Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information Security Manual

Last updated: June 2024

Cyber Security Principles

The cyber security principles

Purpose of the cyber security principles

The purpose of the cyber security principles is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems, applications and data from cyber threats. These cyber security principles are grouped into five functions:

- **GOVERN:** Develop a strong cyber security culture.
- **IDENTIFY:** Identify assets and associated security risks.
- **PROTECT:** Implement controls to manage security risks.
- **DETECT:** Detect and analyse cyber security events to identify cyber security incidents.
- **RESPOND:** Respond to and recover from cyber security incidents.

Govern principles

The govern principles are:

- **GOVERN-1:** A Chief Information Security Officer provides leadership and oversight of cyber security.
- **GOVERN-2:** Security risk management activities for systems, applications and data are embedded into organisational risk management frameworks.
- **GOVERN-3:** Security risks for systems, applications and data are accepted before they are authorised for use and continuously throughout their operational life.

Identify principles

The identify principles are:

- **IDENTIFY-1:** The business criticality of systems, applications and data is determined and documented.
- **IDENTIFY-2:** The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented.

- **IDENTIFY-3:** Security risks for systems, applications and data are identified and documented.

Protect principles

The protect principles are:

- **PROTECT-1:** Systems and applications are designed, deployed, maintained and decommissioned according to their business criticality and their confidentiality, integrity and availability requirements.
- **PROTECT-2:** Systems and applications are delivered and supported by trusted suppliers.
- **PROTECT-3:** Systems and applications are designed and configured to reduce their attack surface.
- **PROTECT-4:** Systems, applications and data are administered in a secure and accountable manner.
- **PROTECT-5:** Vulnerabilities in systems and applications are identified and mitigated in a timely manner.
- **PROTECT-6:** Only trusted and supported operating systems, applications and code can execute on systems.
- **PROTECT-7:** Data is encrypted at rest and in transit between different systems.
- **PROTECT-8:** Data communicated between different systems is controlled and inspectable.
- **PROTECT-9:** Applications, settings and data are backed up in a secure and proven manner on a regular basis.
- **PROTECT-10:** Only trusted and vetted personnel are granted access to systems, applications and data.
- **PROTECT-11:** Personnel are granted the minimum access to systems, applications and data required to undertake their duties.
- **PROTECT-12:** Robust and secure identity and access management is used to control access to systems, applications and data.
- **PROTECT-13:** Personnel are provided with ongoing cyber security awareness training.
- **PROTECT-14:** Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

Detect principles

The detect principles are:

- **DETECT-1:** Event logs are collected and analysed in a timely manner to detect cyber security events.
- **DETECT-2:** Cyber security events are analysed in a timely manner to identify cyber security incidents.

Respond principles

The respond principles are:

- **RESPOND-1:** Cyber security incidents are reported internally and externally to relevant bodies and stakeholders in a timely manner.

- **RESPOND-2:** Cyber security incidents are analysed, contained, eradicated and recovered from in a timely manner.

- **RESPOND-3:** Incident response, business continuity and disaster recovery plans support the recovery of normal business operations during and following cyber security incidents.

Maturity modelling

When implementing the cyber security principles, an organisation can use the following maturity model to assess the implementation of individual principles, individual functions or the cyber security principles as a whole. The five levels of the maturity model are:

- **Incomplete:** The cyber security principles are partially implemented or not implemented.

- **Initial:** The cyber security principles are implemented, but in a poor or ad hoc manner.

- **Developing:** The cyber security principles are sufficiently implemented, but on a project-by-project basis.

- **Managing:** The cyber security principles are established as standard business practices and robustly implemented throughout the organisation.

- **Optimising:** A deliberate focus on optimisation and continual improvement exists for the implementation of the cyber security principles throughout the organisation.

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

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

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

AUSTRALIA

Australian Government

Australian Signals Directorate