tool.
COM-003	Core network paths <b>MUST</b> always be dual thus providing a layer of redundancy.
COM-004	Open shortest path first (OSPF) <b>SHOULD</b> always be the routing protocol used in internal networks.
COM-005	Border gateway protocol (BGP) <b>SHOULD</b> always be the routing protocol used in external or WAN networks.
COM-006	Static routes <b>SHOULD</b> only be used when a technical or security preclusion exists which prevents OSPF or BGP from being used.
COM-007	Permissions to administer core network infrastructure <b>MUST</b> be segregated and only provided to members of the network administration team.
COM-008	Core network infrastructure <b>MUST</b> be on the Australian Signals Directorate (ASD) Evaluated Product List or <b>MUST</b> have obtained an Evaluation Assurance Level 2 (EAL2) or above rating.
COM-009	All network infrastructure <b>SHOULD</b> be on the ASD Evaluated Product List.
COM-010	All network infrastructure <b>SHOULD</b> have a common criteria or EAL certification/rating.
COM-011	Network zones of differing risk or purpose <b>MUST</b> be separated by a firewall which restricts and controls access at a minimum.
COM-012	Information sharing ventures which are allowed or mandated by law <b>MUST</b> obtain assurances from relevant parties that DCJ information will be protected in a suitable manner.
COM-013	Firewall rules which are not Internet based <b>MUST</b> identify a named source, destination and restricted port set.
COM-014	Firewall and routing rules <b>MUST</b> be applied in a least privilege fashion and always attempt to ensure secure protocols are used where technically feasible.
COM-015	Network segments that present a high level of risk <b>SHOULD</b> implement technologies which identify threats and take protective action (i.e. IDS, IPS)
COM-016	Connections to third party providers hosting, storing, creating or using DCJ information <b>MUST</b> be secured.
COM-017	Unused network ports <b>SHOULD</b> be 'shut' or their interfaces disabled to prevent unauthorised connections.

Ref	Directive
COM-018	The DCJ internal network addressing scheme <b>MUST NOT</b> be made visible to external entities other than those we have entered into a contract for service provision from.
COM-019	Routers and firewalls <b>MUST NOT</b> accept external connections that appear to be coming from internal addresses.
COM-020	All internal data transfers which contain credentials <b>SHOULD</b> be encrypted.
COM-021	New network infrastructure with standard/default configurations <b>MUST</b> be overwritten to ensure default credentials etc. are not available.
COM-022	Access from high-risk countries <b>MUST</b> be blocked. Contact Cyber Security <a href="mailto:information.security@justice.nsw.gov.au">information.security@justice.nsw.gov.au</a> for advisories on countries that are listed as high-risk destinations.

#### 4.11 Application security

This section defines the minimum controls that **MUST** be implemented for applications in order to meet the department's Information Security Policy.

Ref	Directive
APP-001	<p><b>Security architecture documentation</b></p> <p>Application security architecture documentation <b>MUST</b> meet the following requirements:</p> <ul style="list-style-type: none"><li>• All application components (either individual or groups of source files, libraries, and/or executable) that are present in the application <b>SHOULD</b> be documented.</li><li>• All components that are not part of the application but that the application relies on to operate <b>SHOULD</b> be documented.</li><li>• A high-level architecture for the application including logical structures, physical structures and dynamic behaviours <b>SHOULD</b> be documented.</li><li>• Application components <b>SHOULD</b> be defined as logical components in terms of the business functions and/or security functions they provide.</li><li>• Application components <b>SHOULD</b> also be described at the physical level of abstraction as deployable libraries, executable or code modules.</li><li>• All components that are not part of the application but that the application relies on to operate are defined in terms of the business functions and/or security functions they provide.</li></ul>

Ref	Directive
APP-002	<p><b>Session management</b></p> <p>Applications <b>MUST</b> meet the following requirements for safely using HTTP requests, responses, sessions, cookies, headers, and logging to manage sessions securely:</p> <ul style="list-style-type: none"> <li>• Sessions <b>MUST</b> be invalidated when the user logs out.</li> <li>• Sessions <b>MUST</b> timeout after a configurable period of inactivity.</li> <li>• All pages that require authentication to access <b>MUST</b> have logout links.</li> <li>• Except where the site is intended to be for anonymous public access, session ids <b>MUST NOT</b> be disclosed other than in cookie headers.</li> <li>• Session ids <b>MUST</b> be changed on re-authentication.</li> <li>• Session ids <b>MUST</b> be changed or cleared on logout.</li> <li>• Applications <b>MUST</b> recognise as valid only those session ids generated by the application.</li> <li>• Authenticated session ids <b>MUST</b> be sufficiently long and unpredictable to withstand typical attacks.</li> <li>• Cookies that contain authenticated session tokens/ids <b>MUST</b> have their domain and path set to an appropriately restrictive value for the site.</li> </ul>
APP-003	<p><b>Security configuration</b></p> <p>Applications <b>MUST</b> meet the following requirements for the secure storage of all configuration information that directs the security-related behaviour of the application:</p> <ul style="list-style-type: none"> <li>• All security-relevant configuration information <b>MUST</b> be stored in locations that are protected from unauthorised access.</li> <li>• The configuration store <b>MUST</b> output in a human-readable format to facilitate audit.</li> </ul>
APP-004	Configuration of automated email forwarding to external non-government domains <b>MUST</b> be controlled and prevented.

## 4.12 Systems acquisition and development

Ref	Directive
SAD-001	All projects which implement new information systems or alter existing ones <b>MUST</b> undergo risk assessment prior to being made production ready.
SAD-002	All projects <b>MUST</b> successfully complete the service transition readiness dashboard prior to being made production ready.
SAD-003	Code maintained by DCJ <b>MUST</b> be stored in an access controlled fashion which suitably tracks versions.

Ref	Directive
SAD-004	Outsourced development providers <b>MUST</b> agree within a contract to act in a manner compliant with DCJ information security policies and standards.
SAD-005	Contracts with outsourced development providers <b>SHOULD</b> contain a right to audit clause.
SAD-006	Approval <b>MUST</b> be obtained from the information owner prior to production information being extracted into a development environment. Furthermore, the data <b>SHOULD</b> be deleted as soon as the testing/development purpose has been achieved.
SAD-007	Production data used in Test environment <b>MUST</b> be scrambled where possible.
SAD-008	System default settings (including default passwords) <b>MUST</b> be reviewed and changed prior to installation.
SAD-009	<p>Where the system is classified as a Crown Jewel, is external facing, or is a cloud service provision, it <b>MUST</b> undertake independent external penetration testing on an annual basis, and after major modification. This applies to all environments, both production and non-production.</p> <p>All other systems <b>SHOULD</b> have periodic penetration tests conducted at least every 3 years, and after major modification. This applies to production environments where technically feasible and in consultation with cyber offensive team consultation.</p> <p>Cyber Security Operations team <a href="mailto:information.security@justice.nsw.gov.au">information.security@justice.nsw.gov.au</a> <b>SHOULD</b> be engaged to:</p> <ul style="list-style-type: none"> <li>• assist with the initiation/planning/operation of the penetration tests</li> <li>• determine whether a system change is classified as 'major' or not</li> </ul>

### 4.13 Supplier relationship

Ref	Directive
SUR-001	Third party providers who transmit, store, use, create or destroy DCJ information <b>MUST</b> undergo a risk assessment prior to procurement to determine if they are compatible with DCJ policy and data privacy and protection requirements.
SUR-002	All third-party providers who are engaged to transmit, store, use, create or destroy DCJ data <b>MUST</b> first sign a non-disclosure agreement with DCJ.
SUR-003	The interconnection configuration of the third party and DCJ <b>MUST</b> be selected based upon the risk profile of the scenario taking into account the connection type, vendor, inferred levels of trust, sensitivity level of data etc.

Ref	Directive
SUR-004	Where possible, all suppliers who transmit, store, use, create or destroy DCJ data <b>SHOULD</b> have ISO 27001 accreditation. Where the third party is a cloud service provider, the information security roles and responsibilities of both parties <b>SHOULD</b> be stated in an agreement as identified in ISO 27017.
SUR-005	Suppliers <b>MUST</b> participate in regular internal or external Information security related audits whose terms of reference covers the services offered to DCJ.
SUR-006	Specific Information security requirements <b>SHOULD</b> be built into the metrics and as part of the commercial agreement and the supplier held accountable for reporting and achieving them.
SUR-007	Suppliers <b>MUST</b> inform DCJ within an acceptable time frame if a security incident has occurred with the potential to impact or interrupt the service offered to DCJ.

#### 4.14 Security incident management

Ref	Directive
SIM-001	Security incidents raised within the service management tool <b>MUST</b> capture the name of the person affected, time the call was raised, general description of the security incident. The incident <b>MUST</b> then be given an appropriate operational and product categorisation and the assigned group set to information security.
SIM-002	Security events which have the potential of affecting other government agencies, or could provide lessons learnt to other government agencies will be shared via GovTEAMS.
SIM-003	Investigations upon a user's internet browsing, email correspondences or use of corporate applications which look to reveal more information than general usage statistics <b>MUST</b> be approved by the appropriate investigative agency e.g. Professional Conduct, Ethics and Performance.
SIM-004	DCJ's incident response plan <b>MUST</b> integrate with the NSW Government Cyber Incident Response Plan and DCJ's Business Continuity Plan and possibly then invoking the relevant disaster recovery technical recovery plan.
SIM-005	An actual or suspected security breach <b>MUST</b> be notified within 48 hours

#### 4.15 Information security in service continuity

Ref	Directive
ISB-001	Recovery plans <b>SHOULD</b> include steps to verify the security controls of the returned service.

ISB-002	Recovery plans <b>SHOULD</b> include steps to securely stand down the recovery environment.
ISB-003	Recovery plans <b>SHOULD</b> include steps to verify the security controls of the recovery environment prior to a continuity being restored.

## 5 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 6 Related legislation, regulation and other documents

This document is related to the IT Security Policy in that it is an implementation of the policy. Other related documents include:

- Cryptographic Control Standards
- Secure Software Development Standards

## 7 Document information

Document name	IT Security Standards
Document reference	D22/1832005
Replaces	IT Security Standards V1.2
Applies to	All staff excluding the Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Chief Digital Information Officer
Approved date	28/09/2023

## 8 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

## 9 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.2	29/06/2022	Annual review	29/06/2023
2.0	28/09/2023	Annual review	28/09/2024



# Cryptographic Control Standards

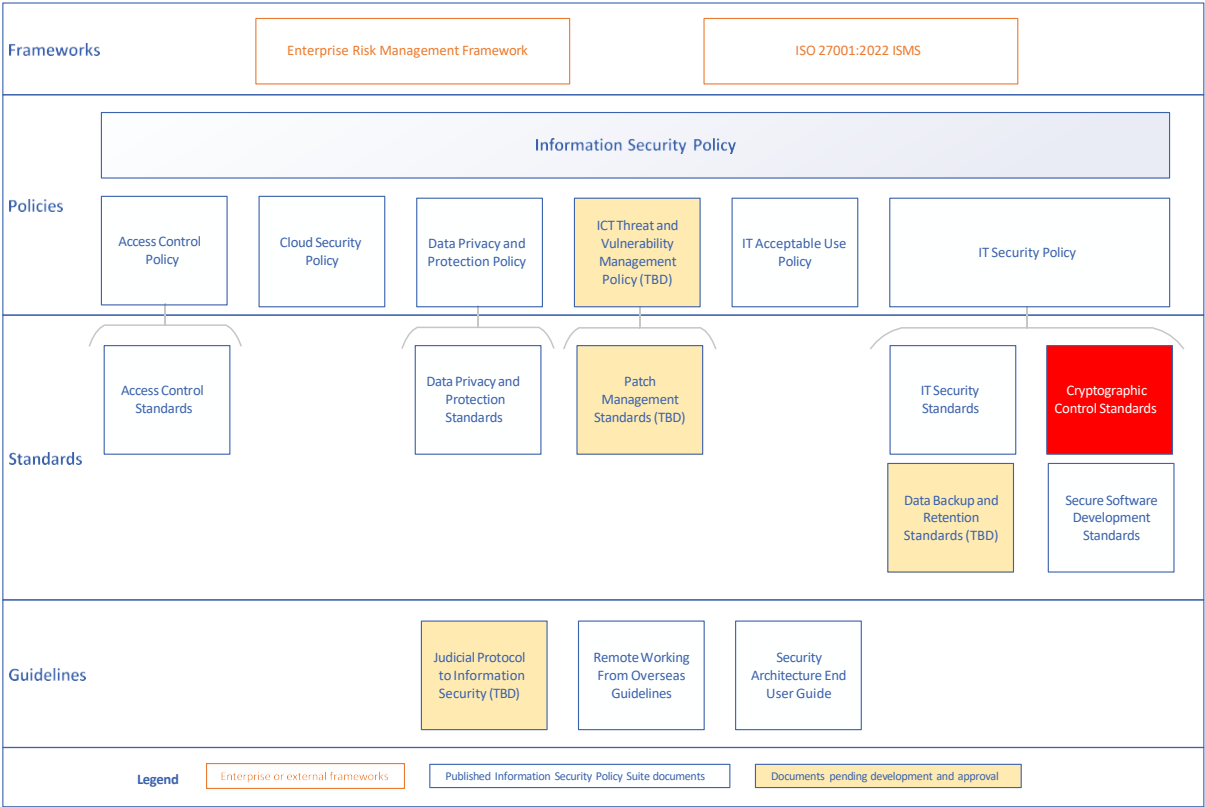
## Contents

	List of Tables .....	2
1	Purpose .....	3
2	Definitions.....	3
3	Scope.....	5
4	Introduction .....	6
	4.1 Data at rest encryption .....	6
	4.2 Data in transit encryption.....	6
5	Approved Cryptographic Algorithms (ACA).....	7
	5.1 Asymmetric Cryptographic Algorithms.....	8
	5.2 Symmetric Cryptographic Algorithms .....	8
	5.3 Hashing.....	8
	5.4 Diffie Hellman Key Exchange .....	9
	5.5 Approved Cryptographic Algorithms and Key Sizes .....	10
6	Asymmetric Key Management .....	11
	6.1 Public Key Certificates .....	11
	6.2 Private Key Management.....	12
7	Approved Cryptographic Protocols (ACPs) .....	12
	7.1 Authentication tokens.....	12
8	SSH - Secure Shell .....	13
	8.1 Using and configuring Secure Shell.....	13
	8.2 SSH Keys usage.....	13
	8.3 SSH-agent.....	14
9	IPsec - Internet Protocol Security .....	15
	9.1 Mode of operation .....	15
	9.2 Protocol selection.....	15
	9.3 Recommended IPsec settings.....	15
10	TLS – Transport Layer Security.....	16
	10.1 Definitions .....	16
	10.2 Using Transport Layer Security .....	16
	10.3 TLS v1.2 secure session key renegotiation .....	17
	10.4 Other HTTPS settings.....	18
	10.5 Which TLS cipher suites to use .....	18

- 10.6 Cipher suites recommended for TLS v1.2 and 1.3..... 20
- 10.7 Unproven TLS cipher suites ..... 21
- 12 Related legislation, regulation and other documents.....22
- 13 Document information .....23
- 14 Support and advice .....23
- 15 Version and review details ..... 23
- A.1 Appendix A - Guidance .....24
- I. References .....28

List of Tables

- Table 1 - Definitions.....5
- Table 2 - Approved Cryptographic Algorithms and key sizes ..... 11
- Table 3 - Approved Cryptographic Protocols..... 12
- Table 4 - SSH Server settings ..... 13
- Table 5 - IPsec settings .....16
- Table 6 - TLS general requirements.....17
- Table 7 - General TLS cipher suites guidance .....20
- Table 8 - Recommended TLS cipher suites.....21
- Table 9 - Not enough researched TLS cipher suites .....22



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

The following standard articulates the Department of Communities and Justice’s (DCJ’s) cryptographic control standards in regard to the IT Security Policy.

2 Definitions

Term	Definition
ACA	Approved Cryptographic Algorithms
ACP	Approved Cryptographic Protocols
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
ASD	Australian Signals Directorate
CBC	Cipher Block Chaining
DH	Diffie-Hellman

Term	Definition
DHE	Ephemeral Diffie-Hellman (for TLS Forward Secrecy)
DLM	Dissemination limiting markers (DLMs) are labels used by the NSW Government to define sensitive information and data
DSA	Digital Signature Algorithm (created by NIST)
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Ephemeral Diffie-Hellman (for TLS Forward Secrecy)
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards (USA)
GCM	Galois/counter - a block cipher
IKE	Internet Key Exchange
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol
May / May not / Recommended	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
MITM	Man-In-The-Middle attack
MD5	Message Digest 5
Must	The item is mandatory Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
NIST	National Institute of Standards and Technology (USA)
NTLM	Windows New Technology LAN Manager. It is the authentication protocol used to authenticate a client to a resource on an Active Directory domain.

Term	Definition
PFS	Perfect forward secrecy. It is an encryption system that changes the keys used to encrypt and decrypt information frequently and automatically to ensure that even if the most recent key is hacked, a minimal amount of sensitive data is exposed.
PSK	Pre-Shared Keys
RSA	Rivest-Shamir-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extension
SHA	Secure Hashing Algorithm
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception is required if condition is not met.
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
Asymmetric encryption	Encryption method based on a public and a private key
Cipher algorithm	A method used for data encryption/decryption (designed specifically to obscure the value and content of data)
Symmetric encryption	Encryption method based on a single (session) key

Table 1 - Definitions

### 3 Scope

The requirements and expectations outlined in this document applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This standard does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

The controls in this document **MUST** be followed for any *new* or *not-yet-deployed* projects and infrastructure, and it **SHOULD** be followed -and ultimately complied with- for the *existing deployments*, while any related non-compliance matters will be assessed and dealt with as per the regular process.

Therefore, it applies to all DCJ information technology deployed on premises or outside the organisation by internal teams or external providers or partners and, in summary, by anyone designing, implementing, operating or using IT components handling DCJ data.

## 4 Introduction

This document has a policy section with prescribed settings and a guidance section in Appendix A.

### 4.1 Data at rest encryption

For the encryption of the stored data / "**data at rest**" various applications based on the approved symmetric and asymmetric encryption may be used.

While no software is bullet-proof, a well-built (and therefore well-reviewed) application that will make use of the symmetric and asymmetric **ACA** (Approved Cryptographic Algorithms) - as shown in the section below- could be deemed as acceptable.

*For example, the PGP (paid) and GnuPG (freeware) encryption applications are using a series of crypto algorithms while the **ACA** (Approved Cryptographic Algorithms) ones should be **preferred**:*

*Asymmetric encryption (Public key)*

- **RSA, DSA, ECDH, ECDSA**

*Symmetric encryption Ciphers*

- **AES-128, -192, and -256 (preferred)**
- **SHA-256, SHA-384, SHA-512, SHA-224**

### 4.2 Data in transit encryption

For the “**data in transit**” (traffic flows) encryption requirements, *Section 7 Approved Cryptographic Protocols* provides the required requirements and guidelines.

4.2.1 Remote access protocols

As related to the traffic flows protection, the remote access protocols **SHOULD** make use of these Approved Cryptographic Protocols.

For example, the SSH v.2 protocol is always preferred whenever usable.

Then, for other platforms, the Microsoft RDP traffic **SHOULD** be implemented to use TLSv1.2 based encryption (with only strong cipher suites) rather than using the native MS RDP protocol encryption.

4.2.2 Authentication mechanisms

Public key-based authentication schemes offer stronger authentication than passphrase-based authentication schemes due to passphrases being more susceptible to guessing attacks.

Therefore, if passphrases are used, countermeasures **SHOULD** be put in place to reduce the chance of a successful brute force attack.

5 Approved Cryptographic Algorithms (ACA)

Cryptographic algorithms are processes or rules, which, through the use of encryption, authentication, and digital signatures, protect data by making sure that unauthorised people can't access.

The ACAs fall into three categories:

- asymmetric/public key algorithms,
- symmetric encryption algorithms, and
- hashing algorithms.

Directive	Definition
ACA-001	<p>The approved asymmetric/public key algorithms are:</p> <ul style="list-style-type: none"><li>• Diffie-Hellman (<b>DH</b>) for session key exchanges</li><li>• Digital Signature Algorithm (<b>DSA</b>) for digital signatures</li><li>• Elliptic Curve Diffie-Hellman (<b>ECDH</b>) for session key exchanges</li><li>• Elliptic Curve Digital Signature Algorithm (<b>ECDSA</b>) for digital signatures</li><li>• Rivest-Shamir-Adleman (<b>RSA</b>) for digital signatures and passing encryption session keys or similar keys</li></ul>

Directive	Definition
ACA-002	As per ACSC, the DH and DSA algorithms are vulnerable to different attacks than ECDH and ECDSA. However, ECDH and ECDSA offer more effective security per bit increase.  For reduced data cost, and to promote interoperability, ECDH and ECDSA <b>SHOULD</b> be used whenever possible.
ACA-003	All block cipher algorithms, where data is transformed from plain text to encrypted text in blocks, <b>MUST NOT</b> be used in Electronic Code Book (ECB) or CBC (Cipher Block Chaining) modes.
ACA-004	For NSW DLM classified information (or above) that requires cryptographic protection, the minimum algorithm/key length (as shown in <i>Section 5.5 Approved Cryptographic Algorithms and Key Sizes</i> ) <b>MUST</b> be satisfied, but a higher rated algorithm or key length may be used as well.

## 5.1 Asymmetric Cryptographic Algorithms

Asymmetric Cryptographic Algorithms are using a public key and a private key, and the mathematical fact that whatever is encrypted with one key can be decrypted only with the other one.

The public key can be given to anyone (like via the public SSL/TLS server's certificate), while the private key **MUST** be kept secret.

## 5.2 Symmetric Cryptographic Algorithms

Different from the Asymmetric Cryptographic Algorithms, the Symmetric Cryptographic Algorithms use the same secret key to encrypt and decrypt sensitive information.

That also makes them computationally faster than the asymmetric cryptographic algorithms group.

Directive	Definition
SCA-001	The only formally approved symmetric encryption algorithm is <b>Advanced Encryption Standard (AES)</b> using key lengths of 128, 192 and 256 bits.

## 5.3 Hashing

Unlike encryption algorithms, the hashing algorithms are one-way transformations of data, so that data cannot be unscrambled and decoded by anyone else.

Hashing of large chunks of data can be used to prove that such data isn't adjusted or altered after the authoring is finished, and therefore it is used to provide integrity checks aimed to validate the integrity of files, documents, and other types of data.



Then, hashing is also widely used in authentication systems to avoid storing plaintext passwords in databases.

Directive	Definition
HASH-001	The only approved hashing algorithm is <b>Secure Hashing Algorithm 2</b> - SHA-2- (i.e., SHA-224, SHA-256, SHA-384 and SHA-512).
HASH-002	The older hashing algorithms (SHA-1 / SHA and MD5) are deemed as ' <i>security weak</i> ' and therefore <b>SHOULD NOT</b> be used hashing algorithms.
HASH-003	SHA-1 and MD5 algorithms MAY only be used (based on a risk analysis) where the hashing manipulation risk is low and is about non-sensitive data cases and only whenever is not possible to use SHA-2.

## 5.4 Diffie Hellman Key Exchange

Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel. Such keys are not actually exchanged but they are jointly derived by the parties.

Diffie Hellman key exchanges provide a level of assurance that two endpoints can communicate secretly. They provide no assurance as to the identity of the endpoint. Consequently, they are not appropriate for authentication.

Directive	Definition
DH-001	Any key exchange using Diffie Hellman <b>MUST</b> securely identify the other endpoint, without exposing any authentication information or key-matter, before any other data is exchanged.

A key modulus of 2048 bits of correctly implemented DH provides 112 bits of effective security strength. Considering projected technological advances, ASD is assessing that, 112 bits of effective security strength (corresponding to a key of 2048 bits) will remain secure until the year 2030.

The recommended "*next generation*" Elliptic Curve DH Groups are predicted to provide adequate encryption protection against modern threats until 2040.

Directive	Definition
DH-002	Therefore, the <b>recommended</b> DH groups are: <ul style="list-style-type: none"> <li>• Diffie-Hellman Group 14 (2048-bit modulus)</li> <li>• Diffie-Hellman Group 15 (3072-bit modulus)</li> <li>• Diffie-Hellman Group 24 (2048-bit modulus and a 256-bit prime subgroup)</li> </ul>

Directive	Definition
DH-003	The <b>recommended</b> <i>Next Generation</i> EDH Elliptic Curve Groups are: <ul style="list-style-type: none"> <li>Diffie-Hellman Group 19 (256-bit random)</li> <li>Diffie-Hellman Group 20 (384-bit random)</li> <li>Diffie-Hellman Group 21 (521-bit random)</li> </ul>
DH-004	Old DH groups (with weaker encryption) that <b>MUST NOT</b> be used, are: <ul style="list-style-type: none"> <li><i>Diffie-Hellman Group 1 (768-bit)</i></li> <li><i>Diffie-Hellman Group 2 (1024-bit)</i></li> <li><i>Diffie-Hellman Group 5 (1536-bit)</i></li> </ul>

## 5.5 Approved Cryptographic Algorithms and Key Sizes

Directive	Definition
ACA-KS-001	For NSW DLM categorised (or above) information that requires cryptographic protection, the minimum algorithm/key length (as shown in <i>Section 5.5 Approved Cryptographic Algorithms and Key Sizes</i> ) <b>MUST</b> be satisfied, but a higher rated algorithm/key length may be used as well.
ACA-KS-002	When using elliptic curve cryptography, a NIST prime curve from FIPS 186-4 <b>MUST</b> be used (refer to <a href="https://csrc.nist.gov/publications/detail/fips/186/4/final">https://csrc.nist.gov/publications/detail/fips/186/4/final</a> ).
ACA-KS-003	The following table shows the Approved Cryptographic Algorithms and the related Key sizes.

Purpose	Type	Algorithm	Key size for Sensitive data	Recommended for Protected data
Encryption ( <i>Shared secret, faster, used for encryption at rest, or streaming</i> )	Symmetric / Session key	AES	AES-128	AES-256
			AES-192	
			AES-256	
Hashing ( <i>Integrity, irreversible transformation</i> )	Hash	SHA-2	SHA-256	SHA-384
			SHA-384	
			SHA-512	
Digital signatures ( <i>Authenticity, integrity, encryption with no shared secret</i> )	Asymmetric / public & private keys	ECDSA	NIST P-256	NIST Curve P- 384
			NIST P-384	
			NIST P-521	
		DSA	2048-bit key or larger	3072-bit key

Purpose	Type	Algorithm	Key size for Sensitive data	Recommended for Protected data
Key exchange (Encryption with no shared secret)	Asymmetric / public & private keys	DH	2048-bit key or larger	3072-bit key
		ECDH	NIST P-256	NIST Curve P- 384
			NIST P-384	
			NIST P-521	
		RSA	2048-bit key or larger	3072 bits key

Table 2 - Approved Cryptographic Algorithms and key sizes

NOTE:

- NIST P-256 = NIST/FIPS defined Curve over Prime Fields with a modulus of 256.

## 6 Asymmetric Key Management

### 6.1 Public Key Certificates

While the public certificates infrastructure is the cornerstone for the public secure Internet communications, some due care is still needed in maintaining and using it. That is because, currently, any trusted Certificate Authority (CA) can validly sign TLS certificates for any web site, including for \*.microsoft.com or

\*.google.com, while that can include some insecure lower tier CAs.

Therefore, highly secure devices -dedicated to some narrow functions- that don't necessarily need to trust all default CAs (e.g., Verisign, Thawte, etc.) by permitting all CAs in their local trusted certificate store(s) that may only create potential security holes, so it is recommended to be removed when not need.

For example, some special purpose appliances, edge or some security devices - like the virtual private network (VPNs)-, would likely benefit from having those **other** non-essential certificate authorities removed.

Doing that will avoid trusting unnecessarily a large list of public CAs, that, by the law of probabilities, it may get a chance to get one such system being breached and issuing rogue TLS certificates. Such a defence may not apply to general use systems and desktops having to browse the larger Internet, but it can be effective to some specialised devices.

Directive	Definition
AMK-001	When relying on a public key certificate as an identifier, the relying system <b>MUST</b> check the entire trust chain of the certificate.
AMK-002	Systems <b>MUST NOT</b> use any information contained in a certificate that is not signed by a Certification Authority (CAs) trusted by that system

Directive	Definition
AMK-003	Systems <b>SHOULD</b> only trust the minimum set of CAs required to satisfy their primary purpose

## 6.2 Private Key Management

Directive	Definition
AMK-004	Asymmetric private keys used to protect SENSITIVE (and above) material <b>MUST NOT</b> appear unencrypted outside the cryptographic boundary of a hardware security module, such as a smart card, etc.

