Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

APRIL 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: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Ongoing cyber security awareness raising and training is provided to personnel and includes:

- *the purpose of the awareness raising and training program*
- *security appointments and contacts within the organisation*
- *the use and protection of systems, applications, media and information*
- *reporting of cyber security incidents and suspected compromises*
- *not to introduce or use unauthorised ICT equipment, media or applications with systems*
- *not to attempt to bypass, strain or test security controls on systems*
- *not to attempt to gain unauthorised access to systems, applications or information.*

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 (GPS) 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 policies 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 (ACSC)'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 a system are documented and agreed upon helps determine if personnel have the appropriate authorisations, security clearances and need-to-know to access the system. Types of system

accounts for which access requirements should be documented include standard users, privileged users, contractors and visitors.

Security Control: 0432; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Each system's System Security Plan (SSP) specifies any authorisations, security clearances and briefings necessary for system access.

Security clearances and briefings

Security clearances and briefings provide assurance that personnel can be trusted with access to information that is processed, stored or communicated by a system.

Security Control: 0434; Revision: 5; Updated: Sep-18; 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 systems.

Security Control: 0435; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All personnel receive any necessary briefings before being granted access to systems.

Standard access to systems

Personnel seeking access to systems 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: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Standard access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1503; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Standard access to systems, applications and information 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 other information with nationality releasability markings, foreign access to such information is strictly controlled.

Security Control: 0409; Revision: 4; Updated: Sep-18; 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 controls and procedures are in place to ensure such information is not accessible to them.

Security Control: 0411; Revision: 4; Updated: Sep-18; 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 controls and procedures are in place to ensure such information is not accessible to them.

Security Control: 0816; Revision: 4; Updated: Apr-19; Applicability: P, S, TS; Priority: Must
Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate information with nationality releasability markings unless effective controls and procedures are put in place to ensure information that is not marked as releasable to their nation is not accessible to them.

Privileged access to systems

Privileged access is considered to be access which can give a user one or more of:

- the ability to change key system configurations
- the ability to change control parameters
- access to audit and security monitoring information
- the ability to circumvent security controls
- access to data, files and accounts used by other users, including backups and media
- special access for troubleshooting a system.

Users of privileged accounts are often targeted as their accounts can potentially give full access to a system. Ensuring that users of privileged accounts do not have access to read emails, open attachments, browse the Web or obtain files via online services such as instant messaging or social media, minimises opportunities for these accounts to be compromised. To further assist in minimising security risks associated with privileged accounts, their use should be restricted.

Security Control: 1507; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1508; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Privileged access to systems, applications and information 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 users 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 processing AUSTEO or AGAO information.

Security Control: 0446; Revision: 2; Updated: Sep-18; Applicability: S, TS; Priority: Must
Foreign nationals, including seconded foreign nationals, do not have privileged access to AUSTEO systems.

Security Control: 0447; Revision: 2; Updated: Sep-18; Applicability: S, TS; Priority: Must
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to AGAO systems.

Security Control: 0448; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems.

Suspension of access to systems

Removing or suspending an account can prevent it from being accessed when there is no longer a legitimate business requirement for its use, such as when a user changes duty or leaves an organisation.

Security Control: 0430; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Access to systems, applications and information is removed or suspended on the same day a user no longer has a legitimate business requirement for access.

Security Control: 1404; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Access to systems, applications and information 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

Under strict circumstances, temporary access to systems may be granted on a case-by-case basis to personnel who lack an appropriate security clearance or briefings. In such circumstances, a security risk assessment should be undertaken and personnel should be closely supervised or 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: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When personnel are granted temporary access to a system, effective security controls are in place to restrict their access to only information that is necessary to undertake their duties, or they are continually supervised by another user who has the appropriate security clearance to access the system.

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 (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Access to information*** policy, at https://www.protectivesecurity.gov.au/information/access-to-information/.