



Information Security Manual

DECEMBER 2021

Guidelines for Personnel Security

Cyber security awareness training

Providing cyber security awareness training

Organisations should ensure that cyber security awareness training is provided to all personnel in order to assist them in understanding their security responsibilities. The content of cyber security awareness training will depend on the security objectives of each organisation; however, personnel with responsibilities beyond that of a standard user will require tailored privileged user training.

Security Control: 0252; Revision: 6; Updated: Jun-20; Applicability: All

Cyber security awareness training is undertaken annually by all personnel and covers:

- the purpose of the cyber security awareness training
- security appointments and contacts within the organisation
- 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: 1565; Revision: 0; Updated: Jun-20; Applicability: All

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

Reporting suspicious contact via online services

Online services such as email, internet forums, messaging apps and direct messaging on social media can all 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: 0817; Revision: 4; Updated: Jan-20; Applicability: All

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: 0820; Revision: 5; Updated: Jan-20; Applicability: All

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

Security Control: 1146; Revision: 2; Updated: Sep-18; Applicability: All

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, 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: 0821; Revision: 3; Updated: Oct-19; Applicability: All

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: 0824; Revision: 2; Updated: Sep-18; Applicability: All

Personnel are advised not to send or receive files via unauthorised online services.

Further information

Further information on email usage policy can be found in the email usage section of the [Guidelines for Email](#).

Further information on web usage policy 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 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: 0432; Revision: 7; Updated: Dec-21; Applicability: All

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

Security Control: 0434; Revision: 6; Updated: Aug-19; Applicability: All

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: 0435; Revision: 3; Updated: Aug-19; Applicability: All

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: 0414; Revision: 4; Updated: Aug-19; Applicability: All

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

Security Control: 0415; Revision: 3; Updated: Aug-19; Applicability: All

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

Security Control: 1583; Revision: 0; Updated: Aug-20; Applicability: All

Personnel who are contractors are identified as such.

Security Control: 0420; Revision: 11; Updated: Dec-21; Applicability: S, TS

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.

Security Control: 0405; Revision: 7; Updated: Dec-21; Applicability: All

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

Security Control: 1566; Revision: 2; Updated: Dec-21; Applicability: All

Use of unprivileged access is logged.

Security Control: 1714; Revision: 0; Updated: Dec-21; Applicability: All

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: 0409; Revision: 7; Updated: Jun-21; Applicability: S, TS

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: 0411; Revision: 6; Updated: Jun-21; Applicability: S, TS

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, audit logs and security configurations for applications.

Privileged users, and in some cases privileged service accounts, are targeted by adversaries 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.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1508, 1649 and 1651-1653 are not applicable.

Security Control: 1507; Revision: 2; Updated: Sep-21; Applicability: All

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

Security Control: 1733; Revision: 0; Updated: Dec-21; Applicability: All

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

Security Control: 1508; Revision: 2; Updated: Sep-21; Applicability: All

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

Security Control: 1175; Revision: 4; Updated: Sep-21; Applicability: All

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

Security Control: 1653; Revision: 0; Updated: Sep-21; Applicability: All

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

Security Control: 1649; Revision: 0; Updated: Sep-21; Applicability: All

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

Security Control: 0445; Revision: 6; Updated: Sep-18; Applicability: All

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

Security Control: 1509; Revision: 1; Updated: Sep-21; Applicability: All

Use of privileged access is logged.

Security Control: 1650; Revision: 0; Updated: Sep-21; Applicability: All

Changes to privileged accounts and groups are logged.

Security Control: 1651; Revision: 0; Updated: Sep-21; Applicability: All

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: 1652; Revision: 0; Updated: Sep-21; Applicability: All

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: 0446; Revision: 5; Updated: Jun-21; Applicability: S, TS

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

Security Control: 0447; Revision: 4; Updated: Jun-21; Applicability: S, TS

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: 0430; Revision: 7; Updated: Sep-19; Applicability: All

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: 1591; Revision: 0; Updated: Aug-20; Applicability: All

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

Security Control: 1404; Revision: 3; Updated: Dec-21; Applicability: All

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

Security Control: 1648; Revision: 0; Updated: Sep-21; Applicability: All

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

Security Control: 1716; Revision: 0; Updated: Dec-21; Applicability: All

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

Security Control: 1647; Revision: 0; Updated: Sep-21; Applicability: All

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

Security Control: 1734; Revision: 0; Updated: Dec-21; Applicability: All

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: 0407; Revision: 4; Updated: Sep-18; Applicability: All

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: 0441; Revision: 7; Updated: Jun-21; Applicability: All

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: 0443; Revision: 3; Updated: Sep-18; Applicability: S, TS

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 organisations do not lose access to systems. As such, organisations should always have a method for gaining access during emergencies. Typically, such emergencies would occur where access to systems cannot be gained via normal authentication processes (e.g. 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 regain 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, actions undertaken will not be directly attributable to an individual, and systems may not generate audit logs. As such, additional security controls need to be implemented in order to ensure the system's integrity. In doing so, organisations should ensure that configuration changes made using a break glass account are identified and documented using change management processes and procedures. This includes documenting the individual using the break glass account, the reason for using the break glass account and the reason for any configuration changes made to a system.

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.

Security Control: 1610; Revision: 0; Updated: Aug-20; Applicability: All

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: 1611; Revision: 0; Updated: Aug-20; Applicability: All

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

Security Control: 1612; Revision: 0; Updated: Aug-20; Applicability: All

Break glass accounts are only used for specific authorised activities.

Security Control: 1613; Revision: 1; Updated: Dec-21; Applicability: All

Use of break glass accounts is logged.

Security Control: 1715; Revision: 0; Updated: Dec-21; Applicability: All

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: 1614; Revision: 0; Updated: Aug-20; Applicability: All

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

Security Control: 1615; Revision: 0; Updated: Aug-20; Applicability: All

Break glass accounts are tested after credentials are changed.

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: 0078; Revision: 5; Updated: Jun-21; Applicability: S, TS

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: 0854; Revision: 6; Updated: Dec-21; Applicability: S, TS

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 temporary access, can be found in the Attorney-General's Department's [Protective Security Policy Framework](#), [Access to information](#) policy.