## 7 Approved Cryptographic Protocols (ACPs)

If any hardware or software implements unapproved protocols, it is possible that these protocols could be used without a user's knowledge. In combination with a potentially wrongly assumed level of security confidence, this can represent a security risk.

As such, one can ensure that only ACPs or high assurance cryptographic protocols can be used by disabling the unapproved protocols.

Directive	Definition
ACP-001	As advised by ACSC, these are the current ACPs (Approved Cryptographic Protocols): <ul style="list-style-type: none"> <li>• Secure Shell (SSH) v.2</li> <li>• Internet Protocol Security (IPsec)</li> <li>• Transport Layer Security (TLS) v.1.2 and above</li> <li>• Wi-Fi Protected Access 2</li> <li>• Wi-Fi Protected Access 3</li> <li>• Kerberos</li> <li>• SAML</li> </ul>
ACP-002	For the encrypted email traffic, the protocols are: <ul style="list-style-type: none"> <li>• Secure/Multipurpose Internet Mail Extension (S/MIME)</li> <li>• OpenPGP Message Format.</li> </ul>

Table 3 - Approved Cryptographic Protocols

### 7.1 Authentication tokens

Whenever applicable, the Kerberos bases authentication mechanisms **MUST** be used in place of NTLM or other legacy protocols.

The SAML v.2.0 tokens are acceptable ways to integrate with various federated authentication services.

## 8 SSH - Secure Shell

### 8.1 Using and configuring Secure Shell

When using equipment or software that implements SSH, the below configuration controls **SHOULD** be followed.

SSH v.2 authentication can use password, SSH-keys and PKI certificates, while all private keys **MUST** be protected against unintended disclosure.

Directive	Definition
SSH-001	SSH ver.1 protocol is insecure and <b>MUST NOT</b> be used.
SSH-002	SSH ver.2 <b>MUST</b> be used while following the bellow secure configuration
SSH-003	Host based authentication <b>MUST NOT</b> be used but only user-based authentication <b>MUST</b> be used.  <i>Automated hosts and applications triggered SSH access can be done in a safer way via the deployment of user based authorised SSH keys.</i>
SSH-004	The below SSH server configuration settings best practices <b>SHOULD</b> be used with any SSH server deployment.

NOTE: This is based on OpenSSH, while other implementations of SSH **SHOULD** adapt these settings to their SSH server version syntax.

SSH v.2 server configuration directive	Value
<i>only listen on the required local interfaces</i>	<b><i>ListenAddress xxx.xxx.xxx.xxx</i></b>
<i>have a suitable login banner</i>	<b><i>Banner x</i></b>
<i>have a login authentication timeout of no more than 60 seconds</i>	<b><i>LoginGraceTime 60</i></b>
<i>disable host-based authentication</i>	<b><i>HostbasedAuthentication no</i></b>
<i>disable rhosts-based authentication</i>	<b><i>IgnoreRhosts yes</i></b>
<i>disable the ability to login directly as root</i>	<b><i>PermitRootLogin no</i></b>
<i>disable empty passwords</i>	<b><i>PermitEmptyPasswords no</i></b>
<i>disable connection forwarding</i>	<b><i>AllowTCPForwarding no</i></b>
<i>disable gateway ports</i>	<b><i>GatewayPorts no</i></b>
<i>disable X11 forwarding</i>	<b><i>X11Forwarding no</i></b>

Table 4 - SSH Server settings

### 8.2 SSH Keys usage

The SSH deployments MAY utilise user based authorised SSH keys instead of password authentication if the client system access to the SSH keys is properly secured.

However, it must be noted that the unsecured and unmanaged SSH keys could be also a source of insecurity.

In terms of management, the SSH keys **MUST** be rotated like the passwords as per the access policy applicable to that related user.

Directive	Definition
SSHK-001	The secure use of properly rotated SSH keys is preferred to the use of passwords, especially for unattended logins.
SSHK-002	The SSH keys rotation <b>MUST</b> be done in the same way as it is done for the passwords while related to the type of related user.
SSHK-003	Access to the private SSH-key <b>MUST</b> be protected and strictly limited as per the “least privilege” principle.
SSHK-004	The access to the private SSH-key <b>SHOULD</b> be protected with a passphrase (compliant with the password standard) in addition to the restricted OS based file access permissions.  (For other options : <a href="https://www.ssh.com/academy/ssh/key#moving-ssh-keys-to-a-root-owned-location">https://www.ssh.com/academy/ssh/key#moving-ssh-keys-to-a-root-owned-location</a> )
SSHK-005	For any unattended uses of SSH-keys based logins, additional login access related restrictions <b>SHOULD</b> be attached to that key usage.
SSHK-006	SSH-keys based access restrictions <b>SHOULD</b> be implemented on the destination server (via ~/.ssh/authorized_keys – on OpenSSH) to further limit the activity of the keys-based login.  This could cover the allowed incoming IPs, working directory, allowed commands, terminal prompt, etc. (For further details see here : <a href="https://www.ssh.com/academy/ssh/authorized_keys/openssh">https://www.ssh.com/academy/ssh/authorized_keys/openssh</a> )

For further details see: <https://www.ssh.com/academy/ssh/key> .

### 8.3 SSH-agent

SSH connections **MAY** make use of agent forwarding in some controlled configurations.

- Agent forwarding is the process by which a remote device can use a key caching agent on a remote device to negotiate authentication to another node.
- SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems

to verify these keys. When an SSH-agent launches, it requests the user’s passphrase to unlock the user’s private key.

- Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their passphrase. Screen locks and expiring key caches ensure that the user’s private key is not left unlocked for a long period of time.

Directive	Definition
SSHA-001	Users <b>MAY</b> run an SSH key caching agent on their local workstations only as long as they are attending the workstation.  SSH private key locking <b>MUST</b> be in place for such workstations.
SSHA-002	SSH key caching agents <b>SHOULD NOT</b> be installed or run on any device other than a user’s local workstation
SSHA-003	SSH connections <b>MAY</b> make use of agent forwarding.
SSHA-004	To limit the exposure of credentials, agent credential forwarding <b>SHOULD only</b> be enabled when <b>SSH traversal</b> (through multiple systems) is required.

## 9 IPsec - Internet Protocol Security

### 9.1 Mode of operation

IPsec can be operated in **transport** mode or **tunnel** mode.

The **transport** mode of operation only encapsulates the payload of the IP packet (therefore leaving all IP datagram header details of the packets in clear text, like source, destination, ports, IP flags, etc.)

The **tunnel** mode of operation provides full encapsulation of IP packets (so the source and destination IPs and ports are encrypted).

**This mode allows the best privacy of the communication.**

### 9.2 Protocol selection

IPsec contains two major protocols, **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)** while AH and ESP can provide authentication for the entire IP packet and the payload respectively.

**ESP** is generally preferred for authentication since AH -by its nature- has network address translation limitations.

*For more IPsec protocol and configuration details check Section A.1.3 IPsec Protocol in the below Section A1 Appendix A - Guidance chapter.*

### 9.3 Recommended IPsec settings

Directive	Definition
IPsec-001	IPsec related protocols that <b>SHOULD</b> be used: ESP, IKE, NAT Traversal
IPsec-002	<b>MUST</b> use Internet Key Exchange ver.1 or ver.2
IPsec-003	<b>SHOULD</b> use ISAKMP “Main” mode (try to <b>AVOID</b> Aggressive mode)
IPsec-004	ISAKMP symmetric encryption <b>MUST</b> use AES (with keys lengths of 128, 196, <b>256 bits</b> )
IPsec-005	Parties’ authentication <b>SHOULD</b> use PKI certificates or Pre Shared Keys longer than 32 chars (best 128 when supported)
IPsec-006	Message Authentication Code <b>MUST</b> use HMAC-SHA256, HMAC- SHA384, HMAC-SHA512
IPsec-007	Perfect Forward Secrecy <b>MUST</b> be used and implemented with : <ul style="list-style-type: none"> <li>• DH groups: 14, 15, 24,</li> <li>• EDH groups 19, 20, 21</li> </ul>
IPsec-008	Security Associations lifetimes <b>SHOULD</b> be <ul style="list-style-type: none"> <li>• For phase#1: 4 hrs/14400 secs,</li> <li>• For phase#2: 1 hr/3600 secs</li> </ul>
IPsec-009	IKE v1 with Xauth <b>MUST NOT</b> be used

Table 5 - IPsec settings

See more details in *Section A1 Appendix A - Guidance*.

## 10 TLS – Transport Layer Security

### 10.1 Definitions

The terms Secure Sockets Layer (SSL) and Transport Layer Security (TLS) traditionally have been used interchangeably. However, as SSL 3.0 is no longer acceptable, instances of ‘SSL’ refer to SSL version 3.0 and below while ‘TLS’ refers to TLS 1.0 and beyond ([refer to Section I References for the ACSC TLS information link](#)).

### 10.2 Using Transport Layer Security

The latest version of TLS is version 1.3, which was released in August 2018 and it is the ACSC advised TLS protocol.

When using equipment or software that implements TLS, the following requirements and guidelines **MUST** be observed for the traffic encryption:

Directive	Definition
<b>MUST</b>	



Directive	Definition
TLS-001	<b>MUST</b> use TLS v1.3 whenever available. TLS v1.2 is allowed as a fall back until TLS v1.3 protocol will become available for that connectivity.
TLS-002	TLS v1.2 <b>MUST</b> be used only with strong cipher algorithms.
TLS-003	The (Perfect) Forward Secrecy ( <b>PFS</b> or just <b>FS</b> ) mode for the session key renewal <b>MUST</b> be used when available as it reduces the impact of the compromise of a TLS session.
TLS-004	DHE or ECDHE <b>MUST</b> be used for key establishment while also the cipher ephemeral variants <b>MUST</b> be used.
TLS-005	SHA-2 certificates signing <b>MUST</b> be used.
TLS-006	Cipher suites <b>MUST</b> be configured to use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function.
TLS-007	Only server-initiated secure renegotiation <b>MUST</b> be used.
<b>SHOULD</b>	
TLS-008	AES in GCM mode <b>SHOULD</b> be used for the symmetric encryption.
TLS-009	Weaker cipher suites that do not support PFS <b>SHOULD</b> be avoided when possible ( <i>refer to Section I <a href="#">References</a> for the external PFS information links</i> ).
<b>MUST NOT</b>	
TLS-010	Any protocols earlier than TLS v1.2 <b>MUST NOT</b> be used.
TLS-011	CBC or SHA-1 based cipher suites <b>MUST NOT</b> be used.
TLS-012	Anonymous DH or ECDH <b>MUST NOT</b> be used.
TLS-013	TLS compression <b>MUST NOT</b> be used (keep disabled).
TLS-014	A combination of strong and weak cipher suites <b>MUST NOT</b> be used for a TLS service if there is a chance for the session automatic selection of a weak cipher over insecure network paths.

Table 6 - TLS general requirements

## NOTES:

- The TLS encryption features of a service can be tested with an SSL scanning tools like this: <https://www.ssllabs.com/ssltest/>.
- Further information about some particular cipher suites and their encryption strength level can be found here: <https://ciphersuite.info>.

### 10.3 TLS v1.2 secure session key renegotiation

TLS 1.3 does not use renegotiation, however, if using TLS 1.2 or earlier, renegotiation may be required under certain circumstances.

For example, when a session has expired but parties wish to send more data, a peer wants to change cipher suites or there is a need for the parties to perform authentication a session key renegotiation is needed. Unfortunately, the TLS v1.2 session key renegotiation is susceptible to MITM attacks.

For TLS 1.2, **server-initiated** secure **renegotiation** **SHOULD** be enabled to reduce susceptibility to MITM attacks.

**Client-initiated renegotiation**, secure or otherwise, imposes a performance impact on web servers. A malicious client can send many renegotiation requests to consume server resources causing a denial of service.

For more information on this subject see McAfee's [Tips for Securing SSL Renegotiation](#) advice.

Directive	Definition
SR-001	For TLS 1.2, server-initiated secure renegotiation <b>SHOULD</b> be enabled to reduce susceptibility to MITM attacks.
SR-002	For TLS 1.2 or earlier, client-initiated renegotiation <b>SHOULD</b> be disabled to prevent some denial-of-service attacks.

## 10.4 Other HTTPS settings

**TLS compression** was used to decrease the bandwidth of TLS communications. However, TLS compression has been found to inadvertently leak information and **MUST** not be used.

**HTTP Strict Transport Security (HSTS)** is a web security policy mechanism that helps protect users. It achieves this by allowing web servers to tell web browsers that they **SHOULD** only interact with a web server over HTTPS.

As such, web browsers will dynamically adjust any HTTP requests to use the HTTPS requests when available. HSTS also helps to protect against eavesdropping, MITM attacks and active network attacks.

HSTS **SHOULD** be aimed to be used for the HTTPS service.

Directive	Definition
TLSO-001	TLS compression <b>MUST</b> be disabled whenever possible.
TLSO-002	HSTS <b>SHOULD</b> be aimed to be used for the HTTPS service.

## 10.5 Which TLS cipher suites to use

### 10.5.1 Security challenge

During a client and server TLS ciphers suites negotiation, the client and the server present to each other their available cipher suites, and they will choose

from those cipher suites that they have in common. This process is called the crypto policy negotiation between the TLS parties.

Each such TLS cipher suite is a set combination of cryptographic algorithms, used for the various phases and aspects of an encrypted traffic flow, which will deal with:

- the initial public key asymmetric encryption,
- the session key symmetric encryption,
- the message integrity hash,
- the session key renegotiation, and
- the perfect forward secrecy algorithm.

Some TLS services (on either the client or the server) are using, sometimes by default, configurations of cryptographically weak ciphers suites mixed together with strong ciphers suites support. This may be, at times, a deliberate decision aimed to provide support to (quite) old browsers.

Such situations will leave the TLS encryption negotiation vulnerable to a **MITM** attack that lowers the encryption grade of the TLS flow to a weak cipher (with known or even published exploits) that can be decrypted by the attacker.

This is done by removing the strong cipher suites from the intercepted initial clear text exchange of the crypto policies between the client and the server, and therefore leaving the client and the server to choose only from a small selection of weak ciphers – that the attacker knows how to decrypt.

*(For more info go to Section I [References for the external MITM article link](#)).*

### 10.5.2 Security mitigation

In order to mitigate for such attacks, the following **MUST** be observed:

Directive	Definition
USE-001	If using Elliptic Curve cryptography, a curve as defined in the NIST (Federal Information Processing Standard) FIPS 186-4 <b>SHOULD</b> be used.
USE-002	For the Certificates Digital Signature Algorithm, it is <b>Recommended</b> to use: <ul style="list-style-type: none"><li>• the Elliptic Curve Digital Signature Algorithm (<b>ECDSA</b>) (256-bit or larger)</li><li>• or Rivest-Shamir-Adleman (<b>RSA</b>) (2048-bit or larger).</li></ul>

Directive	Definition
USE-003	<p>The following deemed “cryptographically weak” cipher algorithms <b>MUST NOT</b> be used in any cipher suites combinations:</p> <ul style="list-style-type: none"><li>• Rivest Cipher 2 (RC2)</li><li>• Rivest Cipher 4 (RC4)</li><li>• Message-Digest 5 (MD5)</li><li>• Data Encryption Standard (DES)</li><li>• EXPORT</li><li>• NULL</li><li>• CBC</li><li>• SHA v.1</li><li>• Anonymous Diffie-Hellman (ADH / DH anon))</li><li>• Anonymous Elliptic Curve Diffie-Hellman (AECDH / ECDH anon)</li></ul>

Table 7 - General TLS cipher suites guidance

Cipher suites **SHOULD** be configured in the order of preference (i.e., servers should prefer the better cipher suites listed in a top to bottom order).

Further best practice advice can be found in **TLS Deployment Best Practices** - <https://www.ssllabs.com/projects/best-practices/>.

For up-to-date ciphers suites strengths information, these can be checked on sites like this: <https://ciphersuite.info>.

## 10.6 Cipher suites recommended for TLS v1.2 and 1.3

TLS v1.3 is always recommended to be used when available. However, when not available using TLS v1.2 with strong ciphers is also acceptable.

Directive	Definition
TLSREC-001	<p>The TLS v1.3 <b>recommended</b> cipher suites are:</p> <ul style="list-style-type: none"><li>• TLS_AES_256_GCM_SHA384</li><li>• TLS_AES_128_GCM_SHA256</li><li>• TLS_AES_128_CCM_SHA256</li><li>• TLS_AES_128_CCM_8_SHA256</li></ul>

Directive	Definition
TLSREC-002	<p>Use with caution this TLS v1.3 cipher suite:</p> <ul style="list-style-type: none"> <li>The cipher suite “TLS_CHACHA20_POLY1305_SHA256” MAY provide better performance on platforms which do not have AES hardware support, such as ARM-based devices like mobile phones, tablets and low-end laptops.</li> <li>However, while there are no publicly disclosed weaknesses with this cipher suite, it has not been subjected to the same standard of review and analysis as the recommended cipher suites.</li> </ul>
TLSREC-003	<p>The TLS v1.2 <b>recommended</b> cipher suites</p> <ul style="list-style-type: none"> <li>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</li> <li>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>TLS_DHE_DSS_WITH_AES_256_GCM_SHA384</li> <li>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</li> <li>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</li> <li>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</li> <li>TLS_DHE_DSS_WITH_AES_128_GCM_SHA256</li> <li>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</li> <li>TLS_ECDHE_ECDSA_WITH_AES_256_CCM</li> <li>TLS_DHE_RSA_WITH_AES_256_CCM</li> <li>TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8</li> <li>TLS_DHE_RSA_WITH_AES_256_CCM_8</li> <li>TLS_ECDHE_ECDSA_WITH_AES_128_CCM</li> <li>TLS_DHE_RSA_WITH_AES_128_CCM</li> <li>TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8</li> <li>TLS_DHE_RSA_WITH_AES_128_CCM_8.</li> </ul>

Table 8 - Recommended TLS cipher suites

More cipher suites information can be found here: <https://ciphersuite.info> .

## 10.7 Unproven TLS cipher suites

As per ACSC, while based on a risk decision, one **MAY** use one of the below unproven cipher suites as they may provide better performance on platforms which do not have AES hardware support, such as ARM-based devices like mobile phones, tablets and low-end laptops.

However, while there are ***no publicly disclosed weaknesses*** with these cipher suites they ***have not been subjected to the same standard of review*** and analysis as the recommended cipher suites.

Therefore, the below cipher suites (crypto algorithms combinations) **SHOULD** be used only in situations where the professionally assessed risk is minimal.

Directive	Definition
UNPRV-001	<p>Use with caution.</p> <p>The unproven / Not enough researched cipher suites are:</p> <ul style="list-style-type: none"> <li>• <b>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256</b></li> <li>• <b>TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256</b></li> <li>• <b>TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256</b></li> <li>• TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384</li> <li>• TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384</li> <li>• TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384</li> <li>• TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384</li> <li>• TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384</li> <li>• TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384</li> <li>• TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256</li> <li>• TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256</li> <li>• TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256</li> <li>• TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256</li> <li>• TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256</li> <li>• TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256</li> <li>• TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256</li> <li>• TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256</li> </ul>

*Table 9 - Not enough researched TLS cipher suites*

Alternatively, for safer protection needs just use just the approved TLS cipher suites even when not using any hardware support.

More information on cipher suites can be found here: <https://ciphersuite.info>.

## 11 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 12 Related legislation, regulation and other documents

This document is related to the IT Security Policy in that it is an implementation of the policy. Other related documents include:

- IT Security Standards

## 13 Document information

Document name	Cryptographic Control Standards
Document reference	D22/1684390
Replaces	Cryptographic Control Standards v1.0
Applies to	Everyone that does any IT work on the DCJ network or provides an IT service for DCJ
Policy administrator	Chief Information Security Officer
Approval	Chief Digital Information Officer
Approved date	28/09/2023

## 14 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:facsecuritygovernance@dcj.nsw.gov.au">facsecuritygovernance@dcj.nsw.gov.au</a>

## 15 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.0	10/06/2022	Annual review due	10/06/2023
2.0	28/09/2023	Annual review Transferred to new DCJ Document Template and minor edits	28/09/2024

## A.1 Appendix A - Guidance

### A.1.1 Using Approved Cryptographic Algorithms

If cryptographic hardware or software implements unapproved cipher algorithms, it is possible that these algorithms could be used without a user's knowledge or control. In combination with an assumed level of security confidence, this situation can represent a security risk.

As the traffic flow encryption security policy (i.e., cipher algorithms) negotiation is agreed between the TLS client and the server based on the comparison of each side's advertised supported ciphers (and each side's default preference), a MITM attack could lower the encryption strength of the traffic to weak common ciphers (i.e., ciphers that have published attacks).

However, while not that frequent, the MITM attacks are more likely to happen over insecure or uncontrollable long routing paths between the TLS traffic partners, like Internet or a long traversal of a large private network ([refer to Section I References for the external MITM article link](#)).

To mitigate that, one can ensure that only approved algorithms can be used for such traffic flows by disabling all unapproved crypto / cipher algorithms.

#### A.1.1.1 Using Diffie-Hellman (DH)

A key modulus of 2048 bits for correctly implemented DH provides 112 bits of effective security strength. Considering projected technological advances, ASD is assessing that 112 bits of effective security strength (corresponding to a key of 2048 bits) will remain secure until 2030.

The recommended "next generation" Elliptic Curve DH Groups are predicted to provide adequate encryption protection against modern threats until 2040.

#### A.1.1.2 Using the Digital Signature Algorithm (DSA)

While RSA is used for secure data encryption, DSA is used for digital signatures and verification. When available, ECDSA is preferable to DSA.

A modulus of 2048 bits for correctly implemented DSA provides 112 bits of effective security strength. Considering projected technological advances, it is assessed (by ASD) that 112 bits of effective security strength will remain secure until 2030, while that is excluding earlier quantum computing practical uses.

Longer keys (modulus) lengths may introduce some slower processing on some encryption platforms while the benefit is not significant for the use cases with data classified below level.

#### A.1.1.3 Using the Elliptic Curve Digital Signature Algorithm (ECDSA)

When using a curve from FIPS 186-4, a base point order and key size of 224 bits for correctly implemented ECDSA provides 112 bits of effective security



strength. Security of a curve selected from another (non FIPS) source cannot be assumed to have the same security using base point order and key size alone.

#### **A.1.1.4 Using Elliptic Curve Diffie-Hellman (ECDH)**

When using a curve from FIPS 186-4, a base point order and key size of at least 224 bits for correctly implemented ECDH provides 112 bits of effective security strength. Security of a curve selected from another (non FIPS) source cannot be assumed to have the same security using base point order and key size alone.

#### **A.1.1.5 Using Elliptic Curve Cryptography**

When using elliptic curve cryptography, a NIST prime curve from FIPS 186-4 **MUST** be used (refer to <https://csrc.nist.gov/publications/detail/fips/186/4/final> ).

### **A.1.2 SSH Guidelines**

#### **A.1.2.1 SSH keys-based login**

If the SSH keys are not rotated regularly, they will present the similar risks as per not rotated passwords.

Further, there are multiple risks arising from the unprotected or mismanaged SSH keys.

See further here: <https://www.ssh.com/academy/iam/ssh-key-management>

#### **A.1.2.2 Automated SSH remote access risks**

If using SSH logins without a passphrase for automation purposes, a number of security risks may arise, specifically:

- if access from unknown Internet Protocol (IP) addresses is not restricted, an adversary could automatically authenticate to systems without needing to know any passphrases
- if port forwarding is not disabled, or it is not configured securely, access may be gained to forwarded ports thereby creating a communication channel between an adversary and a host
- if agent credential forwarding is enabled, an adversary could connect to the stored authentication credentials and use them to connect to other trusted hosts, or even intranet hosts if port forwarding has been allowed as well.
- if X11 display remoting is not disabled, an adversary could gain control of displays as well as keyboard and mouse control functions
- if console access is allowed, every user who logs into the console, on some systems, could run programs that are normally restricted to authenticated users.

- To assist in mitigating these security risks, it is essential that the *'forced command'* option is used to specify what command is executed and parameter checked is enabled.

### A.1.2.3 SSH-agent

Users **MAY** run an SSH key caching agent on their local workstations.

- SSH key caching agents **SHOULD NOT** be installed or run on any device other than a user's local workstation.
- Key caching agents - such as PuTTY's Pageant and OpenSSH's ssh-agent, allow a user to enter their passphrase once (usually at start-up) and then use their SSH key(s) without re-authenticating.

SSH connections **MAY** make use of agent forwarding.

- Agent forwarding is the process by which a remote device can use a key caching agent on a remote device to negotiate authentication to another node
- SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-agent launches, it requests the user's passphrase to unlock the user's private key.
- Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their passphrase. Screen locks and expiring key caches ensure that the user's private key is not left unlocked for a long period of time.

Furthermore, to limit the exposure of credentials, agent credential forwarding **SHOULD only be enabled** when **SSH traversal** (through multiple systems) is **required**.

*For example, Alice is running Pageant on her laptop and is connected via SSH to Bob's server. She wishes to connect from Bob's server to Colin's server but doesn't wish to store her private keys on Bob's server. By using agent forwarding over SSH, Bob's server can ask Alice's agent to complete the authentication sequence automatically.*

## A.1.3 IPsec Protocol

IPsec contains two major protocols, **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)**. In order to provide a secure Virtual Private Network style connection, both authentication and encryption are needed. AH and ESP can provide authentication for the entire IP packet and the payload respectively.

ESP is generally preferred for authentication since AH by its nature has network address translation limitations.

However, if maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH, which will then authenticate the entire IP packet and not just the encrypted payload.

#### A.1.3.1 ISAKMP authentication

Most IPsec implementations can handle a number of methods for parties' authentication as part of **Internet Security Association Key Management Protocol (ISAKMP)**. These can include digital certificates, encrypted nonces or pre-shared keys. These methods are all considered suitable for use if implemented securely.

For example, the IPsec **Pre-Shared Keys (PSKs)** have to be exchanged securely between parties (preferably via encrypted data or over the phone) and have to be longer than 32 characters (preferable up to 128 chars).

#### A.1.3.2 Internet Key Exchange

There are several methods for establishing shared keying material for an IPsec connection, while for most uses the **Internet Key Exchange (IKE)** version 1 or 2 **MUST** be used.

#### A.1.3.3 ISAKMP modes

Always try to use "**Main**" mode for IKE ISAKMP negotiations as it provides greater security than the "**Aggressive**" mode since all exchanges are protected.

#### A.1.3.4 Security association lifetimes

ISAKMP keys negotiation Phase 1 **SHOULD** use a secure association lifetime of 4 hours, or 14400 seconds. The maximum (for the Phase 1 secure association lifetime) use **SHOULD** be 28800 seconds (8 hrs).

The IPsec Phase 2 **SHOULD** use a shorter secure association lifetime of 3600 seconds.

#### A.1.3.5 ISAKMP encryption

For the ISAKMP symmetric encryption the algorithms that **MUST** be used are the AES based ones (128,192 or 256 bits).

#### A.1.3.6 Hashed Message Authentication Code algorithms

The approved Hashed Message Authentication Code (HMAC) algorithms are:

- HMAC-SHA256, HMAC-SHA384, HMAC-SHA512.

#### A.1.3.7 Diffie-Hellman groups

Using a larger DH group provides more security for the key exchange. The minimum modulus size needed is specified in *Section A1.1.1* **Error! Reference source not found..**

### A.1.3.8 Perfect Forward Secrecy (PFS)

PFS **SHOULD** always be used as it reduces the impact of the compromise of a security association.

### A.1.3.9 Internet Key Exchange Extended Authentication

Both IKEv1 and IKEv2 are acceptable to use.

However, XAuth using IKE version 1 has documented security vulnerabilities associated with its use and **SHOULD NOT** be used.

