Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

SEPTEMBER 2019

Guidelines for Personnel Security

Cyber security awareness raising and training

Providing cyber security awareness raising and training

Organisations should ensure that ongoing cyber security awareness raising and training is provided to all personnel in order to assist them in understanding their security responsibilities. The content of cyber security awareness raising and 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: 4; Updated: Sep-19; Applicability: O, P, S, TS; Priority: Must
Ongoing cyber security awareness raising and training is provided to personnel and includes:

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

Using online services

Organisations should ensure personnel know what constitutes suspicious contact and how to report such events. For example, questions regarding work duties or projects being undertaken by their organisation. In addition, socially engineered messages, such as those sent via email, instant messages and direct messaging on social media, are one of the most common techniques used to spread malicious code.

Security Control: 0817; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Personnel are advised what suspicious contact is and how to report it, especially when using online services.

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 collaboration tools or forums and on social media. Even information that appears to be benign in isolation, such as the Global Positioning System information in a picture, 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 maintain separate work and personal accounts for online services, especially when using social media.

Security Control: 0820; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Personnel are advised to not post work information to non-approved online services and to report cases where such information is posted.

Security Control: 1146; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Personnel are advised to maintain separate work and personal accounts for online services.

Posting personal information to online services

Personnel should be aware that any personal information they post to online services such as social media could be used to develop a detailed profile of their lifestyle and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit information from them or to implant malicious code on systems (e.g. by having them open emails or visit websites with malicious content). Furthermore, encouraging personnel to use the privacy settings of online services can minimise who can view their interactions on such services.

Security Control: 0821; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Personnel are advised of security risks associated with posting personal information to online services and, where possible, to restrict access to only those they have authorised to view it.

Sending and receiving files via online services

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

Security Control: 0824; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
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 Management***.

Further information on web usage policies can be found in the web content and connections section of the ***Guidelines for Gateway Management***.

Further information on detecting socially engineered messages be found in the Australian Cyber Security Centre's ***Detecting Socially Engineered Messages*** publication at https://www.cyber.gov.au/publications/detecting-socially-engineered-messages.

Access to systems and their resources

Security clearances

Where this document refers 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: 5; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must

Each system's System Security Plan specifies any authorisations, security clearances and briefings necessary for access to the system and its resources.

Security clearances, briefings and user identification

Security clearances and briefings provide assurance that personnel can be trusted with access to information that is processed, stored or communicated by a system. In addition, having uniquely identifiable users ensures accountability for such access. Furthermore, where systems process, store or communicate Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) information, and foreign nationals have access to such systems, it is important that foreign nationals are identified as such.

Security Control: 0434; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must
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; Priority: Must
Personnel receive any necessary briefings before being granted access to a system and its resources.

Security Control: 0414; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must
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; Priority: Must
The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

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

Security Control: 0420; Revision: 8; Updated: Aug-19; Applicability: S, TS; Priority: Must
Where systems process, store or communicate AUSTEO or AGAO information, personnel who are foreign nationals are identified as such, including by their specific nationality.

Security Control: 1538; Revision: 1; Updated: Aug-19; Applicability: P, S, TS; Priority: Must
Where systems process, store or communicate REL information, 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; Priority: Must
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; Priority: Must
Standard access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

Standard access to systems by foreign nationals

Due to the extra sensitivities associated with Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) and Releasable To (REL) information, foreign access to such information is strictly controlled.

Security Control: 0409; Revision: 5; Updated: Aug-19; Applicability: S, TS; Priority: Must

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

Security Control: 0411; Revision: 5; Updated: Aug-19; Applicability: S, TS; Priority: Must
Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO information unless effective security controls are in place to ensure such information is not accessible to them.

Security Control: 0816; Revision: 5; Updated: Aug-19; Applicability: P, S, TS; Priority: Must
Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate REL information unless effective security controls are in place to ensure REL information that is not marked as releasable to their nation is not accessible to them.

Privileged access to systems

Privileged accounts are considered to be those which have one or more of the following abilities or accesses:

- the ability to change key system configuration settings
- the ability to change or circumvent security controls
- access to audit and security monitoring information
- access to data, files and accounts used by other users, including backups and media
- access to troubleshoot a system.

Privileged accounts 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 privileged accounts to be compromised.

Security Control: 1507; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS; Priority: Must
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; Priority: Must
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; Priority: Must
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; Priority: Must
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; Priority: Must
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 information.

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

Security Control: 0446; Revision: 3; Updated: Aug-19; Applicability: S, TS; Priority: Must
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO information.

Security Control: 0447; Revision: 3; Updated: Aug-19; Applicability: S, TS; Priority: Must
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO information.

Security Control: 1545; Revision: 0; Updated: Aug-19; Applicability: P, S, TS; Priority: Must
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate REL information.

Suspension of access to systems

Removing or suspending access to systems, applications and data repositories can prevent it from being accessed when there is no longer a legitimate business requirement for its use, such as when personnel change duties or leave the organisation.

Security Control: 0430; Revision: 7; Updated: Sep-19; Applicability: O, P, S, TS; Priority: Must
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: 1404; Revision: 2; Updated: Sep-19; Applicability: O, P, S, TS; Priority: Should
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; Priority: Should
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 information they require to undertake their duties.

Security Control: 0441; Revision: 6; Updated: Sep-19; Applicability: O, P, S, TS; Priority: Must
When personnel are granted temporary access to a system, effective security controls are put in place to restrict their access to only information required for them to undertake their duties.

Security Control: 0443; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must

Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.

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: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
Systems processing, storing or communicating AUSTEO or AGAO information remain at all times under the control of an Australian national working for or on behalf of the Australian Government.

Security Control: 0854; Revision: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
Access to AUSTEO or AGAO information 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/.