Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# Information Security Manual

**Last updated**: June 2024

# June 2024 Changes

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

## Cyber Security Principles

### Purpose of the cyber security principles

The existing GOVERN set of cyber security principles was split into separate GOVERN and IDENTIFY sets to draw a clearer distinction between governance related activities and asset/risk identification related activities.

### Govern principles

The previous G4 principle (now GOVERN-2) was amended to clarify that the reference to security risk management processes relates to systems, applications and data.

The previous G5 principle was split into two separate principles to cover the identification and documentation of security risks for systems, applications and data (now IDENTIFY-3) and the acceptance of security risks as part of system, application and data authorisation activities (now GOVERN-3).

### Identify principles

The IDENTIFY-1 principle was amended to clarify that the business criticality of systems, applications and data should be determined and documented.

### Protect principles

The PROTECT-1 principle was amended to clarify that systems and applications are designed, deployed, maintained and decommissioned according to their business criticality and security requirements.

The PROTECT-4 principle was amended to specify that systems, applications and data should be administered in a secure and accountable manner.

The PROTECT-12 principle was amended from ‘multiple methods are used to identify and authenticate personnel’ to ‘robust and secure identity and access management is used’. This includes the protection of credentials that reside on, or are communicated over, systems and networks as well as the hardening of directory services.

### Respond principles

The RESPOND-1 principle was amended to specify that cyber security incidents should be reported to relevant bodies and stakeholders, such as customers impacted by data breaches involving sensitive personal data.

The RESPOND-2 principle was amended to specify that cyber security incidents should be analysed as part of containment, eradication and recovery efforts.

The RESPOND-3 principle was amended to specify that incident response, business continuity and disaster recovery plans should support the recovery of normal business operations during and following cyber security incidents.

## Guidelines for Cyber Security Roles

### Providing cyber security leadership and guidance

The existing control recommending CISOs be appointed to provide cyber security leadership and guidance for their organisation was amended to capture information technology and operational technology. [ISM-0714]

### Reporting on cyber security

The existing control recommending CISOs report to their organisation's senior executive or Board on cyber security matters was amended to specify CISOs regularly report to their organisation's executive committee or board of directors. [ISM-0718]

A new control was added recommending CISOs regularly report to their organisation's audit, risk and compliance committee (or equivalent) on cyber security matters. [ISM-1918]

## Guidelines for Cyber Security Incidents

### Insider threat mitigation program

The existing control recommending the development, implementation and maintenance of 'a trusted insider program' was amended to reference 'an insider threat mitigation program'. [ISM-1625]

The existing control recommending seeking legal advice in the development and implementation of 'a trusted insider program' was amended to reference 'an insider threat mitigation program'. [ISM-1626]

## Guidelines for Security Documentation

### System security plan

The existing control recommending that systems have a system security plan was amended to include additional detail on the minimum elements to be captured by the overview of the system (i.e. the system purpose, the system boundary and how the system is managed). [ISM-0041]

## Guidelines for Procurement and Outsourcing

### Cyber supply chain risk management activities

A number of existing controls relating to cyber supply chain risk management activities for ICT equipment were amended to refer to IT equipment and OT equipment. [ISM-1452, ISM-1568, ISM-1631, ISM-1632, ISM-1882]

### Sourcing applications, IT equipment, OT equipment and services

A number of existing controls relating to sourcing ICT equipment were amended to refer to sourcing IT equipment and OT equipment. [ISM-1787, ISM-1788, ISM-1789]

### Delivery of applications, IT equipment, OT equipment and services

A number of existing controls relating to delivery of ICT equipment were amended to refer to delivery of IT equipment and OT equipment. [ISM-1790, ISM-1791, ISM-1792]

### Access to systems, applications and data by service providers

The existing control recommending that an organisation's systems and data not be accessed or administered by a service provider, unless a contractual arrangement exists between the organisation and the service provider to do so, was amended to include applications. [ISM-1073]

The existing control recommending that if an organisation's systems or data are accessed or administered by a service provider in an unauthorised manner that the organisation be immediately notified was amended to include applications. [ISM-1576]

## Guidelines for System Hardening

### Multi-factor authentication

A new control was added recommending that when multi-factor authentication is used for authenticating to online services or online customer services, all other authentication protocols that do not support multi-factor authentication be disabled. [ISM-1919]

A new control was added recommending that when multi-factor authentication is used to authenticate users to online services, online customer services, systems or data repositories – that process, store or communicate their organisation's sensitive data or sensitive customer data – users be prevented from self-enrolling into multi-factor authentication from untrustworthy devices. [ISM-1920]

## Guidelines for System Management

### Scanning for unmitigated vulnerabilities

A new control was added recommending that the likelihood of system compromise be frequently assessed when working exploits exist for unmitigated vulnerabilities. [ISM-1921]

## Guidelines for Software Development

### Mobile applications – Secure software design and development

A new control was added recommending that the *OWASP Mobile Application Security Verification Standard* be used in the development of mobile applications. [ISM-1922]

### Artificial intelligence applications – Secure software design and development

A new control was added recommending that the *OWASP Top 10 for Large Language Model Applications* be mitigated in the development of large language model applications. [ISM-1923]

A new control was added 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. [ISM-1924]

## Guidelines for Email

### Email server transport encryption

The existing control recommending that MTA-STS be enabled to prevent the unencrypted transfer of emails was reworded slightly to clarify its intent. [ISM-1589]

## Miscellaneous

References to ICT equipment were amended to IT equipment. [ISM-0161, ISM-0218, ISM-0250, ISM-0293, ISM-0305, ISM-0306, ISM-0307, ISM-0310, ISM-0311, ISM-0312, ISM-0313, ISM-0316, ISM-0321, ISM-0332, ISM-0336, ISM-0462, ISM-0520, ISM-0585, ISM-0622, ISM-1123, ISM-1217, ISM-1218, ISM-1493, ISM-1550, ISM-1551, ISM-1598, ISM-1599, ISM-1741, ISM-1742, ISM-1751, ISM-1752, ISM-1753, ISM-1809, ISM-1857, ISM-1858, ISM-1863, ISM-1869, ISM-1878, ISM-1913]

References to high assurance ICT equipment were amended to high assurance IT equipment. [ISM-0286, ISM-0290, ISM-0294, ISM-0296, ISM-0300, ISM-0315, ISM-1079]

Minor grammar edits were made to controls without changing their intent. [ISM-0229, ISM-0402, ISM-1216, ISM-1323, ISM-1327, ISM-1471, ISM-1479, ISM-1535]

# 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**