## I. References

1. ACSC Implementing TLS HTTPS - <https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-https-and-opportunistic-tls>
2. ACSC Cryptographic Fundamentals <https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-cryptography>
3. NIST Elliptic Curve Cryptography - <https://csrc.nist.gov/Projects/elliptic-curve-cryptography> .
4. TLS Deployment Best Practices - <https://www.ssllabs.com/projects/best-practices/>
5. Timing vulnerabilities with CBC - <https://docs.microsoft.com/en-us/dotnet/standard/security/vulnerabilities-cbc-mode>
6. PFS explained <https://www.thesslstore.com/blog/perfect-forward-secrecy-explained/>
7. Configuring PFS <https://www.digicert.com/kb/ssl-support/ssl-enabling-perfect-forward-secrecy.htm>
8. MITM attack - <https://www.rapidsslonline.com/ssl/what-is-ssl-stripping-attack/>



# Data Backup and Retention Standards

---

## Table of contents

Data Backup and Retention Standards..... 1

1 Purpose ..... 2

2 Definitions and acronyms ..... 3

3 Scope ..... 5

4 Data Backup and Retention Standards ..... 6

4.1 General requirements ..... 6

4.2 Data assessment..... 7

4.3 Backup scheduling..... 7

4.4 Retention period ..... 8

4.5 Minimum backup and retention schedule ..... 8

4.6 Monitoring..... 9

4.7 Storage media ..... 10

4.8 Backup testing and disaster recovery (DR)..... 10

4.9 Disposal of data..... 11

4.10 Backup and retention process ..... 11

4.11 Allocation of data backup responsibilities ..... 15

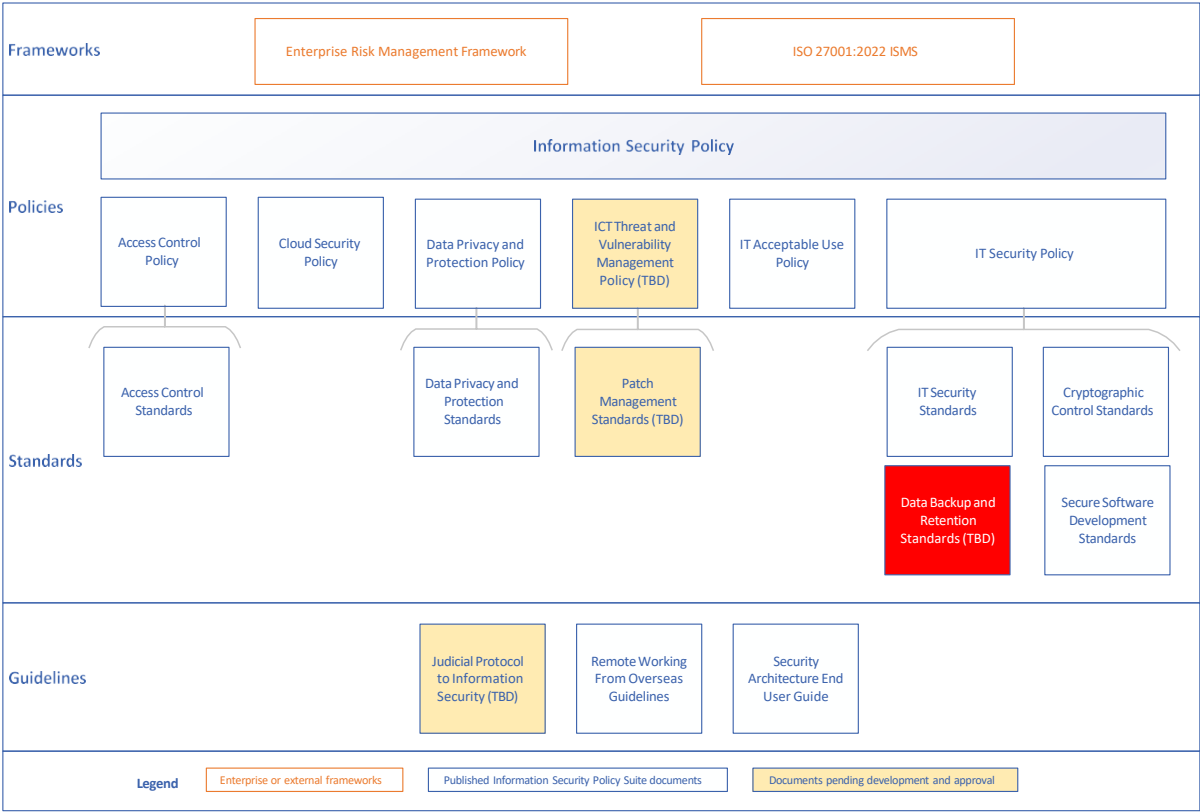
5 Exceptions ..... 17

6 Related legislation and documents ..... 17

7 Document information ..... 18

8 Support and advice ..... 18

9 Appendix A..... 19



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

The following standard articulates the Department of Communities and Justice’s (DCJ’s) data backup and retention standards in regard to the IT Security Policy.

Backups provide protection against many forms of data loss by creating multiple, regular, distributed copies. While they ensure short-term integrity, they are not intended to store data over a long period of time and are not subject to the same retention periods as set by State Archives to the original data. Rather, they are designed to restore a system to a fixed time and date or a particular status before a change and are dependent on the health condition of the system they back up.

The backup and retention process assists with:

- maintaining availability of the ICT production environment
- maintaining the stability of the ICT production environment
- adherence to Australian Signals Directorate (ASD)’s recommendations on mitigating cyber security incidents (Essential Eight risk mitigation strategies).

DCJ has a responsibility to uphold the confidentiality, integrity and availability of the data and information held on its ICT systems on premise, in the cloud or systems and services supplied or managed by third parties.

DCJ is committed to having an up-to-date backup management process in place to help recover its information and reduce the risks of a prolonged outage.

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Australian Cyber Security Centre (ACSC)	The Australian Government's lead agency for cyber security
ASD	Australian Signals Directorate
CISO	Chief Information Security Officer
Cloud Services	A cloud service is where an organisation pays to use, rather than own, the resources that are delivered over the network such as the internet by the cloud service provider. Cloud refers to where the solution is provided
Cyber Security NSW	An entity in the NSW Government that provides leadership and coordination across the whole of government in managing risks against cyber threats
Information asset	Any information (both physical and digital in any format, including audio and visual); Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
Information asset owner	The Owner has the delegated authority and accountability of the information asset. They are concerned with data quality, appropriate access (i.e. the conditions for appropriate use, sharing and distribution), and any risks surrounding the information. They are responsible for ensuring that all legal, regulatory and policy requirements are met in relation to the management of the information. The Owner appoints a Custodian for day-to-day responsibility.
Information custodian	The Custodian is concerned with day-to-day management, primarily responsible for the development, management, and maintenance of the hardware and software infrastructure that the information resides on. This includes backups and redundancy solutions.

Term	Definition
	The custodian works under overall direction and approval from the Information Asset Owner.
ICT	Information and Communication Technology
ICT systems	<p>The term information technology (ICT) systems include:</p> <ul style="list-style-type: none"> <li>• workstations</li> <li>• servers (physical and virtual)</li> <li>• operating systems</li> <li>• standard operating environments (SOEs)</li> <li>• firmware</li> <li>• networks (including hardwired, Wi-Fi, switches, routers)</li> <li>• hardware</li> <li>• software (databases, platforms etc.)</li> <li>• applications (including mobile apps)</li> <li>• cloud services</li> </ul> <p>of any kind that require support, maintenance, or attention in alignment with these standards. They can be physical, virtual, public or private cloud information systems assets</p>
ISMS	Information Security Management System
Key Performance Indicators (KPI)	A KPI is a measurable value that demonstrates how effectively a company is achieving key business objectives. It is a measure of how well something is being done
Key Risk Indicators (KRI)	A KRI is defined as measurements, or metrics, used by an organisation to manage current and potential exposure to various operational, financial, reputational, compliance, and strategic risks. It is an indicator of the possibility of future adverse impact
May / May not	<p>The item is not mandatory.</p> <p>Recommended as best practice for consideration. No policy exception required if condition is not met.</p>
Must	<p>The item is mandatory.</p> <p>Any request for deviation from a “must” must follow the procedures for requesting exceptions.</p>
Must not	<p>Non-use of the item is mandatory.</p> <p>Any request for deviation from a “must not” must follow the procedures for requesting exceptions.</p>
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course.



Term	Definition
	No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.
Software	Firmware, operating systems, standard operating environments (SOEs), network appliances and applications
SIEM	Security Information Event Management System (e.g. Splunk, Intrust)
WORM	Write Once, Read Many disk

### 3 Scope

The requirements and expectations outlined in this document applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This standard does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

These standards are applicable to:

- all DCJ information systems assets that include firmware, operating systems, standard operating environments (SOEs), network appliances and applications (collectively referred to as software) of any kind that require support, maintenance, or attention in alignment with these standards
- physical, virtual, public, or private cloud information systems assets

The types of computer records covered by these standards include, but are not limited to:

- input and output formats from electronic business and records systems, such as the following:

- error or control reports
  - input forms for data entry
  - output used for checking and verifying
  - regular batch reports
  - system reports
  - transaction reports used for checking and control purposes
- reference copies of user manuals and similar documents
- superseded computer logs
- superseded or obsolete computing software
- systems back-ups and associated back-up logs and data
- test data
- data contained in SaaS applications

## 4 Data Backup and Retention Standards

The retention and disposal of back-ups and back-up logs are covered in *State Records Regulation 2015 (S13e)* and the *General Retention and Disposal Authority – Administrative Records (GA28)*.

The controls provided in this standard aim to ensure DCJ will:

- meet the requirements for the DCJ Statement of Applicability (SOA) which is based on ISO 27001
- meet Essential Eight recommendations, namely regular backups of applications and systems
- where possible, maintaining up-to-date backup version levels on all DCJ's ICT systems and services supplied by third parties.

### 4.1 General requirements

Ref	Directive
GR-001	Information asset owners <b>MUST</b> ensure that appropriate backup and recovery procedures exist for all information assets that have backup requirements. These procedures must consider the information security requirements of confidentiality, integrity, and availability
GR-002	Information asset owners <b>MUST</b> determine the types of backups and their minimum frequencies following a risk-based decision regarding the system criticality, data classification, and data type in line with DCJ policies and standards

Ref	Directive
GR-003	Custodians <b>MUST</b> develop backup rotation and retention schedules based on requirements set forth by the information asset owners
GR-004	Data backup and retention <b>MUST</b> be considered during new solution design
GR-005	DCJ's ICT systems and software assets <b>SHOULD</b> aim to achieve ASD's highest maturity level of mitigation strategy for backups and retention, namely regular backups which are retained in a coordinated and resilient manner that is only accessible to approved backup administrators and tested regularly

## 4.2 Data assessment

Ref	Directive
DA-001	All DCJ staff, third parties and consultants <b>MUST</b> ensure appropriate classification of the information they create <sup>1</sup>
DA-002	The information asset owner <b>SHOULD</b> , using a risk-based approach, assess and categorise the data in their information asset/s with consideration to the following aspects: <ul style="list-style-type: none"> <li>• criticality of the system and data to DCJ functions</li> <li>• data classification (Unofficial, Official, Sensitive, Protected etc)</li> <li>• data type (system image, corporate records etc)</li> <li>• frequency of changes to the data</li> </ul>
DA-003	The information asset owner <b>SHOULD</b> use the outputs of this assessment to determine the risk posture of the data and the appropriate backup and retention schedules for their data while aligning with the DCJ minimum requirements for backup and retention for different data types as seen in <i>Section 4.5 Minimum backup and retention schedule</i>

## 4.3 Backup scheduling

Ref	Directive
BS-001	The backup frequency <b>SHOULD</b> be agreed with the information asset owner following a risk-based assessment of the criticality and importance of the data

<sup>1</sup> NSW Government Information, Classification, Labelling and Handling Guidelines, and DCJ Data Privacy and Protection Policy

Ref	Directive
BS-002	A backup <b>MUST</b> occur in the following instances: <ul style="list-style-type: none"> <li>• a new solution (feature, function, process etc) is implemented</li> <li>• major system changes, including upgrades</li> <li>• after patching</li> </ul>
BS-003	Backup copies of information, software and system images <b>SHOULD</b> be taken and tested regularly in accordance with an agreed backup policy <sup>2</sup> , and after patching
BS-004	The minimum backup frequency <b>SHOULD</b> be implemented as depicted in <i>Section 4.5 Minimum backup and retention schedule</i>

#### 4.4 Retention period

Backups are not intended to store data over a long period of time. They are not subject to the same retention periods as the source data set by State Archives.

Ref	Directive
RET-001	Backup data and logs <b>MUST</b> be kept until DCJ has no further administrative or reference use for them
RET-002	The information asset owner <b>SHOULD</b> assess the data and identify if there are any legal or regulatory archival or backup retention requirements regarding the data classification or content
RET-003	The minimum retention period <b>SHOULD</b> be implemented as depicted in <i>Section 4.5 Minimum backup and retention schedule</i>

#### 4.5 Minimum backup and retention schedule

More information on the different types of backups used in DCJ can be found in Appendix A.

Data Type	Backup frequency	Retention period
Data that does not change frequently (system image, operating system, configuration settings)	After a change occurs or every 3 months, whichever is sooner	6 months

<sup>2</sup> ISO27001 Control A.12.3

Transaction /archive logs for applications and databases, excluding underline support system	Every 30 mins / 1 hour / Once per day	90 days
Application and database content and records	<b>Fixed Time Interval:</b> Daily - Differential Weekly – Full backup Monthly – Full backup  <b>Or:</b> After patching or other major changes - Full backup	<b>Fixed Time Interval:</b> Daily - 35 days Weekly – 5 weeks Monthly or after changes - 7 years  <b>Or:</b> Three previous major changes
File servers*	Daily - Incremental Weekly - Incremental Monthly - Incremental	Daily - 35 days Weekly – 5 weeks Monthly - 7 years
Logs (event, system, backup logs)  <b>Note:</b> all logs should be forwarded to the designated SIEM repository	Daily – Incremental Weekly – Incremental	Daily – 35 days Weekly – 90 days
Virtual machines  <b>Note:</b> system image- based snapshot (block level)	Monthly - Incremental After patching or other major changes - Full backup	Monthly- 7 years  <b>Or:</b> Three previous major changes

\*When a file backup is created it is saved on a local disk in Silverwater Data Centre initially, and then digitally replicated to Unanderra Data Centre the next morning. Ex-DoJ data remains on the disk and ex-FACS data is transferred to tape to be stored offline and off-site.

## 4.6 Monitoring

Ref	Directive
MN-001	Backup administrators <b>SHOULD</b> use automated backup monitoring tools to ensure consistent and reliable notification of failure alerts, backup duration, and to show trends of recurring errors. This will reduce the risk of repeat failures and the potential of not having a recent clean copy of backup data in the event of an emergency restoration

Ref	Directive
MN-002	The backup reports <b>SHOULD</b> be reviewed daily, and any error remediated, where possible, prior to the next scheduled backup

## 4.7 Storage media

Ref	Directive
STO-001	The backup storage <b>SHOULD</b> be agreed with the information asset owner following a risk-based assessment of the criticality and importance of the data
STO-002	Where possible, if the risk assessment allows, backups <b>SHOULD</b> be stored in the cloud as it adds redundancy to the infrastructure and improves cost and scalability for DCJ
STO-003	Backups can be stored on different types of media such as external hard drives, tapes, WORM, and in the cloud to reduce the risk of failure related to a specific medium or technology
STO-004	Backup data and logs <b>MUST</b> be provided with the same level of protection as that of the source data. The minimum protections for backup data are identified in the NSW Government Information, Classification, Labelling and Handling Guidelines
STO-005	The backup data <b>SHOULD</b> be encrypted whether onsite or offsite
STO-006	The backup data <b>MUST</b> only be accessible by authorised staff
STO-007	The backup strategy <b>SHOULD</b> follow the "3-2-1" best practice method: <ul style="list-style-type: none"> <li>• 3 copies of data (not including the original data)</li> <li>• 2 copies on different storage media</li> <li>• 1 copy stored off-site in a location that is at a distance that would protect it from damage from any incident at the main site, such as a site wide failure or geographical disaster.</li> </ul>

## 4.8 Backup testing and disaster recovery (DR)

Ref	Directive
DRT-001	The backup and restore process <b>SHOULD</b> be tested at appropriate intervals to provide assurance that backups can facilitate recovery of data <sup>3</sup>

<sup>3</sup> ISO27001 Control A.12.3, and DCJ Patch Management Policy

Ref	Directive
DRT-002	All DR exercises <b>SHOULD</b> be reviewed and tested on an annual basis and/or in response to changes in business requirements, gaps identified in post-incident reviews or through routine DR testing <sup>4</sup>
DRT-003	These exercises <b>SHOULD</b> include data recovery as well as a full failover to the DR environment to confirm that the DR environment is able to facilitate BAU operations in the case of major failure
DRT-004	In the event of a failed restoration due to malware or infection of the source data, the latest backup data <b>SHOULD</b> be restored to a VM with up- to-date anti-virus / anti-malware protection already installed
DRT-005	If the backup is also infected, preceding backup versions <b>SHOULD</b> be restored in this manner until a clean and sanitised version is found. If this approach is not viable, all efforts must be made to retrieve the data safely

## 4.9 Disposal of data

The controls and procedures around appropriate disposal of data are detailed in the Data Privacy and Protection Policy.

Ref	Directive
DD-001	At the end of the data retention period, data sanitisation and disposal <b>MUST</b> be conducted, including where the data is held by a third-party
DD-002	All staff <b>MUST</b> use proper destruction methods and ensure compliance with the <i>State Records Act 1998</i> when disposing of media containing DCJ records and or classified information
DD-003	All media <b>MUST</b> be disposed of in a manner appropriate for the information classification stored within
DD-004	Records <b>MUST</b> be disposed of in such a manner that they cannot be reconstituted. This also applies to backup data held on behalf of DCJ by a third-party
DD-005	DCJ <b>MUST</b> have procedures in place to enforce the appropriate disposal of its data by third-party providers. This may include contractual agreements, periodical inspections, audits etc.

## 4.10 Backup and retention process

<sup>4</sup> DCJ Business Continuity Management Policy, and ICT Service Continuity Management Framework

Ref	Directive
PR-001	A backup and retention process <b>MUST</b> be established within each ICT environment / domain to reduce DCJ's risk of data loss and maintain the ISO27001 certification
PR-002	The IDS Service Manager of each domain is responsible for ensuring the backup and retention process specific to their domain is written and the responsibilities assigned in the process
PR-003	If a third-party supplier manages system/s which require backups, the contract between DCJ and the third-party <b>MUST</b> include a data backup and retention process for that system/s in accordance with the Data Backup and Retention Standards
PR-004	The process <b>MUST</b> align to the Data Backup and Retention Standards and must have, at minimum, the following processes outlined in the following sections (4.10.1 to 4.10.5)

#### 4.10.1 Create an inventory of all ICT assets

Ref	Directive
INV-001	An inventory of all assets (including hardware and software, software versions and patches applied within ICT environment) <b>SHOULD</b> be established and maintained to keep a record of the current backup status of all ICT assets. Where the inventory does not exist, a plan should be in place to build one
INV-002	The inventory <b>MUST</b> contain at least the following information: <ul style="list-style-type: none"> <li>• asset name</li> <li>• asset owner</li> <li>• date of last backup</li> <li>• version of backup</li> <li>• location of the backup</li> </ul>
INV-003	The inventory of assets <b>MUST</b> have controls in place to prevent unauthorised access to it

#### 4.10.2 Risk-based assessment of backup scheduling and retention

Ref	Directive
ASS-001	<b><u>New Systems:</u></b> Backup and data retention <b>MUST</b> be considered during all new solution



Ref	Directive
	designs. These details will be reviewed as part of the Solutions Architecture process and, if a third-party is involved, the Third Party Risk Assessment process
ASS-002	<p><b>Current Systems:</b> The current state of backup scheduling and retention for relevant file level backups (servers and data files), enterprise databases (e.g. SQL and Oracle), and backup logs <b>SHOULD</b> be reviewed regularly. This will confirm the timeframes of the usual cycle for backups, what data / metadata is backed up, where media is stored, and how long media is kept before it is overwritten, deleted, or sent to offsite storage. The following <b>SHOULD</b> also be considered:</p> <ul style="list-style-type: none"> <li>• The number of times backups were used to recover data (monthly, quarterly, and annually)</li> <li>• Length of time taken to recover the data from the monthly or annual backup storage media</li> <li>• Success rate of recovery</li> <li>• Viability of the current storage media (is the data still accessible/readable after multi-year storage?)</li> </ul>
ASS-003	<p>It is important to document the risks and the information provided which allows for the determination of when DCJ no longer needs to maintain a back-up.</p> <p>Use a risk-based approach to determine what are the risks involved, what is the usual cycle, what is the point in time when DCJ ICT has no further administrative or reference use for back-ups. This process can include:</p> <ul style="list-style-type: none"> <li>• analysis of data in the system (data classification, data type, protections in place such as encryption or restricted access)</li> <li>• identifying the data, metadata and system documentation that must be brought forward and retained</li> <li>• an accountable process for deletion of residual data in the system</li> </ul>
ASS-004	<p>The output of this process <b>SHOULD</b> result in definitive figures for the following three categories:</p> <p><b>Recovery Point Objective (RPO)</b> - the amount of data that can be lost within a period before significant harm occurs, from the point of a critical event to the most preceding backup</p> <p><b>Recovery Time Objective (RTO)</b> – the quantity of time spent restoring the system and its data.</p>

Ref	Directive
	<p><b>Maximum Acceptable Outage (MAO)</b> – the maximum allowable time that business services are unavailable before its impact is deemed as unacceptable on the delivery of ICT services to the business.</p> <p>These outputs will assist in determining the frequency of the backup schedule, the media it is stored on, and the data restoration process.</p>

#### 4.10.3 Implementation and monitoring

Ref	Directive
IMP-001	In addition to the RPO, RTO, and MAO, the backup schedule <b>SHOULD</b> also consider the different capacity and load availabilities for each of the environments as their business schedules and technical outages allow. This includes selecting the appropriate type of media that is used to store the backup data to ensure timely restoration of services
IMP-002	Backups, regardless of environment, <b>SHOULD</b> be scheduled based on a customer suitable time
IMP-003	The success or failure of backup activity <b>MUST</b> be assessed, and remedial actions taken to correct failures
IMP-004	Failed backups <b>MUST</b> be investigated to reach a reasonable explanation as to why the failure occurred, and steps be taken to implement a mitigation plan as per the Incident Management process
IMP-005	If a mitigation plan cannot be achieved, then details <b>SHOULD</b> be entered into the cyber risk register and within appropriate team / division registers

#### 4.10.4 Disaster recovery and restoration testing

Ref	Directive
DRP-001	Disaster recovery and restoration testing <b>MUST</b> be included in the Disaster Recovery Plan, having its own specified policies, tools, and procedures to enable the recovery or continuation of systems following a natural or human-induced disaster

#### 4.10.5 Documenting the backup and retention process

Ref	Directive
DOC-001	Managers <b>SHOULD</b> ensure that backup and retention process and procedures are documented in their areas to ensure the backup personnel know what to do when they undertake backup activities

Ref	Directive
DOC-002	The procedures <b>MUST</b> include backup retention details, restoration procedures and documentation, restoration testing procedures, guidelines for how to proceed when backup media has expired etc
DOC-003	They <b>SHOULD</b> also include revision history, and any changes to the document <b>MUST</b> be controlled. This ensures recoverability in the event of any types of catastrophic incidents

#### 4.11 Allocation of data backup responsibilities

Ref	Directive
RES-001	A review of backup roles and responsibilities of ICT staff <b>SHOULD</b> be undertaken to determine if they are correct or if training should be arranged to ensure staff are equipped with the right skills for the role
RES-002	If the key skills required for performing backups are missing in the current team, a business case <b>SHOULD</b> be raised to fill the skills gap

##### 4.11.1 DCJ Executive

- Approves these standards as appropriate
- Ensures that all directorates / divisions adhere with these standards
- Appropriately resources and supports DCJ backup and retention initiatives
- Ensures that staff comply with the Data Backup and Retention Standards

##### 4.11.2 ICT Steering Committee

- Endorses these standards as appropriate

##### 4.11.3 Chief Digital Information Officer (CDIO)

- Ensures these standards are implemented
- Works with IDS Director Infrastructure Operations and End User Services to implement these standards
- Ensures enforcement of these standards across all users and ICT systems whether on premise, remote, cloud, or hybrid

##### 4.11.4 Chief Information Security Officer (CISO)

- Works with the IDS Director Infrastructure Operations and End User Services to ensure that third-party suppliers comply with DCJ's Data Backup and Retention Standards

- Approves request for exemption from these standards

#### **4.11.5 IDS Director Technology Operations and End User Services**

- Define roles and responsibilities related to backup and retention activities
- Identify key performance indicators (KPIs) and key risk indicators (KRIs) for backups and retention
- Ensure KPIs and KRIs are implemented, if required
- Ensure that staff under their control comply with these standards and to ensure there are formalised backup and retention processes in place that comply with the requirements of these standards
- Works with the CISO to ensure that third-party suppliers comply with DCJ's Data Backup and Retention Standards

#### **4.11.6 Custodians of ICT systems / information asset owners**

- Review and assess the backup and retention needs of their systems to ensure they comply with these standards
- Review backup and retention roles and responsibilities of ICT staff to determine if they are correct or if there needs to be a reshuffle
- Work with the Business Continuity Manager and IDS Service Managers to schedule and perform regular DR exercises to test data and system restoration
- Initiate request for an exemption from these standards if required

#### **4.11.7 IDS service managers**

- Ensure backup and retention processes and procedures are developed, followed, and reviewed regularly by the team
- Work with the Business Continuity Manager and Custodians of ICT systems to schedule and perform regular DR exercises to test data and system restoration

#### **4.11.8 Third-party suppliers**

- Ensure backup and retention processes and procedures are adhered to as per the terms of their contract with DCJ
- Where the backup and retention process are managed by a sub-supplier, the contract holding third-party supplier is responsible for ensuring that its sub-supplier is in compliance with the terms of their contract with DCJ

#### 4.11.9 Backup administrators

- Ensure only authorised backup administrators have access to backup data
- Confirm if backups have been reliably performed
- Notify and report of backup testing results to Custodians of the ICT systems
- In the event of a failed backup, remediate the issue until a successful backup is taken

## 5 Exceptions

Requests for exceptions must articulate an appropriate business case to justify deviation from a policy or standard where the minimum data backup and retention requirements cannot be met.

The business case should include relevant information such as the reason for the exception, a designated owner, a scope, and a timeframe for the exception, mitigating or compensating controls to manage risk and a remediation plan to realign with the breached policy or standard.

