Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual Changes Document

APRIL 2019

Content changes

Cyber security framework

- Minor amendment made to 'Purpose' content to clarify that the Australian Cyber Security Centre (ACSC) is a part of the Australian Signals Directorate (ASD).
- Minor amendment made to 'Authority' content.

Guidelines for authorising systems

- Update of website for Information Security Registered Assessors Program (IRAP).

Guidelines for cyber security incidents

- Minor amendment made to 'Roles, responsibilities and procedures' content.
- Security control 0122 was updated to include the documentation of roles relating to the management of cyber security incidents.
- Update of website for reporting cyber security incidents.

Guidelines for outsourcing

- Update of website for certified gateways.
- Update of website for the Managed Service Provider Partner Program (MSP[3]).

Guidelines for security documentation

- Minor amendments made to 'System security documentation' content.
- Minor amendments made to 'Obtaining approval of a system's security documentation' content.

Guidelines for physical security

- Reordering of content within the ***Wireless devices and Radio Frequency transmitters*** section to reduce confusion.
- Amendments to 'Radio Frequency device' content.

- Security control 1543 added to ensure that RF devices used in highly classified environments are recorded in a register.
- Minor amendments to 'Wireless RF point devices' content.

Guidelines for personnel security

- Update of website for the accessing ACSC publications on detecting socially engineered messages.
- Minor amendment made to 'Standard access to systems by foreign nationals' content.
- Security control 0816 was updated to remove the applicability to sensitive information. Nationality releasability markings are only applicable to classified information.

Guidelines for communications infrastructure

- References to Australian Communications Security Instruction (ACSI) versions were updated to reflect their latest release.

Guidelines for enterprise mobility

- Minor amendment to 'Mobile device security policy' content.
- Security control 1533 was updated to clarify it related to a security policy and not an acceptable use policy.
- Security control 0862 was removed due to a duplication of intent with security controls 1533 and 1195.
- Security control 0864 was updated to include the modification of security functions.
- Update of website for the accessing ACSC publications on enterprise mobility.
- Minor amendments made to 'Mobile device usage policy' content.
- Amendments made to 'Using mobile devices in public spaces' content to address the risk of sensitive or classified conversations being overheard.
- Security control 0866 was updated to address sensitive or classified conversations being overheard.
- Security control 0871 was updated to deconflict with security control 0870.
- Security control 0870 was moved from 'Carrying mobile devices' to 'Maintaining control of mobile devices'.
- Security control 0870 was updated to address storage of mobile devices in a secure state when not being actively used.
- Amendments made to 'Maintaining control of mobile devices' content.
- Security control 1088 was moved from 'After travelling overseas with mobile devices' to 'While travelling overs with mobile devices'.
- Amendments made to 'After travelling overseas with mobile devices' content.
- Security control 1300 was updated to recommend resetting mobile devices that are suspected of being compromised following overseas travel.
- Update of website for the accessing ACSC publications on travelling overseas with mobile devices.

Guidelines for evaluated products

- Update of website for the Australasian Information Security Evaluation Program (AISEP).

Guidelines for media management

- Minor amendment to 'Removable media security policy' content.
- Security control 1359 was reworded slightly.

Guidelines for system hardening

- Update of website for various ACSC publications.
- Security control 1235 was moved from the ***Guidelines for gateway management*** to the ***Guidelines for system hardening*** and expanded in scope to cover Microsoft Office and PDF viewers.

Guidelines for system management

- Update of website for various ACSC publications.

Guidelines for software development

- Minor amendment to 'Web browser-based security controls' content.
- Security control 0971 was updated to replace the reference to the OWASP ***Development Guide*** with the newer OWASP ***Application Security Verification Standard***.
- References to the OWASP ***Development Guide*** were replaced with the newer OWASP ***Application Security Verification Standard***.

Guidelines for database systems management

- Security control 0393 was updated to fix a spelling error.

Guidelines for email management

- Update of website for various ACSC publications.

Guidelines for network management

- Update of website for various ACSC publications.

Guidelines for using cryptography

- Amendments made to 'Suite B' content.
- Minor amendment to 'Protecting highly classified information' content.
- Security control 1232 was updated to reflect the correct terminology of 'CNSA Suite algorithms'.
- Security control 1468 was updated to reflect the correct terminology of 'CNSA Suite algorithms'.
- References to ACSI versions were updated to reflect their latest release.
- Security control 0499 was updated to reflect their latest release.

Guidelines for gateway management

- Security control 1235 was moved to the ***Guidelines for system hardening***.
- The 'Gateway user training' content was moved from the ***Gateways*** section to the ***Cross Domain Solutions*** section and modified in scope to just Cross Domain Solutions (CDS).
- Security control 0610 was updated to focus exclusively on CDS.
- Security control 1527 was removed.
- Security control 1528 was expanded to cover the use of evaluated firewalls between official networks and public network infrastructure.
- Security control 1193 was removed.
- Security control 0639 was expanded to cover the use of evaluated firewalls between official networks belonging to different security domains.
- Amendments to 'Using peripheral switches' content.
- Security control 0593 was expanded to cover the use of evaluated peripheral switches between official systems that belong to different security domains.

Guidelines for data transfers and content filtering

- Security control 0661 was reworded slightly.

Supporting information

- Minor amendment to 'content filter' and 'network access control' definitions.

Security assessment aids

- Security control 0122 was updated to reflect changes made to the ***Guidelines for cyber security incidents***.
- Security control 1543 was added to reflect changes made to the ***Guidelines for physical security***.
- Security control 0816 was updated to reflect changes made to the ***Guidelines for personnel security***.
- Security controls 1533, 0864, 0866, 0871, 0870 and 1300 were updated to reflect changes made to the ***Guidelines for enterprise mobility***.
- Security control 1359 was updated to reflect changes made to the ***Guidelines for media management***.
- Security control 1235 was updated to reflect changes made to the ***Guidelines for system hardening***.
- Security control 0971 was updated to reflect changes made to the ***Guidelines for software development***.
- Security control 0393 was updated to reflect changes made to the ***Guidelines for database systems management***.
- Security controls 1232, 1468 and 0499 were updated to reflect changes made to the ***Guidelines for using cryptography***.
- Security controls 0610, 1528 and 0639 were updated to reflect changes made to the ***Guidelines for gateway management***.
- Security control 0661 was updated to reflect changes made to the ***Guidelines for data transfers and content filtering***.

List of modified security controls

Security Control: 0122; Revision: 4; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Roles, responsibilities and procedures for managing cyber security incidents are detailed in each system's security documentation.

Security Control: 1543; Revision: 0; Updated: Apr-19; Applicability: S, TS; Priority: Should
A register is maintained of authorised RF devices that can be used in SECRET and TOP SECRET areas.

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.

Security Control: 1533; Revision: 1; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
A security policy governing the management of mobile devices is developed and implemented.

Security Control: 0864; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Mobile devices prevent personnel from disabling or modifying security functions once provisioned.

Security Control: 0866; Revision: 4; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Sensitive or classified information is not viewed or communicated in public locations unless care is taken to reduce the chance of conversations being overheard or the screen of a mobile device being observed.

Security Control: 0871; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Mobile devices are kept under continual direct supervision when being actively used.

Security Control: 0870; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Mobile devices are carried or stored in a secured state when not being actively used.

Security Control: 1300; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Should
If upon returning from overseas mobile devices are suspected of being compromised, the devices and all passphrases for accounts associated with the devices are reset.

Security Control: 1359; Revision: 2; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Should
A removable media security policy is developed and implemented that includes:

- *details of the removable media authority within the organisation*
- *types of media permitted within the organisation*
- *processes for media registration and auditing*
- *processes for media classification and labelling*
- *processes for the use of media for data transfers*
- *processes for the sanitisation/destruction and disposal of media.*

Security Control: 1235; Revision: 2; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Should
The use of Microsoft Office, web browser and PDF viewer add-ons is restricted to organisation approved add-ons.

Security Control: 0971; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Should
*The OWASP **Application Security Verification Standard** is followed when developing web applications.*

Security Control: 0393; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Databases and their contents are classified based on the sensitivity or classification of information that they contain.

Security Control: 1232; Revision: 4; Updated: Apr-19; Applicability: S, TS; Priority: Must
Suite B or CNSA Suite algorithms are used in an evaluated configuration.

Security Control: 1468; Revision: 3; Updated: Apr-19; Applicability: S, TS; Priority: Should
Preference is given to using CNSA Suite algorithms over Suite B algorithms.

Security Control: 0499; Revision: 8; Updated: Apr-19; Applicability: S, TS; Priority: Must
ACSI 53 E, ACSI 103 A, ACSI 105 B, ACSI 107 B, ACSI 173 A and the latest equipment-specific doctrine is complied with when using HACE.

Security Control: 0610; Revision: 6; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Users are trained on the secure use of a CDS before access to use the CDS is granted.

Security Control: 1528; Revision: 1; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
An evaluated firewall is used between official or classified networks and public network infrastructure.

Security Control: 0639; Revision: 8; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
An evaluated firewall is used between networks belonging to different security domains.

Security Control: 0661; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS; Priority: Must
Users transferring data to and from a system are held accountable for the data they transfer.