Protecting DCJ information while working from home

Protect your information

Information with a security classification of **PROTECTED** and above should be stored in a compliant physically secure premises and **should not** be taken home.

Unclassified data with a **DLM** (e.g. Sensitive) may be taken home if there is a genuine need to have the data and your manager has approved it.

Transferring secure information

External storage devices such as USB thumb drives should not be used to transfer sensitive information unless it has been encrypted first.

Files and folders can be quickly encrypted using Winzip. See: www.winzip.com/en/features/encrypt-zip-file.html

Taking physical files home

If you need to take physical files home, consider how you will secure them (e.g. in a binder) and what the impact would be if they are lost or stolen.

Use trusted devices

If you can't use a DCJ owned computing device to logon from home, you must use a personal device (i.e. not a kiosk/shared computer).

Ensure the anti-virus is up to date and has scanned the device recently. Only use trusted wireless networks such as your phone hotspot or your personal wireless.

Disposing of physical files

If you take home physical files that are sensitive, they **must not** be placed in your recycling/waste bin. They need to be brought back to work and securely disposed of, or shredded at home before disposal.

Emailing sensitive information

Email is not encrypted. Sensitive emails are susceptible to exposure and can be on-forwarded. Consider sharing TRIM links instead or using secure email options, like Accellion, which can be obtained from the former FACS helpdesk.

Home office

All information, whether it be on paper or screen, should be appropriately secured when unattended. Lock your computer when you are not using it and store sensitive documents in lockable cabinets, drawers or rooms when they are not being used.

MS Teams

MS Teams is a collaboration tool, not a document storage system. When using MS Teams to collaborate, consider using screen sharing rather than attaching documents to the application.

Documents should be kept in a DCJ approved Record Management System (such as TRIM).

Security protocols

If you witness a security incident or believe you have found a potential threat or vulnerability, report the matter to the IDS Service Desk immediately.

Former FACS: (02) 9765 3999
Former Justice: (02) 8688 1111

More information

If you have a question, comment or concern relating to information security, email either:
-FACSSecurityGovernance@facs.nsw.gov.au
-Information.Security@justice.nsw.gov.au

To report a scam, email either:
-Infosec@facs.nsw.gov.au
-Security.incident@justice.nsw.gov.au