Where the request is for exemption from performing backups:

- System Administrators within the Technology Operations Cloud Hosting and Infrastructure team should be contacted to initiate a policy exception
- exceptions must be approved by the Director Infrastructure Operations and End User Services and must be recorded in the exceptions register

## 6 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 7 Related legislation, regulation and other documents

This document is related to the IT Security Policy in that it is an implementation of the policy. Other related documents include:

- Patch Management Standards
- IT Security Standards
- Australian Signals Directorate (ASD) Essential Eight (E8) Maturity Model

8 Document information

Document name	Data Backup and Retention Standards
Document reference	
Replaces	N/A
Applies to	All of DCJ
Policy administrator	Director Technology Operations and End User Services
Approval	Chief Digital Information Officer
Approved date	28/09/2023

9 Support and advice

For more advice please contact:

Business unit	Principal Manager Technology Operations Cloud Hosting and Infrastructure Technology Operations and End User Services Information and Digital Services Corporate Services
Email	<a href="mailto:securitypolicy@facs.nsw.gov.au">securitypolicy@facs.nsw.gov.au</a>

10 Version and review details

Version	Effective date	Reason for amendment	Due for review
1.0	28/09/2023	Annual review	28/09/2024

## 11 Appendix A

The different types of backups used in DCJ are:

**Full Backup** – Entire data set, regardless of any previous backups or circumstances

**Incremental Backup** – Additions and alterations since the most recent incremental backup

**Differential Backup** – Additions and alterations since the last full backup

**Continuous Data Protection or Realtime Backup** – Any change to the data set is automatically synchronised to another server, which acts as a replica of the original data set



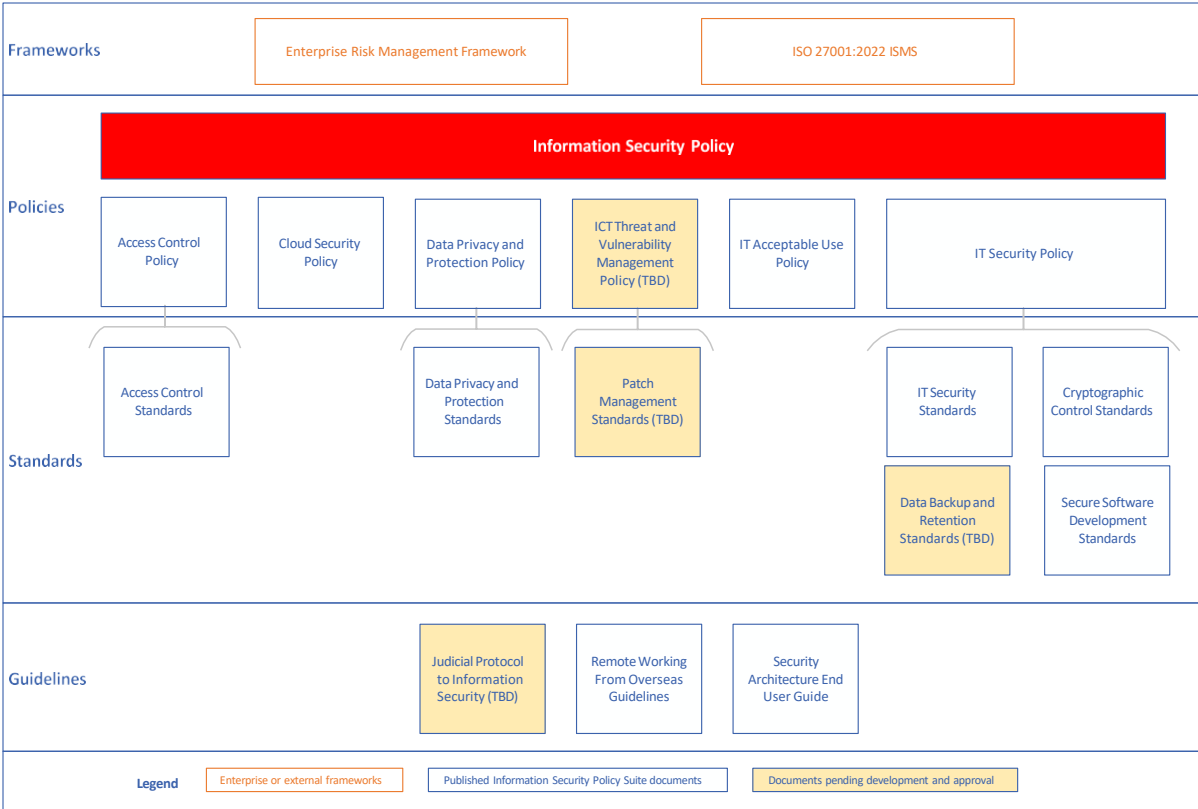
# Information Security Policy

---

## Table of contents

1	Purpose .....	2
1.1	Related policies .....	3
2	Definitions.....	3
3	Scope.....	4
4	Information security policy schema.....	4
5	Policy statement .....	5
6	ISMS objectives .....	5
7	Policy.....	6
7.1	Hardware and software acquisition .....	6
7.2	Risk management process.....	6
7.3	Non-compliance.....	7
7.4	Procedures for requesting exceptions .....	7
7.5	Management commitment to information security .....	7
7.6	Allocation of information security responsibilities.....	8
7.7	Segregation of duties .....	14
7.8	Contact with authorities.....	14
7.9	Awareness .....	14
7.10	Identification of applicable legislation and contractual requirements	15
7.11	Independent review of information security .....	15
7.12	Technical compliance review .....	15
9	Related legislation, regulation and other documents .....	15
9.1	Commonwealth.....	16
9.2	NSW.....	16
10	Document information .....	16
11	Support and advice .....	17
12	Version and review details.....	17
13	Appendix – Engaging information security .....	18





The red highlighted box shows where this document sits within the Information Security Policy Suite.

# 1 Purpose

This policy provides all Department of Communities and Justice (DCJ) employees and approved users with direction and support and establishes an implementation framework for security. The purpose of this policy is to clearly articulate the information security behaviours and practices that DCJ requires its employees and approved users to comply with.

Information security is fundamental to the successful operations of DCJ. As the custodians of information that is politically, commercially or personally sensitive, DCJ has a ‘duty of care’ to protect information from accidental or malicious modification, unauthorised access, loss or release.

DCJ is committed to ensuring the integrity of its information systems.

This policy and supporting documents contain information relating to the responsibilities of all users to appropriately protect the information they use and manage as part of their daily roles.

This policy is written in line with the NSW Cyber Security Policy and ISO/IEC 27000 suite of standards for managing information security.

Definition of DCJ information security:

*“The protection of DCJ information assets against unauthorised access, modification or non-availability, whether in storage, processing, or transit. Information security includes identification of measures necessary to detect and protect DCJ information assets from such risks.”*

## 1.1 Related policies

This document is related to the following policies:

- [IT Security Policy](#)
- [Data Privacy and Protection Policy](#)
- [IT Acceptable Use Policy](#)
- [Access Control Policy](#)
- [Cloud Security Policy](#)
- [End User Computing Policy](#)
- Code of Ethical Conduct
- Enterprise Risk Management Policy
- [NSW Cyber Security Policy](#) 2020 v3.0

## 2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information
CCSO	NSW Chief Cyber Security Officer
CDIO	Chief Digital Information Officer
CISO	Chief Information Security Officer
CITO	Chief Information Technology Officer
DCJ	Department of Communities and Justice
IACS	Industrial automation and control systems
ICT	Information and communication technologies
IDS	Information and Digital Services
Information asset	Any information (both physical and digital in any format, including audio and visual);

	Any application or ICT configuration items (CI) which stores, transmits, creates or uses information.
ISMS	Information security management system
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No policy exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No policy exception required if condition is not met.

### 3 Scope

The requirements and expectations outlined in this policy applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users.
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information.
- any other body authorised to administer, develop, manage and support DCJ information systems and assets.

This policy does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges’ tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

### 4 Information security policy schema

DCJ has developed a hierarchical approach to deploying the Information Security Policy. A suite of policy documents has been designed which segments the policy content into sections which are refined and tailored to a target audience. This approach allows for policies to be targeted at staff to ensure the content is applicable and the reader is not overburdened with information they cannot apply or relate to.

The diagram below depicts this schema and identifies the applicability of the documents to staff.



Documents in bold need to be read by all staff, the remaining documents, however, must be read by staff involved in the procurement, management and design of services and information systems.

5 Policy statement

DCJ is committed to ensuring the confidentiality, integrity and availability of its clients’ information and the information of the organisation as a whole. The Information Security Policy articulates the standards DCJ must operate to, within a security context. DCJ’s security strategy, security improvements register and information security management system (ISMS) enable this standard to be achieved.

DCJ is committed to maintaining and improving an ISMS to meet our obligations to protect its information assets under international industry standards, and where appropriate specified areas of DCJ will be certified to the standard to ensure the effective integration and integrity of this management system.

6 ISMS objectives

- 1. **Executive engagement** – Executive management are engaged by, aware of and support information security within DCJ.

2. **Assess threats and vulnerabilities** – The identification and assessment of security threats and vulnerabilities to key assets is undertaken regularly and tracked over time.
3. **Manage information security risks** – Develop and maintain effective security management processes to address identified risks.
4. **Learn from security incidents** – Record, analyse and investigate all reported security incidents and policy breaches to develop improvements to prevent their reoccurrence.
5. **Cyber vulnerability trend** – Continuous improvement of security of all externally facing systems through a risk based vulnerability management program.
6. **Project engagement** – Ensure all projects engage Information security during the planning phase at a minimum.
7. **Awareness** – Deliver continual security awareness to staff.
8. **Procurement** – Purchasing decisions consider information security.
9. **ISMS Calendar** – An ISMS calendar is maintained which specifies when key actions must occur.
10. **Induction** – Newly hired staff complete an induction program that identifies their responsibilities for Information security and confidentiality.
11. **Compliance** – With legislative and regulatory obligations.

## 7 Policy

### 7.1 Hardware and software acquisition

CITO/CDIO endorsement must be obtained for all acquisitions (Capex and Opex) of:

- Computer Hardware
- Software
- Maintenance renewal
- Any mobile applications (apps) in excess of \$50, or any app that holds client or staff sensitive information

### 7.2 Risk management process

Risk management is an essential part of an effective approach to information security. The DCJ approach to risk management is documented within the Enterprise Risk Management Policy. DCJ's enterprise risk team is actively involved in assisting DCJ cyber security with ensuring the risk framework is

applied in assessing cyber security risks, analysing cyber security risks, and addressing cyber security risks across DCJ.

Staff must consider cyber security risk in all of their activities including decision making. Should staff identify a risk they should raise it with their management and process it as per the Enterprise Risk Management Policy.

### 7.3 Non-compliance

The Information Security Management team is to be informed as soon as possible of any actual or suspected breach of this policy. Non-compliance or breaches of this policy, without an appropriate exception, will be investigated and misconduct escalated with Corporate Governance and Performance, which may result in disciplinary action in accordance with the DCJ Code of Ethical Conduct and NSW Government [Personnel Handbook](#). Non-compliance or breaches may be reported to the IDS Service Desk on 02 9765 3999 (ex-FACS) or 02 8688 1111 (ex-Justice).

Alternatively, you may send an email to the Cyber Risk Audit and Compliance team (CRAC) via [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

### 7.4 Procedures for requesting exceptions

Requests for exceptions must articulate an appropriate business case to justify deviation from a policy or standard. The business case should include relevant information such as the reason for the exception, a designated owner, a scope and a timeframe for the exception, mitigating or compensating controls to manage risk and a remediation plan to realign with the breached policy or standard.

Requests for exceptions are effected by completing a [Security Policy Exception Request form](#). Exceptions must be approved by the information asset owner and the Chief Digital Information Officer and must be recorded in the exceptions register. Exceptions will be reviewed at the cessation of the exception period and will require re-approval should they need to be extended.

### 7.5 Management commitment to information security

Background verification checks on all candidates for employment, contractors, and third-party users must be carried out in accordance with relevant laws, regulations and proportional to the individual's proposed organisational role.

Newly hired staff are required to complete an induction program that identifies their responsibilities for Information security and confidentiality.

All staff are accountable and required to comply with the Information Security Policy and must ensure DCJ facilities, information or information processes will not be knowingly exposed to unacceptable levels of risk.

DCJ takes a top-down approach to information security by which the most senior executive layers of the organisation contribute to, review and approve the Information Security Policy. Updates are communicated to all staff to ensure they act in accordance with the policy. Staff awareness is maintained through appropriate training and communication.

The following information security groups provide DCJ staff with direction and support on information security matters:

- ICT Steering Committee – provides advice and guidance to the DCJ Senior Executive Committee on matters regarding ICT and information management.
- Audit and Risk Committee – supports the CISO and DCJ more broadly by considering cyber security, providing oversight and management of risks and audits, and ensuring DCJ meets its responsibilities. The risk registers inform internal audit planning.

## **7.6 Allocation of information security responsibilities**

Responsibilities outlined below may be delegated but remain the responsible party remains accountable for them.

### **7.6.1 DCJ Executive Board**

- Ensuring DCJ complies with the requirements of the NSW Cyber Security Policy and timely reporting on compliance with the Policy
- Assign overall responsibility for information asset protection and ownership.
- Approves policies as appropriate.
- Ensures DCJ develops, implements and maintains an effective information and cyber security plan.
- Determines DCJ's tolerance for security risks using the approved whole-of-government Enterprise Risk Management Policy.
- Appropriately resources and supports DCJ cyber security initiatives including training and awareness and continual improvement initiatives to support this policy.
- Ensures that staff are aware of and adequately comply with information security policies.

### **7.6.2 Chief Digital Information Officer (CDIO) / Chief Information Technology Officer (CITO)**

- Works with DCJ's CISO to implement this policy.
- Supports the development of a cyber-security plan.

- Ensures that all staff, including consultants, contractors and outsourced service providers understand the cyber security requirements of their roles.
- Clarifies the scope of their responsibilities for cyber security relating to assets such as information, building management systems and IACS.
- Ensures a secure-by-design approach for new initiatives and upgrades to existing systems to ensure compliance with the organisations cyber risk tolerance.
- Ensures all their staff and providers understand their role in building and maintaining secure systems.

### **7.6.3 Chief Information Security Officer (CISO)**

- Ensures that the Secretary of the department and information asset owners are informed of any significant information security issues and the status of the department's information security.
- Defines and implements a cyber-security plan for the protection of the DCJ's information and systems.
- Attends DCJ or cluster risk committee meetings as an advisor or member.
- Implements policies, procedures, practices and tools to ensure compliance with this policy.
- Represents DCJ on whole-of-government collaboration, advisory or steering groups established by the NSW Chief Cyber Security Officer (CCSO).
- Establishes training and awareness programs to increase staff's cyber security capability.
- Builds cyber incident response capability that links to DCJ's incident management and whole of government cyber response plan.
- Collaborates with privacy, audit, information management and risk officers to protect DCJ's information and systems.
- Provides independent assurance to the Chief Digital Information Officer and DCJ Executive on the appropriateness of security objectives and Information Security Policies, standards, processes, procedures, baselines and guidelines to effectively comply with the security objectives.
- Advises, coordinates and promotes security.
- Provides information security advice on new projects and initiatives.
- Establishes and provides security training and awareness programs, including guidance on but not limited to:



- Classifying information and applying DLMs in accordance with the PSPF and NSW Guidelines;
  - Overclassification to mitigate risk of classification not being implemented or ignored;
  - Carriage, transfer, sharing or disposal of information in line with its security classification and management requirements;
  - Use of information within DCJ premises, away from DCJ premises, and when travelling overseas by applying appropriate security controls;
  - Levels of ongoing access permitted to security classified information for each level or security clearance;
  - Ensuring DCJ personnel are cognizant of the need-to-know principle; and
  - How DCJ personnel can report emergencies, breaches, or disclosures of sensitive or security classified information.
- Ensures compliance with government and regulatory information security related requirements.
  - Produces technical security risk assessments and recommendations.
  - Maintains an executive level information security forum to ensure the ISMS meets the expectations of the organisation.
  - Assists to ensure that the risk framework is applied in assessing cyber security risks and assist with setting of risk appetite.

#### **7.6.4 Manager, Risk Audit and Compliance**

- Reports to the Chief Information Security Officer.
- Operational effectiveness of information security controls.
- Risk, Audit and Compliance team responsibilities.
- Coordination of the department's ISMS.
- Development of information security policies, procedures and controls.
- Manage, maintain and measure Information Security Policy standard and process compliance.
- Measure the effectiveness and maturity of information security controls.
- Identify and manage information security improvements.
- Maintains a management level information security forum to ensure the ISMS meets the expectations of the organisation.

### 7.6.5 Manager, Cyber Security

- Reports to the Chief Information Security Officer.
- Operational effectiveness of cyber security controls.
- Cyber team responsibilities.
- Management of information security incidents and investigations

### 7.6.6 Information asset owners (service owners and information owners)

An information asset's owner is responsible for applying the relevant sensitive or security classification to systems under their control. To do this they must assess the Business Impact Level (BIL) based on the likely damage if the information's confidentiality was compromised. The owner remains responsible for controlling the sanitisation, reclassification or declassification of that information.

- Ensure that appropriate security, consistent with the policy, is implemented.
- Appropriately classify official information assets and apply the lowest level of sensitivity or security classification practicable<sup>1</sup>.
- Appropriately sanitise, reclassify, or declassify information assets in line with the classification requirements as prescribed by the *State Records Act 1998*.
- Determine access privileges, and ensure they have the appropriate security clearance required to access the information.
- Apply appropriate DLMs through text-based or colour-based protective markings.
- Appropriately use information within DCJ premises, away from DCJ premises and when travelling overseas by applying appropriate security controls.
- Facilitate regular risk reviews of their information assets with a view to identify any potential risks and assess the controls in place to protect assets. This should be done with the assistance of RAC.
- Regularly review risks and threats which impact their information assets and ensure they are mitigated or escalated appropriately.

---

<sup>1</sup> \*Information asset owners should balance the needs and expectations of DCJ, the wider government and community to protect information and ensure appropriate access. Over classification of information can result in access to information being unnecessarily limited or delayed, increased administrative time and costs, and classifications being devalued or ignored. Security classifications must also not be applied as an effort to restrain competition, hide violations or inefficiencies of legal or administrative processes, or prevent or delay the release of information that does not need protection.

- Ensure security breaches or near misses affecting their information assets are reported to CRAC for investigation, including any inadvertent disclosures or compromises of sensitive and security classified information.
- Maintain business continuity plans and disaster recovery plans.
- Engage CRAC and participate in identifying the information security requirements of their information assets.
- Update auditable registers with holdings for SECRET and TOP SECRET information.
- Ensure that security requirements are incorporated into the design, operation and management of information systems. Appropriately store, carry, transfers, share or dispose of information in line with its security classification and management requirements.
- Ensure that any OFFICIAL: Sensitive information created is managed in accordance with the Information Protection Principles.
- Participate in activities that monitor the effectiveness of cyber security for their systems as needed, including internal and external audits, KPI and SLA reporting, and ISMS management activities.

#### 7.6.7 Custodians

A custodian is a person/s that is delegated responsibility over information by the information asset owner. Custodians are users required to maintain, operate, and implement technology solutions.

- Have responsibility of maintaining and operating the information asset on behalf of the business/information owner.
- Have 'custody' of assets, not necessarily belonging to them, for limited time (e.g. network administrators and operators).
- Implement access requirements as requested by the information asset owners.
- Detect and report on security violation attempts (review and monitoring).
- Approve, reject, remove and review system privileges on a timely basis, to reflect user movements, absences, terminations and investigations.
- Maintain a proactive approach to ensuring the security of the system for which they are responsible is kept at the highest possible security level.
- Ensure that changes to system(s) are appropriately tested.

### 7.6.8 Business Centre Managers

- Ensure that new employees receive appropriate instruction regarding their information security responsibilities during induction.
- Ensure that verification checks on employees (including contract employees) are completed prior to commencement, particularly where the role being filled involves handling highly classified information or exercises significant authority.
- Ensure that contract employees sign an appropriate confidentiality agreement prior to commencement of their employment.
- Advise the relevant system administrators of any access changes that are required as a result of employee terminations, transfers or role changes.
- Recovery of all access cards, keys and tokens from terminated employees (including contract employees).
- Appropriate escalation of security incidents, breaches, and weakness of which they are notified.
- Authorise and issue guidance on the use of removable media within their business centre.

### 7.6.9 Users

- A user is any staff or other authorised person who uses information in the course of daily business activities.
- Use and preserve assets' security by adhering to security policies.
- Are aware of their responsibilities.
- Comply with the requirements of these policies, standards and guidelines.
- Report violations or suspected violations of these policies in a timely manner.
- Maintain confidentiality of operating system and application passwords.
- Use information and information resources for responsible and authorised purposes.
- Must not disclose information publicly or to unauthorised parties without the approval of a Director or above.
- Contract employees (staff) must sign a formal undertaking concerning the need to protect the confidentiality of the department's information, both during and after contractual employment with the department.

### 7.6.10 Security operations

- Implement security to meet operational business needs.
- Operate/administer IT security and adhere to the security policy.
- Maintain a functional information security forum to co-ordinate information security practice and reporting.
- Respond to security incidents.
- Maintain and manage vulnerability management and penetration testing programs.
- Securely managing the provision of user access to the department's information systems as approved by the business centre manager (or delegate).
- Monitor system/security logs for evidence of unauthorised activity.
- Report potential, suspected and actual security breaches to the Manager, Cyber Security.
- Assisting the Manager, Cyber Security in investigation of potential, suspected and actual security breaches.

## 7.7 Segregation of duties

Where practicable, approval and execution duties should be separated to prevent unauthorised access or misuse of information assets. Where this delineation is not controlled or the opportunity for collusion is high, auditing and alerting should be implemented in order to monitor these scenarios.

## 7.8 Contact with authorities

Every contact involving authorities about an information security incident or problem, where possible, should be initiated by a member of the Cyber Security team, legal team, or a DCJ executive.

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers, information security providers and telecommunications operators must be maintained.

## 7.9 Awareness

All staff are required to complete the appropriate level of information security awareness training. The training is targeted at three categories of employees:

- All DCJ employees and contractors who are directly employed by DCJ

- DCJ employees who either manage and/or support DCJ ICT infrastructure and systems, or are responsible for identifying and/or managing risks for their business area
- DCJ executives (Band 1 and higher)

Management are responsible for ensuring that their staff complete all mandatory information security training.

From time-to-time security management may post security advisories. These advisories will be communicated to staff who should remain aware of the information security changes, consider the advice provided and apply it where practical.

### **7.10 Identification of applicable legislation and contractual requirements**

All applicable legal, statutory, contractual, or regulatory requirements must be documented and defined. Specific requirements and responsibilities for controls or other activities related to these legal regulations must then be delegated to the appropriate business unit.

### **7.11 Independent review of information security**

External independent auditors will be engaged by DCJ on an annual basis or more frequently as required to validate security controls in line with the Audit Management Standard.

Findings of these reviews must be tabled in an audit register with an owner, a remediation plan and management commitment.

### **7.12 Technical compliance review**

At regular intervals technical compliance reviews should be conducted to ensure services are compliant with Information Security Policy and standards. Technical findings must be recorded in the DCJ audit register, an owner identified, a remediation plan constructed and management commitment defined.

## **8 Monitoring, evaluation and review**

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## **9 Related legislation, regulation and other documents**

This policy aligns with the NSW Cyber Security Policy.

Compliance to the above supports the intentions of:

## 9.1 Commonwealth

- *Electronic Transactions Act 1999*
- *Electronic Transactions Amendment Act 2011*
- *Copyright Act 1968*
- *Cybercrime Act 2001*
- *Telecommunications (Interception and Access) Act 1979*
- *SPAM Act 2003*
- *Privacy Act 1988*
- *Crimes Act 1914*

## 9.2 NSW

- *Crimes Act 1900*
- *Government Sector Employment Act 2013*
- *Independent Commission Against Corruption Act 1988*
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*
- *Public Finance and Audit Act 1983*
- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*
- *Government Information (Public Access) Act 2009*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

## 10 Document information

Document name	Information Security Policy
Document reference	D22/1832018
Replaces	Information Security Policy V2.2
Applies to	All of DCJ with the exception of Judiciary and NCAT Board members
Policy administrator	Chief Information Security Officer
Approval	Deputy Secretary, Corporate Services
Approved date	28/09/2023

## 11 Support and advice

For more advice please contact:

Business unit	Cyber, Risk, Audit and Compliance Information and Digital Services Corporate Services
Email	<a href="mailto:SecurityPolicy@facs.nsw.gov.au">SecurityPolicy@facs.nsw.gov.au</a>

If you need assistance identifying when you need to engage information security, please see **Appendix – Engaging information security**.

## 12 Version and review details

Version	Effective date	Reason for amendment	Due for review
2.2	29/06/2022	Annual review due	29/06/2023
3.0	28/09/2023	Annual review	28/09/2024



### 13 Appendix – Engaging information security

The following questionnaire can be used to help you determine when you need to engage Cyber Risk Audit and Compliance team.

- Do you believe your password has become known to another party?
- Do you believe your computer has been infected with Malware?
- Have you just received a scam email?
- Have you seen something that breaches the Information Security Policy and need to report it?
- Do you need a security investigation carried out?

If you answer yes to any of the above, please use the following contact points:

- For urgent security incidents outside the business hours 8:30am – 4:30pm, please call 1300 325 29237 (1300 DCJ CYBER)
- For urgent security incidents, please email [security.incident@justice.nsw.gov.au](mailto:security.incident@justice.nsw.gov.au)
- For all other security inquiries please email [information.security@justice.nsw.gov.au](mailto:information.security@justice.nsw.gov.au)

- Are you running or involved with a project which is implementing, updating or removing an ICT component?
- Are you running or involved with a project which has the potential to impact the confidentiality, integrity or availability of DCJ information, services or assets?
- Are you procuring a service from a third party which sees DCJ information being stored, used, created or processed by the third party?
- Are you sharing DCJ information with a non-DCJ party?

If you answer yes to any of the above or related legal advice, please email:

- **CRAC:** [Securityarchitecture@fac.nsw.gov.au](mailto:Securityarchitecture@fac.nsw.gov.au)
- **Legal:** [infoandprivacy@justice.nsw.gov.au](mailto:infoandprivacy@justice.nsw.gov.au)



# Patch Management Policy

---

## Table of contents

- 1 Purpose..... 2
- 2 Definitions and acronyms ..... 2
- 3 Scope..... 5
- 4 Policy statement..... 6
- 5 Patch management objectives ..... 6
- 6 Policy ..... 6
  - 6.1 General requirements ..... 6
  - 6.2 Patching schedule..... 7
  - 6.3 Handling cases where a patch isn't available..... 10
  - 6.4 DCJ change controls..... 11
  - 6.5 Patch management process ..... 11
  - 6.6 Procedure for requesting exceptions ..... 15
  - 6.7 Key performance and risks indicators (KPIs and KRIs)..... 15
  - 6.8 Allocation of patching responsibilities ..... 16
- 7 Related legislation and documents..... 19
- 8 Document information ..... 20
- 9 Support and advice ..... 21

## 1 Purpose

This policy is designed to ensure the proactive management and security patching of the Department of Communities and Justice's (DCJ's) information and communication technology (ICT) systems and all computers and devices.

Patches are modifications to software or hardware to address either known problems (security or otherwise), introduce new functionality or improve usability and performance.

Patch management is the process of controlling the regular deployment of software patches on almost everything from small software to operating systems as well as patches on physical machines and smartphones/computers used by remote workers. The process assists with:

- maintaining operational effectiveness and efficiency
- mitigating security vulnerabilities
- maintaining the stability of the ICT production environment
- adherence to Australian Signals Directorate (ASD)'s recommendations on mitigating cyber security incidents (Essential Eight risk mitigation strategies).

DCJ has a responsibility to uphold the confidentiality, integrity and availability of the data and information held on its ICT systems on premise, in the cloud or systems and services supplied by third parties.

DCJ is committed to having an up-to-date patch management process in place to help protect its information and reduce the risks of a data breach or outage.

## 2 Definitions and acronyms

Term	Definition
ASD	Australian Signals Directorate.
Australian Cyber Security Centre (ACSC)	The Australian Government's lead agency for cyber security.
Change advisory board (CAB)	<p>An authoritative and representative group within the Department of Communities and Justice (DCJ) who are responsible for assessing, from a business and a technical viewpoint, all high impact and/or high risk requests for change (RFCs). The CAB decides on the priorities of RFCs and proposes the allocation of resources to implement those changes.</p> <p>The CAB is chaired by the Change and Transition Manager.</p>
CISO	Chief Information Security Officer.

Term	Definition
Cloud services	A cloud service is where an organisation pays to use, rather than own, the resources that are delivered over the network such as the internet by the cloud service provider. Cloud refers to where the solution is provided.
Cyber Security NSW	An entity in the NSW Government that provides leadership and coordination across the whole of government in managing risks against cyber threats.
DCJ	Department of Communities and Justice.
Exemption	Where a vulnerability has been identified but the standard response will not be actionable due to technical constraints, cost or other consideration(s).  Note: This may also require an information security policy exception e.g. if we will not patch due to technology approaching end of life (EOL).
ICT	Information and communication technology.
IDS	Information and Digital Services, a branch within DCJ's Corporate Services Division.
ICT systems	The term information technology (ICT) systems includes: <ul style="list-style-type: none"> <li>• workstations</li> <li>• servers (physical and virtual)</li> <li>• operating systems</li> <li>• standard operating environments (SOEs)</li> <li>• firmware</li> <li>• networks (including hardwired, Wi-Fi, switches, routers)</li> <li>• hardware</li> <li>• software (databases, platforms etc.)</li> <li>• applications (including mobile apps)</li> <li>• cloud services</li> </ul> of any kind that require support, maintenance, or attention in alignment with this policy. They can be physical, virtual, public or private cloud information systems assets.
ISMS	Information security management system
Key performance indicators (KPI)	A KPI is a measurable value that demonstrates how effectively a company is achieving key business objectives. It is a measure of how well something is being done.

Term	Definition
Key risk indicators (KRI)	A KRI is defined as measurements, or metrics, used by an organisation to manage current and potential exposure to various operational, financial, reputational, compliance, and strategic risks. It is an indicator of the possibility of future adverse impact.
Must	The item is mandatory. Any request for deviation from a “must” must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a “must not” must follow the procedures for requesting exceptions.
Proof of concept (POC)	The realisation of a certain method or idea to demonstrate its feasibility, or a demonstration in principle, whose purpose is to verify that some concept or theory has the potential of being used. A proof of concept is usually small and may or may not be complete.
Security threat	An identified actor that potentially exposes DCJ to cyber attack by exploiting information and communication technologies (ICT) vulnerabilities. Threats need to be assessed to determine the extent of protection and/or controls that are in place to protect DCJ.
Security vulnerability	An identified deficiency or weakness in DCJ ICT controls that has been detected, exists/is current and requires consideration and response.
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course.
SOE	Standard operating environment
Software	Firmware, operating systems, standard operating environments (SOEs), network appliances and applications.
Sub-supplier	A supplier who provides goods or services to another supplier.

