August 2020 ISM Changes

Summary of key changes

- Introduction of a recommendation for system owners to report the security status of each system to its authorising officer at least annually.
- Introduction of a recommendation for system owners to be consulted before targeted cyber intrusion activity is allowed to continue on their systems for the purpose of collecting further information or evidence.
- Introduction of a recommendation to communicate security documentation to all stakeholders.
- Introduction of a recommendation to uniquely identify contractor accounts for systems.
- Introduction of a recommendation to suspend the access of personnel conducting malicious activities as soon as practicable after they are detected.
- Introduction of six recommendations supporting the secure use of break glass accounts for emergency access to systems.
- Introduction of a recommendation that ICT equipment is protected based upon the sensitivity or classification of information that it displays, processes, stores or communicates.
- Introduction of a recommendation that ICT equipment is assessed for any unauthorised modifications or changes to its approved software configuration following maintenance or repair activities.
- Introduction of a recommendation that media is sanitised before it is used for the first time with systems.
- Reintroduction of a recommendation to create Standard Operating Environments (SOEs) for workstations and servers.
- Introduction of a recommendation that when organisations use SOEs provided by third parties they scan them for malicious content and configurations before they are used.
- Introduction of a recommendation to review and update SOEs at least annually.
- Introduction of a recommendation to prevent standard users from bypassing, disabling or modifying security functionality in operating systems.
- Introduction of a recommendation that users only be prevented from installing unapproved applications, thereby allowing for the installation of vetted and approved applications from organisation-managed software repositories or from trusted application marketplaces.
- Introduction of a recommendation to validate cryptographic hash rules, publisher certificate rules and path rules used for application control at least annually.
- Introduction of a recommend to implement Microsoft’s Attack Surface Reduction rules.
- Introduction of a recommendation to prevent standard users from bypassing, disabling or modifying security functionality in applications.
- Introduction of a recommendation to prevent the sharing of passwords/passphrases used for single-factor authentication across different systems.
- Introduction of a recommendation that credentials set or reset on behalf of users should be randomly generated.
- Introduction of a recommendation that users provide sufficient evidence to verify their identity when collecting initial credentials for an account.
- Introduction of a recommendation to sufficiently protect credentials when communicating them to users after setting or resetting them on their behalf.
- Introduction of a recommendation that when initial credentials are set on behalf of a user that they be changed after their first use.
- Introduction of a recommendation to disable authentication methods that are susceptible to replay attacks.
- Introduction of a recommendation that credentials are obscured when entered into systems.
- Introduction of a recommendation that articulates scenarios in which password/passphrase changes should occur.
- Reintroduction of a recommendation to terminate user sessions and reboot workstations after a defined period of inactivity outside of business hours.
- Introduction of a recommendation to implement a vulnerability disclosure program to support the secure development and maintenance of products and services.
- Introduction of a recommendation to implement MTA-STS for email servers.
- Introduction of a recommendation to use data transfer logs to record authorised data imports and exports for systems.

Using the Australian Government Information Security Manual

Executive summary

- Updates to website addresses in ‘further information’ content.

Applying a risk-based approach to cyber security

- Minor update to ‘define the system’ content.
- Update to website address in ‘further information’ content.

Guidelines for Cyber Security Roles

System owners

- Update to ‘responsibilities’ content.
- Security control 1587 was introduced to cover system owners reporting the security status of each system to its authorising officer at least annually.

Security Control: 1587; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
System owners report the security status of each system to its authorising officer at least annually.
Guidelines for Cyber Security Incidents

Detecting cyber security incidents

- Updates to ‘access to sufficient data sources and tools’ content.

Managing cyber security incidents

- Security control 1609 was introduced to ensure that system owners are consulted before targeted cyber intrusion activity is allowed to continue on their systems for the purpose of collecting further information or evidence.

  **Security Control: 1609; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS**
  
  System owners are consulted before allowing targeted cyber intrusion activity to continue on a system for the purpose of collecting further information or evidence.

- Security control 0138 was modified slightly.

  **Security Control: 0138; Revision: 4; Updated: Aug-20; Applicability: O, P, S, TS**
  
  The integrity of evidence gathered during an investigation is maintained by investigators:
  
  - recording all of their actions
  - creating checksums for all evidence
  - copying evidence onto media for archiving
  - maintaining a proper chain of custody.

