Information security manual

September 2025 changes

Last updated: September 2025

Cybersecurity principles

All cybersecurity principles have been assigned a shorthand description for easier reference.

Identify principles

A new identify principle was introduced to capture the identification and documentation of assets for pre-existing systems within organisations. As this new identify principle underpins all other identify principles, it has been labelled as IDE-01. Subsequent identify principles were relabelled in sequential order.

- **IDE-01 – Asset identification:** Systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and documented.

Protect principles

Protect principle PRO-03 was amended to replace ‘trusted suppliers’ with ‘trustworthy suppliers’.

Protect principle PRO-07 was amended to replace ‘trusted operating systems, applications and code’ with ‘trustworthy operating systems, applications and code’.

Protect principle PRO-11 was amended to replace ‘trusted and vetted personnel’ with ‘trustworthy personnel’.

Protect principle PRO-12 was amended to replace ‘personnel’ with ‘personnel and services’.

Detect principles

Detect principles DET-01 and DET-02 were amended to draw a distinction between the collection of both security-related event logs and all configuration changes with their subsequent analysis.

- **DET-01 – Centralised event logging:** Security-relevant event logs and all configuration changes are centrally collected and stored securely.
- **DET-02 – Cybersecurity event detection:** Security-relevant event logs and all configuration changes are analysed in a timely manner to detect cybersecurity events.

Recover principles

A new category of cybersecurity principles, recover (REC), was introduced to capture risk management activities associated with the resumption of normal business operations following cybersecurity incidents. In support of this, respond principle RES-05 was relabelled as recover principle REC-01.

- **REC-01 – Business operations resumption:** Residual security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are accepted prior to the resumption of normal business operations following cybersecurity incidents.

Guidelines for physical security

Bringing photographic and video recording devices into facilities

A new control was added recommending that *an authorised photographic and video recording device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis*. **[ISM-2069]**

A new control was added recommending that *unauthorised photographic and video recording devices are not brought into SECRET and TOP SECRET areas*. **[ISM-2070]**

Guidelines for personnel security

Managing and reporting suspicious requests to disclose or change user account details

A new control was added recommending that *personnel dealing with user account details are advised of what social engineering attacks are, how to manage such situations and how to report them*. **[ISM-2071]**

Guidelines for software development

Secure artificial intelligence application development

The existing control recommending that *large language model applications evaluate the sentence perplexity of user prompts to detect and mitigate adversarial suffixes designed to assist in the generation of sensitive or harmful content* was amended to refer to generative artificial intelligence applications (instead of large language model applications) and preventing the generation of unintended behaviour. **[ISM-1924]**

A new control was added recommending that *artificial intelligence models are stored in a file format that does not allow arbitrary code execution*. **[ISM-2072]**

Guidelines for cryptography

Cryptographic implementation assurance

The existing control recommending that *cryptographic equipment or applications that have completed a Common Criteria evaluation against a Protection Profile are used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data* was amended to refer to 'ASD-endorsed Protection Profiles' instead. **[ISM-0457]**

The existing control recommending that *cryptographic equipment or applications that have completed a Common Criteria evaluation against a Protection Profile are used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure* was amended to refer to 'ASD-endorsed Protection Profiles' instead. **[ISM-0465]**

Existing controls referencing 'cryptographic equipment and applications' were amended to refer to 'cryptographic equipment, applications and libraries' instead. **[ISM-0455, ISM-0457, ISM-0465, ISM-0471, ISM-0481, ISM-1917]**

Transitioning to post-quantum cryptography

A new control was added recommending that *a post-quantum cryptography transition plan is developed, implemented and maintained*. **[ISM-2073]**

Miscellaneous

A number of existing controls referencing 'trusted suppliers' and 'trusted sources' were amended to refer to 'trustworthy suppliers' and 'trustworthy sources' instead to emphasise that trust placed in suppliers and sources should be verifiable. **[ISM-0664, ISM-0665, ISM-0675, ISM-2029]**

An existing control was reworded for consistency of language without changing its intent. **[ISM-1657]**

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

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