Term	Definition
System importance	<p><b>External:</b> DCJ systems that are on internet accessible infrastructure – either publicly accessible, or via a proxy. Includes “untrusted” and “semi-trusted” sites.</p> <p><b>Internal:</b> DCJ systems that sit on an infrastructure that is only available from inside the DCJ ICT network.</p> <p><b>Critical system, external:</b></p> <ul style="list-style-type: none"> <li>• DCJ systems that are public/internet facing.</li> <li>• Systems that have been identified as DCJ’s crown jewels and are public/internet facing.</li> </ul> <p><b>Critical system, internal:</b></p> <ul style="list-style-type: none"> <li>• Internal DCJ systems.</li> <li>• Systems that have been identified as DCJ’s crown jewels and are internal to DCJ only.</li> </ul> <p><b>Non-critical system, internal:</b></p> <ul style="list-style-type: none"> <li>• Other systems that do not hold critical data themselves, but are required in order to perform certain business services e.g. ServiceNow.</li> </ul> <p><b>Other systems:</b></p> <ul style="list-style-type: none"> <li>• Systems not in any of the previous categories and do not directly impact business functions e.g. personal endpoint devices such as employee workstations and laptops.</li> </ul>

### 3 Scope

This policy must be complied with by:

- all DCJ permanent full time, part time, trainee and temporary staff, graduates, contractors, consultants and vendors engaged by DCJ
- anybody authorised to access and make use of any DCJ computing systems, networks and/or information
- all third party suppliers and hosted/managed service providers.

This policy is applicable to:

- all agencies within DCJ
- all DCJ information systems assets that include firmware, operating systems, standard operating environments (SOEs), network appliances and applications (collectively referred to as software) of any kind that require support, maintenance, or attention in alignment with this policy
- physical, virtual, public or private cloud information systems assets.

## 4 Policy statement

DCJ will:

- meet Essential Eight recommendations, namely patching applications and patching operating systems
- where possible, maintaining up-to-date patches and software version levels on all DCJ's ICT systems and services supplied by third parties.

This policy provides a framework for ensuring that DCJ information assets are current, up-to-date and secure.

## 5 Patch management objectives

The objective of this policy is to ensure that:

- appropriate controls are implemented to protect departmental information assets from vulnerabilities
- software patches are tested and implemented in a timely manner with minimal disruption to business operations
- all devices are proactively managed and patched with appropriate security and version updates
- various systems in a network are up-to-date and secure against various kinds of hacking and malware
- application and operating system patches are up-to-date to meet ASD's mandatory mitigation strategies.

## 6 Policy

### 6.1 General requirements

All ICT systems either owned by DCJ, or those in the process of being developed and supported by third party vendors, must be manufacturer supported and have up-to-date and security patched operating systems and application software.

Software assets must be maintained and supported in order to minimise the department's exposure to business risks associated with software vulnerabilities and errors.

Where patches are released by vendors to upgrade the servers and/or firmware in the DCJ environment, the criticality of vendor software patches must be assessed based on their ability to remediate a business risk exposure.

To maximise protection to DCJ and minimise risk of exposure, DCJ's ICT systems and software assets should aim to achieve ASD's highest maturity level of mitigation strategy for patching, namely patching applications and patching operating systems.

Depending on the criticality of the vulnerability and subject to successful testing, any patch update related to security vulnerabilities should always be prioritised and implemented within agreed timeframes as depicted in Table 1.

**Table 1 - Incident/event response**

Patch severity	System importance <sup>1</sup>			
	Critical system, external	Critical system, internal	Non-critical system, internal	All other systems
Emergency/critical	1 Week	2 Weeks	3 Weeks	1 Month
High	2 Weeks	1 Month	1 Month	2 Months
Moderate	2 Months	2 Months	2 Months	3 Months
Low	3 Months	3 Months	3 Months	3 Months

## 6.2 Patching schedule

### 6.2.1 Incident/event response

Patches are deployed in response to an incident or event which may include:

- a security breach that uncovers a vulnerability and network exposure
- a software/hardware failure that prevents or inhibits the business functioning
- a scheduled maintenance activity
- a system enhancement that increases or significantly modifies software functionality.

From the security perspective, the Cyber Risk, Audit and Compliance (CRAC) team constantly monitors DCJ's systems for security threats/vulnerabilities. Notifications of threats can also be received from an initiator (e.g. software vendor, Cyber Security NSW, Australian Cyber Security Centre). Where the threats are classified as critical or emergency by the initiators, CRAC will assess the business impact as soon as possible after the notification/detection in order to determine the appropriate actions to take before referring to the relevant Information and Digital Services (IDS) teams (see Section 4.1 assessment activities of DCJ's Information and Communications Technologies (ICT) Threat and Vulnerability Management Procedure).

In contrast, patches that are not security related, are not assessed by CRAC. Vendor patches (such as routine updates) are received directly by the relevant IDS teams to determine the response time and priority of the patch.

<sup>1</sup> See section 2 for definition.



The following table specifies the response time limits in terms of the importance of the system to the business and the severity (see Table 2) of the incident that has occurred.

**Table 2 - Definition of severity**

Rating	Definition	Consequence <sup>2</sup>
Emergency/ Critical	A threat or vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self- propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs without warnings or prompts. This could mean browsing to a web page or opening e-mail.	Extreme
High	A threat or vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of DCJ data, or of the integrity or availability of processing resources.  These scenarios include common use scenarios where DCJ is compromised with warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.	High
Moderate	Impact of the threat or vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.	Moderate
Low	Impact of the threat or vulnerability is comprehensively mitigated by the characteristics of the affected component.	Insignificant/ Minor

### 6.2.2 Emergency patching

Emergency patches are fixes that must be implemented immediately, either because a significant security threat or weakness in a DCJ system has been identified, or because of a failure that prevents critical business functions from being executed.

In general, the implementation/deployment of a patch follows the instructions in Table 3 [bookmark702](#). The time needed to provide a permanent fix (patch) of the information asset can vary depending on whether it is a patching of a security vulnerability or patching of a business functionality. From the table it can be seen that security-related patches must be implemented according to the prescribed times (Table 1) whilst other, functional patches can vary depending

<sup>2</sup> Refer to the 2019-2020 ICT Business Impact Analysis (Appendix B - Consequence table, Category: Information and Technology) for definition of the consequences

on prevailing factors such as the complexities and contexts involved. The actual implementation schedule is determined by the project team itself.

**Table 3 - Patch response time vs. patching time**

Type of incident	Response time requirement	Patching time requirement
Security related patches	As per Table 1	As per Table 1
Business functionality patches	As per Table 1	<p>This can vary depending on complexities and contexts involved and will be justified by the asset owner. The length of time required may be influenced by factors such as:</p> <ul style="list-style-type: none"> <li>• cloud service (onshore/offshore)</li> <li>• extent of DCJ specific configuration</li> <li>• number of application interfaces</li> <li>• mission criticality of application</li> <li>• degree of testing required.</li> </ul>

### 6.2.3 Routine updates

Routine updates are non-emergency patches/fixes for ICT systems and include fixes for identified security vulnerabilities or business functionalities that do not need to be implemented urgently.

Table 4 below proposes responses for non-emergency patches.

**Table 4 - Responses for non-emergency patches**

Asset types	Patching/review frequency (subject to application dependencies) <sup>3</sup>
Mobile devices (laptops, smart phones and tablets):	<p><b>Smart phones and tablets:</b> Review annually</p> <p><b>Managed laptops (MDM):</b> Automatically synchronised with the server upgrade (e.g. O365/Azure)</p> <p><b>Non-managed laptops:</b> Requires manual intervention (usually initiated by a server upgrade)</p>
Desktops environment including all operating systems (IDS supplied SOE, non-SOE Windows, Linux and OSX)	Quarterly

<sup>3</sup> Patching of a component of a system may make it incompatible with other components of the system. In this case it may be appropriate to defer the patch until all dependencies are met

Asset types	Patching/review frequency (subject to application dependencies) <sup>3</sup>
Applications	<p><b>Core desktop applications</b> (e.g. browsers, Adobe Reader, Office): 3 - 6 monthly</p> <p><b>Commodity/utility applications on ad-hoc workstations:</b> As required</p> <p><b>Core business applications</b> (e.g. ChildStory): Synchronise with the application's release cycle or frequency</p> <p><b>Non-core business applications</b> (e.g. Fieldglass): As required</p>
Operating systems	Quarterly
Internal Servers	Quarterly
Firmware	Annually with very high risk vulnerabilities prioritised accordingly.

The custodians of servers, laptops and desktops where the operating system has reached their end of life (EOL) or is out of support and cannot be patched must ensure the assets are updated or replaced (if possible) with vendor supported versions. Otherwise, a request for exception from patching must be submitted for approval, as per Section 6.6.

### 6.3 Handling cases where a patch isn't available

In the event an application or operation system component requires patching but that patch is not yet available, the vendor would provide a workaround which must be tested by the system/business owner in their user acceptance testing (UAT) environment to ensure applying any workaround does not break anything or does not cause any interruption of the service before submitting the change request for approval.

In the case of a security concern, where a known vulnerability cannot be patched (as in the case of legacy systems), or not patched immediately, custodians must quarantine the ICT system where possible and implement controls to:

- resolve the vulnerability
- prevent exploitation of the vulnerability
- contain the exploit.
- document the risk and associated mitigation (the workaround) in the corporate risk register.

Software vendors must be notified of errors and/or vulnerabilities identified and which may have a significant impact on the stability, operation or security of information assets.

## 6.4 DCJ change controls

All patching requests must be submitted to the relevant ex-Department of Family and Community Services (FACS) or ex-Department of Justice (Justice) change manager group in accordance with the ICT Change Management Procedure (refer to Section 7) as this will be a tracking mechanism for approvals or rejections of each request for patching to be applied.

No patching is to proceed without the full approval of the submitted change. The patching must be applied within the start and end dates as stated in the change request.

It is the responsibility of the custodians to seek approval for an agreed outage either during business hours or after business hours depending on the criticality of the release.

It is the responsibility of all submitting parties to submit relevant documentation in accordance with the Change Advisory Board (CAB) procedure.

Any patches categorised as emergency/critical or high risk by the vendor must be installed within the response timeline as defined in Section 6.2.2 upon the release of the operating system or application from the vendor. Where the emergency patch does not implement all the requirements of the ICT Change Management Procedure, these must be addressed at an appropriately planned date in the future.

Where automatic patch updates are not used, patch implementation should be subject to the change management procedures.

## 6.5 Patch management process

A patch management process must be established within each ICT environment/domain (e.g. Windows, Application, Cloud) to reduce DCJ's exposure to security vulnerabilities and permitting IDS to maintain the ISO27001 certification.

The Operations Manager of each domain is responsible for ensuring the patch management process specific to their domain is written and the responsibilities assigned in the process.

The process must align to the Patch Management Policy and must have, at minimum, the following processes outlined below.

### 6.5.1 Create an inventory of all ICT assets

An inventory of all assets (including hardware and software, software versions and patches applied within ICT environment) should be established and maintained to keep a record of the patches implemented and the current patch status of all ICT assets. Where the inventory does not exist a plan should be in place to build one.

The inventory must contain at least the following information:

- asset name

- patch build
- software/product version
- date applied.

The inventory of assets must have controls in place to prevent unauthorised access to it.

### **6.5.2 Categorise by risks and priority**

Unless it is an emergency fix or advised by CRAC, (see Section 6.2.1), the technical service manager/custodian must determine the priority of the patch. A software patch criticality classification scheme and associated assessment criteria must be defined and documented to ensure that:

- patch criticality is effectively communicated
- assessment is applied consistently
- implementation timetables appropriately reflect risk.

Categorising a software patch must record all details of risk assessments and the criticality ratings determined by them.

In addition, cyber threat intelligence should also be considered in order to prioritise patch deployment based on relevant vulnerabilities being exploited in the wild.

The effect of a patch to the DCJ's infrastructure (e.g. servers, desktops, printers) must be assessed prior to its deployment.

### **6.5.3 Utilise a test environment**

A test environment that is as representative as possible to the production environment should be created to replicate the applications that will be used to test current patch updates.

### **6.5.4 Patch evaluation**

Software patches must be obtained from a trusted source and verified for authenticity and integrity. All software patches must be tested prior to deployment to the production environment.

Business users should be, where possible, invited to participate in patch testing. In some circumstances, particularly where the patch is of a critical nature, the available time for testing may not be adequate to ensure rigorous test coverage; in which case deployment of the patch is at the discretion of IDS, and should be undertaken in the best interest of the department.

Wherever possible, testing of software patches should be completed in isolation from the production environment.

The scope and nature of the testing performed must appropriately reflect the following:

- business importance of the software or application
- assessed criticality of the patch
- available vendor release notes and instructions
- past experience in applying patches from the vendor.

A rollback plan should be devised so that if something does go wrong, the impact to the business is minimal while a solution is found.

#### **6.5.5 Patch monitoring and reporting**

The monitoring process should rely on reputable outside sources for version upgrade and security vulnerability information, such as vendor websites or mailing lists. These reputable information sources must be monitored regularly and frequently (frequency determined by the relevant IDS manager) to ensure that:

- software vulnerabilities that impact on the DCJ's information assets are identified in a timely manner
- vendor patches that address vulnerabilities can be acquired and deployed
- awareness of the availability of the latest software version update.

Separation of control (i.e. no single critical task is in the hand of any individual) must be established to ensure issues are promptly identified and resolved before they become a problem for the department.

Reporting metrics that summarise the outcome of each patching cycle must be compiled to include:

- the patching deployment status to evaluate the current patching levels of all systems
- the assessment of the current level of risk. It should report on the compliance levels as the deadline is reached on the deployment levels.

#### **6.5.6 Create backups on production environment**

Once patches have been deployed in the test environment, they should be monitored for any updates and evaluated to see if any breaks occur.

A full backup of the data and configuration setups must be created once the patch testing has completed. The backups and restore process should be tested periodically to ensure it operates entirely.

#### **6.5.7 Implement configuration management**

In a mature state, changes to the production environment are documented in the configuration management database (CMDB). In the absence of a fully mature

CMDB, the details of what has been changed (including implementation and rollback steps) are recorded in the initiating change request, which can be used as a formal reference point to overcome any challenges during patch deployment.

#### **6.5.8 Implementation**

Implementation of software patches must be performed in compliance with the relevant ex-FACS or ex-Justice change management procedure and in a manner designed to minimise business disruption.

Implementation plans must include details of the sequencing of patch application, including a roll-back plan in case the patching fails. These plans should consider the different outage availabilities for each of the environments as their business schedules and technical outages allow. Patching of the operating system, regardless of environment, should be scheduled with the customer at a suitable time.

Emergency patches must be implemented as soon as possible after business hours to ensure patch authenticity, integrity and stability. The patch being deployed must be closely monitored to ensure a disaster recovery plan can be actioned, as necessary.

Non-emergency patches should be implemented during scheduled maintenance windows.

Security patches must be up-to-date for ICT systems which are being designed and delivered by third party suppliers prior to going operational. Third party suppliers must be prepared to provide evidence of up-to-date patching before ICT systems are accepted into service and become operational.

The success or failure of patch implementation must be assessed and remedial actions taken to correct failures.

Failed deployment needs a reasonable explanation as to why this has occurred and the steps taken to implement a mitigation plan. If a mitigation plan cannot be achieved then details should be entered into the enterprise risk register and within appropriate team/division registers.

Upon successful implementation, all relevant registers must be updated to reflect current patch level.

#### **6.5.9 Regular patch maintenance**

Post patch deployment, the status of hardware and applications on the network should be monitored regularly to make sure there are no breaks or problems.

#### **6.5.10 Documenting the patch management process**

Managers should ensure that patch management process and procedures are documented in their areas to ensure the patching personnel know what to do when they undertake patching activities.

## 6.6 Procedure for requesting exceptions

Requests for exceptions must articulate an appropriate business case to justify deviation from a policy or standard where:

- there are patches that cannot be applied to the systems
- systems or applications that cannot be patched to resolve a known bug or vulnerability
- systems that transmit or store protected data and cannot be patched to resolve a known vulnerability.

The business case should include relevant information such as the reason for the exception, a designated owner, a scope and a timeframe for the exception, mitigating or compensating controls to manage risk and a remediation plan to realign with the breached policy or standard.

Where the request is for deferral of patching:

- Infrastructure operations and end user services team should be contacted to initiate a policy exception.
- Exceptions must be approved by the Director, Infrastructure Operations and End User Services and must be recorded in the exceptions register. Exceptions will be reviewed at the cessation of the exception period and will require re-approval should they need to be extended.

Where the request is for exemption from patching:

- the Cyber Risk, Audit and Compliance team should be contacted to initiate a policy exception
- exceptions must be approved by the Chief Information Security Officer and must be recorded in the exceptions register.

## 6.7 Key performance and risks indicators (KPIs and KRIs)

Where possible, appropriate measures should be implemented to demonstrate the effectiveness and efficiency of the patch management process to ensure continuous improvement of DCJ's security posture, and highlight increasing or decreasing risk levels, for example:

- For KPI's:
  - mean time to apply patches **or**
  - percentage of ICT systems fully patched at any given time.
- For KRI's:
  - percentage of downtime due to scheduled patching activities



- percentage of critical systems without up-to-date patches (aka patch coverage rate)

## **6.8 Allocation of patching responsibilities**

A review of patching roles and responsibilities of ICT staff should be undertaken to determine if they are correct or if training should be arranged to ensure staff are equipped with the right skills for the role. If the key skills required for patching are missing in the current team, a business case should be raised to fill the skills gap.

### **6.8.1 DCJ executive**

- Approves the policy as appropriate.
- Ensures that all directorates/divisions adhere this policy.
- Appropriately resources and supports DCJ patch management initiatives.
- Ensures that staff comply with Patch Management Policy.

### **6.8.2 ICT subcommittee**

- Endorses the policy as appropriate.

### **6.8.3 Chief Digital Information Officer (CDIO)**

- Ensures this policy is implemented.
- Ensures IDS develops, implements and maintains an effective Patch Management Plan.
- Works with IDS Director, Infrastructure Operations and End User Services to implement this policy.
- Ensures enforcement of this policy across all users and ICT systems whether on premise, remote, cloud or hybrid cloud.

### **6.8.4 Chief Information Security Officer (CISO)**

- Implements a vulnerability management framework that Security Administrator uses to identify vulnerabilities.
- Works with the IDS Director, Infrastructure Operations and End User Services to ensure that third party suppliers comply with DCJ's Patch Management Policy.
- Approves request for exemption from patching (no patch).

### **6.8.5 IDS Director, Infrastructure Operations and End User Services**

- Approves exception request to defer patching.
- Define roles and responsibilities related to patching activities.

- Identify key performance indicators (KPIs) and key risk indicators (KRIs) for patching.
- Ensure KPIs and KRIs for patching are implemented, if required.
- Ensure that staff under their control comply with the policy and to ensure there are formalised patch management processes in place that comply with the requirements of this policy.
- Works with the CISO to ensure that third party suppliers comply with DCJ's patch management policy.

#### **6.8.6 Custodians of ICT systems**

- Review and assess the hardware updates or patches.
- Assess the operating system patches.
- Review and assess the firmware updates.
- Review and assess the security patches.
- Review, assess and monitor critical bugs.
- Review, assess and make the comments on the change requested submitted by the vendors.
- Allocate the patches to be fixed.
- Approves for the patches to be implemented in production.
- Review patching roles and responsibilities of ICT staff to determine if they are correct or if there needs to be a reshuffle.
- Initiate request for an exception from patching if required.

#### **6.8.7 IDS service managers**

- Ensure all known and reasonable defences are in place to reduce network vulnerabilities while keeping the network operating
- Ensure the patch management processes and procedures are developed, followed and reviewed regularly by the team.
- Ensures that the required patches or mitigating actions are prioritised and applied.
- Define sources for identifying patches.
- Monitors publication of patches via mailing lists, electronic vendor notification and vendor web sites for the release of patches and version upgrades.

#### **6.8.8 Third party suppliers (providing the patches)**

- Assesses the need for applying patches, including emergency/urgent patches.

- Ensure third party managed security patches for DCJ systems must be up-to-date prior to going operational.
- Once DCJ's ICT systems are operational, ensure the vulnerability patching is carried out regularly.
- Reviewing reports and patch or mitigate the reported vulnerabilities.
- Monitor vendor announcements of critical bugs.
- Scheduling system outages with the DCJ service managers.
- Raising a change to apply the patches.
- Applying the necessary patches.
- Updating DCJ operations managers when patches are completed.
- Uninstall/rollback any patch causing degradation of system.
- Escalate to IDS operations managers if any issues.
- Where systems are managed by a sub-supplier, the third party supplier is responsible for ensuring that sub-supplier's systems are maintained in compliance with the third party supplier's patch management policies and procedures.

#### **6.8.9 Change Advisory Board**

- Responsible for approving the patch management deployment requests.

#### **6.8.10 End users**

- Ensure the patch is installed and the machine is rebooted as required.
- Report any problem to IDS Service Desk.
- Ensure prudent and responsible use of computing and network resources.

#### **6.8.11 System administrators**

- Acquire patches for systems.
- Categorise the criticality of the patch.
- Notify operations teams (quality assurance (QA), development, pre-production and production) of patching schedules.
- Test services after patching.
- Notify and report testing results to the operations teams.
- Work with security administrators to remediate issues, as necessary.

- Perform a proof of concept (POC) followed by an impact assessment to the current infrastructure (include consultation with backup team and other vendors to see confirm they are OK for DCJ to do the patching).
- Confirm with developer/vendor whether any particular patch should not be applied.
- Allow reasonable outages for third party supplier to apply patches and upgrades in a timely manner.
- Perform application testing after patches have been applied
- Provide UAT to the third party supplier following the patching of third part supplier software, to ensure that the applied patches have not had any unexpected effects.
- Apply patches in a timely manner to prevent vulnerability exploitation, outage or breach, or failure of a critical business function.

#### **6.8.12 Security administrators**

- Scan DCJ networks for vulnerability status of devices, apps and databases.
- Assess and mitigate security weaknesses.
- Determine the risk and the relevance of the patch, as well as when the system should be patched.
- Scan for patches as part of the vulnerability management procedure.
- Work with system administrators to remediate issues, as necessary.
- Assess the criticality of vendor software patches based on their ability to remediate a business risk exposure .
- Define sources for identifying vulnerabilities.

## **7 Related legislation and documents**

This policy ensures compliance with the NSW Cyber Security Policy.

Compliance to the above supports the intentions of:

- *Crimes Act 1900*
- *Government Sector Employment Act 2013*
- *Independent Commission Against Corruption Act 1988*
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*
- *Public Finance and Audit Act 1983*
- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*

- *Government Information (Public Access) Act 2009*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

This document is related to the following policies:

- [Information Security Policy](#)
- [IT Security Policy](#)
- [Data Privacy and Protection Policy](#)
- Enterprise Risk Management Framework
- Information Security Management System (ISMS) Framework
- Information Security Policy Exception Request (available from the [Information Security Policy](#) page)
- [Access Control Policy](#)
- [IT Acceptable Use Policy](#)
- [Cloud Security Policy](#)
- [NSW Cyber Security Policy](#)
- [Australian Signals Directorate Essential Eight Maturity Model](#)
- ICT Threat and Vulnerability Management Procedure
- ICT Change Management Procedure v2.2 for ex- FACS (available at D17/1287372)
- Digital and Technology Services (DTS) Change Management Procedure for ex-Justice (available at D07/26832)
- 2019-2020 ICT Business Impact Analysis.

## 8 Document information

Document name	Patch Management Policy
Applies to	All DCJ ICT systems, computers and devices.
Replaces	Department of Justice DTS Patch Management Policy
Document reference	AF21/7807
Approval	Director, Infrastructure Operations and End User Services 2 July 2020
Version	1.0
Commenced	29 March 2021
Due for review	March 2022

Policy owner	Infrastructure Operations and End User Services Information and Digital Services Corporate Services
--------------	---

## 9 Support and advice

It is the responsibility of CRAC to monitor compliance with and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

Reviews shall incorporate:

- assessment of opportunities for improvement of the approach to information security
- consideration of changes to the organisational environment, business circumstances, relevant laws, legal conditions, or technical environment
- changes in external and internal issues that are relevant to the ISMS
- results of risk assessments and status of risk treatments
- fulfilment of security objectives
- results of management review of information security
- results of independent review of information security
- results of security incidents.

You can get advice and support about this policy from:

Business unit	Principal Manager SOE, Packaging and Antivirus Infrastructure Operations and End User Services Information and Digital Services Corporate Services
Email	<a href="mailto:client.environment@justice.nsw.gov.au">client.environment@justice.nsw.gov.au</a>

This policy is subject to change. The latest published version of the policy is available on the DCJ intranet.

## PRIVACY POLICY

Version 2.0 December 2017

- About this Policy
- What is Personal Information?
- What personal information do we collect?
- Personal Information provided by you
- Automatic and Indirect collection of personal information
- Storage and Security
- Social Networking Services
- Anonymity
- Use of Personal Information
- Disclosure of personal information
- Quality of personal information
- How can I access or amend my personal information
- Data Breach
- Complaints
- Review

### About this Policy

The *Privacy and Personal Information Protection Act 1998* (PIIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) applies to NSW public sector agencies including local councils and universities.

This Privacy Policy outlines the personal information handling practices of the Department of Justice (the Department). It also describes how the Department deals with personal information and other data collected. The Department's Privacy Policy provides a framework outlining how the Department manages personal and health information. We are committed to responsibly and properly managing the personal information we collect and protecting the privacy of our stakeholders, staff and members of the public.

The specific legal obligations of the Department when collecting and handling your personal information are outlined in the PIIP Act and the HRIP Act, the Codes of Practice and Privacy Regulations (<https://www.ipc.nsw.gov.au/privacy-laws>).

## **What is Personal Information?**

Personal Information is defined in the PIIP Act as information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from that information or opinion. Personal Information includes, for example, names, addresses, telephone numbers, email addresses, dates of birth and passport numbers.

Under the PIIP Act / HRIP Act some of the types of information about an individual that are not considered personal information, include:

- when it relates to a person who has been dead for more than 30 years;
- when it is contained in a publicly available publication;
- information arising out of a Royal Commission or Special Commission of Inquiry;
- information contained in Cabinet documents; or
- the exercise of judicial functions by a court or tribunal.



## What personal information do we collect?

Personal information is collected by the Department through:

- the Department's website;
- call centres - telephone enquiries;
- general e-mail enquiry accounts;
- correspondence received from members of the public;
- individuals signing up to mailing lists;
- individuals who register for events; and
- feedback forms.

Personal information we collect is handled in accordance with the PPIP Act and the HRIP Act. The types of personal information collected include:

- names;
- addresses;
- telephone numbers;
- email addresses;
- dates of birth;
- IP addresses; and
- Other personal information as specified in this Policy.

More detailed information about how the Divisions within the Department (Veterans Affairs, Juvenile Justice, Corrective Service NSW, Office for Police, Office of Emergency Management, Justice Services, Justice Strategy and Policy, Court and Tribunal Services, Corporate Services, Office of the Secretary) handle personal information is set out in the Department's Privacy Management Plan (<http://www.justice.nsw.gov.au/lsb/Pages/privacy-management-plan/privacy-management-plan.aspx>).

## Personal Information provided by you

The Department aims to collect personal information about you directly from you. This may occur when you:

- Contact us to ask for information;
- Contact us for assistance with or consideration of an application specific to your circumstances;
- Inform or notify the Department about an issue;
- Provide submissions to the Department;
- Make a complaint;
- Ask for access to information held by the Department; or
- Apply for a job with the Department / provide referee reports.

We may collect your personal information from third parties, for example, your legal or other authorised representative or respondents to a complaint or inquiry.

We may also collect personal information from publicly available sources, for example, to enable us to contact stakeholders who may be interested in our work or in participating in our consultation.

Some agencies in the Department are lawfully authorised to collect information about you from third parties such as law enforcement agencies, investigative agencies or other public sector or private sector organisations when authorised by law, enabled by a privacy or health code of practice, public interest direction or with the consent of the individual.

When an agency in the Department (<http://www.justice.nsw.gov.au/about-us>) collects personal information as part of its functions and activities, the agency will have its own privacy statement(s) and/or collection notices explaining how your personal information will be collected, used, stored and disclosed.