Reporting cyber security incidents

- Update to website address in ‘further information’ content.

Guidelines for Outsourcing

Information technology and cloud services

- Update to ‘further information’ content to include a reference to the ACSC’s guidance on conducting security assessments of cloud service providers and their cloud services.

- Updates to website addresses in ‘further information’ content.

Guidelines for Security Documentation

Development and maintenance of security documentation

- Minor update to ‘approval of security documentation’ content to move content related to the communication of security documentation under a new heading.

- New ‘communication of security documentation’ content was added.

- Security control 1602 was introduced to ensure security documentation is communicated to all stakeholders.

  **Security Control: 1602; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS**
  
  Security documentation, including notification of subsequent changes, is communicated to all stakeholders.

- Minor updates to ‘further information’ content.
Guidelines for Physical Security

Facilities and systems

- Minor update to ‘further information’ content.

ICT equipment and media

- Minor updates to ‘further information’ content.

Wireless devices and Radio Frequency transmitters

- Minor update to ‘further information’ content.

Guidelines for Personnel Security

Cyber security awareness training

- Minor updates to ‘further information’ content.
- Update to website address in ‘further information’ content.

Access to systems and their resources

- Update to ‘privileged access to systems’ content.
- Security control 0432 was amended slightly to capture any requirements for system access beyond authorisations, security clearances and briefings.

  Security Control: 0432; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
  Each system’s system security plan specifies any requirements for access to the system and its resources.

- Amendments were made to ‘user identification’ content to focus on the identification of system users.
- Security control 1583 was introduced to assist in uniquely identifying contractor accounts for systems.

  Security Control: 1583; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  Personnel who are contractors are identified as such.

- Amendments were made to ‘suspension of access to systems’ to cover scenarios in which personnel are discovered undertaking malicious activities.
- Security control 1591 was introduced to ensure that the access of personnel conducting malicious activities is suspended as soon as practicable after such activities are detected.

  Security Control: 1591; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.

- Addition of new ‘emergency access to systems’ content.
- Six security controls were introduced to cover the secure use of break glass accounts for gaining emergency access to systems.

  Security Control: 1610; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  A method of emergency access to systems is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.
Security Control: 1611; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are only used when normal authentication processes cannot be used.

Security Control: 1612; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are only used for specific authorised activities.

Security Control: 1613; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are monitored and audited for unauthorised use or modification.

Security Control: 1614; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass account credentials are changed by the account custodian after they are accessed by any other party.

Security Control: 1615; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are tested after credentials are changed.

Guidelines for Communications Infrastructure

Cable management

- Update to website address in ‘further information’ content.

Guidelines for Communications Systems

Telephone systems

- Minor update to ‘further information’ content.

Video conferencing and Internet Protocol telephony

- Minor updates to ‘video conferencing and Internet Protocol telephony gateways’ content.
- Minor updates to ‘further information’ content.

Fax machines and multifunction devices

- Minor updates to ‘further information’ content.

Guidelines for Enterprise Mobility

Mobile device management

- Minor update to ‘privately-owned mobile devices’ content to note that it relates to the access of an organisation’s systems or information.
- Security controls 1400 and 0694 were amended to note that they relate to the access of an organisation’s systems or information.

Security Control: 1400; Revision: 4; Updated: Aug-20; Applicability: O, P
Personnel accessing official or classified systems or information using a privately-owned mobile device use an ACSC approved platform, a security configuration in accordance with ACSC guidance, and have enforced separation of official and classified information from any personal information.

Security Control: 0694; Revision: 5; Updated: Aug-20; Applicability: S, TS
Privately-owned mobile devices do not access highly classified systems or information.
Minor update to ‘seeking legal advice for privately-owned mobile devices’ content to note that it relates to the access of an organisation’s systems or information.

Security control 1297 was amended to note that it relates to the access of an organisation’s systems or information.

Security Control: 1297; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
Legal advice is sought prior to allowing privately-owned mobile devices to access official or classified systems or information.

Minor update to ‘organisation-owned mobile devices’ content to note that it relates to the access of an organisation’s systems or information.

