Information security manual

Guidelines for personnel security

Last updated: September 2026

Cyber security awareness training

Providing cyber security awareness training

An organisation should ensure that cyber security awareness training is provided to all personnel to assist them in understanding their security responsibilities and the cyber threats they may be exposed to in the course of their duties. Furthermore, the content of cyber security awareness training should be tailored to the needs of specific groups of personnel, such as general personnel and different classes of high-risk personnel. Finally, personnel with privileged access to systems and their resources, such as application administrators, system administrators and network administrators, will require tailored privileged user training.

Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cyber security awareness training is undertaken annually by all personnel and covers:

- *the purpose of the cyber security awareness training*
- *security appointments and contacts*
- *authorised use of systems and their resources*
- *protection of systems and their resources*
- *reporting of cyber security incidents and suspected compromises of systems and their resources.*

Control: ISM-1565; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Tailored privileged user training is undertaken annually by all personnel with privileged access to systems and their resources.

Control: ISM-2022; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A cyber security awareness training register is developed, implemented and maintained.

General-purpose artificial intelligence usage policy

As there are security risks associated with the use of general-purpose AI applications, it is important that an organisation develops, implements and maintains a general-purpose AI usage policy governing the use of such applications by personnel.

Control: ISM-2074; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A general-purpose AI usage policy is developed, implemented and maintained.

Web usage policy

As there are security risks associated with the use of web services, it is important that an organisation develops, implements and maintains a web usage policy governing its use by personnel.

Control: ISM-0258; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A web usage policy is developed, implemented and maintained.

Managing requests to change banking details or transfer funds

Business email compromise, a form of financial fraud, is when malicious actors attempt to defraud an organisation of money or assets with the assistance of a compromised email account. Malicious actors will typically attempt to achieve this via invoice fraud, employee impersonation or company impersonation.

With invoice fraud, malicious actors will compromise a vendor's email account and through it have access to legitimate invoices. Malicious actors will then amend invoices and send them to customers with the compromised email account. Customers will then pay the invoices, thinking that they are paying the vendor, but instead be sending money to malicious actors' bank accounts.

With employee impersonation, malicious actors will compromise an organisation's email account and impersonate an employee via email. This is then used to commit financial fraud in several ways. One common method is to impersonate a person in a position of authority, such as a chief executive officer or chief financial officer, and have a false invoice raised. Another method is to request a change to an employee's banking details. The funds from the false invoice or the employee's salary are then sent to malicious actors' bank accounts.

With company impersonation, malicious actors register a domain with a name similar to another organisation. Malicious actors then impersonate that organisation in an email to a vendor and requests a quote for a quantity of expensive assets, such as laptop computers, and subsequently negotiate for the assets to be delivered to them prior to payment. The assets are then delivered to a location specified by malicious actors, with the invoice being sent to the legitimate organisation who never ordered or received the assets.

To mitigate business email compromise, personnel should be educated to look for the following warning signs:

- an unexpected request for a change of banking details
- an urgent payment request, or threats of serious consequences if payment is not made
- unexpected payment requests from a person in a position of authority, particularly if payment requests are unusual from this person
- an email received from a suspicious email address, such as an email address not matching an organisation's name.

In dealing with such situations, personnel should have clear guidance to verify bank account details; think critically before actioning unusual payment requests; and have a process to report threatening demands for immediate action, pressure for secrecy, or requests to circumvent normal business processes and procedures.

Control: ISM-1740; Revision: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel dealing with banking details and payment requests are advised of what business email compromise is and how to manage and report it.

Managing requests to modify user accounts

Requests to modify user accounts, such as resetting a password, changing a mobile phone number or email address, temporarily disabling multi-factor authentication, or re-enrolling for multi-factor authentication, could indicate a malicious actor attempting to conduct a help desk attack.

In dealing with such situations, personnel should have clear guidance to think critically before actioning unusual requests as well as a process to report threatening demands for immediate action, pressure for secrecy or requests to circumvent normal business processes and procedures.

Control: ISM-2071; Revision: 0; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel dealing with user account details are advised of what social engineering attacks are, how to manage such situations and how to report them.