## **Automatic and Indirect collection of personal information**

The Department does not collect personal information and other data from you through the use of Cookies or other automated means including server logs. When you access the Department's website we will record information that identifies, for each page accessed, the IP (Internet Protocol) address of the machine that accessed it.

We use Google Analytics to collect data about your interaction with the Department's website. The sole purpose of collecting your data by using Google Analytics, is to improve your experience when using the Department's website. The types of data we collect include:

- your device's IP address (collected and stored in an anonymised format);
- device screen size;
- device type, operating system and browser information;
- geographic location (country only);
- referring domain and out link if applicable;
- search terms and pages visited; and
- date and time when website pages were accessed.

The collecting of the data noted above is combined with similar logged information. This combined information is used to improve the services provided by the Justice website. The Department will extract and publish this combined information about usage patterns from these records. For example, our usage reports will examine trends based on the following information – your server address, your top level domain name (for example .com, .gov, .au, .uk etc), the date and time of visit to the site, the pages accessed, documents downloaded, the previous site visited and the type of browser used and operating system

The Department will gather extensive information relating to access to our website in the following circumstances:

- unauthorised attempts to access information that is not published on the Department of Justice website pages;
- unauthorised tampering or interference with information published on the Department's website;

- unauthorised attempts to index the contents of the Department's website by other websites;
- attempts to intercept messages of other Department of Justice website users;
- communications that are defamatory, abusive, vilify individuals or groups or that give rise to a suspicion that a criminal offence is being committed; and
- attempts to compromise the security of the web server, breach the laws of the State of New South Wales or Commonwealth of Australia, or interfere with the enjoyment of the Department's website by other users.

On its websites the Department provides feedback facilities to allow users to provide input into the future development of its websites and comment on the provision of services.

Users are required to provide the Department with a name and an email address to enable a reply to any feedback. This information will only be used for the purpose for which it was provided. Your name and email address will not be added to any mailing list.

## **Storage and Security**

We take steps to protect the security of the personal information we hold from both internal and external threats by:

- regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification or disclosure of information;
- providing targeted privacy training to the various agencies in the Department;
- where appropriate, staff and service providers are required to sign confidentiality agreements regarding access to personal information held by the Department; and
- Agencies in the Department are encouraged to develop robust governance frameworks in relation to the handling of personal information.

Information collected by the Department is stored securely in accordance with State Archives requirements. More detailed information on security standards and practices is available in our Privacy Management Plan (<http://www.justice.nsw.gov.au/lrb/Pages/privacy-management-plan/privacy-management-plan.aspx>).

Access by Departmental employees, contractors or other authorised parties to personal information held by the Department is determined by role and the need for access. Unauthorised access to and use of personal information is taken seriously as it constitutes a data breach and disciplinary or other action may be taken by the Department.

Personal Information is only retained as long as necessary and securely destroyed or de-identified once it is no longer required by law. Further information about records disposal authorities relevant to agencies in the Department is set out in the Department's Privacy Management Plan (<http://www.justice.nsw.gov.au/lrb/Pages/privacy-management-plan/privacy-management-plan.aspx>) and the State Records Authority.

## **Social Networking Services**

We use social networking services such as Twitter, Facebook, LinkedIn and YouTube to communicate with the public about our work. When you communicate with us using these services we do not collect your personal information.

## **Anonymity**

We will require your name, contact information and sufficient information relating to your inquiry in order to carry out most of our functions in order to provide you with a service.

Where possible we will allow you to interact with us anonymously or by using a pseudonym. For example, if you contact an enquiry line with a general question you will not be required to provide your name unless we need your personal information to adequately handle your question.

## **Use of Personal Information**

The personal information you provide to the Department will be used for the primary purpose for which you provided it and any secondary purposes where it is directly related to that primary purpose. Detailed information in relation to the use of information collected by the agencies in the

Department is detailed in the Privacy Management Plan (<http://www.justice.nsw.gov.au/lrb/Pages/privacy-management-plan/privacy-management-plan.aspx>).

## **Disclosure of personal information**

The Department will disclose your personal information in the following circumstances:

- where you have already been made aware of the disclosure to third parties;
- the disclosure is required to be made to an investigative or law enforcement agency (as defined in the PPIP Act)'
- the disclosure is authorised or required by law;
- the disclosure to a third party is necessary to prevent or lessen a serious and imminent threat to the life or health of you or another person; or
- with your consent.

More specific information about disclosure of information is contained in the Department's Privacy Management Plan (<http://www.justice.nsw.gov.au/lrb/Pages/privacy-management-plan/privacy-management-plan.aspx>) and privacy statements relevant to each agency's functions and activities.

To protect the personal information we disclose we may, where appropriate:

- enter into a contract or Memorandum of Understanding (MOU) requiring the service provider to only use or disclose the information for the purposes of the contract or MOU; and / or
- include special privacy requirements / clauses in the contract or MOU, where necessary.

## **Quality of personal information**

To ensure the personal information we collect is accurate, up-to-date and complete we:

- record information in a consistent format;
- where necessary, confirm the accuracy of information we collect if the information is collected from a third party or a public source; and

- promptly add updated or new personal information to existing records.

We also take reasonable steps to review the quality of personal information before we use or disclose it to third parties as set out in the Privacy Management Plan (<http://www.justice.nsw.gov.au/lrb/Pages/privacy-management-plan/privacy-management-plan.aspx>).

## **How can I access or amend my personal information**

Under the PPIP Act and the HRIP Act you have a right to ask for access to personal information / health information we hold about you. You also have a right to ask that we correct that personal / health information if you believe it is incorrect.

You can ask for access to your personal information or for a correction to that personal information by contacting us. If you ask, we must give you access to your personal information unless there is a lawful reason preventing that access. We must take reasonable steps to correct personal information if we consider it is inaccurate or incorrect, unless a law prevents us from doing so. If we refuse to correct your personal information, you can ask us to associate with it (for example, attach or link) a statement that you believe the information is incorrect and why you hold this belief.

You also have the right under the *Government Information (Public Access) Act 2009* (GIPA) to request access to documents that we hold. Excluded information of some agencies, as set out in Schedule 2 of the GIPA Act ( e.g the Office of the Legal Services Commissioner, NSW Trustee and Guardian) cannot be accessed under the GIPA Act. Further information about accessing information under the GIPA Act is available on the Justice Access to Information (<http://www.justice.nsw.gov.au/contact-us/access-to-information>) page.

## **Data Breach**

### The *Privacy Amendment (Notifiable Data Breaches) Act 2017*

(<https://www.legislation.gov.au/Details/C2017A00012>) establishes a Notifiable Data Breaches (NDB) scheme which is due to commence on 22 February 2018. NDB applies to the Department as a tax file number recipient (TFN) as the Department holds Tax File Numbers for employment and other business related purposes. A TFN recipient is any person who is in possession or control of a record that contains TFN information

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any person to whom the information relates. A data breach may occur where personal information held by the Department is lost or subject to unauthorised access or disclosure.

Further information in relation to the scheme is accessible through the following links:

- entities covered by the NDB scheme (<https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/draft-entities-covered-by-the-ndb-scheme#tfn-recipients>)
- identifying eligible data breaches (<https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/draft-identifying-eligible-data-breaches>)

A data breach or allegation of a breach relating to any agency within the Department will be promptly notified to the Office of the General Counsel, Department of Justice. The Office of the General Counsel will coordinate a response to deal with the incident/alleged breach. Responding to a data breach notification to the Office of the General Counsel may include targeted inquiries about the nature and extent of the breach, notification of affected individuals, notifying the NSW Privacy Commissioner and facilitating remedial action.

## Complaints

If you would like to make a complaint regarding an alleged breach of privacy by the Department of Justice you may do so in writing to the Office of the General Counsel, Department of Justice. Further information on how to lodge a complaint, the internal review application form and assistance on how





# Records Management Policy

---

## Table of contents

Purpose ..... 2

Definitions ..... 2

Scope ..... 4

Related legislation and documents..... 6

    Legislation ..... 6

    Standards..... 7

    Principles..... 7

    State Records Regulations 2015 ..... 8

    Information Security Requirements ..... 8

Roles and responsibilities ..... 9

    The Secretary..... 9

    Chief Digital Information Officer ..... 9

    Director, Information Management ..... 10

    Principal Manager Records ..... 10

    Records Management Unit..... 11

    All managers ..... 12

    Project Sponsor/Leads ..... 13

    Non-government organisations, contractors and consultants..... 13

    All employees..... 14

Authorised recordkeeping systems ..... 15

Working remotely..... 16

    Privacy ..... 17

Records retention and disposal authorities ..... 17

Definition of a record..... 17

    Outsourcing..... 19

Document information..... 20

Support and advice..... 20

## Purpose

This policy applies to all Department of Communities and Justice (DCJ) employees who create, receive and record digital records and/or digitise hard copy records for capture into an approved electronic document records management system. It outlines how responsibility for records management has been assigned and how employees are expected to contribute to and interact with the records program and implement sound recordkeeping practices in accordance with relevant legislation, policies, guidelines and NSW State Records Act 1998.

This policy sets the framework for the creation, capture, management and use of records in all formats to support working remotely and the transition from paper to digital recordkeeping. The policy also endorses the principles of digital continuity for electronic records to ensure that records are complete, available and useable for as long as needed by all potential users, including for purposes beyond the intended original use.

To support the DCJ's business and to meet legal and policy requirements, systems that manage information need to operate so that the records they contain:

- are accurate and can be trusted
- enables information to be managed securely as a valued asset, now and into the future
- are complete and unaltered
- allows the sharing of trusted information with government and with the community
- are managed across the full lifecycle, protected from unauthorised use and inappropriate deletion are findable and readable
- can be proven to be genuine.

## Definitions

Term	Definition
State record	<i>State Records Act 1998</i> : Section 3(1): The definition of a State record has been amended to: State record means a record made or received by a person, whether before or after the commencement of this section: <ol style="list-style-type: none"><li>1. in the course of exercising official functions in a public office, or</li><li>2. for the purpose of a public office, or</li><li>3. for the use of a public office.</li></ol>
Business systems	Systems that create, process and manage data to support business processes.

Term	Definition
Corporate records	All corporate information which is evidence of the business of DCJ including decisions, actions, transactions, communications and outputs.
Custodian	A delegate responsible for the safe use, proper custody, security and maintenance of corporate information and records.
Disposal	The destruction of records or their transfer to the Museums of History NSW.
Disposal authority	A disposal instrument approved by the Board of the State Records Authority of NSW. A disposal authority identifies the records required as State archives and provides approval for the destruction of other records after the mandatory minimum retention periods have been met.
Documents	Structured units of recorded information, published or unpublished, in hard copy or electronic form and managed as discrete units in information systems.
EDRMS	Electronic document and records management system
Electronic records	Any information that is recorded in a form that only a computer can process and that satisfies the definition of a record. These may include: computer records, video, audio data. Records may be born digital, or converted to electronic format as a result of scanning or digitisations.
Employees	All personnel employed by the DCJ. This includes all permanent and non-ongoing employees, consultants and contractors.
Files/containers	A file is a collection of documents that show organisational activities through an identifiable sequence of transactions.
Inactive records	Records no longer required for use by the organisation in the conduct of its activities and functions.
Information management	The discipline and organisational function of managing records to meet operational business needs, accountability requirements and community expectations.
Information management systems	Specific applications used to maintain, manage and provide access to an organisations record resources.
Information security	The preservation of the confidentiality, integrity and availability of information

Term	Definition
Metadata	Data describing data and data systems. Information that is used to facilitate intellectual control of, and structured access to, other information. For example, when data was captured, who has accessed it, if/when/how it has been edited or altered.
Personal information	Correspondence that is of a private or non-public nature, that relates solely to an individual's own affairs that do not relate to or have any effect upon the conduct of DCJ business.
Records	Records are the information, regardless of format or media, created, received, or maintained by employees in the course of DCJ business which are evidence of business activities and transactions as well as the associated actions, decisions, outputs, and outcomes.
Recordkeeping	Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.
Records management program	A records management program encompasses the management framework, the people and the systems required within DCJ to manage full and accurate records over time. This includes the identification and protection of records with longer-term value that may be required as state archives.
Sentencing	Applying a disposal authority to a record.
State record	<p>State Records Act 1998: Section 3(1): The definition of a State record has been amended to:</p> <p>State record means a record made or received by a person, whether before or after the commencement of this section:</p> <ol style="list-style-type: none"> <li>1. in the course of exercising official functions in a public office, or</li> <li>2. for the purpose of a public office, or</li> <li>3. for the use of a public office.</li> </ol>

## Scope

This policy covers all divisions of DCJ. It applies to all officers, consultants, contractors, approved users and service providers who have been contracted to undertake outsourced DCJ business activities. This policy does not apply to the Judiciary and NCAT board members.

This policy applies to all hard copy and digital records created and captured in the course of the normal business activities of DCJ, including:

- records and information managed in all business processes
- information in all business systems
- records held in all formats including audio and visual.

This policy applies to all records and associated metadata from the time of creation or capture and covers:

- all DCJ employees, regardless of employment type
- all aspects of DCJ's business operations
- all types and formats of records created to support business activities
- all business applications used to create records
- organisations and businesses, including their employees, to which DCJ has outsourced its functions or activities, and therefore associated recordkeeping responsibilities.

All employees are accountable for the efficient, effective and appropriate use, management and security of records and information resources that are received, created, acquired or retained in the performance of official duties.

All employees are to record and update the location of each record with every movement of the record. This ensures that records, as assets, can be accounted for in the same way that other assets of DCJ are.

Whilst paper processes still occur, most of DCJ's work is conducted digitally, which means the majority of our recordkeeping revolves around digital systems. DCJ is transitioning to in-place recordkeeping, where records are stored and managed in the systems they are created in. This policy supports the changing administrative structure, functions and technology environment of DCJ. In this respect, a key aspect of the DCJ approach to records management is to determine electronic business systems that need to be managed as records management systems. Before a decision is made to acquire, develop or upgrade an electronic business system, the records management capability of the system must be considered.

The key objectives of this policy seek to ensure that:

- records of all activities and decisions are created, managed and retained for the length of time legally required
- records are managed in a way that ensures the security and privacy of personal and health information
- records are managed efficiently and effectively in support of business objectives
- records are stored appropriately and as cost-effectively as possible

- when no longer required records are disposed of in a timely and efficient manner in accordance with this records management policy and using the appropriate disposal authority
- digital and other technology dependent records are maintained in an authentic and accessible form for as long as they are required in accordance with this policy
- records can be easily accessed and used for as long as they are required.

## Related legislation and documents

DCJ is accountable to Ministers, NSW Parliament, clients and the public for its decisions and actions and operates within a highly regulated environment.

To achieve good management practice, DCJ is responsible for maintaining records that document its business activities having regards to legislation requirements, regulations and standards.

To meet and support its obligations, DCJ has regard to records management legislation and standards for recordkeeping, as well as access and security and privacy protections which apply to all NSW Government agencies.

## Legislation

Good government recordkeeping, and its effective management, are essential to sound management of government business, to the delivery of quality services to the people of NSW and to public accountability. The Government expects high standards in recordkeeping across government as it does in respect of any other aspect of public management. Employees must be aware of the legislation, regulations and standards that govern how records should be managed, in order to comply with NSW laws.

Key records management provisions of the [State Records Act 1998](#) require public offices to:

- make and keep records that fully and accurately document their operations and administration
- establish and maintain a records management program in conformity with standards and codes of best practice approved by State Records NSW and Museums of History NSW
- ensure that records are stored in conditions appropriate to their format and preservation requirements
- ensure that records held in digital or other technology dependent formats are accessible for as long as they required
- ensure records are managed in accordance with the [Privacy and Personal Information Protection Act 1998 \(PPIP Act\)](#), the Health Records and information

Privacy Act 2002 (HRIPA) the [Government Information \(Public Access\) Act 2009 \(GIPA Act\)](#) and the [State Records Act 1998](#). These obligations are set out in the DCJ's Privacy Policy and Privacy Management plan.

## Standards

Recordkeeping standards are mandatory, measurable and include minimum compliance requirements. They are outcomes oriented, rather than prescriptive.

Standards issued by State Records NSW under the Act include:

- Standard on the physical storage of State records: The purpose of this standard is to establish minimum requirements for the storage of paper-based State records and to guide decisions for storing and protecting such records.
- Standard on records management: This standard establishes the requirements for effective records and information management.

The Principal Manager Records is to be informed as soon as practicable of any actual or suspected breach of this policy. Non-compliance or breaches of this policy, without an appropriate exception could leave DCJ open to reputational damage and criticism where an investigation identifies recordkeeping practices were an issue. This may be investigated and any misconduct escalated with Human Resources. Failure to comply with a code of best practice may result in disciplinary action in accordance with the DCJ's code of conduct.

Compliance to the above standards supports compliance with the [State Records Act 1998](#).

## Principles

Records and information are at the core of government business and are core assets.

In NSW public offices, records and information help organisations plan for and achieve short and long term outcomes that are relevant and valuable to the community, business and government.

Records and information need to be:

- trustworthy and managed accountably
- readily accessible, understandable and useable
- valued as critical to business operations
- governed by appropriate risk management approaches
- maintained to meet business, government and community purposes.

To achieve these outcomes, records and information must be supported by effective records and information management. This policy outlines the principles for effective records management based on the three core principles of the Standard on Records

Management. It complements the Information Management Policy and creates the framework for managing records in all formats that are created, received and used in the conduct of DCJ business.

Principle 1: Organisations take responsibility for records and information management.

The core responsibility of DCJ is to ensure records and information can support all business activities, and the DCJ is required to establish governance frameworks.

Principle 2: Records and information management support business.

The core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short and long-term business activities.

Principle 3: Records and information management are well managed.

Effective management of records and information underpins trustworthy, useful and accountable records and information which are accessible and retained for as long as they are needed. This management extends to records and information in all formats, in all business activities, and in all types of systems

## State Records Regulations 2015

Whole-of-government policies and directives issued by the Department of Premier and Cabinet, Treasury, the Public Service Commission or the Department of Customer Service can also establish requirements with respect to the making, keeping and management of records.

Cyber Security NSW have carriage of Cyber Security Policy and the requirement to report to State Records NSW on any “cyber incident that involves information damage or loss” <https://www.digital.nsw.gov.au/policy/cyber-security-policy/roles-and-responsibilities>

## Information Security Requirements

How records are classified and handled securely within the Department is defined within the *DCJ Data Privacy & Protection Policy*. This policy informs information security practices in relation to hardcopy and digital information, including:

- Protective markings
- Classification
- Use
- Carriage and Storage
- Transfer



- Destruction

## Roles and responsibilities

DCJ is part of the Stronger Communities cluster. All business records created in DCJ belong to DCJ and are State records. Management and control of these records is the responsibility of every person in DCJ. The other departments in the Stronger Communities cluster are responsible for the management and control of their own records. This management extends to records and information in all formats, in all business environments and in all types of systems.

DCJ may obtain support for recordkeeping and records management from an internal shared service provider or an external provider. However the responsibility for appropriate management and control remains with DCJ.

In the event of an administrative/machinery of government change that impacts the location of functions across government, the responsibility for the management and control of records follows that transfer of functions. Guidelines have been issued by State Records NSW and Museums of History NSW for the accountable transfer of records in this instance.

Compliance with this policy by all employees, including consultants, contractors, and service providers who have been contracted to undertake outsourced DCJ business activities is mandatory. All officers working for DCJ have a responsibility to follow this policy and to maintain sound recordkeeping practices in their daily work. This policy supersedes all previous recordkeeping and records management policies.

The main roles and responsibilities for implementation of this policy are as follows:

### The Secretary

The Secretary of DCJ is responsible for:

- compliance by DCJ cluster with the requirements of the [State Records Act 1998](#) and the standards and requirements issued under the Act (Section 10 of the Act)
- allocating responsibility for records and information management throughout the organisation down through various levels of management
- holding ultimate responsibility for records and information management in accordance with business requirements and relevant legislation.

### Chief Digital Information Officer

The Chief Information Digital Officer is responsible for:

- providing IT infrastructure and resources to ensure successful operation of records management systems
- resourcing and supporting the technical implementation of the records management system.

## Director, Information Management

The Director, Information Management is identified as the Senior Responsible Officer for records management for DCJ and liaises with Senior Responsible Officers for records management within the DCJ cluster.

The Director of Information Management is responsible for:

- providing strategic direction and oversight of the records management program
- issuing the DCJ Records Management Policy and DCJ corporate records and information strategies
- issuing standards and procedures consistent with this policy
- reporting to the Executive on the Records Management Program
- ownership of the Access Directions
- ensuring the records management program meets business needs and complies with relevant legislation and regulations
- ensuring DCJ has skilled records management employees or access to appropriate skills
- identifying systems and repositories containing records and their business owners
- building capability in DCJ for managing high risk records and systems.

## Principal Manager Records

The Principal Manager Records is responsible for:

- cooperating and liaising with State Records NSW and Museum of History NSW
- identifying Access Directions transfer plans under the Act
- managing transfers using the relevant Service Portal
- providing records management policies, procedures and business rules which support business and comply with legal and regulatory requirements
- identifying and mitigating risks to records and information
- responding to monitoring/reporting requests from the State Records Authority of NSW.
- reporting any cyber incident that involves information damage or loss of records to State Records of NSW (as per requirement in <https://www.digital.nsw.gov.au/policy/cyber-security-policy/roles-and-responsibilities>)
- identifying systems and repositories containing records and their business owners

- developing key performance indicators around elements of the records management program, including capture, storage, maintenance and monitoring, disposal and transfer of records, access directions (as per Part 6 of the State Records Act)
- monitoring and reviewing performance and compliance of the records management program to assess how it meets business needs and accountability requirements
- identifying all records and information required to meet or support business and recordkeeping requirements, including accountability and community expectations
- design and oversight of records disposal processes and documentation, including the approval of records destruction, identification of state archives and transfer of custody and/or ownership of records and state archives
- working with business managers to confirm that management strategies are in place to ensure that high risk, high value areas of business and systems managing such business are identified and assessed, and that records and information management is integrated into high risk and high value business activities, systems and processes
- identifying and addressing records management requirements in contractual arrangements for outsourced, cloud or other service providers based on risk assessments
- identifying and advising business unit managers on the requirements for recordkeeping in outsourcing and service delivery contracts
- ensuring access to records and information is managed appropriately in accordance with legal and business requirements.

It is the responsibility of the Principal Manager Records to monitor and update this policy when required. This policy will be reviewed annually and earlier when any significant new information, legislative or organisational change warrants amendments.

## **Records Management Unit**

Employees in the Records Management Unit are responsible for:

- providing advice and guidance to support the maintenance and protection of records when technology, systems, services and processes change
- Implementing the Records Management Assessment Tool (RMAT) across DCJ. The RMAT will enable public offices covered by the State Records Act 1998 to assess the maturity of records and information management in their organisation, or a part of the organisation
- providing online training, guidelines and advice

- regularly updating training material and the records management home page on the DCJ intranet
- liaising with State Records NSW and Museums of History NSW regarding approval and maintenance of retention and disposal authorities
- providing advice regarding records disposal processes and documentation, including the destruction of records, identification of state archives and transfer of records to the Government Records Repository (GRR)
- providing records management control tools to govern how records are created, captured and stored, including developing business rules and procedures in collaboration with business managers
- providing advice to DCJ employees regarding the creation and maintenance of DCJ records and the systems in which they are maintained and;
- providing access to records in secondary storage and those designated as state archives, in accordance with access directions, where records are not open to public access by default.

## All managers

All managers are responsible for:

- incorporating records management responsibilities into employees role descriptions and performance management plans
- ensuring employees understand their obligation to comply with the [Privacy and Personal Information Protection Act 1998](#) and the [Health Records and Information Privacy Act 2002](#) when handling personal information
- ensuring good records management is integrated into business activities, systems and processes
- ensuring employees have the knowledge of systems and local business rules to capture records of work they do and use to do their work
- ensuring employees including consultants, contractors, and service providers who have been contracted to undertake outsourced DCJ business activities comply with this policy
- monitoring employees to ensure they understand and comply with the Records Management Policy and associated procedures
- advising the Principal Manager Records of high risk and high value areas of business and the information captured, used and managed in such business
- planning and managing business activities involving the collection of information and the creation of records in accordance with business needs and regulatory requirements, including protecting sensitive records

- ensuring employees engage in records management training, cyber security training, privacy training and professional development opportunities.

## **Project Sponsor/Leads**

Project Sponsor/Leads are responsible for:

- supporting the owner and custodian in the identification and prioritisation of records management improvement initiatives
- determining that all legal, regulatory and policy requirements are met in relation to the management of the records.
- controlling any records management risks associated with projects
- ensuring records and information requirements are considered and that records are maintained and protected when technology, systems, services and processes change
- advising the Principal Manager Records that records and information management risk have been considered as part of the development process when moving to a new service environment, systems or service (including cloud based services), or when improving existing work processes, systems or services
- ensuring that records management requirements are incorporated in contractual arrangements for outsourced, cloud or other service providers based on risk assessments.

## **Non-government organisations, contractors and consultants**

Non-government organisations (NGOs), contractors and consultants undertaking work for DCJ must uphold similar standards of records management and adhere to obligations outlined in service agreements and relevant schedules.

They have responsibility for:

- complying with applicable Notified Policies, Standards, Accounting Standards and laws including the [Privacy and Personal Information Protection Act 1998](#) and the [Health Records and Information Privacy Act 2002](#)
- creating and capturing accurate records of relating to contracted services and to provide evidence of their work
- ensuring the of records created or used as part of the service arrangement can be provide, if required,
- ensuring records containing personal or health information are used solely for the purposes for which they were created, unless otherwise lawfully authorised
- securing records relating to contracted services to ensure appropriate protection and handling of information

- notifying the relevant DCJ business units of any inadvertent disclosure or loss of information held by NGOs, contractors and consultants.

## All employees

All employees are accountable for the efficient, effective and appropriate use, management and security of records and information resources that are received, created, acquired or retained in the performance of official duties.

They also have responsibility to:

- understand the records management responsibilities associated with their role and the need to keep records
- understand their obligations to comply with the obligations set out in the [Privacy and Personal Information Protection Act 1998](#) and the [Health Records and Information Privacy Act 2002](#)
- understand their responsibility for creating and capturing accurate records of their actions, decisions and events, to provide evidence of their work, including making records of work where records are not automatically created (e.g. minutes of meetings, notes of telephone conversations)
- know and apply the Records Management Policy and associated procedures
- use records management control tools to create, capture and maintain full and accurate records of business activities as business is conducted
- use and share records appropriately to support collaboration and authorised re-use of information. For example, DCJ may be unwilling to share a dataset publicly because of the risk of identifying individuals. However, DCJ may be comfortable with sharing that dataset with data protections in place, such as the removal of names and addresses, and as long as it is only accessed by authorised employees
- undertake records management training, cyber security training, privacy training and professional development
- understand the requirements for retaining and disposing of records
- know and apply requirements for creating, capturing and managing personal records
- protect records from inappropriate or unlawful access, loss or damage
- ensure that those records that have personally been created are used solely for the purposes for which they were created, unless otherwise lawfully authorised
- notifying their manager and ensuring that any loss or unlawful disclosure of a record, hardcopy, on USB etc is communicated to the Director, Open Government, Information and Privacy, Law Reform and Legal Services as soon as practicable at [infoandprivacy@dcj.nsw.gov.au](mailto:infoandprivacy@dcj.nsw.gov.au) The DCJ [Data Breach](#)

[Response Plan](#) provides information about immediate steps that can be taken in the event of a loss or unlawful disclosure of information. It is important to take remedial action as soon as possible, such as recalling the email or contacting the recipient to request immediate deletion of the email.

## Authorised recordkeeping systems

DCJ records must be captured and maintained on official DCJ infrastructure.

Content Manager (formerly known as TRIM) is the primary electronic document and record management system for DCJ. It manages both physical and electronic records (documents and files/containers) along with the required associated metadata.

DCJ also uses client information systems (CIS) which are comprehensive, integrated systems of clinical, administrative, and financial records that provides information necessary and useful to deliver client services. Information may be maintained electronically, in hard copy or both.

OneSAP is also an authorised recordkeeping system. SAP stands for Systems Applications and Products in Data Processing and is the name of the platform used by DCJ for human resources and financial recordkeeping and transactions.

DCJ records (irrespective of format) stored in shared drives, personal drives, email folders, SharePoint sites, workstations and on backup disks or drives e.g. USB drives are not compliant with DCJ's recordkeeping obligations. These drives and locations are not compliant because they:

- do not capture sufficient metadata to meet the legal recordkeeping requirements for retention and disposal
- do not allow records to be widely searchable or accessible to all who need them
- are not authenticated and are not secure from alteration or deletion.

