



Information Security Manual

Published: 10 March 2022

Guidelines for Personnel Security

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. Furthermore, the content of cyber security awareness training should be tailored to the needs of specific groups of personnel. For example, personnel with responsibilities beyond that of a normal user will require tailored privileged user training.

Security Control: ISM-0252; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: 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.*

Security Control: ISM-1565; Revision: 0; Updated: Jun-20; Applicability: All; Essential Eight: N/A

Tailored privileged user training is undertaken annually by all privileged users.

Managing and reporting suspicious changes to banking details or payment requests

Business email compromise, a form of financial fraud, is when an adversary attempts to scam an organisation out of money or assets with the assistance of a compromised email account. An adversary will typically attempt to achieve this via invoice fraud, employee impersonation or company impersonation.

With invoice fraud, an adversary will compromise a vendor's email account and through it have access to legitimate invoices. The adversary 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 the adversary's bank account.

With employee impersonation, an adversary 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 is then sent to the adversary's bank account.

With company impersonation, an adversary registers a domain with a name similar to another organisation. The adversary then impersonates that organisation in an email to a vendor and requests a quote for a quantity of expensive assets, such as laptops, and subsequently negotiates for the assets to be delivered to them prior to payment. The assets are then delivered to a location specified by the adversary, 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.

Security Control: ISM-1740; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: 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.

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 an adversary 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.

Security Control: ISM-0817; Revision: 4; Updated: Jan-20; Applicability: All; Essential Eight: 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 special care not to post work information to online services unless authorised to do so, especially in internet forums and on social media. 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 accounts for online services, especially when using social media.

Security Control: ISM-0820; Revision: 5; Updated: Jan-20; Applicability: All; Essential Eight: N/A

Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

Security Control: ISM-1146; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Personnel are advised to maintain separate work and personal 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 an adversary 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 an adversary 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.

Security Control: ISM-0821; Revision: 3; Updated: Oct-19; Applicability: All; Essential Eight: 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 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.

Security Control: ISM-0824; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: 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 fax machine and multifunction device usage can be found in the fax machines and 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 Cyber Security Centre (ACSC)'s [Detecting Socially Engineered Messages](#) publication.

Further information on business email compromise can be found in the ACSC's [Protecting Against Business Email Compromise](#) publication.

Further information on the use of social media can be found in the ACSC's [Security Tips for Social Media and Messaging Apps](#) publication.

Further information on the sanitisation of documents before posting them to authorised online services can be found in the ACSC's [An Examination of the Redaction Functionality of Adobe Acrobat Pro DC 2017](#) publication.

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 access requirements

Documenting access requirements for a system and its resources can assist in determining if personnel have the appropriate authorisation, security clearance, briefings and need-to-know to access the system and its resources. Types of users for which access requirements should be documented include unprivileged users, privileged users, foreign nationals and contractors.

Security Control: ISM-0432; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Access requirements for a system and its resources are documented in its system security plan.

Security Control: ISM-0434; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Personnel undergo appropriate employment screening and, where necessary, hold an appropriate security clearance before being granted access to a system and its resources.

Security Control: ISM-0435; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A

Personnel receive any necessary briefings before being granted access to a system and its resources.

User identification

Having uniquely identifiable users ensures accountability for access to a system and its resources. Furthermore, where a system processes, stores or communicates Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) data, and foreign nationals have access to the system, it is important that the foreign nationals are identified as such.

Security Control: ISM-0414; Revision: 4; Updated: Aug-19; Applicability: All; Essential Eight: N/A

Personnel granted access to a system and its resources are uniquely identifiable.

Security Control: ISM-0415; Revision: 3; Updated: Aug-19; Applicability: All; Essential Eight: N/A

The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

Security Control: ISM-1583; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

Personnel who are contractors are identified as such.

Security Control: ISM-0420; Revision: 11; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A

Where a system processes, stores or communicates 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, applications and data repositories should have a genuine business requirement validated by their manager or another appropriate authority.

Finally, to assist with incident response activities, it is important that unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-0405; Revision: 7; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Requests for unprivileged access to systems, applications and data repositories are validated when first requested.

Security Control: ISM-1566; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Use of unprivileged access is logged.

Security Control: ISM-1714; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Unprivileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

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.

Security Control: ISM-0409; Revision: 7; Updated: Jun-21; Applicability: S, TS; Essential Eight: 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 security controls are in place to ensure such data is not accessible to them.

Security Control: ISM-0411; Revision: 6; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A

Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO data unless effective security controls are in place to ensure such data is not accessible to them.

Privileged access to systems

Privileged accounts are considered to be those which can alter or circumvent a system's security controls. This can also apply to users who have only limited privileges, such as software developers, but can still bypass security controls. A privileged account often has the ability to modify system configurations, account privileges, event logs and security configurations for applications.

Privileged users, and in some cases privileged service accounts, are often targeted by an adversary as they can potentially give full access to systems. As such, ensuring that privileged accounts do not have the ability to access the internet, email and web services minimises opportunities for these accounts to be compromised.

Finally, to assist with incident response activities, it is important that privileged access event logs and privileged account and group change event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1507; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Requests for privileged access to systems and applications are validated when first requested.

Security Control: ISM-1733; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Requests for privileged access to data repositories are validated when first requested.

Security Control: ISM-1508; Revision: 2; Updated: Sep-21; Applicability: All; Essential Eight: ML3

Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

Security Control: ISM-1175; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Privileged user accounts are prevented from accessing the internet, email and web services.

Security Control: ISM-1653; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

Privileged service accounts are prevented from accessing the internet, email and web services.

Security Control: ISM-1649; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

Just-in-time administration is used for administering systems and applications.

Security Control: ISM-0445; Revision: 6; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.

Security Control: ISM-1509; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Use of privileged access is logged.

Security Control: ISM-1650; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Changes to privileged accounts and groups are logged.

Security Control: ISM-1651; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

Privileged access event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1652; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

Privileged account and group change event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Privileged access to systems by foreign nationals

As privileged accounts often have the ability to bypass a system's security 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.

Security Control: ISM-0446; Revision: 5; Updated: Jun-21; Applicability: S, TS; Essential Eight: N/A

Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL data.

Security Control: ISM-0447; Revision: 4; Updated: Jun-21; Applicability: S, TS; Essential Eight: 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, applications and data repositories 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.

Security Control: ISM-0430; Revision: 7; Updated: Sep-19; Applicability: All; Essential Eight: N/A

Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.

Security Control: ISM-1591; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.

Security Control: ISM-1404; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Unprivileged access to systems and applications is automatically disabled after 45 days of inactivity.

Security Control: ISM-1648; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Privileged access to systems and applications is automatically disabled after 45 days of inactivity.

Security Control: ISM-1716; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Access to data repositories is automatically disabled after 45 days of inactivity.

Security Control: ISM-1647; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.

Security Control: ISM-1734; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Privileged access to data repositories is automatically disabled after 12 months unless revalidated.

Recording authorisation for personnel to access systems

Retaining records of system account requests will assist in maintaining personnel accountability. This is needed to ensure there is a record of all personnel authorised to access a system, their user identification, who provided the authorisation, when the authorisation was granted and when the access was last reviewed.

Security Control: ISM-0407; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A

A secure record is maintained for the life of each system covering:

- *all personnel authorised to access the system, and their user identification*
- *who provided authorisation for access*
- *when access was granted*
- *the level of access that was granted*
- *when access, and the level of access, was last reviewed*
- *when the level of access was changed, and to what extent (if applicable)*
- *when access was withdrawn (if applicable).*

Temporary access to systems

Under strict circumstances, temporary access to systems, applications or data repositories 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.

Security Control: ISM-0441; Revision: 7; Updated: Jun-21; Applicability: All; Essential Eight: N/A

When personnel are granted temporary access to a system, effective security controls are put in place to restrict their access to only data required for them to undertake their duties.

Security Control: ISM-0443; Revision: 3; Updated: Sep-18; Applicability: S, TS; Essential Eight: 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 their systems. As such, an organisation should always have a method for gaining access during emergencies. Typically, emergencies would occur when access to systems 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, a break glass account (also known as an emergency access account) can be used to gain access. As break glass accounts generally have the highest level of privileges available for systems, extreme care should be taken to both protect them and to monitor for any signs of compromise or abuse.

When break glass accounts are used, any administrative activities performed will not be directly attributable to an individual, and systems may not generate event logs. As such, additional security 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 a break glass account are identified and documented in support of change management processes and procedures. This includes documenting the individual using the break glass account, the reason for using the break glass account and any administrative activities performed using the break glass account.

As the custodian of each break glass account should be the only party who knows the 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 and testing can assist in reducing the administrative overhead of such activities.

Finally, to assist with incident response activities, it is important that break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Security Control: ISM-1610; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

A method of emergency access to systems is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Security Control: ISM-1611; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

Break glass accounts are only used when normal authentication processes cannot be used.

Security Control: ISM-1612; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

Break glass accounts are only used for specific authorised activities.

Security Control: ISM-1614; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

Break glass account credentials are changed by the account custodian after they are accessed by any other party.

Security Control: ISM-1615; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

Break glass accounts are tested after credentials are changed.

Security Control: ISM-1613; Revision: 1; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Use of break glass accounts is logged.

Security Control: ISM-1715; Revision: 0; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Break glass event logs are centrally stored and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

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.

Security Control: ISM-0078; Revision: 5; Updated: Jun-21; Applicability: S, TS; Essential Eight: 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.

Security Control: ISM-0854; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: 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 Attorney-General's Department's [Protective Security Policy Framework](#), [Access to information](#) policy.

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 accounts can be found in the ACSC's [Restricting Administrative Privileges](#) publication.

Further information on event logging can be found in the event logging and monitoring section of the [Guidelines for System Monitoring](#).