# Information security manual

## March 2026 changes

**Last updated:** March 2026

# Cyber security principles

## Implementing the cyber security principles

Important contextual information was included on how the *Information security manual*'s cyber security principles should be implemented by organisations.

*Within each function, the cyber security principles are listed in a logical sequence that reflects how they should be considered for implementation. The numbers used for the cyber security principles are identifiers only and do not indicate an implementation order.*

*When implementing the cyber security principles, each cyber security principle should be supported by administrative and technical controls proportionate to an organisation's size, complexity, operating environment and risk profile. These controls should be subject to ongoing risk-based monitoring and assurance activities. Where the term 'systems' is used, the elements listed in brackets define the scope of that cyber security principle.*

*Overall, the cyber security principles are interdependent and must be implemented collectively to achieve comprehensive cyber security outcomes.*

## Govern cyber security principles

References to 'cyber supply chains' as a system component within the Govern function were removed to support the creation of a Protect cyber security principle (PRO-16) on that topic. **[GOV-03, GOV-05, GOV-06, GOV-12]**

A new cyber security principle on 'executive artificial intelligence accountability' was added recommending that *the board of directors or executive committee is accountable for ensuring that artificial intelligence is secure, controllable, human-supervised and used in an ethical and accountable manner*. **[GOV-08]**

The existing cyber security principle on 'executive cyber security leadership' was renamed to 'cyber security leadership'. Furthermore, it was amended to recommend that the chief information security officer also deliver regular and timely risk-based reporting to the board of directors or executive committee on their

organisation's cyber security posture, the effectiveness of controls, current security risks and emerging cyber threats. **[GOV-02]**

The existing cyber security principle on 'cyber security resourcing' was amended to recommend that suitable and sufficient personnel and resources be maintained following their initial acquisition. **[GOV-04]**

A new cyber security principle on 'security risk management responsibilities' was added recommending that *security risk management responsibilities for an organisation and their suppliers, partners and customers, including any shared responsibilities, are documented and communicated to all relevant parties with accountability arrangements in place to ensure their effective implementation*. **[GOV-09]**

The existing cyber security principle on 'security risk management' was renamed to 'security risk management assurance'. Furthermore, its scope was expanded from 'systems' to 'an organisation and their systems' with security risk management activities being subject to ongoing monitoring and assurance activities by the board of directors or executive committee. **[GOV-03]**

The existing cyber security principle on 'security risk acceptance' was amended to include inherited and shared security risks. **[GOV-05]**

The existing cyber security principle on 'security risk communication' was amended to include inherited and shared security risks. **[GOV-06]**

A new cyber security principle on 'system exposure minimisation' was added recommending that *information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged*. **[GOV-10]**

The existing cyber security principle on 'trustworthy suppliers' was renamed to 'supplier cyber security assurance' and moved from the Protect function (PRO-03) to the Govern function (GOV-11). Furthermore, it was amended to recommend that supplier cyber security practices are independently verified, or otherwise risk-assessed, on a regular basis. **[GOV-11]**

The existing cyber security principle on 'trustworthy personnel' was renamed to 'personnel suitability assurance' and moved from the Protect function (PRO-11) to the Govern function (GOV-12). Furthermore, it was amended to replace the reference to 'trustworthy personnel' with 'personnel whose suitability and trustworthiness have been established and are subject to ongoing assurance'. **[GOV-12]**

A new cyber security principle on 'cyber security and safety' was added recommending that *controls for systems (infrastructure, operating systems, applications and data) do not compromise human, physical or environmental safety*. **[GOV-13]**

A new cyber security principle on 'legacy system management' was added recommending that *systems (infrastructure, operating systems, applications and data) that are not capable of meeting cyber security requirements are managed using compensating controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned or replaced*. **[GOV-14]**

The existing cyber security principle on 'security risk insights' was renamed to 'continuous cyber security improvement'. Furthermore, it was rewritten to recommend that *security risk management and associated cyber security activities are continually measured and reviewed using cyber threat intelligence and assurance activities, including exercises informed by real-world cyber threats, to identify, prioritise and incorporate improvements in governance arrangements, shared responsibilities and the effectiveness of controls*. **[GOV-07]**

# Identity cyber security principles

References to 'cyber supply chains' as a system component within the Identify function were removed to support the creation of a Protect cyber security principle (PRO-16) on that topic. **[IDE-01, IDE-02, IDE-03, IDE-04]**

The existing cyber security principle on 'asset identification' was amended to include identities and credentials as system components. Furthermore, it was amended to recommend that assets be continually and centrally identified and documented. **[IDE-01]**

A new cyber security principle on 'asset interdependencies' was added recommending that *interdependencies between systems (infrastructure, operating systems, applications and data) are continually and centrally identified and documented, including how the compromise of one system could affect the security or business operations of other dependent systems*. **[IDE-05]**

The existing cyber security principle on 'business criticality identification' was renamed to 'business criticality rating identification'. Furthermore, it was amended slightly for consistency with other cyber security principles without significantly changing its intent. **[IDE-02]**

The existing cyber security principle on 'security requirement identification' was amended slightly for consistency with other cyber security principles without significantly changing its intent. **[IDE-03]**

A new cyber security principle on 'resilience requirement identification' was added recommending that *resilience requirements for systems (infrastructure, operating systems, applications and data) are identified and documented*. **[IDE-06]**

The existing cyber security principle on 'security risk identification' was amended to expand its scope from 'systems' to 'an organisation and their systems'. Furthermore, it was amended to recommend that security risks identification activities include the use of current strategic and sector-specific cyber threat intelligence and threat modelling. **[IDE-04]**

# Protect cyber security principles

References to 'cyber supply chains' as a system component within the Identify function were removed to support the creation of a Protect cyber security principle (PRO-16) on that topic. **[PRO-06, PRO-12, PRO-13]**

The existing cyber security principle on 'secure system lifecycle' was amended to include resilience requirements as part of secure system lifecycle considerations. **[PRO-01]**

The existing cyber security principle on 'secure by design' was merged into the existing cyber security principle on 'secure system lifecycle'. **[PRO-02]**

A new cyber security principle on 'cyber supply chain security' was added recommending that *cyber supply chains supporting systems (infrastructure, operating systems, applications and data) are secure, resilient and support effective and coordinated cyber security incident response*. **[PRO-16]**

The existing cyber security principle on 'robust access control' was renamed to 'identity, credential and access management'. Furthermore, it was amended to reference supporting effective detection of identity and credential misuse. **[PRO-13]**

The existing cyber security principle on 'secure administration' was amended to recommend that administration activities be conducted in an auditable manner. **[PRO-05]**

The existing cyber security principle on 'attack surface reduction' was renamed to 'secure configuration management'. Furthermore, it was rewritten to recommend that *systems (infrastructure, operating systems and applications) are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently enforced*. **[PRO-04]**

The existing cyber security principle on 'vulnerability management' was amended to recommend that vulnerabilities be identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness. **[PRO-06]**

The existing cyber security principle on 'trustworthy software execution' was renamed to 'trustworthy software'. Furthermore, it was amended to recommend that only software that is supported, verified and authorised be permitted to execute on systems. **[PRO-07]**

The existing cyber security principle on 'data encryption' was renamed to 'data protection'. Furthermore, it was rewritten to recommend that *data is encrypted and authenticated at rest and in transit using ASD-approved algorithms and protocols to protect its confidentiality and integrity.* **[PRO-08]**

A new cyber security principle on 'cryptographic agility' was added recommending that *systems (infrastructure, operating systems and applications) are designed, configured and managed to support timely, prioritised and orderly changes to cryptography, including post-quantum cryptography*. **[PRO-17]**

The existing cyber security principle on 'regular proven backups' was renamed to 'regular and proven backups'. Furthermore, it was amended to include infrastructure as a system component and capture the validation of restoration capabilities as part of establishing proven backups. **[PRO-10]**

A new cyber security principle on 'network segmentation and segregation' was added recommending that *systems (infrastructure, operating systems and applications) are segmented into network zones based on business criticality and trust levels, with only authorised, controlled and monitored inbound and outbound communication paths between network zones permitted*. **[PRO-18]**