This business information remains non-compliant until it is registered as a record in Content Manager or an authorised business system.

A business information system (BIS) is an information reporting and/or transaction system used within DCJ. Business information systems are not automatically records management compliant – they contain structured data that potentially constitutes part of a record but this does not by default contain the contextual information to ensure reliability, authenticity and usability. Further, legal recordkeeping retention and disposal requirements (beyond keeping backups of data) are usually not adequately catered for.

Before being authorised to store and manage records, all DCJ business information systems must be assessed by the Principal Manager Records in consultation with relevant stakeholders. All BIS must be able to collect all information required for the activity – it should be fit for purpose and:



- capture content, structure and context of the record
- provide adequate and compliant storage of records
- provide protection of record integrity and authenticity
- ensure the security of records
- be readily accessible to all employees who need to use the records contained within the system, for as long as the record is needed
- undertake the disposal of records in accordance with approved disposal authorities
- ensure the recoverability of records in the event of a disaster
- ensure the availability of records in a useable format through technology changes and migration.

DCJ employees are encouraged to use a business system checklist that has been developed by State Records NSW to assess whether their business system is compliant as a recordkeeping system. Undertaking an assessment upfront helps define technical specifications needed to ensure that the organisation's recordkeeping requirements are addressed and considered.

The checklist offers a basic recordkeeping functionality assessment. When planning to procure or implement new systems, or when prioritising further developments of existing business systems consideration should be given to:

- the value of the records that are or will be created in and/or managed by the business system and category of records, e.g. Cabinet
- the risks associated with the business that the system supports
- inherent information risks
- any recordkeeping requirements that relate specifically to the business being conducted
- the organisational context in which the business system operates (when making decisions about any remedial work that may be required)
- whether the business the system supports is subject to any recordkeeping requirements
- how well the system is currently functioning as a recordkeeping system
- what action may be required to enable the system to meet recordkeeping requirements.

Please refer to the [State Records NSW website](#) for the most current version of the checklist.

## Working remotely

---



The most important aspect of taking work and subsequently DCJ's information off-site is the security of the data and records held. Whether in an office or home, how employees manage records and data is no different - all employees must comply with DCJ policies and procedures. While working remotely, employees need to be extra vigilant regarding the security of information and devices. For guidance, employees must follow the requirements outlined in the [DCJ Data Protection and Privacy Policy](#).

## Privacy

If handling/using records with personal health information, employees must be mindful of compliance requirements; the information must not be made available to any unauthorised people. It is essential that personal and health information, particularly if it is sensitive information, is not exposed to any risk of potential data breach or misuse. For guidance, employees must follow the requirements outlined in the [DCJ Data Protection and Privacy Policy](#).

## Records retention and disposal authorities

Under the *State Records Act 1998*, State records may only be disposed of with the authority of State Records NSW and Museums of History NSW, or via normal administrative practice as defined in section 22 of the Act and the State Records Regulation 2015.

Records and information are kept for as long as they are needed for business, legal and accountability requirements. Records and information are sentenced according to current authorised retention and disposal authorities.

Please refer to [State Records NSW and Museums of History NSW website](#) for the most current version.

Further advice and support regarding records disposal authorities and how to implement them is available by lodging a request to Records Management Unit through ServiceNow.

## Definition of a record

Records are evidence of business conducted by an organisation. Any reference to a record in this policy refers to records in any format as defined in the *State Records Act 1998*.

DCJ employees are responsible for keeping a record of business activities conducted as part of their role.

Examples of business activities include:

- actions
- decisions

- events
- conversations
- advice
- contracts and agreements
- client interaction or activities
- directions (operational, financial and other)
- inputs and outputs
- statistics and reporting
- formation of policy and procedure
- maintenance of inventories and registers maps or plans.

Records can be held in any format. This includes but is not limited to:

- data in business systems – e.g., SAP, ChildStory, CIMS, OIMS
- hard copy information including work diaries (printed, handwritten)
- electronic (born digital) documents – e.g. Word, Excel, Power Point
- electronic files – e.g. EDRMS containers
- electronic messaging – e.g. email, voicemail, instant messaging SMS (short message service), multimedia message service (MMS). Please note that employees should not be using personal messaging services such as email for business related work
- corporate social media – e.g. Twitter, Facebook, LinkedIn, blogs, wikis, discussion boards/forums
- web content – e.g. agency approved intranet and internet sites
- photographs – e.g. official photographs documenting business activities
- videos – e.g. agency approved YouTube, Vimeo, webinars, video conferencing, teleconferencing, video instant messaging and podcasts
- models, plans and architectural drawings
- survey tools.

SharePoint and social media platforms are forms of collaboration and communication which allow users to collaborate on the creation, review and approval of various types of content, including documents for the DCJ, however they are not recordkeeping systems (i.e. a system purposely designed to capture, maintain and provide access to records over time). For SharePoint to be used as a compliant recordkeeping system, it must be configured and/or enhanced with add-on software to enable employees to capture, identify and classify records so that their content,

structure and context of creation are fixed in time and space. This facilitates the making of complete, authentic and usable records.

Employees who use these tools for their work should be aware that content published in this media may constitute a record as defined in this policy. DCJ records should only be stored and shared via agency approved systems. Personal email messaging, personal social media sites such as Facebook, Messenger and WhatsApp should not be used to create or store DCJ records. If there is anything substantial discussed in a teams or MS Teams meeting, employees are to create a record of the discussion and any decisions made and retain it in the appropriate business systems.

Guidance regarding the capture of records and associated metadata, from communications conducted via social media platforms, are provided on the intranet and are to be followed.

DCJ information stored physically or on electronic and computing devices whether owned or leased by DCJ, the employee or a third party, remains the sole property of DCJ. Use of instant messaging or MMS for key business decisions must be transferred to a compliant records management system.

Social media information is a record under the definitions of the [State Records Act 1998](#). This does not mean that all social media information must be captured and managed as an official record but it does mean that some high risk and key business value social media information will need to be managed and kept for appropriate periods of time.

For a record in digital format to be meaningful and to serve as admissible evidence of a business transaction, it must have full and accurate metadata to provide adequate context and to support its authenticity and management over time. This will help to ensure that DCJ's business, accountability and archival requirements are met in a systematic and consistent way, and that digital records are described, reliable, meaningful, admissible as evidence, accessible, sharable and re-usable for as long as they lawfully need to be retained.

## Outsourcing

DCJ conducts its business using both internal resources and outsourcing arrangements. This policy applies to any party contracted to perform services to/for DCJ.

Outsourcing can take many forms, including:

- engaging a private sector organisation, contractor or consultant
- funding agreements with not-for-profit or non-government organisations/funded service providers
- sharing arrangements with other government agencies e.g. a small office using the resources of a larger office

- shared services internal to DCJ and cluster agencies
- shared services procured from centralised whole-of-government services, or from private sector organisations.

The [State Records Act 1998](#) does not apply to private sector service providers as a matter of course. DCJ records management requirements must be incorporated into all procurement, contractual or other government arrangements for outsourcing, cloud or other service providers. Each contract/arrangement should specify how those requirements will be monitored and reported for compliance. Guidance on appropriate wording of these obligations in contractual arrangements can be obtained from Law Reform and Legal Services, DCJ.

Where DCJ makes outsourcing arrangements with other government agencies the [State Records Act 1998](#) will apply and it remains appropriate to specify records management requirements in these contractual agreements or service level agreements.

## Document information

Document name	Records Management Policy
Applies to	All of DCJ
Replaces	Records Management Policy D20/646903
Document reference	D23/1336330
Approval	ICT sub - committee
Version	0.4
Commenced	14 June 2023
Due for review	14 June 2025
Policy owner	Director, Information Management

## Support and advice

For support, advice or further information contact:

Business unit	Information and Digital Services Corporate Services
Email	RecordsManagementCompliance@dcj.nsw.gov.au

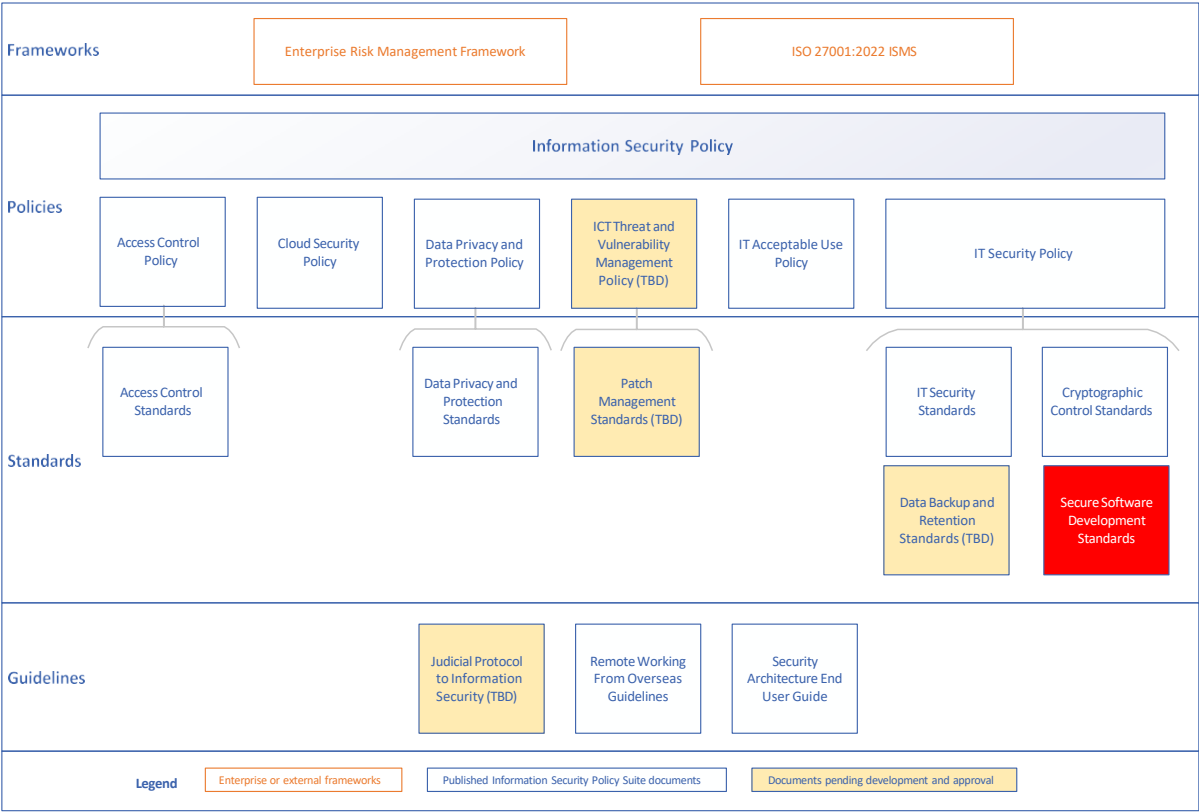


# Secure Software Development Standards

---

## Table of contents

1	Purpose.....	2
2	Definitions.....	2
3	Scope.....	4
4	Secure Software Development Standards.....	4
4.1	Principles .....	5
4.2	Service, Solution Design and Architectural Considerations.....	5
4.3	Procurement Considerations.....	10
4.4	Project Management Process Considerations.....	11
4.5	Operational Considerations.....	15
4.6	Exceptions .....	16
5	Monitoring, evaluation and review .....	16
6	Related legislation, regulation and other documents.....	17
7	Document information .....	17
8	Support and advice .....	17
9	Version and review details .....	17
10	Appendix A.....	18



The red highlighted box shows where this document sits within the Information Security Policy Suite.

1 Purpose

The following standard articulates the Department of Communities and Justice’s (DCJ’s) secure software development standards in regard to the IT Security Policy.

2 Definitions

Term	Definition
Approved user	A volunteer, contracted service provider, graduates, consultants, vendors engaged by DCJ and any other authorised individuals accessing DCJ systems, networks and / or information.
Australian Cyber Security Centre (ACSC)	The Australian Government’s lead agency for cyber security
Cyber Security NSW	An entity in the NSW Government that provides leadership and coordination across the whole of government in managing risks against cyber threats
Employee	For the purposes of this policy, the term Employee includes persons directly employed by DCJ, as well as contractors,

Term	Definition
	volunteers and students engaged by DCJ in the capacity of an employee. The policy excludes members of the Judiciary and NCAT Members.
Confidentiality	Protect against unauthorised information disclosure.
Integrity	Protect against unauthorised, unintentional or incorrect modification of software or data.
Availability	Ensure the availability of systems and information.
Authentication	The process of establishing confidence in the identity of users or information systems.
Authorisation	Establish access rights to resources.
DiD / Castle Approach	Defense-in-Depth. An approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, then another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors
ICT	Information and Communication Technology
IDS	Information and Digital Services, a branch within DCJ's Corporate Services Division
Least Privilege / Access	This is the technical implementation of the "need-to-know" principle that determines the minimal access to data for an entity as needed to produce the expected business outcome.
LoB	Line of Business
May / May not	The item is not mandatory. Recommended as best practice for consideration. No policy exception required if condition is not met.
Must	The item is mandatory. Any request for deviation from a "must" must follow the procedures for requesting exceptions.
Must not	Non-use of the item is mandatory. Any request for deviation from a "must not" must follow the procedures for requesting exceptions.
Need-to-know	A principle which states that resources must get only the <i>minimal</i> set of access to information needed to perform the related business function
SaaS	Software as a Service

Term	Definition
SAST / White box testing	Static Application Security Testing. This is a testing methodology that analyses source code to find security vulnerabilities that make applications susceptible to attack. It scans the application before the code is compiled.
SDLC	Software Development Life Cycle
Should	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing a different course. No exception required if condition is not met.
Should not	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this different course. No exception required if condition is not met.
Software	Firmware, operating systems, standard operating environments (SOEs), network appliances and applications
TLS	Transport Layer Security. A cryptographic protocol that encrypts data and authenticates connection when moving data over the internet via HTTP

### 3 Scope

The requirements and expectations outlined in the document applies to:

- all DCJ permanent full time, part time, trainee and temporary employees and approved users
- anybody authorised to access and make use of any DCJ computing systems, networks and / or information
- any other body authorised to administer, develop, manage and support DCJ information systems and assets

This standard does not apply to the Judiciary and NSW Civil and Administrative Tribunal (NCAT) board members who are subject to the Judicial Protocol to Information Security.

Judicial staff including the judges' tipstaves and associates who are DCJ employees are covered by the Information Security Policy suite. This also applies to tribunal staff who are DCJ employees.

### 4 Secure Software Development Standards



4.1 Principles

DCJ provides access to software applications to enable Employees to fulfil the duties of their role.

This standard assigns Information and Digital Services (IDS) the responsibility for the procurement, allocation, maintenance, support, upgrade, and decommissioning of applications and platforms that are managed by IDS. Furthermore, IDS will be a key stakeholder and provide technology governance, assurance and guidance to inform software development projects and solutions managed internally within business centres.

The software applications/solutions covered by this standard include enterprise software applications and Line-of-Business (LoB) applications. Further, in keeping with the architectural principles of “buy before build” and “cloud first”, this standard applies equally to procured software (Software-as-a-Service (SaaS) arrangements) and internally developed software.

Computer software applications are acquired or created to address business needs. This follows a repeatable process, where functional and non-functional requirements are gathered and documented, followed by design, sourcing and implementation. The requirements include consideration of usage, availability, accessibility, security controls, performance, architectural principles, and the ongoing management of software.

It is important to embed security considerations throughout the software solution development and/or acquisition process. Failure to identify risks and implement proper controls can result in inadequate security, potentially putting entities at risk of data breaches, compromise to systems/networks and reputational exposure, loss of public trust, financial penalties and/or legal liability.

4.2 Service, Solution Design and Architectural Considerations

The Service, Solution Design and Architectural Considerations for acquiring and/or implementing software solutions commence very early in the Service / Solution implementation life cycle.

Ref	Directive
SSD-001	The IDS CRAC team <b>SHOULD</b> be engaged during the Project Start-up Phase (see Appendix A – Project Management Life Cycle).
SSD-002	Project documentation <b>MUST</b> be sufficiently detailed to demonstrate the extent to which each identified security activity is applied.
SSD-003	All solution design and implementation information <b>SHOULD</b> be included in the documentation apart from passwords and various types

	of operational secrets, and the documentation <b>MUST</b> be retained for auditing purposes.
SSD-004	Development of systems and applications <b>MUST</b> be performed securely and in a way that does not expose the internal network, production systems or production information to unmanaged risks. <sup>1</sup>
SSD-005	Internally facing systems and applications <b>SHOULD</b> undergo vulnerability assessment prior to production release. Systems and applications which are externally facing must undergo vulnerability assessment before release. High risk solutions should leverage external vulnerability assessment services.
SSD-006	Defense in Depth (DiD) approach <b>SHOULD</b> be used to protect data and information from different attack vectors in the case that any one protection fails
SSD-007	Avoid “security by obscurity” as it is not effective and <b>SHOULD</b> avoid security design complexity as it has a tendency to get out of control and thus lowers security.
SSD-008	When building web applications, developers <b>SHOULD</b> take into consideration, at a minimum, the Open Web Application Security Project (OWASP) <a href="#">Top 10 Security Risks</a> .

The following security-related aspects **MUST** be considered during service and solution design:

#### 4.2.1 Programming code writing

Ref	Directive
PRC-001	Role-based security training, particularly secure coding practises, <b>SHOULD</b> be provided to support those involved in software development
PRC-002	Code repositories <b>MUST</b> be secured with multifactor authentication (MFA) and access logs / tracking logs should be managed external to the repository
PRC-003	<b>AVOID</b> storing authentication secrets in code (compiled code or scripts). If this is not possible, they <b>MUST NOT</b> be stored in clear text.
PRC-004	Third-party certificates and certificate chains <b>MUST</b> be checked and verified against relevant Certificate Authorities (CAs)
PRC-005	Relevant controls for user uploaded data <b>SHOULD</b> be used, including data and file types verification, input validation and enforcing input data and file size caps.

<sup>1</sup> IT Security Policy 5.7.4

Ref	Directive
PRC-006	<b>SHOULD</b> implement “fail safe / fail closed” for any activity based on any access control method failure. If something fails to authenticate or crashes (or it is hijacked), then the access to data must be immediately stopped.
PRC-007	<b>MUST NOT</b> provide unnecessary information not strictly related to the business logic needs (e.g., app versions, libraries, tailored error codes, etc.).
PRC-008	When building any code <b>SHOULD</b> only use reputable software libraries, with active support and without any reported vulnerabilities. Any non- actively supported software or libraries (commercial or freeware) <b>SHOULD NOT</b> be used.
PRC-009	<b>SHOULD</b> implement “input fields validation” on the server side, as the client side code cannot be trusted due to being subject to modifications by the client.
PRC-010	Cookies <b>SHOULD</b> be encrypted, and any application information stored on the client side. Cookies <b>SHOULD NOT</b> be shared with any website that does not require them.
PRC-011	Where available, secure settings <b>SHOULD</b> be implemented for all the default options. A lack of specific configuration should always have the entity (application, system or device) fall back to the safest settings.

#### 4.2.2 Programming code review

Ref	Directive
PRR-001	When a new application is developed, all programming code <b>SHOULD</b> be scanned with an appropriate Static application security testing (SAST) tool <sup>2</sup> as appropriate to that code and platform.
PRR-002	If scanned by a SAST tool, the produced report <b>MUST</b> be available for review. Note: While the SAST based code review is not the exhaustive way to review that code, this should be a basic code review practice.
PRR-003	Modifications applied to code, systems or applications <b>MUST</b> be documented and where possible previous code versions should be securely maintained <sup>3</sup>
PRR-004	Code testing requirements (e.g., peer review, source code review, static and dynamic code analysis and penetration testing) <b>MUST</b> be defined for each development phase.

<sup>2</sup> More information on SAST tools, their strengths and weaknesses, and list of available tools can be found on the OWASP website [here](#)

<sup>3</sup> IT Security Policy 5.7.4

Ref	Directive
PRR-005	Any vendor undertaking software development associated with the services offered to DCJ, <b>MUST</b> maintain a secure code development program which mandates appropriate security testing of code releases.

#### 4.2.3 System/Service Criticality and Availability

The criticality level reflects the business value of the function provided by the system and the potential business damage that might result from a loss of access to this functionality. The System/service criticality also reflects the availability required by the business.

Ref	Directive
SCA-001	When initiating an application or system, the criticality of the system <b>MUST</b> be established through the IDS CRAC team's Criticality Assessment Framework. This includes consideration of the data value criticality, which relates to what ensuing valuable data is available if the data is disclosed (data classification, Secure Shell (SSH) keys, encryption keys, firewall rules etc)

#### 4.2.4 Classification of Information/Data

Ref	Directive
CIN-001	All information contained within, manipulated by or passing through a system or application <b>MUST</b> be assessed to determine its classification and labelled accordingly <sup>4</sup>
CIN-002	Classification <b>MUST</b> reflect the importance of the information's confidentiality and integrity and <b>MUST</b> follow the <a href="#">NSW Government Information, Classification, Labelling and Handling Guidelines</a>
CIN-003	The information classification level for the handled data <b>MUST</b> be documented in the design documents.
CIN-004	The custodian of the data that resides within the application or platform <b>SHOULD</b> align with the delegated data owner identified in the <a href="#">Information Asset Register</a> . <a href="#">Please contact Information Strategy and Architecture team for access to the register and for any changes to the register where the business has confirmed the custodian and owner do not align (Information.Management@dcj.nsw.gov.au)</a>

#### 4.2.5 Encryption

Ref	Directive
-----	-----------

<sup>4</sup> DCJ Data Privacy and Protection Policy

ENC-001	All data in transit and at rest that needs protection <b>MUST</b> be encrypted as per the IT Security Policy and the Cryptographic Controls Standard
ENC-002	Strong encryption protocols and algorithms, such as TLSv1.3 and TLSv1.2, <b>SHOULD</b> be used and weak cipher suites should be avoided
ENC-003	Third-party certificates and certificate chains <b>MUST</b> be checked and verified against relevant CAs
ENC-004	CA TLS certificate signers <b>SHOULD</b> only be trusted for their specific usages
ENC-005	<p>Login access keys, encryption keys, secrets etc. require the following security considerations:</p> <ul style="list-style-type: none"> <li>• <b>MUST</b> be stored external to the application or system in safe storage and be encrypted with a passphrase. E.g., encrypt the SSH key (for login access) or the PGP key, with a passphrase</li> <li>• If needed, <b>MAY</b> be stored in a special file and directory protected by stringent OS</li> <li>• If in the cloud, <b>MUST</b> use the CSP abilities to secure secrets based on application and user permissions controlled by Identity and Access Management (IAM)</li> </ul>

#### 4.2.6 Authentication - Establish System Identity Credential Requirements

Ref	Directive
ACR-001	All applications or systems which require authentication <b>MUST</b> establish a reliable user identity credential.
ACR-002	Trust no request (from user, server, application or location) without a positive authentication and allow only controlled authorisation based on the “need to know” concept.
ACR-003	The identity credential <b>MUST</b> reflect the required confidence level that the person seeking to access the system is who they claim to be.
ACR-004	SaaS systems which require the use of an email address as a username <b>SHOULD NOT</b> use a shared mailbox, only a unique individual email address.
ACR-005	The authentication method utilised (for users or applications) <b>MUST</b> follow the security best practices and <b>MUST</b> be in line with the Access Control Policy and Access Control Standards.
ACR-006	Credentials <b>MUST</b> be rotated regularly, including keys and passphrases
ACR-007	Dynamic tokens, such as JSON Web Token (JWT) authenticated by OKTA, <b>SHOULD</b> be used for API based authentication

Ref	Directive
ACR-008	Mutual TLS certificates-based authentication <b>MAY</b> be used when the certificates' private keys are controlled, and the parties do not have a mutual authentication store.

#### 4.2.7 Authorisation – Access to Data

Ref	Directive
AAC-001	Application and user-based access to data <b>MUST</b> be authorised and logged properly to allow access to only the required resources and establish the accountability for that access (e.g., an infrastructure admin account should not have access to modify application data, or a server admin account should not be also a database admin)
AAC-002	All provisioned access <b>MUST</b> follow the “least privilege/access” principle – that is the technical implementation of the “need to know” concept.
AAC-003	All required application, system and network security controls used to protect the handled data must be documented in the respective design documents.

#### 4.2.8 Third-Party Cyber Risk Assessment

Ref	Directive
CRA-001	The IDS CRAC team <sup>5</sup> <b>MUST</b> be engaged regarding a Third-Party Cyber Risk Assessment prior to project commencement and/or engagement of a third-party provider.

### 4.3 Procurement Considerations

#### 4.3.1 Commercial Contract Arrangements (Terms and Conditions)

Ref	Directive
CON-001	Any procurement activities and commercial arrangements <b>MUST</b> be conducted in accordance with the <a href="#">DCJ Procurement Policy</a>
CON-002	All IT Contracts <b>MUST</b> be endorsed by an official representative with the appropriate delegations as outlined in <i>Section 7.6 Allocation of information security responsibilities</i> in the DCJ Information Security Policy.

<sup>5</sup> Contact IDS CRAC via [securityarchitecture@facns.nsw.gov.au](mailto:securityarchitecture@facns.nsw.gov.au)

### 4.3.2 Sovereignty of data (Cloud Service Providers)

Ref	Directive
CSP-001	If not previously addressed during Third-Party Cyber Risk Assessment, specific consideration <b>MUST</b> be given to sovereignty of data in line with the <a href="#">Cloud Security Policy</a> when engaging Cloud Service Providers

## 4.4 Project Management Process Considerations

### 4.4.1 Define Security Roles and Responsibilities

Ref	Directive
ROL-001	Security roles <b>MUST</b> be defined and each security activity within the SDLC <b>MUST</b> be clearly assigned to one or more security roles.
ROL-002	Security roles <b>MUST</b> be clearly documented including the security activities and identify the persons responsible for those activities

### 4.4.2 Establish System Identity Credential Requirements

Using identity access management in software development significantly mitigates various application threats that may otherwise present unacceptable levels of risk to the Department.

Ref	Directive
CRE-001	Third-party providers <b>MUST</b> use federation solutions which leverage SAML, Oauth and OpenID and integrate with DCJ OKTA.
CRE-002	Wherever technically possible, the application <b>SHOULD</b> use the DCJ's approved IAM solution to validate and authenticate system and user credentials.  Where this is not possible, the solution <b>MUST</b> utilise MFA and ensure that strong processes are in place for the provisioning and deprovisioning of configured users on an external authentication store.

### 4.4.3 Establish System Security Profile Rights/Permissions

The makeup of a system and software from a security perspective is its security profile and includes security concepts such as confidentiality, availability, authentication, authorisation as well as auditing among others, which must be considered and documented as part of the development process.

Ref	Directive
SSP-001	When initiating the development of an application or system, the security profile objectives <b>MUST</b> be identified and documented.

Ref	Directive
SSP-002	These objectives <b>MUST</b> state the importance and relevance of identified security concepts to the system and indicate the extent and rigor with which each security concept is to be built in or reflected in the system and software.
SSP-003	The security profile <b>MUST</b> adequately consider all federal, state and external security mandates for which the system must be compliant.

#### 4.4.4 Create a System Profile

A system profile is a high-level overview of the application that identifies the application's attributes such as the physical topology, the logical tiers, components, services, actors, technologies, external dependencies, and access rights.

Ref	Directive
SYP-001	The system or application being developed <b>MUST</b> be iteratively profiled by technical teams within the SDLC.
SYP-002	Accurate traffic flows documentation <b>MUST</b> be built and maintained for all applications by any entity changing them throughout their active life.

#### 4.4.5 Assess Vulnerabilities and Threats

The Third-Party Cyber Risk Assessment process (see Section 4.2.8 Third-Party Cyber Risk Assessment above) plays an important part in the assessment of risks for new solution. The identified risks (and the Penetration Test findings) together with any Security Architecture Review risks are included in a report for the System Owner.

Ref	Directive
VUL-001	Vulnerability assessments (or Penetration Tests for external facing solutions) <b>MUST</b> be performed prior to deployment, with particular attention to any critical or internet-facing application.
VUL-002	Such assessments <b>MUST</b> consider not only technical threats, but also administrative and physical threats that could have a potential negative impact on the confidentiality, availability and integrity of the system.

#### 4.4.6 Assess Risks

Ref	Directive
RIS-001	All realistic threats and vulnerabilities identified in the threat assessments <b>MUST</b> be addressed in the risk assessments.



Ref	Directive
RIS-002	Security risk assessments <b>MUST</b> be iteratively performed within the SDLC process through consultation with the CRAC team. These begin as an informal, high-level process early in the SDLC and become a formal, comprehensive process prior to placing a system or software into production.
RIS-003	The risk assessments <b>MUST</b> be based on the value of the information in the system, the classification of the information, the value of the business function provided by the system, the potential threats to the system, the likelihood of occurrence, the impact of the failure of the system and the consequences of the failure of security controls.
RIS-004	Security risks and recommendations <b>MUST</b> be managed in accordance with the DCJ Enterprise Risk Management Framework.

#### 4.4.7 Select and Document Security Controls

Ref	Directive
SCO-001	Appropriate security controls <b>MUST</b> be implemented to mitigate risks that are not avoided, transferred or accepted.
SCO-002	Security controls <b>MUST</b> be justified and documented based on the risk assessments, threat assessments and analysis of the cost of implementing a potential security control relative to the decrease in risk afforded by implementing the control.
SCO-003	Residual risks <b>MUST</b> be documented and maintained at acceptable levels. A formal risk acceptance, with executive management sign-off, <b>MUST</b> be performed for medium and high risks that remain after mitigating controls have been implemented.
SCO-004	Security control requirements <b>MUST</b> be periodically reviewed and updated as necessary whenever the system or the underlying risk assessment is modified.

#### 4.4.8 Create Test Data

Ref	Directive
TST-001	A process for the development of significant test data <b>MUST</b> be created for all applications.
TST-002	A test process <b>MUST</b> be available for applications to perform security and regression testing
TST-003	Data classified as Sensitive DLM and above <b>MUST NOT</b> be used for testing purposes.

Ref	Directive
TST-004	Production data <b>MUST NOT</b> be used in a non-Production environment unless a policy exception has been approved (see <i>Section 4.6 Exceptions</i> below)
TST-005	If production data is used in non-Production environments, then that data <b>MUST</b> have the same access protection as the original Production data in compliance with NSW and DCJ policies and standards regarding the protection and disposal of production data. <sup>6</sup>
TST-006	If less stringent data protection environments (dev, UAT, staging etc) are unable to maintain the same data protections as production data, a reliable and non-reversible data masking process <b>MUST</b> be used to transform the Production data into Test data

#### 4.4.9 Test Security Controls

Ref	Directive
TSC-001	All controls <b>MUST</b> be thoroughly tested in pre-production environments that are identical, in as much as feasibly possible, to the corresponding production environment. This includes the hardware, software, system configurations, controls, and any other customisations.
TSC-002	The testing process, including regression testing, <b>MUST</b> demonstrate that all security controls have been applied appropriately, implemented correctly and are functioning properly to counter the threats and vulnerabilities for which they are intended.
TSC-003	As applicable, all applications testing <b>SHOULD</b> follow approved checklists and should use any methods or tools for static and dynamic application security testing.
TSC-004	Appropriate separation of duties <b>MUST</b> be observed throughout the testing processes, ensuring that different individuals are responsible for development, quality assurance and accreditation.
TSC-005	If an application requires Penetration Testing, the risk findings from the Penetration Test report <b>MUST</b> be incorporated into the final risk assessment before the security assessment is deemed complete

#### 4.4.10 Project Technology Risks

Ref	Directive
PTR-001	Any open risks <b>MUST</b> be remediated, or where this is not possible or feasible currently, the risk <b>MUST</b> be escalated to the business representative with the appropriate delegation for acceptance, as per

<sup>6</sup> NSW Government Information Classification, Labelling and Handling Guidelines. DCJ Data Privacy and Protection Policy, DCJ IT Security Policy Suite

	<i>Section 5.8.1 Information security in project management</i> in the IT Security Policy.
PTR-002	At the conclusion of the project, outstanding technology risks <b>MUST</b> be included in part of the project closure report, along with the risks' planned mitigation and business risk acceptance, to the CRAC team for inclusion in the Cyber Risk Register

Any open risks will need to be remediated, or where this is not possible or feasible currently, the risk **MUST** be escalated to the business representative with the appropriate delegation for acceptance.

## 4.5 Operational Considerations

Following software implementation, it is important to maintain security controls and embed security consideration practices into operations such as management of changes to software and ongoing security reviews.

### 4.5.1 Manage and Control Change

Ref	Directive
CHG-001	The IDS Change Management process <b>MUST</b> be followed whenever a system or application is modified in order to avoid direct or indirect negative impacts that the change might impose

### 4.5.2 Measure Security Compliance

All applications and systems are required to undergo periodic security compliance assessments to ensure they reflect a security posture commensurate with the definition of acceptable risk.

Ref	Directive
MSC-001	Where a system is classified as a Crown Jewel, is externally facing, or is a cloud service provision, it <b>MUST</b> undertake security assessments periodically or after any major change <sup>7</sup> . These assessments can include the following activities: <ul style="list-style-type: none"> <li>• Refresh of Third-Party Cyber Risk Assessment</li> <li>• Elevated Access/Privileged User Access Reviews and Attestations</li> <li>• Regular Vulnerability Scans</li> <li>• Penetration tests</li> <li>• Currency of Security Patching (and timely application of critical security patches and responses to Security Incidents)</li> <li>• Vendor-related service providers – security reporting and compliance with contractual security requirements</li> </ul>
MSC-002	Penetration tests <b>MUST</b> occur annually if the system is a Crown Jewel, external facing, cloud-based, or has major changes. The Security

<sup>7</sup> IT Security Policy 5.8.11 and Cloud Security Policy 5.3.5

Ref	Directive
	<p>Operations team <b>SHOULD</b> be engaged to assess whether a system change is classified as “major”.</p> <p>All other systems <b>SHOULD</b> have periodic penetration tests conducted at least every 3 years, or after major modification. For any queries related to penetration testing, the user can contact <a href="mailto:InfoSec@dcj.nsw.gov.au">InfoSec@dcj.nsw.gov.au</a>.</p>

#### 4.5.3 Perform System Disposal

Ref	Directive
DIS-001	<p>The information contained in applications and systems <b>MUST</b> be protected once a system has reached end of life and the information retained according to applicable retention requirements</p> <p>Information without retention requirements <b>MUST</b> be discarded or destroyed and all disposed media <b>MUST</b> be sanitized in accordance with relevant DCJ Information Security policies and standards.</p>
DIS-002	<p>Where DCJ terminates/exits the contract with the Cloud Service Provider (CSP), the following <b>MUST</b> be performed on all devices:</p> <ul style="list-style-type: none"> <li>• Data sanitisation</li> <li>• Device return merchandised authorisation or device decommission</li> <li>• CSP-issued destruction certificate as evidence that DCJ data has indeed been sanitised</li> </ul>

#### 4.6 Exceptions

Requests for exceptions must articulate an appropriate business case to justify deviation from a policy or standard where the secure software development standard cannot be met.

The business case should include relevant information such as the reason for the exception, a designated owner, a scope, and a timeframe for the exception, mitigating or compensating controls to manage risk and a remediation plan to realign with the breached policy or standard.

Where the request is for exemption from secure software development standard directives:

- Relevant IDS Business Partners or Application Managers within the Enterprise Applications and Platform Management team should be contacted to initiate the policy and standard exception process with the CRAC team (as per Information Security Policy 7.3 and 7.4)
- Exceptions must be endorsed by the Director Enterprise Applications and Platform Management and must be recorded in the exceptions register.

## 5 Monitoring, evaluation and review

It is the responsibility of the Policy Administrator (with standing delegation to the Senior Policy Officer) to monitor and update this policy annually or more frequently when any significant new information, legislative or organisational change warrants amendments to this document.

## 6 Related legislation, regulation and other documents

This document is related to the IT Security Policy in that it is an implementation of the policy.

## 7 Document information

Document name	Secure Software Development Standard
Document reference	D22/1772684
Replaces	Secure Software Development Standards v1.0
Applies to	All Employees
Policy administrator	Director, Enterprise Applications and Platform Management
Approval	Chief Digital Information Officer
Approved date	28/09/2023

## 8 Support and advice

To submit a request employees should refer to ServiceNow.

For support employees should contact their relevant IT service desk:

- FACS accounts – 02 9765 3999
- Justice accounts – 02 8688 1111

For additional information on the standard directives, employees should contact their relevant IDS Business Partner.

## 9 Version and review details

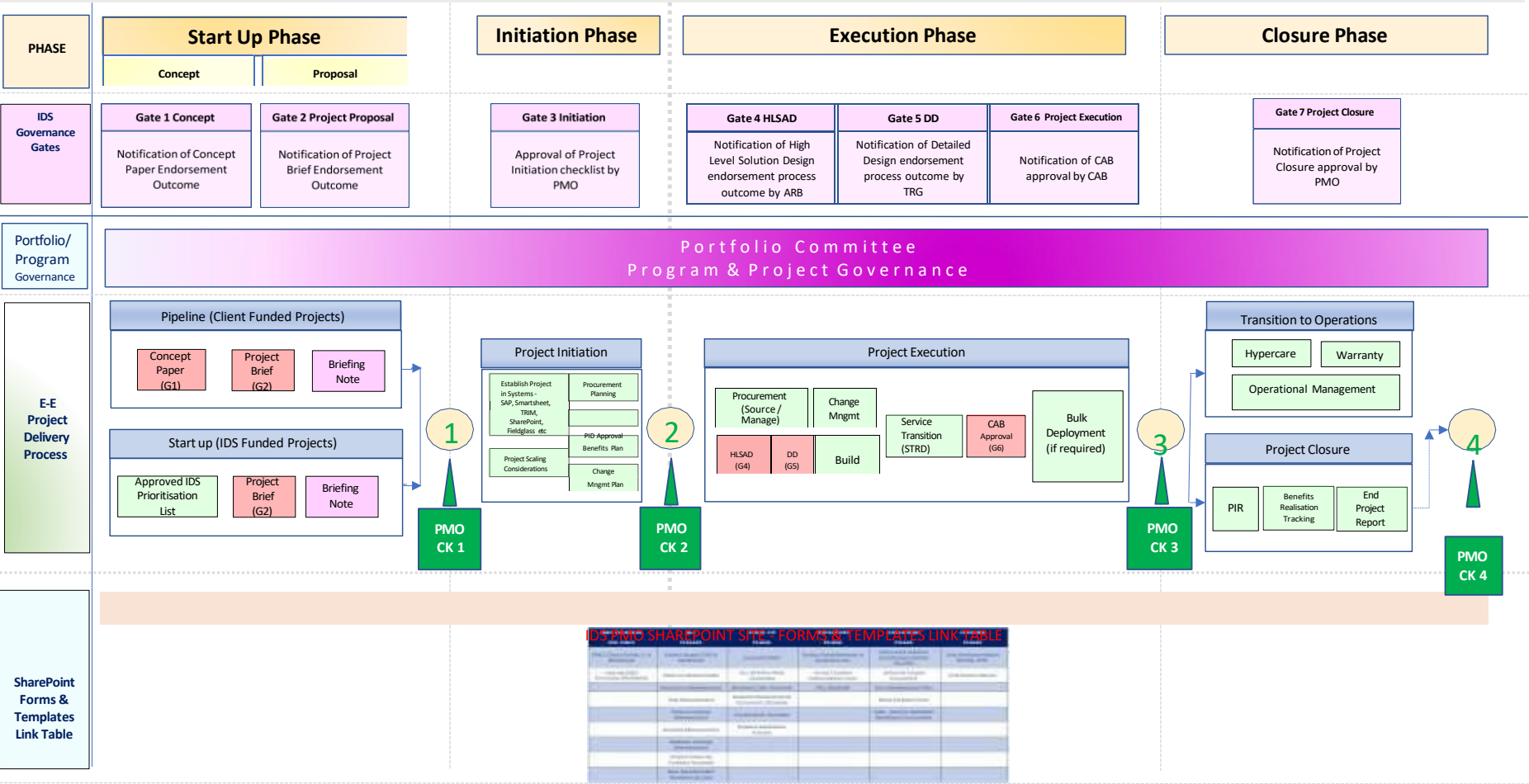
Version	Effective date	Reason for amendment	Due for review
1.0	23/06/2022	New document	23/06/2023
2.0	28/09/2023	Annual review	28/09/2024



Communities and Justice

10 Appendix A

IDS End to End Project Management Process Outline





Communities  
& Justice

# Statement of Business Ethics

This Statement of Business Ethics (Statement) provides guidelines on what is expected when conducting business with the Department of Communities and Justice (DCJ). The DCJ Code of Conduct (Code) requires its employees to maintain high standards of integrity and ethical conduct. DCJ will conduct all business dealings in a fair, honest and consistent manner.

This Statement serves as a guide for contractors, consultants, suppliers, tenderers and business partners (referred to as third party providers or suppliers throughout this Statement) who conduct business with DCJ. DCJ requires all providers of goods and services and business partners to observe the principles outlined in this Statement.

If you are doing business with DCJ, you should be aware of our core business principles:

- DCJ requires all its employees and anyone acting on behalf of DCJ to comply with this Statement.
- Support the Aboriginal Procurement Policy by providing employment opportunities for Aboriginal people within Aboriginal owned businesses and non-Aboriginal owned businesses.
- DCJ conducts all business with honesty, transparency, fairness and impartiality.
- DCJ needs to obtain value for money for public spending.
- All decisions and actions by DCJ are made fairly, objectively, reasonably and recorded.
- DCJ employees and those who supply goods and services will be held accountable for their decisions and actions.
- Procedures about the giving and receiving of gifts and benefits must be followed.
- Care must be taken to avoid actual, perceived or potential conflicts of interest (COI).
- Information should be accessed and shared only for the purposes of conducting DCJ business and in accordance with the relevant delegations and legislation.
- Information acquired in the course of work with DCJ must be managed with utmost confidentiality as per relevant legislation such as the *Privacy Act 1988*.

These principles are explained more fully below.

## GENERAL ETHICAL PRINCIPLES

### Best value for money – Procurement and Selection Process

The money DCJ spends on obtaining goods and services comes from the public and must be spent responsibly. The purchase of goods and services is through established NSW Government contract systems and in accordance with the State Government's policies, procedures, codes and regulations for procurement of goods and services.

DCJ makes decisions on tenders and purchasing considering cost but also factors such as quality, reliability, delivery time and support services.

In the case of third party providers, experience, qualifications and knowledge are taken into account as well as cost. These selection criteria will be stated in the tender documents.

- All parties are expected to approach the tender process with honesty, fairness, transparency, co-operation, lawfully and with no improper advantage.
- The parties must not seek or submit tenders without a firm intention to proceed.
- There should be no anti-competitive practices, such as collusion between tenderers.
- All parties are expected to keep their bid details confidential.
- All parties are expected to disclose any potential, perceived or real conflicts of interest.

### Confidentiality and Accountability

All communications made or received by DCJ will be managed in a secure and confidential manner. DCJ keeps records of all business transactions to ensure transparency, an effective audit trail and as a way to monitor and review the performance of contracts.

DCJ requires its employees to keep detailed and relevant records of all stages of the procurement process. Any departure from established processes needs to be approved by senior management, with reasons recorded.

The supplier of goods or services is likewise expected to fulfil their side of the bargain or report immediately to DCJ any problems in doing so.

### Fairness and Impartiality

DCJ recognises that suppliers of goods and services invest time, effort and resources in preparing and submitting bids.

In return, suppliers are assured of the following:

- Impartial and fair treatment at all stages of the procurement process.
- To receive equal access to information and to have the same opportunities to submit bids or tenders.
- To be subject to probity and audit checks, if required.
- To have their intellectual property rights recognised and respected, and to receive fair compensation for any access to, license or use of those rights.
- Selection criteria and tender specifications will be established and documented prior to the calling of the bid. If any change needs to be made, all bidders will be given the altered details and treated equitably.
- DCJ will publish details of contracts awarded on the e-Tendering website, as required by legislation.



## SPECIFIC ETHICAL PRINCIPLES

### What DCJ expects from its employees:

- To demonstrate the core values of the Public Sector and Department at all times (as specified under the Code and noting the core values are included under the *Ethical Framework for the Government Sector*).
- Always act professionally and respectfully.
- Always act with courtesy and fairness.
- Always act in the public interest.
- Disclose and manage any conflicts of interest.
- Not accept or solicit money, gifts, hospitality, benefits or travel for performing official duties. Please refer to the DCJ Gifts, Benefits and Bequests Policy and Procedure.
- Not accept payment or any form of entertainment, including meals, and only interact with third party providers when a clear business purpose exists (DCJ employees are generally not entitled to use government funds to pay for entertainment).
- DCJ pays the business travel and accommodation costs for our employees. Only DCJ can agree to accept this benefit from a third party provider, not an individual.
- Manage all information gained in the course of official duties sensitively.
- Not make public/social media comment about providers that have business dealings with DCJ.
- Manage all information securely to prevent unauthorised access.
- Obtain approval in writing prior to engaging in other paid employment outside their official duties.
- Not use or take advantage of confidential information obtained in the course of their employment with DCJ when, or if, other employment is sought.
- Engage in a fair and ethical way that is free from bullying, harassment, victimisation and abuse.
- Report wrong-doing (including fraud, corruption, breach of privacy and maladministration).
- Pay suppliers on time.

### What DCJ expects from third party providers including their supply chains such as sub-contractors

- Compliance with applicable laws, regulations, policies, procedures and good business practices in all their dealings with DCJ.

- Take reasonable measures to prevent unethical practices in their businesses to the extent that it may affect DCJ.
- Actively promote and instil a culture of compliance with this Statement from their staff, contractors and other appropriate entities.
- Seek assistance when unsure about how to implement or apply the Statement.
- Ensure third parties acting on behalf of the supplier comply with this Statement.
- Provide accurate, timely and reliable advice and information, including tender briefings.
- Declare in writing any potential, actual or perceived conflicts of interest arising in their business activities with DCJ.
- Not engage in any form of collusive practice, including offering DCJ employees inducements, incentives, gifts, bribes or private employment and other commercial opportunities that may conflict with their public duties. (Ways for reporting breaches are outlined on the last page of this Statement).
- Protect and prevent the release of commercial-in-confidence information obtained in the course of their business dealings with DCJ.
- Ensure the security and proper use of government information, assets and materials.
- Not to discuss DCJ business practices or information in the media or other public forums, without approval from DCJ.
- Provide fair value for money in supplying DCJ with goods and services.
- Cooperate in preventing unethical practices and unprofessional conduct.
- Comply with all applicable laws and regulations relating to work, health and safety.
- Comply with the relevant international and Australian standards on compliance, risk management and fraud and corruption.
- Provide a fair and ethical workplace free from bullying, harassment, victimisation and abuse.
- Make all reasonable efforts to ensure that businesses within their supply chain are not engaged in, or complicit with, human rights abuses, such as forced or child labour.
- Minimise the environmental impact of their operations and maintain environmentally responsible policies and practices.
- Pay employees and sub-contractors on time.

## Assessment and Audit

DCJ may undertake assessments/probity checks of potential third party providers where there may be a risk of an actual, potential or perceived COI.

Where a material risk has been identified, this will affect DCJ's decision in the tendering process.

DCJ expects third party providers including their supply chains such as sub-contractors to have an assurance framework in place to ensure their business is operating in accordance with relevant legislation, industry standards and guidelines.

DCJ reserves the right to verify compliance with this Statement, relevant legislation, industry standards and guidelines by conducting an audit or investigation.

## Gifts and Benefits

DCJ employees (including contractors) are not permitted to request financial or non-financial benefits and are expected to decline such offers. The acceptance of gifts or benefits in the course of employment has the potential to create a conflict of interest, or the appearance of a conflict of interest, and could lead to corrupt conduct.

Suppliers must not at any time offer or provide any financial or non-financial benefits to DCJ employees..

If a gift or benefit is offered to a DCJ employee in the course of their employment it must be declared and recorded in the centralised DCJ gift register in accordance with DCJ policy, irrespective whether they accept or decline the gift or benefit.

Any offer of payment, gratuity, benefit or service, made in order to induce a DCJ employee to neglect their duty, give preferential treatment to, or act in any way other than in accordance with the proper discharge of their duties is considered bribery and must be reported. Bribery in any form is illegal and will be reported to the relevant authority. It may result in serious penalties, including imprisonment.

## Conflicts of Interest

A conflict of interest involves an actual, potential or perceived conflict between the public duty and private interests of a public official, as set out below. A conflict of interest can arise when a person's business and private interests intersect. Private interests can include a person's own professional and financial interests, as well as past and present associations with other individuals, groups or family.

The Independent Commission Against Corruption (ICAC) defines a conflict of interest as: *When a reasonable person might perceive that a public official's private interests could be favoured over their public duties.*

A conflict of interest can also occur when a third party provider undertaking official duties, or those associated with it, could favour their personal interests over their public duties. Private interests could include the interests of the third party providers, related sub-contractors and related individuals (such as officeholders, managers and staff of the third party provider).

Third party providers must avoid intentionally placing DCJ employees in a conflict of interest situation. DCJ expects that any conflict of interest identified by a third party supplier is resolved in favour of DCJ's interests and the public interest. Where third party suppliers are not sure about declaring and resolving conflicts of interest, DCJ expects third party suppliers to err on the side of caution to ensure that the public interest has priority.

Conflicts of interest that lead to biased decision-making may constitute corrupt conduct. Perceived conflicts of interest, when unmanaged, can damage public trust in government decisions.

## Management and Disclosure of a Conflict of Interest

Where there is an actual, potential or perceived conflict of interest it must be declared in writing and strategies be put in place to manage it. This is to ensure that the honesty, transparency and integrity of both DCJ and the third party provider are maintained and to prevent the conflict from having a detrimental effect on any of the parties involved.

Conflicts of interest, whether actual, potential or perceived, must be immediately reported to the relevant NSW Government department or agency.

DCJ is committed to declaring, recording and managing conflicts of interests.

DCJ requires its employees to disclose all conflicts of interest in accordance with the DCJ Conflicts of Interest Policy and Procedure.

Third party suppliers are required to disclose any conflicts of interest by completing the required documentation that form part of the tendering process.

Failure to identify, declare, record and manage a conflict of interest is where serious corruption often begins. For this reason managing conflicts of interest, including perceived and potential conflicts of interest, is an important corruption prevention strategy.

### Reporting Corrupt Conduct

DCJ is committed to preventing wrongdoing and corrupt conduct and to ensure that:

- All DCJ employees are guided and encouraged to behave with integrity;
- Clear policy and procedures are available that instil proper process; and
- Supervision and monitoring serve as checks to ensure that wrongdoing and corrupt conduct are disclosed and appropriately dealt with.

Corrupt conduct is defined by the ICAC as deliberate or intentional wrongdoing, not negligence or a mistake. It has to involve or affect a NSW public official or public sector organisation.

While it takes many forms, corrupt conduct occurs when:

- A public official improperly uses, or tries to improperly use, the knowledge, power or resources of their position for personal gain or the advantage of others.
- A public official dishonestly exercises his or her official functions, or improperly exercises his or her official functions in a partial manner, breaches public trust or misuses information or material acquired during the course of his or her official functions.
- A member of the public influences, or tries to influence, a public official to use his or her position in a way that affects the probity of the public official's exercise of functions.
- A member of the public engages in conduct that could involve one of the matters set out in section 8(2A) of the NSW ICAC Act where such conduct impairs, or could impair, public confidence in public administration. Some examples of this are:
  - a) collusive tendering,
  - b) fraud in relation to applications for licences, permits or other authorities under legislation designed to protect health and safety or the environment or designed to facilitate the management and commercial exploitation of resources,
  - c) dishonestly obtaining or assisting in obtaining, or dishonestly benefiting from, the payment or

application of public funds for private advantage or the disposition of public assets for private advantage,

- d) defrauding the public revenue,
- e) fraudulently obtaining or retaining employment or appointment as a public official.

DCJ considers it an obligation of its employees and third party providers that such conduct be promptly reported.

In accordance with legislation, the DCJ Code of Ethical Conduct and the DCJ Fraud and Corruption Programs, DCJ employees are required to report any suspected corrupt conduct or wrongdoing. One of the options available to public officials (current or former government employees) is the Public Interest Disclosures (PID) Act 1994. This Act offers protection to public officials who give information about corruption, mal-administration or substantial waste of public money and deems it a criminal offence to take any detrimental action against the person(s) who reported the information.

A public official in section 4A of the PID Act includes:

- (a) an individual who is engaged by a public authority under a contract to provide services to or on behalf of the public authority; or
- (b) if a corporation (third party) is engaged by a public authority under a contract to provide services to or on behalf of the public authority, an employee or officer of the corporation (third party) who provides or is to provide the contracted services or any part of those services.

While the PID Act does not apply to individuals who are not public officials, DCJ will treat confidentially and sensitively all information provided in respect to wrongdoing and corrupt conduct. DCJ requires those who do business with DCJ to report to DCJ any suspected corrupt conduct, wrongdoing, fraud or breach of this Statement involving a DCJ employee or involving any other person working or contracted or undertaking work on behalf of DCJ.

Further, DCJ requires suppliers and their sub-contractors to protect and support people who report wrongdoing.

Where a third party provider is concerned about any conduct that could involve fraud, corrupt conduct, maladministration, or serious and substantial waste of public funds, this can be reported via the list of reporting channels outlined below. For example,

reports of corrupt conduct may be made directly to the ICAC.

### **Security in Correctional Facilities and Youth Justice Centres**

In addition to the general business principles explained above, third party providers and others entering correctional facilities are reminded that it is a criminal offence and a serious risk to the community to take anything into a correctional facility for an offender, or to take anything out of a correctional facility on behalf of an offender. DCJ will provide training about specific security issues for those entering a correctional facility as and when required.

### **Implications of non-compliance with this Statement**

Third party providers should be aware that non-compliance with this Statement when doing business with DCJ, as well as proven corrupt or unethical conduct, could lead to:

- termination of contract/s.
- loss of future work.
- loss of reputation.
- investigation for corruption.
- criminal investigation.
- suspension/removal from prequalification schemes and panel arrangements.
- loss of public confidence.

## Additional information

---

### **Confidentiality and intellectual property rights**

Information provided by or collected from the NSW Government is provided on a confidential basis, unless otherwise explicitly indicated, or the information is already in the public domain. The NSW Government and our suppliers (actual and potential) will respect and honour each other's confidentiality and intellectual property rights.

### **Environmental sustainability**

We expect our suppliers to minimise the environmental impact of their operations and maintain environmentally responsible policies and practices.

### **Sponsorship**

Any sponsorship arrangement must be open and transparent and should not create any perception that it will improperly influence the decision making of the NSW Government.

### **Labour and human rights**

We expect our suppliers to provide a fair and ethical workplace. Our suppliers are also expected to take all reasonable efforts to ensure that businesses within their supply chain are not engaged in, or complicit with, human rights abuses, such as forced or child labour.

### **Work, health and safety**

We expect our third party providers to provide a safe work environment and integrate sound health and safety management practices into their business.

Providers must comply with all applicable laws and regulations relating to work, health and safety.

## How do I report wrongdoing?

If you are concerned about a possible breach of this Statement, including but not limited to concerns about being treated fairly during the procurement and selection process, or would like to provide information about suspected fraud, corruption, conflicts of interest, unethical behaviour or maladministration you should report this directly to the Department of Communities and Justice (DCJ) via one of the following channels:

- DCJ Fraud and Corruption Hotline call 1800 950 649 or email [DCJFraudHotline@coreintegrity.com.au](mailto:DCJFraudHotline@coreintegrity.com.au).
- Additional information on reporting fraud and corruption can be found here at [DCJ Fraud and Corruption Prevention](#).
- Public Interest Disclosure (PID) Officer for former or current public officials only: email [reece.collin@dcj.nsw.gov.au](mailto:reece.collin@dcj.nsw.gov.au) or mobile number 0401 710 688
- Feedback Assist Widget on government public facing websites

You can also report concerns about any conduct that could involve fraud, corruption, maladministration, or serious and substantial waste of public funds to one of these external channels:

Corrupt conduct – [Independent Commission Against Corruption \(ICAC\)](#)

Maladministration – [NSW Ombudsman](#)

Serious and substantial waste – [NSW Audit Office](#)

Access to government information (GIPA) – <https://www.ipc.nsw.gov.au/>

Signature Area

Organisation Name:  
The NSW Department of Communities and Justice

-----  
Role/Title:  
A/CDIO

-----  
Name:  
JAY HUNTLEY

-----  
Signature: 

Signed By:

JAY HUNTLEY

A7440A503E614E9...

07 April 2025 | 21:08:35 AEST

(dd.mm.yyyy | hh:mm:ss)