



Information security manual

September 2026 changes

Last updated: September 2026

Guidelines for cyber security incidents

Handling and containing intrusions

The existing security control recommending the use of a separate system for planning and coordination of intrusion remediation activities to the system which has been compromised, was amended to recommend using trusted systems separate from a compromised system. **[ISM-1731]**

The existing security control recommending all intrusion activities be conducted in the same planned outage window was amended to recommend intrusion remediation activities be coordinated and sequenced to minimise opportunities for re-compromise of a system while balancing operational risk and business continuity requirements. **[ISM-1732]**

The existing security control recommending the capture of full network traffic for at least seven days following intrusion remediation activities was amended to recommend conducting enhanced monitoring until there is sufficient evidence-based confidence that malicious actors have been eradicated from a system and have not re-established access. **[ISM-1213]**

Guidelines for procurement and outsourcing

Access to systems by service providers

A new security control was introduced recommending access by a service provider to an organisation's systems be restricted to remote management tools, source network addresses and time windows explicitly approved by the organisation. **[ISM-2124]**

The existing security control recommending an organisation be immediately notified if their systems are accessed or administered by a service provider in an unauthorised manner was amended to recommend such events be treated as a cyber security incident. **[ISM-1576]**

A new security control was introduced recommending all access to an organisation's systems by a service provider be independently logged by the organisation in a manner that the service provider cannot modify

or delete, and analysed in a timely manner to detect any anomalous, unexpected or unauthorised activity. **[ISM-2125]**

Guidelines for personnel security

Synthetic impersonation

A new security control was introduced recommending personnel dealing with banking details, payment requests or user account details be advised that voice and video communications can be synthetically generated and that individuals requesting changes to banking details, transfers of funds or modifications to user account details need to be positively identified using a pre-established authentication method or independent trusted communication channel. **[ISM-2126]**

Guidelines for system hardening

Hardening operating system configurations

A new security control was introduced recommending digital signature verification functionality for drivers be enforced before they are loaded. **[ISM-2127]**

A new security control was introduced recommending the ability to install, load or modify kernel-mode code, including drivers, kernel modules and extensions, be limited to privileged users who require such abilities as part of their duties or functions. **[ISM-2128]**

Windows Management Instrumentation

A new security control was introduced recommending WMI activity, including the creation of permanent event subscriptions, be centrally logged. **[ISM-2129]**

Artificial intelligence applications

The existing security control recommending AI applications are configured to flag organisationally defined risky actions for human approval prior to their execution was amended to recommend AI applications be configured to require human approval before executing sensitive or high-impact actions. **[ISM-2113]**

Microsoft Active Directory Services

A number of existing security controls referencing Microsoft AD CS CA servers were amended to reference Microsoft AD CS servers instead. **[ISM-1830, ISM-1926, ISM-1927, ISM-1928]**

Microsoft Active Directory Domain Services account hardening

The existing security control recommending at least an annual review of user accounts with DCSync permissions was amended to recommend a review at least every six months. **[ISM-1934]**

Microsoft Active Directory Certificate Services

The existing security control recommending CA Certificate Manager approval be required for certificate templates that allow a Subject Alternative Name to be supplied was amended without changing its intent. **[ISM-1948]**

A new security control was introduced recommending web-based enrolment interfaces for Microsoft AD CS servers be disabled unless required, and where enabled, be configured to require HTTPS and Extended Protection for Authentication. **[ISM-2130]**

A new security control was introduced recommending certificate templates be reviewed at least every three months to identify and remediate misconfigurations that could enable privilege escalation or unauthorised certificate enrolment. **[ISM-2131]**

A new security control was introduced recommending certificate enrolment events, including successful and unsuccessful requests and changes to certificate templates or Microsoft AD CS configurations, be centrally logged. **[ISM-2132]**

Guidelines for system access

Artificial intelligence agent identification

A new security control was introduced recommending each AI agent be assigned a unique identity that is distinct from the user accounts of personnel and the identities of other AI agents. **[ISM-2133]**

Artificial intelligence agent register

A new security control was introduced recommending an AI agent register be developed, implemented, maintained and regularly verified. **[ISM-2134]**

A new security control was introduced recommending an AI agent register contain the following for each AI agent: its unique identifier; its owner and business purpose; the identities assigned to it; any user accounts and credentials it uses; the tools, permissions and data repositories it can access. **[ISM-2135]**

Authenticating to systems

A new security control was introduced recommending risk-based access decisions, informed by contextual signals, be enforced for access to systems and their resources. **[ISM-2136]**

Third-party application access and device code authentication

A new security control was introduced recommending human users be prevented from granting consent to third-party OAuth applications, with such consent granted only by an authorised administrator. **[ISM-2137]**

A new security control was introduced recommending OAuth application consents, including their granted permissions, be reviewed at least every six months, with unused applications and excessive permissions revoked. **[ISM-2138]**

