Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual Changes Document

MARCH 2019

Content changes

Cyber security framework

- Replacement of reference to NIST SP 800-37 Rev. 1, ***Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach***, with the newer NIST SP 800-37 Rev. 2, ***Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy***.

Guidelines for authorising systems

- Change of section title from '***Conducting accreditations***' to '***Authorising systems***' to match steps undertaken as part of normal risk management activities.
- Change of section title from '***Conducting certifications***' to '***Conducting security assessments***' to match steps undertaken as part of normal risk management activities.
- Minor amendments made to 'Authorising officers' content.
- Amendments made to 'Assessors' content.

Guidelines for physical security

- Amendments made to 'Securing ICT equipment and media' content.
- Security control 0161 was revised to clarify that ICT equipment and media needs to be secured when not in use.
- Security control 0829 was revised to clarify that it applies to unauthorised RF devices rather than all active RF devices.

Guidelines for personnel security

- Reference to '***Guidelines for connecting networks and security domains***' was changed to '***Guidelines for gateway management***'.

Guidelines for communications systems

- Reference to '***Guidelines for connecting networks and security domains***' was changed to '***Guidelines for gateway management***'.

Guidelines for enterprise mobility

- Security controls 1399 and 1481 were revised to mirror the intent of security controls 1400 and 1482.

Guidelines for evaluated products

- Amendments made to 'Evaluated products' content to ensure organisations use the Common Criteria website at https://www.commoncriteriaportal.org/products/.
- Minor amendment made to 'Protection profiles' content.
- References to 'Common Criteria evaluated products' were replaced with 'Common Criteria certified products' to match terminology used on the Common Criteria website.

Guidelines for ICT equipment management

- Security control 1223 was revised to remove duplicate guidance within the security control.

Guidelines for media management

- Security control 0325 was revised to fix a grammar error (i.e. to replace 'assured' with 'ensured').

Guidelines for system hardening

- Security control 1470 was revised from a 'must' to a 'should' as high risk functionality of specific products are captured in separate security controls.
- Security control 1173 was reworded.
- Security control 1401 was revised to clarify that any two different authentication factors constitute multi-factor authentication (e.g. the use of biometrics and a U2F security key).

Guidelines for email management

- Minor amendments made to 'Webmail services' content.
- Security control 0267 was reworded.
- Amendments made to 'Protective markings for emails' content.
- Security control 0270 was revised to broaden its scope to allow for the use of non-government protective marking standards.
- Security control 0273 was merged with security control 0270.
- Amendments made to 'Protective marking tools' content.
- Security control 0271 was reworded.
- Security control 0272 was reworded.
- Security control 1089 was reworded.
- Amendments made to 'Handling emails with inappropriate, invalid or missing protective markings' content.
- Security control 0565 was reworded.
- Security control 1023 was reworded.

- Security control 0278 was rescinded.
- Security control 1368 was merged with security control 0565.
- Security control 1022 was rescinded.
- Security control 0563 was merged with security control 0565.
- Security control 0564 was merged with security control 0565.
- Security control 0566 was rescinded as it is covered by the intent of security control 0565.
- Security control 1539 was modified from a priority of 'should' to 'must'.
- Change of section title from '***Email infrastructure***' to '***Email gateways and servers***'.
- Minor amendments to 'Centralised email gateways' content.
- Amendments to 'Email gateway maintenance activities' content.
- Security control 0568 was rescinded as it is covered by the intent of security control 1163.
- Minor amendments to 'Open relay email servers' content.
- Security control 0571 was reworded.
- Security control 0567 was reworded.
- Amendments to 'Email server transport encryption' content.
- Security control 1152 was reworded.
- Minor amendments to 'DomainKeys Identified Mail' content.
- Security control 0861 was reworded.
- Amendments to 'Email content filtering' content.
- Security control 1234 was revised to include content filtering for email body contents.
- Security control 1057 was merged into security control 1234.
- Minor amendments to 'Blocking suspicious emails' content.
- Security control 0561 was reworded.
- Security control 1502 was reworded.
- Minor amendments to 'Undeliverable messages' content.

Guidelines for network management

- Reference to '***Guidelines for connecting networks and security domains***' was changed to '***Guidelines for gateway management***'.

Guidelines for using cryptography

- Reference to '***Guidelines for connecting networks and security domains***' was changed to '***Guidelines for gateway management***'.

Guidelines for gateway management

- Change of title from '***Guidelines for connecting networks and security domains***' to '***Guidelines for gateway management***' to match the naming convention for similar guidelines.
- Minor amendments to 'Deploying gateways' content.
- Minor amendments to 'Applying the security controls' content.
- Security control 0628 was reworded.
- Security control 0611 was reworded.
- Minor amendments to 'Purpose of Cross Domain Solutions' content.
- The contents of 'Consultation when implementing Cross Domain Solutions' was merged with the contents of 'Consultation when modifying Cross Domain Solutions'.
- References to using the ***Evaluated Products List*** to select evaluated products was removed as a greater selection of products are available via the Common Criteria website at https://www.commoncriteriaportal.org/products/.

Security assessment aids

- Security controls 0161 and 0829 were updated to reflect changes made to the ***Guidelines for physical security***.
- Security controls 1399 and 1481 were updated to reflect changes made to the ***Guidelines for enterprise mobility***.
- Security control 1223 was updated to reflect changes made to the ***Guidelines for ICT equipment management***.
- Security control 0325 was updated to reflect changes made to the ***Guidelines for media management***.
- Security controls 1470, 1173 and 1401 were updated to reflect changes made to the ***Guidelines for system hardening***.
- Security controls 0267, 0270, 0271, 0272, 1089, 0565, 1023, 1539, 0571, 0567, 1152, 0861, 1234, 0561 and 1502 were updated to reflect changes made to the ***Guidelines for email management***.
- Security controls 0273, 0278, 1368, 1022, 0563, 0564, 0566, 0568 and 1057 were removed to reflect changes made to the ***Guidelines for email management***.

List of modified security controls

Security Control: 0161; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
ICT equipment and media are secured when not in use.

Security Control: 0829; Revision: 4; Updated: Mar-19; Applicability: S, TS; Priority: Should
Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.

Security Control: 1399; Revision: 2; Updated: Mar-19; Applicability: O; Priority: Should
Personnel accessing official information using a privately-owned mobile device use an ACSC approved platform, a security configuration in accordance with ACSC hardening guidance, and have enforced separation of official and personal information.

Security Control: 1481; Revision: 1; Updated: Mar-19; Applicability: O; Priority: Should
Personnel accessing official information using an organisation-owned mobile device use an ACSC approved platform with a security configuration in accordance with ACSC hardening guidance.

Security Control: 1223; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Memory in network devices is sanitised using the following processes, in order of preference:

- *following device-specific guidance provided by the ACSC*
- *following vendor sanitisation guidance*
- *if guidance is unavailable, performing a full reset and loading of a dummy configuration file.*

Security Control: 0325; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Any media connected to a system is classified as the same sensitivity or classification as the system, unless the media is read-only, the media is inserted into a read-only device or the system has a mechanism through which read-only access can be ensured.

Security Control: 1470; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
Any unrequired functionality in Microsoft Office, web browsers and PDF viewers is disabled.

Security Control: 1173; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.

Security Control: 1401; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor (U2F) security keys, physical one-time password (OTP) tokens, biometrics or smartcards.

Security Control: 0267; Revision: 7; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Access to non-approved webmail services is blocked.

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

Security Control: 0271; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
Protective marking tools do not automatically insert protective markings into emails.

Security Control: 0272; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.

Security Control: 1089; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Protective marking tools do not allow users replying to or forwarding an email to select a protective marking that is lower than previously used for the email.

Security Control: 0565; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Email servers are configured to block, log and report emails with inappropriate protective markings.

Security Control: 1023; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
The intended recipients of any blocked inbound emails, and the sender of any blocked outbound emails, are notified.

Security Control: 1539; Revision: 1; Updated: Mar-19; Applicability: P, S, TS; Priority: Must
Emails containing nationality releasability information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

Security Control: 0571; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
When users send email from outside their network, an authenticated and encrypted channel is configured to allow email to be routed via a centralised email gateway.

Security Control: 0567; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Email servers only relay emails destined for or originating from their domains.

Security Control: 1152; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Incoming emails that fail SPF checks are blocked or marked in a manner that is visible to the recipients.

Security Control: 0861; Revision: 2; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
DKIM signing is enabled on emails originating from an organisation's domains.

Security Control: 1234; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Email content filtering controls are implemented for email bodies and attachments.

Security Control: 0561; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Emails addressed to internal email aliases where the source address is from outside the domain are blocked at the email gateway.

Security Control: 1502; Revision: 1; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Emails arriving via an external connection where the source address uses an internal domain name are blocked at the email gateway.

Security Control: 0628; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
All systems are protected from systems in other security domains by one or more gateways.

Security Control: 0611; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Access to gateway administration functions is limited to the minimum roles and privileges to support the gateway securely.