



Information security manual

Last updated: June 2025

Cybersecurity principles

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 five 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 and recover from cybersecurity incidents.

Govern principles

The govern principles are:

- **GOV-01:** The board of directors or executive committee is accountable for cybersecurity.
- **GOV-02:** A chief information security officer provides leadership and oversight of cybersecurity activities.
- **GOV-03:** Security risk management activities for systems (cyber supply chains, infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks.
- **GOV-04:** Suitable and sufficient personnel and resources are identified and acquired in support of cybersecurity activities.
- **GOV-05:** 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 risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are transparently and mutually communicated with stakeholders.

- **GOV-07:** 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:** The business criticality of systems (cyber supply chains, infrastructure, operating systems, applications and data) is determined and documented.
- **IDE-02:** The confidentiality, integrity and availability requirements for systems (cyber supply chains, infrastructure, operating systems, applications and data) are determined and documented.
- **IDE-03:** 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:** 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:** 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:** Systems (infrastructure, operating systems, applications and data) are delivered and supported by trusted suppliers.
- **PRO-04:** Systems (infrastructure, operating systems and applications) are configured to reduce their attack surface.
- **PRO-05:** Systems (infrastructure, operating systems, applications and data) are administered in a secure and accountable manner.
- **PRO-06:** Vulnerabilities in systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and mitigated in a timely manner.
- **PRO-07:** Only trusted and supported operating systems, applications and code can execute on systems.
- **PRO-08:** Data is encrypted at rest and in transit.
- **PRO-09:** Data communicated between different security domains is controlled and inspectable.
- **PRO-10:** Operating systems, applications, settings and data are backed up in a secure and proven manner on a regular basis.
- **PRO-11:** Only trusted and vetted personnel are granted access to systems (cyber supply chains, infrastructure, operating systems, applications and data).

- **PRO-12:** Personnel are granted the minimum access to systems (cyber supply chains, infrastructure, operating systems, applications and data) required to undertake their duties.
- **PRO-13:** 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:** Personnel are provided with ongoing cybersecurity awareness training tailored to their duties.
- **PRO-15:** Physical access to systems (infrastructure) is restricted to authorised personnel and monitored for unusual activities.

Detect principles

The detect principles are:

- **DET-01:** Security-relevant event logs are centrally collected and stored securely, then analysed in a timely manner to detect cybersecurity events.
- **DET-02:** Security-relevant configuration changes are centrally collected and stored securely, then analysed in a timely manner to detect cybersecurity events.
- **DET-03:** Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Respond principles

The respond principles are:

- **RES-01:** 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 incidents, including associated response activities, are reported internally and externally to relevant bodies and stakeholders in a timely manner.
- **RES-03:** Cybersecurity incidents are contained, eradicated and recovered from in a timely manner.
- **RES-04:** Lessons learnt from cybersecurity incidents are captured, and areas for improvement are identified and actioned in a timely manner.
- **RES-05:** 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.

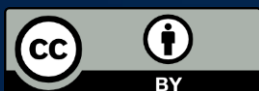
The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2025.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

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 (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate