Information security manual

Guidelines for personnel security

Last updated: December 2025

Cyber security awareness training

Providing cyber security awareness training

An organisation should ensure that cyber security awareness training is provided to all personnel in order 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 users and different classes of high-risk users. Finally, personnel with privileges beyond that of a normal user, such as software developers and system 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: 0; Updated: Jun-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Tailored privileged user training is undertaken annually by all privileged users.

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.

Managing and reporting suspicious changes to banking details or payment requests

Business email compromise, a form of financial fraud, is when malicious actors attempt to scam an organisation out 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 edit contact and bank details on 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 a number of 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: 0; Updated: Mar-22; 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, how to manage such situations and how to report it.

Managing and reporting suspicious requests to disclose or change user account details

Suspicious requests to disclose or change user account details, such as changing mobile phone numbers or email addresses, could indicate a malicious actor attempting to access private user details, facilitate password resets or conduct multi-factor authentication bypass attacks against user accounts.

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.

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 in an attempt 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 information to online services

Personnel should be advised to take particular care not to post work information to online services unless authorised to do so, especially for chat services, internet forums, social media and artificial intelligence tools. Even information that appears to be benign in isolation could, along with other information, have a considerable security impact. In addition, to ensure that personal opinions of individuals are not misinterpreted, personnel should be advised to maintain separate work and personal user accounts for online services, especially when using social media.

Control: ISM-0820; Revision: 5; Updated: Jan-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

Control: ISM-1146; Revision: 3; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised to maintain separate work and personal user accounts for online services.

Posting personal information to online services

Personnel should be advised that any personal information they post to 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 in order 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. Furthermore, posting information on movements and activities may allow malicious actors to time attempted financial fraud to align with when a person in a position of authority will be uncontactable, such as attending meetings or travelling. Finally, encouraging personnel to use any available privacy settings for online services can reduce security risks by restricting who can view their information as well as their interactions with such services.

Control: ISM-0821; Revision: 3; Updated: Oct-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.

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 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 on detecting socially engineered messages be found in the Australian Signals Directorate's (ASD) *Detecting socially engineered messages* publication.

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

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

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

Access to systems and their resources

Security clearances

Where these guidelines refer to security clearances, it applies to Australian security clearances or security clearances from a foreign government which are formally recognised by Australia.

System usage policy

To allow an organisation to be capable of holding personnel accountable for the actions they perform on their systems, it is important that the organisation develops, implements and maintains a system usage policy governing the use of systems and their resources.

Control: ISM-1864; Revision: 0; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A system usage policy is developed, implemented and maintained.

General-purpose artificial intelligence usage policy

As there are security risks associated with the use of general-purpose artificial intelligence tools, it is important that an organisation develops, implements and maintains a general-purpose artificial intelligence usage policy governing the use of such tools by their users.

Control: ISM-2074; Revision: 0; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A general-purpose artificial intelligence 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 users of systems.

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.

System access requirements

Documenting access requirements for systems and their resources, such as applications and data repositories, can assist in determining if personnel meet the appropriate authorisation, security clearance, briefing and need-to-know requirements for access. Types of users for which access requirements should be documented include unprivileged users, privileged users, foreign nationals and contractors.

Control: ISM-0432; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access requirements for systems and their resources are documented in their system security plan.

Control: ISM-0434; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance before being granted access to systems and their resources.

Control: ISM-0435; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel receive any necessary briefings before being granted access to systems and their resources.

Control: ISM-1865; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel agree to abide by system usage policies before being granted access to systems and their resources.

User identification

Having uniquely identifiable users ensures accountability for access to systems and their resources. Furthermore, where systems process, store or communicate Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) data, and foreign nationals have access, it is important that the foreign nationals are identified as such.

Control: ISM-0414; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel granted access to systems and their resources are uniquely identifiable.

Control: ISM-0415; Revision: 3; Updated: Aug-19; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

Control: ISM-1583; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Personnel who are contractors are identified as such.

Control: ISM-0420; Revision: 12; Updated: Jun-25; Applicable: S, TS; Essential 8: N/A
Where systems process, store or communicate AUSTEO, AGAO or REL data, personnel who are foreign nationals are identified as such, including by their specific nationality.

Unprivileged access to systems

Personnel seeking access to systems and their resources should have a genuine business requirement validated by their manager or another appropriate authority.

In addition, centrally logging and analysing unprivileged access events can assist in monitoring the security posture of systems and their resources, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-0405; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Requests for unprivileged access to systems and their resources are validated when first requested.

Control: ISM-1852; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.

Control: ISM-1566; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Use of unprivileged access is centrally logged.

Unprivileged access to systems by foreign nationals

Due to the extra sensitivities associated with AUSTEO, AGAO and REL data, foreign access to such data is strictly controlled.

Control: ISM-0409; Revision: 8; Updated: Jun-22; Applicable: S, TS; Essential 8: N/A
Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO or REL data unless effective controls are in place to ensure such data is not accessible to them.

Control: ISM-0411; Revision: 7; Updated: Jun-22; Applicable: S, TS; Essential 8: N/A
Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO data unless effective controls are in place to ensure such data is not accessible to them.

Privileged access to systems

Privileged user accounts are considered those that can alter or circumvent system controls. This also applies to user accounts that may only have limited privileges but still have the ability to bypass some system controls.

Privileged user accounts are often targeted by malicious actors as they can potentially give full access to systems and their resources. As such, ensuring that privileged user accounts are prevented from accessing the internet, email and web services minimises opportunities for these accounts to be compromised. However, if privileged user accounts are explicitly authorised to access online services, they should be strictly limited to only what is required for users and services to undertake their duties.

Finally, centrally logging and analysing privileged access events, as well as privileged user account and security group management events, can assist in monitoring the security posture of systems and their resources, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-1507; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Requests for privileged access to systems and their resources are validated when first requested.

Control: ISM-1508; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Privileged access to systems and their resources is limited to only what is required for users and services to undertake their duties.

Control: ISM-1175; Revision: 6; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.

Control: ISM-1883; Revision: 1; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.

Control: ISM-1649; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML3
Just-in-time administration is used for the administration of systems and their resources.

Control: ISM-0445; Revision: 8; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML1, ML2, ML3
Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.

Control: ISM-1263; Revision: 5; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unique privileged user accounts are used for administering individual server applications.

Control: ISM-1509; Revision: 3; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged access events are centrally logged.

Control: ISM-1650; Revision: 3; Updated: Sep-24; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged user account and security group management events are centrally logged.

Privileged access to systems by foreign nationals

As privileged user accounts often have the ability to bypass system controls, it is strongly encouraged that foreign nationals are not given privileged access to systems that process, store or communicate AUSTEO, AGAO or REL data.

Control: ISM-0446; Revision: 5; Updated: Jun-21; Applicable: S, TS; Essential 8: N/A
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.

Control: ISM-0447; Revision: 4; Updated: Jun-21; Applicable: S, TS; Essential 8: N/A
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO data.

Suspension of access to systems

Removing or suspending access to systems and their resources, ideally using an automatic mechanism, can prevent them from being accessed when there is no longer a legitimate business requirement for their use,

such as when personnel change duties, leave an organisation or are detected undertaking malicious activities.

Control: ISM-0430; Revision: 8; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to systems and their resources are removed or suspended the same day personnel no longer have a legitimate requirement for access.

Control: ISM-1591; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to systems and their resources are removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.

Control: ISM-1404; Revision: 5; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Unprivileged access to systems and their resources are disabled after 45 days of inactivity.

Control: ISM-1648; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged access to systems and their resources are disabled after 45 days of inactivity.

Control: ISM-1647; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: ML2, ML3
Privileged access to systems and their resources are disabled after 12 months unless revalidated.

Recording authorisation for personnel to access systems

Retaining records of account requests for systems and their resources will assist in maintaining personnel accountability. Such records should include each user's user identification, their agreement to abide by system usage policies, who provided the authorisation for their access, when their authorisation was granted and when their access was last reviewed.

Control: ISM-0407; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A secure record is maintained for the life of systems and their resources that covers the following for each user:

- *their user identification*
- *their signed agreement to abide by system usage policies*
- *who authorised their access*
- *when their access was granted*
- *the level of access they were granted*
- *when their access, and their level of access, was last reviewed*
- *when their level of access was changed, and to what extent (if applicable)*
- *when their access was withdrawn (if applicable).*

Temporary access to systems

Under strict circumstances, temporary access to systems and their resources may be granted to personnel who lack an appropriate security clearance or briefing. In such circumstances, personnel should have their access controlled in such a way that they only have access to data required for them to undertake their duties.

Control: ISM-0441; Revision: 9; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When personnel are granted temporary access to systems and their resources, effective controls are put in place to restrict their access to only data required for them to undertake their duties.

Control: ISM-0443; Revision: 3; Updated: Sep-18; Applicable: S, TS; Essential 8: N/A
Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.

Emergency access to systems

It is important that an organisation does not lose access to systems and their resources. As such, an organisation should always have a method for gaining access during emergencies. Typically, emergencies can occur when access cannot be gained via normal authentication processes, such as due to misconfigurations of authentication services, misconfigurations of security settings or due to a cyber security incident. In these situations, break glass accounts (also known as emergency access accounts) can be used to gain access. As break glass accounts have the highest level of privileges available, extreme care should be taken to protect them, as well as monitor them for any signs of compromise or abuse.

When break glass accounts are used, any administrative activities performed will not be directly attributable to individuals, and event logs may not be generated. As such, additional controls need to be implemented in order to maintain the system's integrity. In doing so, an organisation should ensure that any administrative activities performed using break glass accounts are identified and documented in support of change management processes and procedures. This includes documenting the individuals using break glass accounts, the reasons for using break glass accounts and any administrative activities performed using break glass accounts.

As the custodian of each break glass account should be the only party who knows the break glass account's credentials, credentials will need to be changed and tested by custodians after any authorised access by another party. Modern password managers that support automated credential changes can assist in reducing the administrative overhead of such activities.

Finally, centrally logging and analysing break glass account events can assist in monitoring the security posture of systems and their resources, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Control: ISM-1610; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A method of emergency access to systems and their resources is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Control: ISM-1611; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass accounts are only used when normal authentication processes cannot be used.

Control: ISM-1612; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass accounts are only used for specific authorised activities.

Control: ISM-1614; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass account credentials are changed by the account custodian after they are accessed by any other party.

Control: ISM-1615; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break glass accounts are tested after credentials are changed.

Control: ISM-1613; Revision: 2; Updated: Dec-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Use of break glass accounts is centrally logged.

Control of Australian systems

Due to extra sensitivities associated with AUSTEO and AGAO data, it is essential that control of systems that process, store or communicate such data are maintained by Australian nationals working for or on behalf of the Australian Government. Furthermore, AUSTEO and AGAO data should only be accessible from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government.

Control: ISM-0078; Revision: 5; Updated: Jun-21; Applicable: S, TS; Essential 8: N/A
Systems processing, storing or communicating AUSTEO or AGAO data remain at all times under the control of an Australian national working for or on behalf of the Australian Government.

Control: ISM-0854; Revision: 6; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A
AUSTEO and AGAO data can only be accessed from systems under the sole control of the Australian Government that are located within facilities authorised by the Australian Government.

Further information

Further information on access to government resources, including required security clearances, can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Further information on access to highly sensitive government resources, including required briefings, can be found in the Government Security Committee's *Australian Government Security Caveat Guidelines*. This publication is available from the Protective Security Policy GovTEAMS community or the Australian Security Intelligence Organisation by email.

Further information on restricting the use of privileged user accounts can be found in ASD's *Restricting administrative privileges* publication.

Further information on administering systems and their resources can be found in the 'System administration' section of the *Guidelines for system management*.

Further information on event logging can be found in the 'Event logging and monitoring' section of the *Guidelines for system monitoring*.

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