|  |
| --- |
| Information security incident report |
|  |
| HUMAN SERVICES CONTRACT MANAGEMENT | Form | 20 December 2023 |

You may use this form to help your organisation report to the Department of Communities and Justice (DCJ) your initial investigation following a suspected information security incident.

This report can also be used as a follow up to an incident your organisation has already notified to DCJ. If you haven’t already notified DCJ of the incident, get further instructions from our website by pressing Ctrl + Click on the dark blue button.

Get further instructions **→**

If you have any questions, contact your lead DCJ contract manager.

Send the completed and endorsed report by email to your lead DCJ contract manager or other nominated DCJ contact.

# Part 1. Your organisation’s details

|  |  |
| --- | --- |
| Organisation name  State your organisation’s name as it appears in the contract. | Click or tap here to enter text. |
| Trading name or legal name  If applicable. Otherwise, state ‘Not applicable’. | Click or tap here to enter text. |
| ABN | Click or tap here to enter text. |
| Date of this report | Click or tap to enter a date. |
| Organisation’s representative handling the incident | Name: <Name>  Position: <Position title>  Contact number: <Contact number>  Email address: <[name@domain](mailto:name.name@facs.nsw.gov.au)> |
| Organisation’s representative authorising this report | Name: <Name>  Position: <Position title>  Contact number: <Contact number>  Email address: <[name@domain](mailto:name.name@facs.nsw.gov.au)> |

# Part 2. About the incident

|  |  |
| --- | --- |
| Date and time the incident occurred or when your organisation became aware of, or suspected it. | Click or tap to enter a date. |
| Describe the type of information security incident. | Your response  For example:   * a breach of, or an attack on your organisation’s ICT systems * loss of client records due to theft, fire or flood * loss of program records with no identified client data * an email sent to wrong person (including who the information was wrongly sent to) and the nature of confidential client information * other security incident involving client or program data. |
| Outline your organisation’s risk assessment of the incident. | Your response |
| Describe the impacts for your clients, organisation and DCJ including any potential harm. | Your response |
| Provide details of any lost or potentially compromised information/data. | Your response  For example:   * staff user names and/or passwords to DCJ systems * personal or health information about clients, and whether the data could be used to identify the client(s) * program information * sensitive financial, commercial or legal documents. |
| How many individuals or records are affected? (approximately) | Your response |
| Is it suspected that the incident was a result of misconduct by an employee, executive or public official? | Your response  Yes  No |

# Part 3. Your organisation’s response

|  |  |
| --- | --- |
| Describe the actions your organisation has taken or is planning to take to manage the incident. | Your response  For example:   * implemented your business continuity plan or similar * put in place workarounds if your ICT systems are disabled * notified other parties of the incident * temporarily suspended your staff access to DCJ electronic systems, if applicable. |
| Describe the actions your organisation has taken or is planning to take to correct or mitigate any data lost or compromised. | Your response  For example, steps you have taken to inform clients whose information may have been lost or compromised. |
| Does the incident affect ongoing delivery of DCJ’s contracted services? | Yes  No  Unsure |
| If ‘Yes’ or ‘Unsure’, describe the actions your organisation has taken or is planning to take to ensure any disruption is minimised. | Your response |
| Provide any other details relevant to DCJ resulting from your investigation of the incident. | Your response |

**Note that your lead DCJ contract manager or another DCJ representative may contact your organisation if further information is required; for example, to understand any impact on our electronic systems. We may also contact you to provide information that may help your organisation to manage the incident.**

**If an incident is assessed as an eligible data breach under the *Mandatory Notification of Data Breach (MNDB) Scheme,* we will work with you to report the incident to the Privacy Commissioner and affected individuals.**