



Information Security Manual

DECEMBER 2021

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 organisations can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond.

- **Govern:** Identifying and managing security risks.
- **Protect:** Implementing security controls to reduce security risks.
- **Detect:** Detecting and understanding cyber security events.
- **Respond:** Responding to and recovering from cyber security incidents.

Govern principles

- **G1:** A Chief Information Security Officer provides leadership and oversight of cyber security.
- **G2:** The identity and value of systems, applications and data is determined and documented.
- **G3:** The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented.
- **G4:** Security risk management processes are embedded into organisational risk management frameworks.
- **G5:** Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life.

Protect principles

- **P1:** Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.
- **P2:** Systems and applications are delivered and supported by trusted suppliers.
- **P3:** Systems and applications are configured to reduce their attack surface.
- **P4:** Systems and applications are administered in a secure, accountable and auditable manner.
- **P5:** Security vulnerabilities in systems and applications are identified and mitigated in a timely manner.

- **P6:** Only trusted and supported operating systems, applications and computer code can execute on systems.
- **P7:** Data is encrypted at rest and in transit between different systems.
- **P8:** Data communicated between different systems is controlled, inspectable and auditable.
- **P9:** Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis.
- **P10:** Only trusted and vetted personnel are granted access to systems, applications and data repositories.
- **P11:** Personnel are granted the minimum access to systems, applications and data repositories required for their duties.
- **P12:** Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories.
- **P13:** Personnel are provided with ongoing cyber security awareness training.
- **P14:** Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

Detect principles

- **D1:** Cyber security events and anomalous activities are detected, collected, correlated and analysed in a timely manner.

Respond principles

- **R1:** Cyber security incidents are identified and reported both internally and externally to relevant bodies in a timely manner.
- **R2:** Cyber security incidents are contained, eradicated and recovered from in a timely manner.
- **R3:** Business continuity and disaster recovery plans are enacted when required.

Maturity modelling

When implementing the cyber security principles, organisations can use the following maturity model to assess the implementation of either individual principles, groups of principles or the cyber security principles as a whole. The five levels in the maturity model are:

- **Incomplete:** The cyber security principles are either 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.