



Information security manual

June 2026 changes

Last updated: June 2026

Cyber security principles

Protect cyber security principles

The existing cyber security principle on 'data protection' was renamed to 'cryptographic protection' and amended to replace the reference to 'ASD-approved algorithms and protocols' with 'ASD-approved cryptography' as to not unintentionally exclude the use of high assurance cryptographic algorithms and protocols. **[PRO-08]**

Guidelines for cyber security documentation

Continuous monitoring plan

The existing control on developing and implementing continuous monitoring plans was split into two controls to separate documentation development from the performance of security assessments. **[ISM-1163, ISM-2118]**

Guidelines for personnel security

Posting work-related information on online services

A new control was added recommending that *personnel are advised not to post information about their security clearance and briefings on unauthorised online services, and to report cases where such information is posted.* **[ISM-2104]**

A new control was added recommending that *personnel are advised to limit posting information about their work-related duties on unauthorised online services, and to report cases where such information is posted.* **[ISM-2105]**

A new control was added recommending that *personnel are advised to limit posting information about their work-related skills and experience on unauthorised online services, and to report cases where such information is posted.* [ISM-2106]

Posting personal information on online services

The existing control recommending that *personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information* was split into two controls to separate the posting of personal information to online services from the use of any available privacy settings. [ISM-0821, ISM-2107]

Guidelines for enterprise mobility

Encrypted communications

For the avoidance of doubt, a new control was added recommending that *mobile applications encrypt all sensitive or classified data communicated over public network infrastructure using ASD-approved cryptography.* [ISM-2108]

Guidelines for media

Encrypting media

A new control was added recommending that *pre-boot authentication using passwords, or managed network-based key release, is implemented for media containing encrypted system volumes.* [ISM-2109]

Guidelines for system hardening

User application releases

The existing control recommending that *the latest release of office productivity suites, web browsers and their extensions, email clients, PDF applications, and security products are used* was expanded to include extensions for all of the application types listed. [ISM-1467]

Hardening user application configurations

A new control was added recommending that *user applications are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.* [ISM-2110]

The existing control recommending that *unneeded components, services and functionality of office productivity suites, web browsers, email clients, PDF applications and security products are disabled or*

removed was expanded to all user applications and amended to include unneeded user accounts.

[ISM-1470]

The existing control recommending that *add-ons, extensions and plug-ins for office productivity suites, web browsers, email clients, PDF applications and security products are restricted to an organisation-approved set* was expanded to all user applications. **[ISM-1235]**

A new control was added recommending that *all temporary installation files created during user application installation processes are removed after user applications have been installed*. **[ISM-2111]**

Artificial intelligence applications

A new control was added recommending that *AI applications that process classified data have their ability to directly access external public data sources disabled*. **[ISM-2112]**

A new control was added recommending that *AI applications are configured to flag organisationally defined risky actions for human approval prior to their execution*. **[ISM-2113]**

A new control was added recommending that *baselines of expected behaviour and performance for AI applications are established and monitored for unexpected deviations*. **[ISM-2114]**

Hardening server application configurations

A new control was added recommending that *extensions for server applications are restricted to an organisation-approved set*. **[ISM-2115]**

The existing control recommending that *all temporary installation files and logs created during server application installation processes are removed after server applications have been installed* was amended to remove the requirement that logs be removed. **[ISM-1245]**

User account lockouts

The existing control recommending that *user accounts, except for break glass accounts, are locked out after a maximum of five failed logon attempts* was amended to capture the use of risk-based lockout mechanisms that implement automated lockout durations, such as Smart Lockout functionality used by Microsoft Entra ID. **[ISM-1403]**

Functional separation between operating environments

Existing controls relating to software-based isolation mechanisms were amended to replace references to 'physical server hardware' with 'physical computing resources'. **[ISM-1460, ISM-1461, ISM-1604, ISM-1605, ISM-1606, ISM-1607, ISM-1848]**

Guidelines for security assurance

Security monitoring policy

The existing control recommending that *an event logging policy is developed, implemented and maintained* was amended to reference a security monitoring policy instead. **[ISM-0580]**

Event log monitoring

A new control was added recommending that *cyber threat intelligence services are used to support the detection of cyber security events and the identification of cyber security incidents*. **[ISM-2116]**

A new control was added recommending that *suitable AI models are used to augment the detection of cyber security events and the identification of cyber security incidents*. **[ISM-2117]**

Vulnerability assessments and penetration tests

A new control was added recommending that *suitable AI models are used to augment vulnerability assessments and penetration tests*. **[ISM-2119]**

Guidelines for software development

Introduction to software development

The introduction to the 'software development fundamentals' section was amended to clarify that it applies to human, artificial intelligence (AI)-assisted, AI-powered and AI-driven software development activities. This includes noting that where a reference is made to software developers that it applies to both humans and AI agents.

Secure software development

A new control was added recommending that *a secure software development policy is developed, implemented and maintained*. **[ISM-2120]**

A new control was added recommending that *software developers that lack sufficient cyber security knowledge and skills required for their projects or tasks are not used*. **[ISM-2121]**

The existing control recommending that *software developers that lack sufficient cyber security knowledge and skills required for their projects or tasks undertake suitable training on secure software development and programming practices* was amended to including upskilling. **[ISM-2037]**

Software security testing

A new control was added recommending that *suitable AI models are used to augment software security testing*. **[ISM-2122]**

Data collection, retention and use

A new control was added recommending that *all prompts and outputs associated with chat sessions are securely deleted when chat sessions are removed from AI applications*. **[ISM-2123]**

Guidelines for cryptography

Using cryptographic algorithms

The existing control recommending that *an ASD-Approved Cryptographic Algorithm (AACA) or high assurance cryptographic algorithm is used when encrypting media* was amended to capture all scenarios where data is encrypted at rest. **[ISM-1080]**

Using cryptographic protocols

The existing control recommending that *an ASD-Approved Cryptographic Protocol (AACP) or high assurance cryptographic protocol is used to protect data when communicated over network infrastructure* was amended to capture all scenarios where data is encrypted in transit. **[ISM-0469]**

Miscellaneous

For the avoidance of doubt, controls that referenced data being ‘encrypted’ were amended to clarify that ASD-approved cryptography must be used. **[ISM-0233, ISM-0869, ISM-1059, ISM-1085, ISM-1277, ISM-1781, ISM-1928, ISM-1984, ISM-2017]**

Minor grammar corrections were made to principles and controls that did not affect their intent. **[GOV-11, PRO-10, ISM-0043, ISM-0072, ISM-0120, ISM-0138, ISM-0211, ISM-0294, ISM-0305, ISM-0306, ISM-0307, ISM-0310, ISM-0332, ISM-0336, ISM-0385, ISM-0459, ISM-0484, ISM-0526, ISM-0549, ISM-0694, ISM-0725, ISM-0820, ISM-0835, ISM-0846, ISM-0853, ISM-1036, ISM-1037, ISM-1076, ISM-1146, ISM-1219, ISM-1243, ISM-1272, ISM-1289, ISM-1293, ISM-1297, ISM-1400, ISM-1417, ISM-1419, ISM-1429, ISM-1452, ISM-1483, ISM-1493, ISM-1543, ISM-1569, ISM-1574, ISM-1579, ISM-1582, ISM-1598, ISM-1637, ISM-1645, ISM-1676, ISM-1713, ISM-1736, ISM-1738, ISM-1740, ISM-1801, ISM-1866, ISM-1869, ISM-1939, ISM-1940, ISM-1941, ISM-1942, ISM-1966, ISM-1970, ISM-1983, ISM-2005, ISM-2006, ISM-2007, ISM-2008, ISM-2035, ISM-2053, ISM-2057, ISM-2069, ISM-2084, ISM-2085, ISM-2095]**

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