Security control 1482 was amended to note that it relates to the access of an organisation’s systems or information.

Security Control: 1482; Revision: 3; Updated: Aug-20; Applicability: O, P, S, TS
Personnel accessing official or classified systems or information using an organisation-owned mobile device use an ACSC approved platform with a security configuration in accordance with ACSC guidance.

Minor update to ‘further information’ content.

Update to website address in ‘further information’ content.

Mobile device usage

Update to website address in ‘further information’ content.

Guidelines for Evaluated Products

Evaluated product acquisition

Updates to website addresses in ‘further information’ content.

Evaluated product usage

Minor update to ‘further information’ content.

Guidelines for ICT Equipment

Change of chapter title to ‘Guidelines for ICT Equipment’.

ICT equipment usage

Introduction of new guidance on the handling of ICT equipment that contains media.

Security control 1599 was introduced to ensure ICT equipment is protected based upon the sensitivity or classification of information that it displays, processes, stores or communicates.

Security Control: 1599; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
ICT equipment is handled in a manner suitable for its sensitivity or classification.

Minor update to ‘further information’ content.

ICT equipment maintenance and repairs

Introduction of new ‘inspection of ICT equipment following maintenance and repairs’ content.
Security control 1598 was introduced to ensure that ICT equipment is assessed for any unauthorised modifications or changes to its approved software configuration following maintenance or repair activities.

**Security Control: 1598; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS**

Following maintenance or repair activities for ICT equipment, the ICT equipment is inspected to confirm it retains its approved software configuration and that no unauthorised modifications have taken place.

- Minor update to ‘further information’ content.

**ICT equipment sanitisation and disposal**

- Minor update to ‘further information’ content.

**Guidelines for Media**

- Change of chapter title to ‘Guidelines for Media’.

**Media usage**

- Security control 1600 was introduced to ensure that media is sanitised before it used for the first time with systems.

  **Security Control: 1600; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS**

  Media is sanitised before it is used with systems for the first time.

- Amendments were made to the ‘using media for data transfers’ content to cover the sanitisation of rewritable media when used for manual data transfers.

- Security control 0947 was moved from the media sanitisation section and amended to cover situations where rewritable media is used for manual data transfers between systems belonging to different security domains.

  **Security Control: 0947; Revision: 5; Updated: Jun-20; Applicability: O, P, S, TS**

  If not using write-once media for transferring data manually between two systems belonging to different security domains, the media is sanitised between each data transfer.

- Minor updates to ‘further information’ content.

**Media sanitisation**

- The ‘sanitising media prior to reuse’ content was removed.

- Security control 0947 was moved to the media usage section of the chapter.

- Minor update to ‘further information’ content.

- Update to website address in ‘further information’ content.

**Media destruction**

- Update to ‘media destruction equipment’ content to reference the National Security Agency’s *Evaluated Products List for Magnetic Degaussers* and remove the reference to the National Cyber Security Centre’s list of certified degaussers.

- Security control 1160 was modified to remove reference to the National Cyber Security Centre’s list of certified degaussers.

  **Security Control: 1160; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS**

  If using degaussers to destroy media, degaussers evaluated by the United States’ National Security Agency are used.
• Minor updates to ‘further information’ content.
• Update to website address in ‘further information’ content.

Media disposal

• Minor update to ‘further information’ content.

Guidelines for System Hardening

Operating system hardening

• New ‘Standard Operating Environments’ content was added.
• Security control 1406 from previous releases of the ISM was reintroduced and modified to focus on the development of SOEs for workstations and servers.

  Security Control: 1406; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
  SOEs are developed for workstations and servers.

• Security control 1608 was introduced to ensure that when organisations use SOEs that are provided by third parties they scan them for malicious content and configurations before they are used.

  Security Control: 1608; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  SOEs provided by third parties are scanned for malicious content or configurations before being used.

• Security control 1588 was introduced to ensure that SOEs are reviewed and updated at least annually.

  Security Control: 1588; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  SOEs are reviewed and updated at least annually.

• Security control 1584 was introduced to ensure that standard users as prevented from bypassing, disabling or modifying security functionality in operating systems.

