Information security is **everyone's responsibility**

01 Your password is your passport at work

Don't share your password with anyone.

Remember, you're accountable for all actions taken under your username.

02 Outsourcing IT systems and sharing DCJ data must be controlled

DCJ has legal obligations to secure its information appropriately. This includes information about DCJ and its staff, programs and clients held by the organisations we contract.

Ensure due diligence when outsourcing your organisation's IT systems and/or sharing DCJ-related information. We want to ensure the security and privacy of our clients.

03 Be wary of suspicious or unsolicited emails

Stop and think before opening links or attachments in email, and don't provide sensitive information to anyone without careful consideration.

If you're unsure that a call, email or text message is actually from a trusted organisation, search for their official website or call their listed phone number.

Don't use contact details provided in email, over the phone or in text messages, as these may be fraudulent.

04 Close the door on tailgating

Information security attacks don't just happen online. Physical security breaches, such as tailgating, can have a devastating impact and often go undetected.

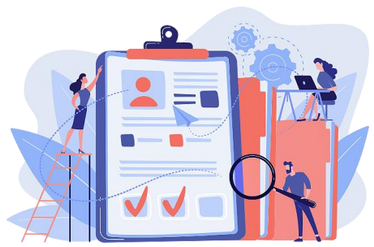
Look out for suspicious people loitering near building access points. If someone unfamiliar asks you to hold the door open for them, don't. And don't lend your security pass to others.

Ensure doors to secured areas are closed immediately.

05 Secure your documents and systems when unattended

Make sure all information systems and documents are appropriately secured when they're unattended.

Lock your computer when you're not using it. Store sensitive documents in lockable cabinets, drawers or rooms when they're not being used.



06 Review access rights

Regularly review access rights to sensitive information or systems to ensure only the right people have the right level of access at the right time.

07 Work safely when working remotely

Ensure you're connected to a trusted network and use your smart phone as a private hotspot if working in a public space.

Be aware of people around you, and make sure they can't see your screen or sensitive information.

08 Preparation and protection are prevention

Cyberattacks can occur at any time, so it's important to be prepared and take protective measures.

Regularly update your devices, networks and software, and backup your data.

09 Remember your responsibilities

You're required to comply with the requirements of relevant legislation and policy, as well as the provisions of your contract with us, in relation to privacy, information management and your information and communications technology (ICT) systems.

10 Don't delay and notify DCJ

Notify DCJ immediately if you detect an actual or suspected information security incident involving information about DCJ or its staff, personal information about clients or their families, or related program data.