Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information Security Manual

Last updated: December 2024

December 2024 Changes

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

Using the Information Security Manual

Select controls

The 'NC' applicability marking has been introduced for controls applicable to non-classified systems used by either government or non-government entities. In doing so, the 'All' applicability that previously captured such systems has been replaced by the 'NC, OS, P, S, TS' applicability marking. Note, government entities operating non-classified systems can continue to refer to them as OFFICIAL systems.

Guidelines for Cyber Security Roles

Overseeing the cyber security program

A new control was added recommending that *the CISO develops, implements, maintains and verifies on a regular basis a register of systems used by their organisation*. **[ISM-1966]**

Protecting systems and their resources

The existing control recommending that *system owners ensure controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended* was split into two controls to clearly articulate that non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET systems can be assessed by an organisation's own assessors or an IRAP assessor while TOP SECRET systems, including sensitive compartmented information systems, need to be assessed by ASD assessors (or their delegates). **[ISM-1636, ISM-1967]**

The existing control recommending that *system owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation* was split into two controls to clearly articulate that only Director-General ASD (or their delegate) can accept security risks associated with the operation of TOP SECRET systems, including sensitive compartmented information systems.
[ISM-0027, ISM-1968]

Guidelines for Cyber Security Incidents

Handling and containing malicious code infections

A new control was added recommending that *malicious code, when stored or communicated, is treated beforehand to prevent accidental execution*. **[ISM-1969]**

A new control was added recommending that *malicious code processed for cyber security incident response or research purposes is done so in a dedicated analysis environment that is segregated from other systems*. **[ISM-1970]**

Guidelines for Procurement and Outsourcing

Assessment of managed service providers

The existing control recommending that *managed service providers and their managed services undergo a security assessment by an IRAP assessor at least every 24 months* was amended to specify that this recommendation relates to non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET managed services. In addition, the recommendation was amended to specify that the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release) needs to be used. **[ISM-1793]**

A new control was added recommending that *managed service providers and their TOP SECRET managed services, including sensitive compartmented information managed services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months*. **[ISM-1971]**

Assessment of outsourced cloud service providers

The existing control recommending that *outsourced cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months* was amended to specify that this recommendation relates to non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET cloud services. In addition, the recommendation was amended to specify that the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release) needs to be used. **[ISM-1570]**

A new control was added recommending that *outsourced cloud service providers and their TOP SECRET cloud services, including sensitive compartmented information cloud services, undergo a security assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security assessment (or a subsequent release), at least every 24 months*. **[ISM-1972]**

Guidelines for Physical Security

Physical access to systems

A new control was added recommending that *non-classified systems are secured in suitably secure facilities*. **[ISM-1973]**

The existing control recommending that *systems are secured in facilities that meet the requirements for a security zone suitable for their classification* was amended to specify that this recommendation relates to classified systems. **[ISM-0810]**

Physical access to servers, network devices and cryptographic equipment

A new control was added recommending that *non-classified servers, network devices and cryptographic equipment are secured in suitably secure server rooms or communications rooms*. **[ISM-1974]**

The existing control recommending that *servers, network devices and cryptographic equipment are secured in server rooms or communications rooms that meet the requirements for a security zone suitable for their classification* was amended to specify that this recommendation relates to classified servers, network devices and cryptographic equipment. **[ISM-1053]**

A new control was added recommending that *non-classified servers, network devices and cryptographic equipment are secured in suitably secure security containers*. **[ISM-1975]**

The existing control recommending that *servers, network devices and cryptographic equipment are secured in security containers or secure rooms suitable for their classification taking into account the combination of security zones they reside in* was amended to specify that this recommendation relates to classified servers, network devices and cryptographic equipment. In addition, the control was amended to remove the reference to secure rooms. **[ISM-1530]**

The existing control recommending that *server rooms, communications rooms, security containers and secure rooms are not left in unsecured states* was amended to remove the reference to secure rooms. **[ISM-0813]**

The existing control recommending that *keys or equivalent access mechanisms to server rooms, communications rooms, security containers and secure rooms are appropriately controlled* was amended to remove the reference to secure rooms. **[ISM-1074]**

Guidelines for Communications Infrastructure

Cable colours

The existing control recommending that *OFFICIAL: Sensitive and PROTECTED cables are coloured neither salmon pink nor red* was expanded to include non-classified cables. **[ISM-0926]**

Cable inspectability

The existing control recommending that *cables are inspectable at a minimum of five-metre intervals* was amended to clarify that cables should be inspectable every five-metres or less. **[ISM-1112]**

Wall outlet box colours

The existing control recommending that *OFFICIAL: Sensitive and PROTECTED wall outlet boxes are coloured neither salmon pink nor red* was expanded to include non-classified wall outlet boxes. **[ISM-1107]**