A new cyber security principle on 'operational technology isolation' was added recommending that *operational technology systems (infrastructure) are logically and physically isolated from information technology systems (infrastructure) and all external infrastructure, with only authorised, controlled and monitored communication paths between systems permitted*. **[PRO-19]**

A new cyber security principle on 'remote access to operational technology' was added recommending that *access to operational technology systems (infrastructure, operating systems, applications and data) over untrusted infrastructure is authorised, controlled and monitored*. **[PRO-20]**

The existing cyber security principle on 'content filtering' was amended to specify infrastructure and applications as system components. Furthermore, it was amended to capture that data flows between different security domains should be controlled and subject to inspection and verification. **[PRO-09]**

The existing cyber security principle on 'cyber security awareness training' was amended to recommend that cyber security awareness training cover operational security considerations as well as being tailored to the access levels of personnel and current cyber threats. **[PRO-14]**

The existing cyber security principle on 'physical access restriction' was renamed to 'physical access control'. Furthermore, it was amended to include data as a system component and capture physical access to facilities. **[PRO-15]**

## Detect cyber security principles

The existing cyber security principle on 'centralised event logging' was amended to specify infrastructure, operating systems, applications and data as system components. Furthermore, it was amended to recommend that security-relevant event logs and configuration changes be protected against unauthorised modification or deletion, and retained to support effective cyber security event detection and investigation. **[DET-01]**

A new cyber security principle on 'baselined high-risk access activities' was added recommending that *baseline patterns of identity and credential access activities, privileged access activities, and remote access activities are established and maintained for systems (infrastructure, operating systems, applications and data) to enable the detection of anomalous or unexpected behaviour*. **[DET-04]**

The existing cyber security principle on 'cyber security event detection' was rewritten to recommend that *anomalous or unexpected events and behaviours for systems (infrastructure, operating systems, applications and data) are analysed in a timely manner to detect cyber security events*. **[DET-02]**

A new cyber security principle on 'detection capability efficacy' was added recommending that *cyber security event detection capabilities are regularly evaluated for effectiveness and continuously refined, including by using current strategic and sector-specific cyber threat intelligence, to improve the detection of cyber security events*. **[DET-05]**

## Respond cyber security principles

The existing cyber security principle on 'cyber security incident planning' was amended to specify infrastructure, operating systems, applications and data as system components. **[RES-01]**

A new cyber security principle on 'cyber security incident coordination' was added recommending that *cyber security incident roles and responsibilities are defined, documented and exercised to support the internal and external coordination and management of cyber security incidents, including responsibilities for declaring cyber security incidents and undertaking pre-approved response and recovery activities*. **[RES-05]**

The existing cyber security principle on 'cyber security incident reporting' was amended to include reporting on recovery activities in addition to response activities. **[RES-02]**

The existing cyber security principle on 'cyber security incident insights' was amended to include the prioritisation of areas for improvement that are identified following cyber security incidents. **[RES-04]**

## Recovery cyber security principles

References to 'cyber supply chains' as a system component within the Recover function were removed to support the creation of a Protect cyber security principle (PRO-16) on that topic. **[REC-01]**

A new cyber security principle on 'system recovery assurance' was added recommending that *following cyber security incidents, systems (infrastructure, operating systems, applications and data) are verified through assurance activities to ensure they are secure and capable of supporting the resumption of normal business operations*. **[REC-02]**

The existing cyber security principle on 'business operations resumption' was amended to include inherited and shared security risks. **[REC-01]**

# Guidelines for cyber security roles

## Protecting systems and their resources

The existing control recommending that *system owners, in consultation with each system's authorising officer, determine the system boundary, business criticality and security objectives for each system based on an assessment of the impact if it were to be compromised* was amended to capture the determination of resilience objectives if it were to be attacked. **[ISM-1633]**

The existing control recommending that *system owners, in consultation with each system's authorising officer, select controls for each system and tailor them to achieve desired security objectives* was amended to capture the selection of controls to achieve desired resilience objectives. **[ISM-1634]**

A number of existing controls relating to system owners obtaining an authorisation to operate for each of their systems were slightly reworded for clarity without changing their intent. **[ISM-0027, ISM-1968]**

The existing control recommending that *system owners monitor each system, and associated cyber threats, security risks and controls, on an ongoing basis* was amended to capture that cyber threats, security risks and controls should also be managed by system owners. **[ISM-1526]**

# Guidelines for communication infrastructure

## Emanation security risk assessments

A number of existing controls were amended to replace 'emanation security threat assessment' with 'emanation security risk assessment'. **[ISM-0246, ISM-0249, ISM-1137]**

An existing control was amended to replace 'TEMPEST requirements statements' with 'emanation security mitigation advice'. **[ISM-1885]**

# Guidelines for enterprise mobility

## Privately-owned mobile devices and desktop computers

A number of existing controls were reworded for consistency with the new ISM-2095 control without changing their intent. **[ISM-1400, ISM-1866]**

A new control was added recommending that *personnel using privately-owned mobile devices or desktop computers to access OFFICIAL: Sensitive or PROTECTED systems or data are disallowed from granting access to unapproved artificial intelligence agents*. **[ISM-2095]**

## Organisation-owned mobile devices and desktop computers

The existing control recommending that classified data and personal data be separated on organisation-owned mobile devices and desktop computers was reworded for consistency with other similar controls without changing its intent. **[ISM-1482]**

## Mobile devices and desktop computers accessing the internet

The existing control recommending that *mobile devices and desktop computers access the internet via a VPN connection to an organisation's internet gateway rather than via a direct connection to the internet* was amended to remove the explicit reference to a VPN connection to allow for alternative technical solutions that achieve the same security objective. **[ISM-0874]**

## Maintaining mobile device security

A new control was added recommending that *mobile devices are configured to enforce separation between organisational and personal mobile applications and data*. **[ISM-2096]**

A new control was added recommending that *mobile devices are configured with always on VPN functionality*. **[ISM-2097]**

The existing control recommending that *mobile devices are configured with secure lock screens* was amended to clarify that secure lock screens need to be password-based. **[ISM-1888]**

A new control was added recommended that *mobile devices are configured to prevent data transfers over Universal Serial Bus connections*. This covers both USB and Lightning cables as both can establish USB connections with other devices/accessories. **[ISM-2098]**

## Connecting mobile devices to connected vehicles

A new control was added recommending that *mobile devices are not connected to the infotainment systems of connected vehicles*. **[ISM-2099]**

## Using mobile devices within or near connected vehicles

A new control was added recommending that *sensitive or classified data is not viewed on mobile devices within or near connected vehicles*. **[ISM-2100]**

A new control was added recommending that *sensitive or classified phone calls and conversations are not conducted within or near connected vehicles*. **[ISM-2101]**

# Guidelines for system hardening

## Microsoft Active Directory Domain Services account hardening

The existing control recommending that *user accounts are not configured with password never expires or password not required* was rescinded. **[ISM-1837]**

# Guidelines for software development

## Software artefacts

The existing control recommending that software artefacts be scanned for 'malicious code' before being imported into the authoritative source for software was amended to reference 'malicious content' instead. **[ISM-2026]**

The existing control recommending that *all imported or referenced third-party software artefacts are tested using static application security testing (SAST), dynamic application security testing (DAST) and software composition analysis (SCA) before being imported into the authoritative source for software and periodically throughout the software development life cycle* was split into two separate controls to differentiate between the initial testing of new software artefacts and the periodic testing of existing software artefacts. **[ISM-2028, ISM-2102]**

## Secure artificial intelligence application development

A new control was added recommending that *organisational data generated, collected or processed by artificial intelligence applications is not used for training, fine-tuning or improving artificial intelligence models unless informed and explicit consent has been obtained from data owners in advance*. **[ISM-2103]**

# Guidelines for cryptography

## Using post-quantum cryptographic algorithms

The existing control recommending that *when using ML-DSA and ML-KEM, as per FIPS 204 and FIPS 203 respectively, adherence to pre-requisite FIPS publications is preferred* was amended to replace the reference to 'pre-requisite FIPS publications' with 'pre-requisite FIPS 140-3 validation'. **[ISM-1990]**

# 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