Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information security manual

Last updated: March 2025

March 2025 changes

A summary of the content changes for the latest update of the *Information security manual* (ISM) are covered below.

Guidelines for cybersecurity roles

Embedding cybersecurity

A new control was added recommending that *the board of directors or executive committee defines clear roles and responsibilities for cybersecurity both within the board of directors or executive committee and broadly within their organisation*. **[ISM-1997]**

A new control was added recommending that *the board of directors or executive committee ensures that cybersecurity is integrated throughout all business functions within their organisation*. **[ISM-1998]**

A new control was added recommending that *the board of directors or executive committee ensures the cybersecurity strategy for their organisation is aligned with the overarching strategic direction and business strategy for their organisation*. **[ISM-1999]**

A new control was added recommending that *the board of directors or executive committee seeks regular briefings or reporting on the cybersecurity posture of their organisation, as well as the threat environment in which they operate, from internal and external subject matter experts*. **[ISM-2000]**

Championing a positive cybersecurity culture

A new control was added recommending that *the board of directors or executive committee champions a positive cybersecurity culture within their organisation, including through leading by example*. **[ISM-2001]**

Building cybersecurity expertise

A new control was added recommending that *the board of directors or executive committee maintains a sufficient level of cybersecurity literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations*. **[ISM-2002]**

A new control was added recommending that *the board of directors or executive committee maintains awareness of key cybersecurity recruitment activities, retention rates for cybersecurity personnel, and cybersecurity skills and experience gaps within their organisation*. **[ISM-2003]**

A new control was added recommending that *the board of directors or executive committee supports the development of cybersecurity skills and experience for all personnel via internal and external cybersecurity awareness raising and training opportunities*. **[ISM-2004]**

Identifying critical business assets

A new control was added recommending that *the board of directors or executive committee understands the business criticality of their organisation's systems, applications and data, including at least a basic understanding of what exists, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified*. **[ISM-2005]**

Planning for major cybersecurity incidents

A new control was added recommending that *the board of directors or executive committee plans for major cybersecurity incidents, including by participating in exercises, and understand their duties in relation to such cybersecurity incidents*. **[ISM-2006]**

Protecting systems and their resources

The existing control recommending that *system owners determine the type, value and security objectives for each system based on an assessment of the impact if it were to be compromised* was amended to recommend that system owners determine the system boundary, business criticality and security objectives for each system in consultation with the system's authorising officer. **[ISM-1633]**

The existing control recommending that *system owners select controls for each system and tailor them to achieve desired security objectives* was amended to recommend that this activity be conducted in consultation with the system's authorising officer. **[ISM-1634]**

The existing control recommending that *system owners ensure controls for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system and its operating environment undergo a security assessment by their organisation's own assessors or Infosec Registered Assessor Program (IRAP) assessors to determine if they have been implemented correctly and are operating as intended* was amended to recommend that this activity be conducted in consultation with the system's authorising officer. **[ISM-1636]**

The existing control recommending that *system owners ensure controls for each TOP SECRET system and its operating environment, including each sensitive compartmented information system and its operating environment, undergo a security assessment by ASD assessors (or their delegates) to determine if they have been implemented correctly and are operating as intended* was amended to recommend that this activity be conducted in consultation with the system's authorising officer. **[ISM-1967]**

Guidelines for physical security

Bringing medical devices into facilities

A new control was added recommending that *an authorised medical device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis*. **[ISM-2007]**

A new control was added recommending that *medical devices that are authorised to be brought into SECRET and TOP SECRET areas meet, at a minimum, the following criteria:*

- *are listed on the Australian Register of Therapeutic Goods*

- *have been prescribed by a legally qualified medical practitioner*
- *have been commercially purchased within Australia*
- *do not have inbuilt cellular connectivity*
- *are capable of operating independently of mobile devices*
- *where possible, have Wi-Fi, Bluetooth and other forms of wireless connectivity disabled when operating within SECRET and TOP SECRET areas*. **[ISM-2008]**

A new control was added recommending that *unauthorised medical devices are not brought into SECRET and TOP SECRET areas*. **[ISM-2009]**