Synthetic impersonation

Advances in artificial intelligence (AI) now allow malicious actors to convincingly impersonate executives, employees and customers using synthetic voice and video. As such, personnel dealing with user account details, banking details or financial transactions should not rely on voice or video alone to authenticate requests to modify user account details, modify banking details or conduct financial transactions. Instead, individuals should first be positively identified using a pre-established authentication method or independent trusted communications channel. Such mechanisms may include digitally signed approvals or in-built system approval mechanisms protected by phishing-resistant multi-factor authentication.

Control: ISM-2126; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel positively identify requestors using a pre-established authentication method or independent trusted communication channel before actioning requests to modify user account details, modify banking details or conduct financial transactions.

Reporting suspicious contact via online services

Online services, such as email, internet forums, messaging apps and direct messaging on social media, can be used by malicious actors to elicit sensitive or classified information from personnel. As such, personnel should be advised of what suspicious contact via online services is and how to report it.

Control: ISM-0817; Revision: 4; Updated: Jan-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of what suspicious contact via online services is and how to report it.

Posting work-related information on online services

Personnel should be advised to take particular care not to post work-related information on online services unless authorised to do so, especially for chat services, internet forums, social media and AI tools. Even information that appears to be benign in isolation could, along with other information, have a considerable security impact or lead to increased targeting by malicious actors.

Control: ISM-0820; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised not to post work-related information on unauthorised online services, and to report cases where such information is posted.

Control: ISM-2104; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised not to post information about their security clearance and briefings on unauthorised online services, and to report cases where such information is posted.

Control: ISM-2105; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to limit posting information about their work-related duties on unauthorised online services, and to report cases where such information is posted.

Control: ISM-2106; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to limit posting information about their work-related skills and experience on unauthorised online services, and to report cases where such information is posted.

Posting personal information on online services

Personnel should be advised that any personal information they post on online services, such as social media, could be used by malicious actors to develop a detailed understanding of their lifestyle and interests. In turn, this information could be used to build trust to elicit sensitive or classified information from them, or influence them to undertake specific actions, such as opening malicious email attachments or visiting malicious websites. In addition, personnel posting information on their movements and activities could allow malicious actors to time attempted financial fraud to align with when their target, if in a position of authority, would be uncontactable, such as attending meetings or travelling.

Furthermore, to ensure that personal opinions are not misinterpreted as the official position of an organisation they work for, personnel should maintain separate personal user accounts from any work user accounts they use for online services, especially for social media.

Finally, encouraging personnel to use any available privacy settings for online services can reduce security risks by restricting who can view their personal information, as well as their interactions with online services.

Control: ISM-0821; Revision: 4; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of security risks associated with posting personal information on online services.

Control: ISM-1146; Revision: 4; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to maintain separate personal user accounts from any work user accounts they use for online services.

Control: ISM-2107; Revision: 0; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are encouraged to use any available privacy settings to restrict who can view personal information they post on online services.

Sending and receiving files via online services

When personnel send and receive files via unauthorised online services, such as messaging apps and social media, they often bypass security controls put in place to detect and quarantine malicious code. Advising personnel to send and receive files via authorised online services instead will ensure files are appropriately protected and scanned for malicious code.

Control: ISM-0824; Revision: 2; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised not to send or receive files via unauthorised online services.

Further information

Further information on telephone system usage can be found in the 'Telephone systems' section of the *Guidelines for communications systems*.

Further information on multifunction device usage can be found in the 'Multifunction devices' section of the *Guidelines for communications systems*.

Further information on mobile device usage can be found in the 'Mobile device usage' section of the *Guidelines for enterprise mobility*.

Further information on removable media usage can be found in the 'Media usage' section of the *Guidelines for media*.

Further information on email usage can be found in the 'Email usage' section of the *Guidelines for email*.

Further information on web usage can be found in the 'Web proxies' section of the *Guidelines for gateways*.

Further information and training resources on privileged user training can be found on the Australian Signals Directorate's (ASD) Privileged User Training webpage.

Further information on business email compromise can be found in ASD's *Protecting against business email compromise* publication.

Further information on detecting socially engineered messages can be found in ASD's *Detecting socially engineered messages* publication.

Further information on the use of social media can be found in ASD's *Security tips for social media and messaging services* publication.

Further information on reporting cybercrime incidents and reporting cyber security incidents, including ASD's limited use obligation, is available from ASD.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre