Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual: June 2021 Changes

JUNE 2021

Applying ISM updates

Please note: There is no requirement for organisations to immediately implement updates to the ***Australian Government Information Security Manual*** (ISM). Instead, organisations are encouraged to review the security risks for their systems (using the latest version of the ISM available at the time) based on a frequency suitable for their business requirements and in accordance with their corporate risk management framework. For example, every month, every three months (quarterly), every six months (semi-annually) or every year (annually).

Terminology changes

For this release of the publication, the focus on the 'protection of information' has shifted to the more encompassing 'protection of data'. This has resulted in a large number of changes. As such, changes related to the replacement of references to 'information' with 'data' haven't been individually captured in this changes document.

Guidelines for Communications Infrastructure

Cabling infrastructure

Cable register

- Security control 0208 was amended to focus on the information that is maintained for each cable within a cable register. The recommendation to include a site/floor plan diagram in the cable register has been moved into newly created security control 1645 reflecting that it is a separate set of diagrams in its own right.

  Security Control: 0208; Revision: 5; Updated: Mar-21; Applicability: O, P, S, TS
  Cable registers contain the following information:

  - *cable identifier*
  - *cable colour*
  - *sensitivity/classification*
  - *source*
  - *destination*
  - *site/floor plan diagram*
  - *seal numbers (if applicable).*

Security Control: 0208; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
A cable register contains the following for each cable:

- *cable identifier*
- *cable colour*
- *sensitivity/classification*
- *source*
- *destination*
- *location*
- *seal numbers (if applicable).*

Floor plan diagrams

- A new topic on floor plan diagrams was introduced reflecting that floor plan diagrams exist separately to cable registers.

  Floor plan diagrams, developed using computer-aided design and drafting software, providing an accurate scaled view for each floor and using alphanumeric grid referencing, are critical to ensuring that cabling infrastructure components can be easily located by installers and inspectors. In doing so, floor plan diagrams should track all cabling infrastructure changes throughout the life of a system.

- Security control 1645 was added to cover the maintenance and use of floor plan diagrams.

  Security Control: 1645; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
  Floor plan diagrams are maintained and regularly audited.

- Security control 1646 was added to cover the contents of floor plan diagrams.

  Security Control: 1646; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
  Floor plan diagrams contain the following:

  - *cable paths (including ingress and egress points between floors)*
  - *cable reticulation system and conduit paths*
  - *floor concentration boxes*
  - *wall outlet boxes*
  - *network cabinets.*

Emanation security

Further information

- References to Australian Communications Security Instructions (ACSIs) were removed. This publication will no longer be maintaining references to specific ACSI publications and their versions.

Guidelines for Enterprise Mobility

Mobile device usage

Using mobile devices in public spaces

- The content of this topic was amended to draw a clear distinction between using data services (e.g. accessing emails) and using voice services (e.g. making phone calls).

  Personnel should be aware of the environment they use mobile devices in to view or communicate sensitive or classified data, especially in public areas such as public transport, transit lounges and coffee shops. In such locations, personnel should take care to ensure that sensitive or classified data is not observed by other parties. In some cases, privacy filters can be applied to the screen of a mobile device to prevent onlookers from reading content off its screen. In addition, personnel should maintain awareness of the environments from which they conduct sensitive or classified phone calls and the potential for their conversations to be overheard.

- Security control 0866 was amended to remove references to phone conversations being overheard.

  Security Control: 0866; Revision: 4; Updated: Apr-19; Applicability: O, P, S, TS
  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: 0866; Revision: 5; Updated: Jun-21; Applicability: O, P, S, TS
  Sensitive or classified data is not viewed or communicated in public locations unless care is taken to reduce the chance of the screen of a mobile device being observed.

- Security control 1644 was introduced to cover phone conversations being overheard.

  Security Control: 1644; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
  Sensitive or classified phone calls are not conducted in public locations unless care is taken to reduce the chance of conversations being overheard.

Guidelines for System Hardening

Authentication hardening

Session and screen locking

- Security control 0428 was amended to note that only session contents needs to be concealed (instead of all contents) when a screen is locked (i.e. corporate lock screen backgrounds are acceptable).

  Security Control: 0428; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
  Systems are configured with a session or screen lock that:

  - *activates after a maximum of 15 minutes of user inactivity or if manually activated by the user*
  - *completely conceals all information on the screen*
  - *ensures that the screen does not enter a power saving state before the screen or session lock is activated*
  - *requires the user to reauthenticate to unlock the system*
  - *denies users the ability to disable the session or screen locking mechanism.*

Security Control: 0428; Revision: 7; Updated: Jun-21; Applicability: O, P, S, TS
Systems are configured with a session or screen lock that:

- *activates after a maximum of 15 minutes of user inactivity, or if manually activated by the user*
- *conceals all session content on the screen*
- *ensures that the screen does not enter a power saving state before the session or screen lock is activated*
- *requires the user to reauthenticate to unlock the system*
- *denies users the ability to disable the session or screen locking mechanism.*

Guidelines for System Management

System patching

Patch management process and procedures

- Security control 1493 was amended to split out the contents of the software register into a separate security control as per similar security control pairs for other types of registers.

  Security Control: 1493; Revision: 1; Updated: Aug-19; Applicability: O, P, S, TS
  A software register, including versions and patch histories of applications, drivers, operating systems and firmware for workstations, servers, mobile devices, network devices and all other ICT equipment, is maintained and regularly audited

  Security Control: 1493; Revision: 2; Updated: Jun-21; Applicability: O, P, S, TS
  Software registers are maintained and regularly audited for workstations, servers, mobile devices, network devices and all other ICT equipment.

- Security control 1643 was introduced to cover the contents of software registers.

  Security Control: 1643; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
  Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.

Guidelines for Email

Email usage

Protective markings for emails

- The content of this topic was amended to note that the protective marking applied to an email reflects the highest sensitive or classification of the subject, body and attachments for the email.

  Implementing protective markings for emails ensures that appropriate security controls are applied to data, and also helps to prevent unauthorised data being released into the public domain. In doing so, it is important that protective markings reflect the highest sensitivity or classification of the subject, body and attachments of emails.

- Security control 0270 was amended to note that the protective marking applied to an email reflects the highest sensitive or classification of the subject, body and attachments for the email.

  Security Control: 0270; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
  Protective markings are applied to emails and reflect the information in their subject, body and attachments.

__Security Control: 0270; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS__
Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments.

Guidelines for Cryptography

Cryptographic fundamentals

Further information

- References to Australian Communications Security Instructions (ACSIs) were removed. This publication will no longer be maintaining references to specific ACSI publications and their versions.

Cryptographic system management

High Assurance Cryptographic Equipment

- The content of this topic was amended to remove references to ACSIs.

  HACE can be used by organisations to protect highly classified data. Organisations using HACE must comply with all communications security and equipment-specific doctrine produced by the ACSC for the management and use of HACE.

- Security control 0499 was amended to replace references to specific ACSIs with a requirement to comply with all communications security and equipment-specific doctrine produced by the ACSC.

  __Security Control: 0499; Revision: 8; Updated: Apr-19; Applicability: S, TS__
  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: 0499; Revision: 9; Updated: Jun-21; Applicability: S, TS__
  All communications security and equipment-specific doctrine produced by the ACSC for the management and use of HACE is complied with.

Further information

- References to Australian Communications Security Instructions (ACSIs) were removed. This publication will no longer be maintaining references to specific ACSI publications and their versions.

Cyber Security Terminology

Glossary of abbreviations

- The ‘ACSI’ abbreviation was removed as it no longer appears in the publication.

Glossary of cyber security terms

- The ‘logical access controls’ term was removed as it no longer appears in the publication.