A new security control was introduced recommending consent grants, token issuance and token use for third-party OAuth applications be centrally logged. **[ISM-2139]**

A new security control was introduced recommending the OAuth device code authentication flow be disabled unless required, and where required, be restricted to authorised user accounts and managed devices. **[ISM-2140]**

Setting credentials for user accounts

The existing security control recommending human users provide sufficient evidence to verify their identity when requesting credentials was amended to capture when first requesting credentials, when requesting the reset of any credentials, when requesting the temporary disabling of any credentials, and when requesting the enrolment or re-enrolment of any credentials. **[ISM-1593]**

Application and workload credentials

A new security control was introduced recommending applications and workloads use short-lived dynamically issued credentials in preference to long-lived static credentials. **[ISM-2141]**

A new security control was introduced recommending static credentials used by applications and workloads be centrally managed using a credential or secrets management solution. **[ISM-2142]**

A new security control was introduced recommending applications and workloads use unique credentials that are not shared with other applications or workloads, or across development, testing, staging and production environments. **[ISM-2143]**

Changing credentials

The existing security control recommending credentials for user accounts are changed if they are discovered stored on networks in the clear was amended to expand the scope from networks to systems. **[ISM-1590]**

A new security control was introduced recommending static credentials used by applications and workloads be changed or revoked if: they are compromised or suspected of being compromised, they are discovered stored on systems in the clear, they are discovered being transferred across networks in the clear, or they are no longer required. **[ISM-2144]**

The existing security control recommending credentials for the KRBTGT service account be changed at least annually was amended to recommend they be changed at least every six months. **[ISM-1847]**

Revoking credentials

A new security control was introduced recommending credentials for user accounts be revoked when they are no longer required. **[ISM-2145]**

A new security control was introduced recommending static credentials used by applications and workloads be revoked when they are no longer required. **[ISM-2146]**

Protecting credentials

The existing security control recommending networks be scanned at least monthly to identify any credentials that are being stored in the clear was amended to expand the scope from networks to systems. **[ISM-1875]**

Protecting authentication artefacts

A new security control was introduced recommending authentication tokens, session cookies and refresh tokens be cryptographically bound to the device on which they were issued. **[ISM-2147]**

A new security control was introduced recommending active sessions, refresh tokens and other authentication artefacts be revoked when credentials are reset or re-enrolled, when credentials are compromised or suspected of being compromised, when a device no longer meets compliance requirements, or when high-risk sign-in activity is detected. **[ISM-2148]**

Guidelines for system management

Administrative tools

A new security control was introduced recommending a list of authorised remote monitoring and management (RMM) tools and remote access tools be developed, enforced and maintained. **[ISM-2149]**

A new security control was introduced recommending network connections for unauthorised RMM tools and remote access tools be blocked at gateways. **[ISM-2150]**

Backup modification and deletion

A new security control was introduced recommending backups be stored using a technically enforced immutability mechanism that prevents their modification or deletion for the duration of their retention period. **[ISM-2151]**

A new security control was introduced recommending backup infrastructure, including backup servers, repositories and management consoles, be segregated from production environments and use a separate authentication mechanism for administrative access. **[ISM-2152]**

Guidelines for security assurance

Threat hunting

A new security control was introduced recommending threat hunting activities, informed by current strategic and sector-specific cyber threat intelligence, be conducted at least every three months.

[ISM-2153]

Vulnerability assessments and penetration tests

The existing security control recommending at least annual vulnerability assessments and penetration tests for systems was amended to recommend they be conducted at least every six months. **[ISM-2118]**

Guidelines for software development

Secure software development

The existing security control recommending a software developer cyber security knowledge and skills register be implemented and maintained was amended to include its initial development. **[ISM-2038]**

Software artefacts

A new security control was introduced recommending software artefact dependencies be pinned to approved versions in source code. **[ISM-2154]**

The existing security control recommending scanning be used during commits to identify plain text or encoded secrets and keys, which are then blocked from being stored in the authoritative source for software, was amended to include credentials. **[ISM-2030]**

Build solution

A new security control was introduced recommending software be built using reproducible build practices that enable independent verification that release artefacts were produced from the stated source code.

[ISM-2155]

Excessive agency

A new security control was introduced recommending agentic AI applications be restricted to the minimum set of tools, functions and permissions required for their intended purpose. **[ISM-2156]**

A new security control was introduced recommending tools invoked by agentic AI applications be subject to both the access controls of the invoking user and agent-specific, task-scoped authorisation, with effective permissions limited to the minimum permitted by both. **[ISM-2157]**

A new security control was introduced recommending external content retrieved by agentic AI applications be treated as untrusted data throughout processing, be clearly delimited from system instructions, be subject to validation and sanitisation measures applied to other untrusted input, remain untrusted following such processing, and be prevented from modifying or overriding system instructions, security policies, access controls, tool permissions or human approval requirements. **[ISM-2158]**

A new security control was introduced recommending all tool invocations, external requests and outputs generated by agentic AI applications be centrally logged with sufficient detail to support cyber security incident investigations. **[ISM-2159]**

Guidelines for networking

Networked management interfaces

A new security control was introduced recommending networked management interfaces for IT equipment only be accessible from a dedicated management network that is segregated from the wider network and the internet. **[ISM-2160]**

Using Internet Protocol version 6

The existing security control recommending IPv6 functionality be disabled in dual stack network devices unless being used was rescinded. **[ISM-0521]**

802.1X authentication and key exchange

The existing security control recommending the use of 802.1X with EAP-TLS for mutual authentication was amended to include key exchange. **[ISM-1321]**

Evaluation of 802.1X implementations

The existing security control recommending evaluated supplicants, authenticators and authentication servers be used in wireless networks was amended to also capture wired networks. **[ISM-1322]**

Generating and issuing X.509 certificates for authentication

The existing security control recommending certificates be required for devices and human users authenticating to wireless networks was amended to capture wired networks implementing 802.1X. **[ISM-1323]**

Existing security controls referring to the use of certificates for authenticating to networks implementing 802.1X were amended to refer to X.509 certificates. **[ISM-1324, ISM-1327]**

Network device integrity

A new security control was introduced recommending the integrity of network device firmware and running configurations be verified against a known-good baseline following patching, on detection of anomalous behaviour and at least monthly. **[ISM-2161]**

Network device hardening

A new security control was introduced recommending unneeded components, services and functionality of network devices be disabled or removed. **[ISM-2162]**

Media Access Control Security

A new security control was introduced recommending that when using MACsec, confidentiality protection mode be enabled using GCM-AES-128, GCM-AES-256, GCM-AES-XPB-128 or GCM-AES-XPB-256, preferably GCM-AES-256 or GCM-AES-XPB-256. **[ISM-2163]**

A new security control was introduced recommending a connectivity association lifetime of less than 24 hours (86400 seconds) be used for MACsec connections. **[ISM-2164]**

A new security control was introduced recommending that when using EAP-TLS, each device perform a fresh EAP-TLS authentication each time a new Connectivity Association Key is required. **[ISM-2165]**

A new security control was introduced recommending a secure association lifetime of less than four hours (14400 seconds) be used for MACsec connections. **[ISM-2166]**

A new security control was introduced recommending the use of a Pre-Shared Key as a fallback authentication method for MACsec be disabled. **[ISM-2167]**

Guidelines for cryptography

Context

MACsec has been included as an ASD-approved cryptographic protocol.

Configuring Transport Layer Security

The existing security control recommending that when using DH or ECDH for key establishment of TLS connections that the ephemeral variant be used was merged into the security control recommending DH or ECDH be used for key establishment of TLS connections. **[ISM-1372, ISM-1448]**

Miscellaneous

Human users

A number of existing security controls referencing ‘users’ were amended to reference ‘human users’.
[ISM-0382, ISM-0407, ISM-0428, ISM-0445, ISM-0610, ISM-0661, ISM-0974, ISM-1173, ISM-1380, ISM-1487, ISM-1489, ISM-1491, ISM-1504, ISM-1505, ISM-1585, ISM-1592, ISM-1593, ISM-1594, ISM-1595, ISM-1671, ISM-1679, ISM-1680, ISM-1682, ISM-1748, ISM-1824, ISM-1825, ISM-1832, ISM-1854, ISM-1872, ISM-1892, ISM-1893, ISM-1894, ISM-1919, ISM-1920, ISM-2011, ISM-2012, ISM-2047]

Security controls

A number of existing principles and security controls referencing ‘controls’ were amended to reference ‘security controls’. [GOV-02, GOV-07, GOV-13, GOV-14, ISM-0009, ISM-0041, ISM-0409, ISM-0411, ISM-0441, ISM-1526, ISM-1563, ISM-1634, ISM-1635, ISM-1636, ISM-1809, ISM-1967]

Security control assessments

A number of existing security controls referencing security assessments were amended to reference security control assessments. [ISM-1562, ISM-1564, ISM-1636, ISM-1638, ISM-1737, ISM-1967, ISM-1971, ISM-1972, ISM-2019]

Grammatical edits

A number of existing principles and security controls were amended without changing their intent.
[GOV-12, PRO-12, ISM-0272, ISM-0407, ISM-0408, ISM-0414, ISM-0415, ISM-0428, ISM-0430, ISM-0441, ISM-0489, ISM-0665, ISM-0846, ISM-0853, ISM-1089, ISM-1211, ISM-1255, ISM-1270, ISM-1401, ISM-1408, ISM-1508, ISM-1536, ISM-1565, ISM-1591, ISM-1638, ISM-1688, ISM-1689, ISM-1737, ISM-1852, ISM-1883, ISM-1958, ISM-2012]

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.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>).

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/legalcode.en>).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>).



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre