Australian Government
Australian Signals Directorate

Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Personnel Security

Cyber security awareness training

Providing cyber security awareness training

Organisations should ensure that ongoing 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 objectives of the organisation; however, personnel with responsibilities beyond that of a standard user will require tailored content to meet their needs.

Security Control: 0252; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
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: O, P, S, TS
Tailored privileged user training is undertaken annually by all privileged users.

Reporting suspicious contact via online services

Online services such as email, internet forums, instant messaging apps and direct messaging on social media can all be used by an adversary in an attempt to elicit information from personnel. As such, personnel should be advised of what constitutes suspicious contact via online services and how to report it.

Security Control: 0817; Revision: 4; Updated: Jan-20; Applicability: O, P, S, TS
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 interpreted as official policy, 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: O, P, S, TS
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: O, P, S, TS
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 profile of their lifestyle in order to build a relationship with them. This relationship could then be used to attempt to elicit information or influence them to undertake specific actions, such as opening malicious emails or visiting malicious websites. Furthermore, encouraging personnel to use the privacy settings of online services can minimise who can view their information and interactions on such services.

Security Control: 0821; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
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 online services, such as instant messaging apps and social media, they often bypass security controls put in place to detect and quarantine malicious code. Advising personnel to only send and receive files via authorised online services will ensure files are appropriately protected and scanned for malicious code.

Security Control: 0824; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
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 policies 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 at https://www.cyber.gov.au/acsc/view-all-content/publications/detecting-socially-engineered-messages.

Further information on the use of social media can be found in the ACSC's ***Security Tips for Social Media and Social Networking Apps*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-social-media-and-social-networking-apps.

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 at https://www.cyber.gov.au/acsc/view-all-content/publications/examination-redaction-functionality-adobe-acrobat-pro-dc-2017.

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

Ensuring that the requirements for access to systems and their resources are documented and agreed upon helps determine if personnel have the appropriate authorisations, security clearances and need-to-know to access a system and its resources. Types of users for which access requirements should be documented include standard users, privileged users, foreign users and contractors.

Security Control: 0432; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
Each system's system security plan specifies any requirements for access to the system and its resources.

Security Control: 0434; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS
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: O, P, S, TS
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 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 to such systems, it is important that foreign nationals are identified as such.

Security Control: 0414; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
Personnel granted access to a system and its resources are uniquely identifiable.

Security Control: 0415; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
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: O, P, S, TS
Personnel who are contractors are identified as such.

Security Control: 0975; Revision: 7; Updated: Aug-19; Applicability: O, P, S, TS
Personnel who are foreign nationals are identified as such, including by their specific nationality.

Security Control: 0420; Revision: 10; Updated: Jun-21; Applicability: S, TS
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.

Standard access to systems

Personnel seeking access to systems, applications and data repositories should have a genuine business requirement verified by their manager. Once a requirement to access a system is established, personnel should be given only the privileges that they need to undertake their duties.

Security Control: 0405; Revision: 5; Updated: Sep-19; Applicability: O, P, S, TS
Standard access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1503; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Standard access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

Security Control: 1566; Revision: 0; Updated: Jun-20; Applicability: O, P, S, TS
The use of standard accounts, and any activities undertaken with them, are monitored and audited.

Standard 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 users are considered to be those which can alter or circumvent a system's security measures. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security measures. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.

Privileged users are often targeted by adversaries as they can potentially give full access to systems. As such, ensuring that privileged users do not have the ability to read emails, browse the web or obtain files via online services, such as instant messaging or social media, minimises opportunities for their accounts to be compromised.

Security Control: 1507; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1508; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

Security Control: 0445; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.

Security Control: 1509; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The use of privileged accounts, and any activities undertaken with them, are monitored and audited.

Security Control: 1175; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Privileged access to systems by foreign nationals

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

Security Control: 0448; Revision: 6; Updated: Sep-19; Applicability: O, P, S, TS
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems, applications and data repositories.

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 the organisation or are detected undertaking malicious activities.

Security Control: 0430; Revision: 7; Updated: Sep-19; Applicability: O, P, S, TS
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: O, P, S, TS
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: 2; Updated: Sep-19; Applicability: O, P, S, TS
Access to systems, applications and data repositories is removed or suspended after one month of inactivity.

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: O, P, S, TS
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 briefings. In such circumstances, personnel should have their access controlled in such a way that they only have access to data they require to undertake their duties.

Security Control: 0441; Revision: 7; Updated: Jun-21; Applicability: O, P, S, TS
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 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, actions undertaken will not be directly attributable to an individual, and systems may not generate audit logs. As such, additional activities need to be taken in order to ensure a system's integrity. In doing so, organisations should ensure that configuration changes made using a break glass account are identified and documented using configuration management processes. 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 the authorised access by another party. Modern password managers that support automated credential changes and testing can assist in reducing the administrative overheads of such activities.

Security Control: 1610; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
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: O, P, S, TS
Break glass accounts are only used when normal authentication processes cannot be used.

Security Control: 1612; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are only used for specific authorised activities.

Security Control: 1613; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are monitored and audited for unauthorised use or modification.

Security Control: 1614; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
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: O, P, S, TS
Break glass accounts are tested after credentials are changed.

Control of Australian systems

Due to extra sensitivities associated with AUSTEO and AGAO systems, it is essential that control of such systems is maintained by Australian citizens working for the Australian Government and that such systems can only be accessed from facilities under the sole control of 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: 5; Updated: Jun-21; Applicability: S, TS
Access to AUSTEO or AGAO data from systems not under the sole control of the Australian Government is prevented.

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, at https://www.protectivesecurity.gov.au/information/access-to-information/Pages/default.aspx.