  Security Control: 1584; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  Standard users are prevented from bypassing, disabling or modifying security functionality of operating systems.

• The ‘application management’ content was amended to capture scenarios in which standard users could be allowed to install vetted and approved applications from organisation-managed software repositories or from trusted application marketplaces.

• Security control 1592 was introduced to ensure that users are only prevented from installing unapproved applications, thereby allowing for the installation of applications from approved software repositories and marketplaces.

  Security Control: 1592; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  Users do not have the ability to install unapproved software.

• Security control 0382 was modified to remove the recommendation that users not have the ability to install software.

  Security Control: 0382; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
  Users do not have the ability to uninstall or disable approved software.

• Security control 1582 was introduced to ensure that cryptographic hash rules, publisher certificate rules and path rules used for application control are validated at least annually.

  Security Control: 1582; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Cryptographic hash rules, publisher certificate rules and path rules used for application control are validated at least annually.

- Minor update to ‘Enhanced Mitigation Experience Toolkit and exploit protection’ content.
- Minor update to ‘antivirus software’ content to fix grammar error.
- The ‘endpoint device control software’ was amended slightly to provide an example of why such software might be used.
- Minor update to ‘further information’ content.
- Addition of reference to the ACSC’s new *Hardening Microsoft Windows 10 version 1909 Workstations* publication within the ‘further information’ content.
- Updates to website addresses in ‘further information’ content.

**Application hardening**

- Security control 1601 was introduced to ensure that Microsoft’s Attack Surface Reduction rules are implemented.
  
  *Security Control: 1601; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS*
  
  If supported, Microsoft’s Attack Surface Reduction rules are implemented.

- Security control 1585 was introduced to ensure that standard users are prevented from bypassing, disabling or modifying security functionality in applications.
  
  *Security Control: 1585; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS*
  
  Standard users are prevented from bypassing, disabling or modifying security functionality of applications.

- Minor update to ‘further information’ content.
- Updates to website addresses in ‘further information’ content.

**Authentication hardening**

- Minor update to ‘account types’ content.
- Introduction of ‘authentication types’ content.

- Security control 1596 was introduced to prevent the sharing of passwords/passphrases used for single-factor authentication across different systems.
  
  *Security Control: 1596; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS*
  
  Passphrases used for single-factor authentication can not be used to authenticate to multiple different systems.

- Security control 1384 was moved across from the system administration section of the *Guidelines for System Management* and modified slightly.
  
  *Security Control: 1384; Revision: 3; Updated: Aug-20; Applicability: O, P, S, TS*
  
  Multi-factor authentication is used to authenticate privileged users each time they perform privileged actions.

- New ‘setting and resetting credentials’ content was introduced to address the previous lack of guidance on how to provide credentials to users if they are reset on their behalf.

- Security control 1227 was amended to recommend that when setting or resetting passwords/passphrases that they be randomly generated.
  
  *Security Control: 1227; Revision: 4; Updated: Aug-20; Applicability: O, P, S, TS*
  
  Passwords/passphrases set or reset on users’ behalf are randomly generated.
Security controls 1593, 1594 and 1595 were introduced to ensure that users provide sufficient evidence to verify their identity when collecting account credentials, that those credentials are provided to them in a secure manner and that they are changed upon first use.

**Security Control:** 1593; **Revision:** 0; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Users provide sufficient evidence to verify their identity when collecting a password/passphrase for their account.

**Security Control:** 1594; **Revision:** 0; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Passwords/passphrases are provided to users via a secure communications channel or, if not possible, split into parts with part being provided to the user and part provided to the user’s supervisor.

**Security Control:** 1595; **Revision:** 0; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Users that do not set their own initial password/passphrase are required to change it on first use.

The ‘account lockouts’ content was amended to note that alternative methods exist to reduce the risk of password spraying attacks beyond strict lockout functionality.

The ‘account unlocks’ content was amended to focus on processes associated with account unlocks – not password/passphrase resets.

Security control 0976 was amended to focus on account unlocks.

**Security Control:** 0976; **Revision:** 6; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Users provide sufficient evidence to verify their identity when requesting an account unlock.

The ‘unsecure authentication methods’ content was update to reference authentication methods susceptible to replay attacks.

Security control 1603 was introduced to cover disabling of authentication methods susceptible to replay attacks.

**Security Control:** 1603; **Revision:** 0; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Authentication methods susceptible to replay attacks are disabled.

The ‘protecting credentials’ content was amended to cover obscuring credentials when they are entered into systems in order to reduce risks associated with shoulder surfing and screen scraping.

Security control 1597 was introduced to ensure credentials are protected as they are entered into systems.

**Security Control:** 1597; **Revision:** 0; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Credentials are obscured as they are entered into systems.

Security control 1402 was amended to focus on the storage of credentials on systems.

**Security Control:** 1402; **Revision:** 5; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Stored passwords/passphrases are protected by ensuring they are hashed, salted and stretched.

Security control 1590 was introduced to cover scenarios in which password/passphrase changes should occur.

**Security Control:** 1590; **Revision:** 0; **Updated:** Aug-20; **Applicability:** O, P, S, TS
Passwords/passphrases are changed if:
- they are directly compromised
- they are suspected of being compromised
- they appear in online data breach databases
- they are discovered stored in the clear on a network
- they are discovered being transferred in the clear across a network
- membership of a shared account changes
they have not been changed in the past 12 months.

- New ‘session termination’ content was introduced to support both system patching activities and to assist in mitigating an adversary that has gained access to a user session but has failed to gain persistence.

- Security control 0853 was introduced to ensure that user sessions are terminated and workstations are rebooted after a defined period of inactivity outside of business hours.

  *Security Control: 0853; Revision: 1; Updated: Aug-20; Applicability: O, P, S, TS
  Outside of business hours, and after an appropriate period of inactivity, user sessions are terminated and workstations are rebooted.*

- Minor update to ‘logon banner’ content to include the system’s sensitivity or classification.

- Updates to website addresses in ‘further information’ content.

- Additional references added to ‘further information’ content to assist in the self-generation of strong passphrases.

**Virtualisation hardening**

- New section introduced to cover the use of hypervisors, containers and virtualised environments.

- New ‘containerisation’ content was added.

- Security control 1460, 1462 and 1461 were moved from the network design and configuration section of the *Guidelines for Networking*.

- Security control 1460 was split into 5 different security controls (i.e. 1460, 1604 1605, 1606 and 1607) to allow for sufficient focus on each aspect of hardening software-based isolation mechanisms.

  *Security Control: 1460; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
  When using a software-based isolation mechanism to share a physical server’s hardware, the isolation mechanism is from a vendor that uses secure coding practices and, when security vulnerabilities have been identified, develops and distributes patches in a timely manner.*

  *Security Control: 1604; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  When using a software-based isolation mechanism to share a physical server’s hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.*

  *Security Control: 1605; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  When using a software-based isolation mechanism to share a physical server’s hardware, the underlying operating system running on the server is hardened.*

  *Security Control: 1606; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  When using a software-based isolation mechanism to share a physical server’s hardware, patches are applied to the isolation mechanism and underlying operating system in a timely manner.*

  *Security Control: 1607; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  When using a software-based isolation mechanism to share a physical server’s hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.*

- New ‘further information’ content was added.
Guidelines for System Management

System administration

- Security control 1384 was moved to the authentication hardening section of the Guidelines for System Hardening.
- Minor updates to ‘further information’ content.
- Updates to website addresses in ‘further information’ content.

System patching

- Update to website address in ‘further information’ content.

Data backup and restoration

- Minor update to ‘testing restoration of backups’ content.
- Minor update to ‘further information’ content.

Guidelines for System Monitoring

Event logging and auditing

- Update to ‘event logging policy’ content.
- Security control 0582 was amended to including the capture of data transfers from external media.

Security Control: 0582; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
The following events are logged for operating systems:

- access to important data and processes
- application crashes and any error messages
- attempts to use special privileges
- changes to accounts
- changes to security policy
- changes to system configurations
- Domain Name System (DNS) and Hypertext Transfer Protocol requests
- failed attempts to access data and system resources
- service failures and restarts
- system startup and shutdown
- transfer of data to and from external media
- user or group management
- use of special privileges.
- Update to ‘event log protection’ content.
Guidelines for Software Development

Application development

- Minor change to ‘development environments’ content.
- Security control 0400 was modified slightly.

  *Security Control: 0400; Revision: 5; Updated: Aug-20; Applicability: O, P, S, TS*
  *Development, testing and production environments are segregated.*

- Minor changes to ‘software testing’ content.
- New ‘vulnerability disclosure program’ content was added.
- Security control 1616 was introduced to recommend the use of a vulnerability disclosure program to assist with the security development and maintenance of products and services.

  *Security Control: 1616; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS*
  *A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.*

- Minor changes to ‘further information’ content.
- Update to website address in ‘further information’ content.
- Addition of references for vulnerability disclosure programs added to ‘further information’ content.

Web application development

- Minor update to ‘further information’ content.
- Updates to website addresses in ‘further information’ content.

Guidelines for Database Systems

- Change of chapter title to ‘Guidelines for Database Systems’.

Database servers

- Minor update to ‘further information’ content.

Guidelines for Email

- Change of chapter title to ‘Guidelines for Email’.

Email gateways and servers

- The ‘email server transport encryption’ content was modified to capture Mail Transfer Agent Strict Transport Security (MTA-STS).
- Security control 1589 was introduced to ensure MTA-STS is implemented for email servers.

  *Security Control: 1589; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS*
  *MTA-STS, as defined in IETF RFC 8461, is enabled to prevent the transfer of unencrypted emails between complying servers.*

- Updates to website addresses in ‘further information’ content.
• Updates to ‘further information’ content to include links to additional reading on IETF RFC 8461.

Guidelines for Networking

• Change of chapter title to ‘Guidelines for Networking’.

Network design and configuration

• Minor changes to ‘network segmentation and segregation’ content.
• Security controls 1460, 1462 and 1461 were moved to the new virtualisation hardening section of the Guidelines for System Hardening.
• Security control 1028 was modified slightly.
  Security Control: 1028; Revision: 7; Updated: Aug-20; Applicability: O, P, S, TS
  NIDS or NIPS are deployed in all gateways between an organisation’s networks and other networks they do not manage.
• Minor updates to ‘further information’ content.
• Update to website address in ‘further information’ content.

Wireless networks

• Minor update to ‘generating and issuing certificates for authentication’ content.
• Minor update to ‘further information’ content.

Guidelines for Cryptography

• Change of chapter title to ‘Guidelines for Cryptography’.

Cryptographic fundamentals

• Updates to website addresses in ‘further information’ content.

ASD Approved Cryptographic Algorithms

• Updates to website addresses in ‘further information’ content.

ASD Approved Cryptographic Protocols

• Minor update to ‘further information’ content.

Transport Layer Security

• Minor update to ‘further information’ content.
• Introduction of ‘further information’ content to direct readers to the ACSC’s Implementing Certificates, TLS and HTTPS publication.

Guidelines for Gateways

• Change of chapter title to ‘Guidelines for Gateways’.
Gateways

- Minor updates to ‘further information’ content.

Cross Domain Solutions

- Minor updates to ‘further information’ content.
- Updates to website addresses in ‘further information’ content.

Guidelines for Data Transfers

Data transfers

- Update to ‘monitoring data import and export’ content.
- Security control 1586 was introduced to ensure authorised data imports and exports for systems are captured in data transfer logs.

  Security Control: 1586; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
  Data transfer logs are used to record all data imports and exports from systems.

- Security controls 1294 and 0660 were amended to capture both data imports and data exports. As such, security control 1295 and 0673 were removed.

  Security Control: 1294; Revision: 3; Updated: Aug-20; Applicability: O, P
  Data transfer logs are partially audited at least monthly.

  Security Control: 0660; Revision: 7; Updated: Aug-20; Applicability: S, TS
  Data transfer logs are fully audited at least monthly.

- Minor updates to ‘further information’ content.

Cyber Security Terminology

Glossary of cyber security terms

- Additional of ‘interactive authentication’ and ‘non-interactive authentication’ definitions.

Please note: There is no requirement for organisations to be compliant with every monthly update 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. Further information on applying the ISM can be found in the Using the Australian Government Information Security Manual chapter.