Guidelines for cybersecurity documentation

Change and configuration management plan

The previously rescinded control on change management processes was reinstated and amended to cover the development of change and configuration management plans for systems, specifically: *Systems have a change and configuration management plan that includes:*

- *what constitutes routine and urgent changes to the configuration of systems*
- *how changes to the configuration of systems will be requested, tracked and documented*
- *who needs to be consulted prior to routine and urgent changes to the configuration of systems*
- *who needs to approve routine and urgent changes to the configuration of systems*
- *who needs to be notified of routine and urgent changes to the configuration of systems*
- *what additional change management and configuration management processes and procedures need be to followed before, during and after routine and urgent changes to the configuration of systems.* **[ISM-0912]**

Guidelines for information technology equipment

IT equipment selection

The existing control on the selection of IT equipment was rescinded due to duplication of an existing procurement control within the *Guidelines for procurement and outsourcing*. **[ISM-1857]**

Guidelines for system hardening

Host-based intrusion detection and response

The existing control recommending that *a HIPS is implemented on workstations* was amended to specify that either a HIPS or Endpoint Detection and Response (EDR) solution can be used. **[ISM-1341]**

The existing control recommending that *a HIPS is implemented on critical servers and high-value servers* was amended to specify that either a HIPS or EDR solution can be used. **[ISM-1034]**

Microsoft Active Directory Domain Services account hardening

A new control was added recommending that *service accounts configured with an SPN use the Advanced Encryption Standard for encryption*. **[ISM-2010]**

Multi-factor authentication

A new control was added recommending that *when phishing-resistant multi-factor authentication is used by user accounts, other non-phishing-resistant multi-factor authentication options are disabled for such user accounts*. **[ISM-2011]**

Session locking

The existing control recommending that *systems are configured with a session or screen lock that […]* was amended to focus exclusively on session locking. This includes new recommendations that a maximum of 12 hours overall be adopted before session locking occurs (i.e. before forced re-authentication) and that users use all authentication factors when re-authenticating a session. **[ISM-0428]**

Screen locking

A new control was added recommending that *systems are configured with a screen lock that […]*. This control was split from ISM-0428 with the addition of a new recommendation that users use all authentication factors when re-authenticating to unlock a system. **[ISM-2012]**

Guidelines for system management

System administration processes and procedures

The existing control recommending that *system administrators document requirements for administrative activities, consider potential security impacts, obtain any necessary approvals, notify users of any disruptions or outages, and maintain system and security documentation* was amended to *system administrators perform system administration activities in accordance with the system's change and configuration management plan*. **[ISM-1211]**

Guidelines for software development

Development, testing, staging and production environments

The existing control recommending that *development, testing and production environments are segregated* was amended to include staging environments. **[ISM-0400]**

The existing control recommending that *data from production environments is not used in a development or testing environment unless the environment is secured to the same level as the production environment* was amended to instead refer to any non-production environment that isn't secured to at least the same level as the production environment. **[ISM-1420]**

Secure software development

The existing control recommending that *files containing executable content are digitally signed as part of software development* was amended to recommend the use of a certificate with a verifiable chain of trust. **[ISM-1796]**

Network application programming interfaces

The existing control recommending that *authentication and authorisation of clients is performed when clients call web APIs that facilitate modification of data* was amended to refer to network APIs that are accessible over the internet. **[ISM-1818]**

A new control was added recommending that *authentication and authorisation of clients is performed when clients call network APIs that facilitate modification of data but are not accessible over the internet*. **[ISM-2013]**

The existing control recommending that *authentication and authorisation of clients is performed when clients call web APIs that facilitate access to data not authorised for release into the public domain* was amended to refer to network APIs that are accessible over the internet. **[ISM-1817]**

A new control was added recommending that *authentication and authorisation of clients is performed when clients call network APIs that facilitate access to data not authorised for release into the public domain but are not accessible over the internet*. **[ISM-2014]**

The existing control recommending that *web API calls that facilitate modification of data, or access to data not authorised for release into the public domain, are centrally logged* was amended to refer to network APIs that are accessible over the internet. **[ISM-1910]**

A new control was added recommending that *network API calls that facilitate modification of data, or access to data not authorised for release into the public domain, but are not accessible over the internet, are centrally logged*. **[ISM-2015]**

