Information security manual

Cybersecurity principles

Last updated: September 2025

The cybersecurity principles

Purpose of the cybersecurity principles

The purpose of the cybersecurity principles is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems from cyberthreats. These cybersecurity principles are grouped into six functions:

- **Govern (GOV):** Develop and maintain a strong and resilient cybersecurity culture.
- **Identify (IDE):** Identify assets and associated security risks.
- **Protect (PRO):** Implement and maintain controls to manage security risks.
- **Detect (DET):** Detect and analyse cybersecurity events to identify cybersecurity incidents.
- **Respond (RES):** Respond to cybersecurity incidents.
- **Recover (REC):** Resume normal business operations following cybersecurity incidents.

Govern principles

The govern principles are:

- **GOV-01 – Executive cybersecurity accountability:** The board of directors or executive committee is accountable for cybersecurity.
- **GOV-02 – Executive cybersecurity leadership:** A chief information security officer provides leadership and oversight of cybersecurity activities.
- **GOV-03 – Security risk management:** Security risk management activities for systems (cyber supply chains, infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks.
- **GOV-04 – Cybersecurity resourcing:** Suitable and sufficient personnel and resources are identified and acquired in support of cybersecurity activities.

- **GOV-05 – Security risk acceptance:** Residual security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are accepted before they are authorised for use and continuously monitored and managed throughout their operational life.
- **GOV-06 – Security risk communication:** Residual security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are transparently and mutually communicated with stakeholders.
- **GOV-07 – Security risk insights:** Security risk management, and associated cybersecurity activities, are regularly reviewed to identify potential improvements in processes and procedures.

Identify principles

The identify principles are:

- **IDE-01 – Asset identification:** Systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and documented.
- **IDE-02 – Business criticality identification:** The business criticality of systems (cyber supply chains, infrastructure, operating systems, applications and data) is determined and documented.
- **IDE-03 – Security requirements identification:** The confidentiality, integrity and availability requirements for systems (cyber supply chains, infrastructure, operating systems, applications and data) are determined and documented.
- **IDE-04 – Security risk identification:** Security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and documented along with any associated risk management decisions.

Protect principles

The protect principles are:

- **PRO-01 – Secure system lifecycle:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality and their confidentiality, integrity and availability requirements.
- **PRO-02 – Secure by design:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned using Secure by Design and Secure by Default principles and practices.
- **PRO-03 – Trustworthy suppliers:** Systems (infrastructure, operating systems, applications and data) are delivered and supported by trustworthy suppliers.
- **PRO-04 – Attack surface reduction:** Systems (infrastructure, operating systems and applications) are configured to reduce their attack surface.
- **PRO-05 – Secure administration:** Systems (infrastructure, operating systems, applications and data) are administered in a secure and accountable manner.
- **PRO-06 – Vulnerability management:** Vulnerabilities in systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and mitigated in a timely manner.

- **PRO-07 – Trustworthy software execution:** Only trustworthy and supported operating systems, applications and code can execute on systems.
- **PRO-08 – Data encryption:** Data is encrypted at rest and in transit.
- **PRO-09 – Content filtering:** Data communicated between different security domains is controlled and inspectable.
- **PRO-10 – Regular proven backups:** Operating systems, applications, settings and data are backed up in a secure and proven manner on a regular basis.
- **PRO-11 – Trustworthy personnel:** Only trustworthy personnel are granted access to systems (cyber supply chains, infrastructure, operating systems, applications and data).
- **PRO-12 – Least privilege access:** Personnel and services are granted the minimum access to systems (cyber supply chains, infrastructure, operating systems, applications and data) required to undertake their duties.
- **PRO-13 – Robust access control:** Robust and secure identity, credential and access management is used to control access to systems (cyber supply chains, infrastructure, operating systems, applications and data).
- **PRO-14 – Cybersecurity awareness training:** Personnel are provided with ongoing cybersecurity awareness training tailored to their duties.
- **PRO-15 – Physical access restriction:** Physical access to systems (infrastructure) is restricted to authorised personnel and monitored for unusual activities.

Detect principles

The detect principles are:

- **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.
- **DET-03 – Cybersecurity incident identification:** Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Respond principles

The respond principles are:

- **RES-01 – Cybersecurity incident planning:** Cybersecurity incident response, business continuity and disaster recovery plans support continued business operations during cybersecurity incidents, and the resumption of normal business operations following cybersecurity incidents.
- **RES-02 – Cybersecurity incident reporting:** Cybersecurity incidents, including associated response activities, are reported internally and externally to relevant bodies and stakeholders in a timely manner.

- **RES-03 – Cybersecurity incident response:** Cybersecurity incidents are contained, eradicated and recovered from in a timely manner.
- **RES-04 – Cybersecurity incident insights:** Lessons learnt from cybersecurity incidents are captured, and areas for improvement are identified and actioned in a timely manner.

Recover principles

The recover principles are:

- **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.

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