Emanation security threat assessments

The existing control recommending that *system owners deploying OFFICIAL: Sensitive or PROTECTED systems with radio frequency transmitters (including any wireless capabilities) that will be located within 20 meters of SECRET or TOP SECRET systems contact ASD for an emanation security threat assessment* has been rescinded. **[ISM-0248]**

Existing controls relating to emanation security threat assessments, that included OFFICIAL: Sensitive and PROTECTED systems within their scope, have been re-scoped to apply exclusively to SECRET and TOP SECRET systems. **[ISM-0246, ISM-1885]**

Guidelines for Communications Systems

Speakerphones

The existing control recommending that *speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in an audio secure room, the room is audio secure during conversations and only personnel involved in conversations are present in the room* was expanded to include non-classified telephone systems. **[ISM-0235]**

Off-hook audio protection

The existing control recommending that *in SECRET and TOP SECRET areas, push-to-talk handsets or push-to-talk headsets are used to meet any off-hook audio protection requirements* was expanded to include non-classified telephone systems. **[ISM-0931]**

Microphones and webcams

The existing control recommending that *microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas* was expanded to include non-classified workstations. **[ISM-0559]**

The existing control recommending that *microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas* was expanded to include non-classified workstations. **[ISM-1450]**

Guidelines for Enterprise Mobility

Using Bluetooth functionality

Existing controls relating to the use of Bluetooth functionality with OFFICIAL: Sensitive and PROTECTED mobile devices were expanded to include non-classified mobile devices. **[ISM-1196, ISM-1198, ISM-1199, ISM-1200]**

Guidelines for System Hardening

Operating system event logging

A new control was added recommending that *security-relevant events for Apple macOS operating systems are centrally logged*. **[ISM-1976]**

A new control was added recommending that *security-relevant events for Linux operating systems are centrally logged*. **[ISM-1977]**

The existing control recommending that *security-relevant events for operating systems are centrally logged, including […]* was simplified and re-scoped to Microsoft Windows operating systems. **[ISM-0582]**

Microsoft Office macros

The existing control recommending that *allowed and blocked Microsoft Office macro execution events are centrally logged* was rescinded. **[ISM-1677]**

Server application event logging

A new control was added recommending that *security-relevant events for server applications on internet-facing servers are centrally logged*. **[ISM-1978]**

A new control was added recommending that *security-relevant events for server applications on non-internet-facing servers are centrally logged*. **[ISM-1979]**

Protecting credentials

A new control was added recommending that *credential hint functionality is not used for systems*. **[ISM-1980]**

The existing control recommending that *credentials are kept separate from systems they are used to authenticate to, except for when performing authentication activities* was amended to reflect that the control relates to physical credentials, such as written down memorised secrets, security keys, smart cards and one-time password tokens. **[ISM-0418]**

Guidelines for System Management

Software register

The existing control recommending that *software registers for workstations, servers, network devices and other IT equipment are developed, implemented, maintained and verified on a regular basis* was amended to re-scope 'other IT equipment' to 'networked IT equipment'. **[ISM-1493]**

Cessation of support

The existing control recommended that *network devices and other IT equipment that are no longer supported by vendors are replaced* was split into three controls focusing on internet-facing network devices, non-internet-facing network devices and networked IT equipment. **[ISM-1753, ISM-1981, ISM-1982]**

The existing control recommending that *when applications, operating systems, network devices or other IT equipment that are no longer supported by vendors cannot be immediately removed or replaced, compensating controls are implemented until such time that they can be removed or replaced* was amended to re-scope 'other IT equipment' to 'networked IT equipment'. **[ISM-1809]**

Guidelines for System Monitoring

Centralised event logging facility

The existing control recommended that *a centralised event logging facility is implemented and event logs are sent to the facility as soon as possible after they occur* was split into two controls. **[ISM-1405, ISM-1983]**

A new control was added recommending that *event logs sent to a centralised event logging facility are encrypted in transit*. **[ISM-1984]**

A new control was added recommending that *event logs are protected from unauthorised access*. **[ISM-1985]**

Event log monitoring

A new control was added recommending that *event logs from critical servers are analysed in a timely manner to detect cyber security events*. **[ISM-1986]**

A new control was added recommending that *event logs from security products are analysed in a timely manner to detect cyber security events*. **[ISM-1987]**

Event log retention

The existing control recommending that *event logs, excluding those for Domain Name System services and web proxies, are retained for at least seven years* was rescinded. **[ISM-0859]**

The existing control recommending that *event logs for Domain Name System services and web proxies are retained for at least 18 months* was rescinded. **[ISM-0991]**

A new control was added recommending that *event logs are retained in a searchable manner for at least 12 months*. **[ISM-1988]**

A new control was added recommending that *event logs are retained as per minimum retention requirements for various classes of records as set out by the National Archives of Australia's Administrative Functions Disposal Authority Express (AFDA Express) Version 2 publication*. **[ISM-1989]**

Guidelines for Networking

Network access controls

The existing control recommending that *network access controls are implemented on networks to prevent the connection of unauthorised network devices and other IT equipment* was amended to re-scope 'other IT equipment' to 'networked IT equipment'. **[ISM-0520]**

Guidelines for Cryptography

ASD-Approved Cryptographic Algorithms

The following cryptographic algorithms have been approved as ASD-Approved Cryptographic Algorithms and endorsed for the following purposes:

- Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for digital signatures
- Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) for encapsulating encryption session keys (and similar keys).

Clarification has been provided that Secure Hashing Algorithm 2 (SHA-2) is the only approved hashing algorithm for general purpose use. However, Secure Hashing Algorithm 3 (SHA-3), including its extendable-output functions (XOFs), has been approved exclusively for use within ML-DSA and ML-KEM.

Using Diffie-Hellman

The existing control recommending that *when using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used, preferably 3072 bits* was extended to the protection of non-classified data. **[ISM-0472]**

Using Elliptic Curve Diffie-Hellman

The existing control recommending that *when using ECDH for agreeing on encryption session keys, a base point order and key size of at least 224 bits is used, preferably the NIST P-384 curve* was extended to the protection of non-classified data. **[ISM-0474]**

Using the Elliptic Curve Digital Signature Algorithm

The existing control recommending that *when using ECDSA for digital signatures, a base point order and key size of at least 224 bits is used, preferably the P-384 curve* was extended to the protection of non-classified data. **[ISM-0475]**

Using post-quantum cryptographic algorithms

A new control was added recommending that *when using ML-DSA and ML-KEM, as per FIPS 204 and FIPS 203 respectively, adherence to pre-requisite FIPS publications is preferred*. **[ISM-1990]**

Using the Module-Lattice-Based Digital Signature Algorithm

A new control was added recommending that *when using ML-DSA for digital signatures, ML-DSA-65 or ML-DSA-87 is used, preferably ML-DSA-87*. **[ISM-1991]**

A new control was added recommending that *when using ML-DSA for digital signatures, the hedged variant is used whenever possible*. **[ISM-1992]**

A new control was added recommending that *pre-hashed variants of ML-DSA-65 and ML-DSA-87 are only used when the performance of default variants is unacceptable*. **[ISM-1993]**

A new control was added recommending that *when the pre-hashed variants of ML-DSA-65 and ML-DSA-87 are used, at least SHA-384 and SHA-512 respectively are used for pre-hashing*. **[ISM-1994]**

Using the Module-Lattice-Based Key Encapsulation Mechanism

A new control was added recommending that *when using ML-KEM for encapsulating encryption session keys (and similar keys), ML-KEM-768 or ML-KEM-1024 is used, preferably ML-KEM-1024*. **[ISM-1995]**

Using Rivest-Shamir-Adleman

The existing control recommending that *when using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 2048 bits is used, preferably 3072 bits* was extended to the protection of non-classified data. **[ISM-0476]**

Using Secure Hashing Algorithms

The existing control recommending that *when using SHA-2 for hashing, an output size of at least 224 bits is used, preferably SHA-384* was amended to 'preferably SHA-384 or SHA-512' and extended to the protection of non-classified data. **[ISM-1766]**

The existing control recommending that *when using SHA-2 for hashing, an output size of at least 256 bits is used, preferably SHA-384* was amended to 'preferably SHA-384 or SHA-512'. **[ISM-1767]**

The existing control recommending that *when using SHA-2 for hashing, an output size of at least 384 bits is used, preferably SHA-384* was amended to 'preferably SHA-384 or SHA-512'. **[ISM-1768]**

Using symmetric cryptographic algorithms

The existing control recommending that *when using AES for encryption, AES-128, AES-192 or AES-256 is used, preferably AES-256* was extended to the protection of non-classified data. **[ISM-1769]**

Transitioning to post-quantum cryptography

The existing control recommending that *future cryptographic requirements and dependencies are considered during the transition to post-quantum cryptographic standards* was replaced with a recommendation that *the development and procurement of new cryptographic equipment and software ensures support for the use of ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030*. **[ISM-1917]**

Post-quantum traditional hybrid schemes

A new control was added recommending that *when a post-quantum traditional hybrid scheme is used, either the post-quantum cryptographic algorithm, the traditional cryptographic algorithm or both are AACAs*. **[ISM-1996]**

Miscellaneous

References to 'accounts' were changed to 'user accounts' in order to more closely match Microsoft Active Directory account types (i.e. 'users' and 'computers').
[ISM-0380, ISM-0383, ISM-1146, ISM-1247, ISM-1249, ISM-1250, ISM-1260, ISM-1304, ISM-1403, ISM-1554, ISM-1555, ISM-1556, ISM-1806]

A number of existing controls were reworded for increased clarity without changing their intent.
[ISM-0421, ISM-0477, ISM-1400, ISM-1482, ISM-1559, ISM-1607, ISM-1765]

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 cyber security incident, contact us:

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

Australian Government

Australian Signals Directorate