



# Information security manual

## December 2025 changes

Last updated: December 2025

## Guidelines for personnel security

### General-purpose artificial intelligence usage policy

A new control was added recommending that *a general-purpose artificial intelligence usage policy is developed, implemented and maintained*. [ISM-2074]

## Guidelines for communications systems

### Multifunction device usage policy

The existing control recommending that *a fax machine and MFD usage policy is developed, implemented and maintained* was amended to remove the reference to fax machines. [ISM-0588]

### Connecting multifunction devices to digital telephone systems

The existing control recommending that *a direct connection from an MFD to a digital telephone system is not enabled unless the digital telephone system is authorised to operate at the same sensitivity or classification as the network to which the MFD is connected* was tightened to *MFDs are not connected to digital telephone systems*. [ISM-0245]

### Observing multifunction device use

The existing control recommending that *fax machines and MFDs are located in areas where their use can be observed* was amended to remove the reference to fax machines. [ISM-1036]

### Sending and receiving fax messages

Existing controls relating to sending and receiving fax messages were rescinded. [ISM-0241, ISM-1075, ISM-1092]

A new control was added recommending *fax machines, and online fax services, are not used for sending or receiving fax messages*. [ISM-2075]

# Guidelines for information technology equipment

## Sanitising fax machines

Existing controls relating to sanitising fax machines were rescinded. [ISM-1225, ISM-1226]

# Guidelines for system hardening

## Insecure authentication methods

A new control was added recommending that *security questions are not used for authentication purposes*. [ISM-2076]

A new control was added recommending that *email is not used for out-of-band authentication purposes*. [ISM-2077]

## Password strength

The existing control recommending that *passphrases used for single-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are at least 4 random words with a total minimum length of 15 characters* was amended to move the reference to 4 random words to ISM-1558. [ISM-0421]

The existing control recommending that *passphrases used for single-factor authentication on SECRET systems are at least 5 random words with a total minimum length of 17 characters* was amended to move the reference to 5 random words to ISM-1558. [ISM-1557]

The existing control recommending that *passphrases used for single-factor authentication on TOP SECRET systems are at least 6 random words with a total minimum length of 20 characters* was amended to move the reference to 6 random words to ISM-1558. [ISM-0422]

The existing control recommending that *passphrases used for single-factor authentication are not a list of categorised words; do not form a real sentence in a natural language; and are not constructed from song lyrics, movies, literature or any other publicly available material* was amended to include the recommended minimum number of words in passphrases. [ISM-1558]

A new control was added recommending that *passwords appearing in lists of commonly used passwords or lists of compromised passwords are not used*. [ISM-2078]

A new control was added recommending that *maximum length limits for passwords are not less than 64 characters*. [ISM-2079]

A new control was added recommending that *password complexity requirements are not imposed for passwords*. [ISM-2080]

A new control was added recommending that *all ASCII printable characters are supported for passwords*. [ISM-2081]

## Changing credentials

The existing control recommending that credentials for user accounts be changed in response to specific events was amended to remove the recommendation for time-based password changes. **[ISM-1955]**

# Guidelines for software development

## Cryptographic bill of materials

A new control was added recommending that *if a cryptographic bill of materials is available for imported third-party software components, it is used during software development to ensure such software components provide support for standardised implementations of Australian Signals Directorate (ASD)-approved cryptographic algorithms.* **[ISM-2082]**

A new control was added recommending that *a cryptographic bill of materials is produced and made available to consumers of software.* **[ISM-2083]**

## Software event logging

The existing control recommending that *security-relevant software crashes and error messages are centrally logged* was reworded for clarity and amended to include security-relevant usage of software. **[ISM-1911]**

## Secure artificial intelligence application development

The existing control recommending that *the OWASP Top 10 for Large Language Model Applications are mitigated in the development of large language model applications* was rescinded. **[ISM-1923]**

A new control was added recommending that *artificial intelligence-specific documentation, including model and system cards (or equivalent artefacts), is used to document model characteristics, system architectures, use cases and security risks.* **[ISM-2084]**

A new control was added recommending that *the exposure of exact artificial intelligence model confidence scores in API responses or user interfaces is prevented.* **[ISM-2085]**

## Artificial intelligence model poisoning

A new control was added recommending that *the source and integrity of artificial intelligence models, structures and weights are verified.* **[ISM-2086]**

A new control was added recommending that *the source and integrity of training data for artificial intelligence models is verified.* **[ISM-2087]**

A new control was added recommending that *data validation and verification techniques are used to ensure the reliability and accuracy of training data used by artificial intelligence models.* **[ISM-2088]**

## Unbounded consumption

A new control was added recommending that *artificial intelligence model performance metrics are monitored and anomalies are investigated.* **[ISM-2089]**

A new control was added recommending that *rate limiting is applied to inference queries for artificial intelligence models*. [ISM-2089]

A new control was added recommending that *resource limits are enforced for artificial intelligence models*. [ISM-2090]

## Excessive agency

A new control was added recommending that *access control policies are implemented to enforce fine-grained permissions for artificial intelligence applications*. [ISM-2090]

A new control was added recommending that *role-based access controls are implemented for artificial intelligence applications to restrict access to sensitive data*. [ISM-2091]

## Sensitive data disclosure and improper output

A new control was added recommending that *content filtering is implemented by artificial intelligence applications to detect and block sensitive data exposure and improper output*. [ISM-2092]

## Miscellaneous

A number of existing controls referencing ‘memorised secrets’ or ‘passphrases’ were amended to replace such terms with ‘passwords’ to align with preferred language under the finalised NIST SP 800-63B-4 publication. [ISM-0417, ISM-0421, ISM-0422, ISM-0487, ISM-0488, ISM-1449, ISM-1557, ISM-1558, ISM-1559, ISM-1560, ISM-1561, ISM-1596]

A number of existing controls were amended to replace ‘cybersecurity’ with ‘cyber security’. [ISM-0047, ISM-0718, ISM-0888, ISM-1602, ISM-1997, ISM-1998, ISM-1999, ISM-2000, ISM-2001, ISM-2002, ISM-2003, ISM-2004, ISM-2006, ISM-2020, ISM-2022, ISM-2037, ISM-2038, ISM-2051]

A number of existing controls were reverted to prior versions to use ‘cyber security’ instead of ‘cybersecurity’. [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-0720, ISM-0724, ISM-0725, ISM-0726, ISM-0732, ISM-0733, ISM-0735, ISM-1228, ISM-1478, ISM-1617, ISM-1618, ISM-1784, ISM-1803, ISM-1819, ISM-1880, ISM-1881, ISM-1906, ISM-1907, ISM-1918, ISM-1960, ISM-1961, ISM-1970, ISM-1986, ISM-1987]

A number of existing controls were reverted to prior versions to use ‘cyber threat’ instead of ‘cyberthreat’. [ISM-1526, ISM-1617]

A number of existing controls were reworded without changing their intent. [ISM-0585, ISM-1847, ISM-1955, ISM-1956, ISM-2072]

## 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 2025

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