Software input handling

The existing control recommending that *validation or sanitisation is performed on all input handled by web applications* was amended to refer to input received over the internet by software. **[ISM-1240]**

A new control was added recommending that *validation or sanitisation is performed on all input received over a local network by software*. **[ISM-2016]**

Web security policy response headers

The existing control recommending that *web applications implement Content-Security-Policy, HSTS and X-Frame-Options via security policy in response headers* was amended to refer to web server software instead. **[ISM-1424]**

Software interaction with databases

The existing control recommending that *all queries to databases from web applications are filtered for legitimate content and correct syntax* was amended to expand its applicability from web applications to all applications. **[ISM-1275]**

The existing control recommending that *parameterised queries or stored procedures, instead of dynamically generated queries, are used by web applications for database interactions* was amended to expand its applicability from web applications to all applications. **[ISM-1276]**

The existing control recommending that *web applications are designed or configured to provide as little error information as possible about the structure of databases* was amended to expand its applicability from web applications to all applications. **[ISM-1278]**

The existing control recommending that *all queries to databases from web applications that are initiated by users, and any resulting crash or error messages, are centrally logged* was amended to expand its applicability from web applications to all applications. **[ISM-1536]**

Software event logging

The existing control recommending that *web application crashes and error messages are centrally logged* was amended to expand its applicability from web applications to all applications. **[ISM-1911]**

Guidelines for database systems

Segregation of development, testing, staging and production database servers

The existing control recommending that *development and testing environments do not use the same database servers as production environments* was amended to include staging environments. **[ISM-1273]**

Segregation of development, testing, staging and production databases

The existing control recommending that *database contents from production environments are not used in development or testing environments unless the environment is secured to the same level as the production environment* was amended to instead refer to any non-production environment that isn't secured to at least the same level as the production environment. **[ISM-1274]**

Guidelines for networking

Encrypted Domain Name System Services

A new control was added recommending that *DNS traffic is encrypted by clients and servers wherever supported*. **[ISM-2017]**

Guidelines for gateways

Border Gateway Protocol routing security

A new control was added recommending that *routes for RPKI-registered IP addresses that are advertised from invalid Autonomous Systems, or that are longer than allowed, are rejected or deprioritised by routers that exchange routes via BGP*. **[ISM-2018]**

Assessment of gateways

The existing control recommending that *gateways undergo a security assessment by an IRAP assessor at least every 24 months* was amended to align with recommendations for outsourced gateway services at SECRET and below, i.e. that the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release) is used for the IRAP assessment. **[ISM-0100]**

A new control was added recommending that *TOP SECRET gateways undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the assessment (or a subsequent release), at least every 24 months*. **[ISM-2019]**

Miscellaneous

References to ‘cyber security’ were changed to ‘cybersecurity’ to align with Australia’s national dictionary. **[ISM-0039, ISM-0043, ISM-0109, ISM-0120, ISM-0123, ISM-0125, ISM-0140, ISM-0141, ISM-0252, ISM-0576, ISM-0714, ISM-0717, ISM-0718, ISM-0720, ISM-0724, ISM-0725, ISM-0726, ISM-0732, ISM-0733, ISM-0735, ISM-1228, ISM-1478, ISM-1526, ISM-1617, ISM-1618, ISM-1784, ISM-1803, ISM-1906, ISM-1907, ISM-1918, ISM-1960, ISM-1961, ISM-1970, ISM-1986, ISM-1987]**

References to ‘cyber threat(s)’ were changed to ‘cyberthreat(s)’ to align with Australia’s national dictionary. **[ISM-1526, ISM-1617]**

References to ‘security documentation’ were changed to ‘cybersecurity documentation’. **[ISM-0047, ISM-0888]**

References to ‘application development’ were changed to ‘software development’. **[ISM-0401, ISM-1238, ISM-1780, ISM-1796, ISM-1797, ISM-1798]**

A number of existing controls were reworded for clarity without changing their intent. **[ISM-0383, ISM-0401, ISM-0402, ISM-0718, ISM-0866, ISM-0938, ISM-1271, ISM-1304, ISM-1460, ISM-1568, ISM-1632, ISM-1644, ISM-1743, ISM-1754, ISM-1806, ISM-1826, ISM-1882, ISM-1908]**

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate