Australian Government
Attorney-General's Department

Protective Security Policy Framework

PRINCIPLES

Principles apply to every area of security. As fundamental values that represent what is desirable for all entities, security principles guide decision-making.

1. Security is everyone's responsibility. Developing and fostering a positive security culture is critical to security outcomes.
2. Security enables the business of government. It supports the efficient and effective delivery of services.
3. Security measures applied proportionately protect entities' people, information and assets in line with their assessed risks.
4. Accountable authorities own the security risks of their entity and the entity's impact on shared risks.
5. A cycle of action, evaluation and learning is evident in response to security incidents.

OUTCOMES

Outcomes outline the desired end-state results the government aims to achieve.

GOVERNANCE

Each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring: clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.

INFORMATION

Each entity maintains the confidentiality, integrity and availability of all official information.

PERSONNEL

Each entity ensures its employees and contractors are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.

PHYSICAL

Each entity provides a safe and secure physical environment for their people, information and assets.

CORE REQUIREMENTS

Core requirements articulate what entities must do to achieve the government's desired protective security outcomes.

1 Role of accountable authority

The accountable authority is answerable to their minister and the government for the security of their entity.

The accountable authority of each entity must:

a) determine their entity's tolerance for security risks

b) manage the security risks of their entity, and

c) consider the implications their risk management decisions have for other entities, and share information on risks where appropriate.

The accountable authority of a lead security entity must:

a) provide other entities with advice, guidance and services related to government security

b) ensure that the security support it provides helps relevant entities achieve and maintain an acceptable level of security, and

c) establish and document responsibilities and accountabilities for partnerships or security service arrangements with other entities.

2 Management structures and responsibilities

The accountable authority must:

a) appoint a Chief Security Officer (CSO) at the Senior Executive Service level [1] to be responsible for security in the entity

b) empower the CSO to make decisions about:

i. appointing security advisors within the entity

ii. the entity's protective security planning

iii. the entity's protective security practices and procedures

iv. investigating, responding to, and reporting on security incidents, and

c) ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this.

3 Security planning and risk management

Each entity must have in place a security plan approved by the accountable authority to manage the entity's security risks. The security plan details the:

a) security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities

b) threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets

c) entity's tolerance to security risks

d) maturity of the entity's capability to manage security risks, and

e) entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

4 Security maturity monitoring

Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.

5 Reporting on security

Each entity must report on security:

a) each financial year to its portfolio minister and the Attorney-General's Department on:

i. whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF

ii. the maturity of the entity's security capability

iii. key risks to the entity's people, information and assets

iv. details of measures taken to mitigate or otherwise manage identified security risks

b) to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation

c) to the Australian Signals Directorate in relation to cyber security matters.

6 Security governance for contracted goods and service providers

Each entity is accountable for the security risks arising from procuring goods and services, and must ensure contracted providers comply with relevant PSPF requirements.

7 Security governance for international sharing

Each entity must adhere to any provisions concerning the security of people, information and assets contained in international agreements and arrangements to which Australia is a party.

8 Sensitive and classified information

Each entity must:

a) identify information holdings

b) assess the sensitivity and security classification of information holdings, and

c) implement operational controls for these information holdings proportional to their value, importance and sensitivity.

9 Access to information

Each entity must enable appropriate access to official information. This includes:

a) sharing information within the entity, as well as with other relevant stakeholders

b) ensuring that those who access sensitive or security classified information have an appropriate security clearance and need to know that information, and

c) controlling access (including remote access) to supporting ICT systems, networks, infrastructure and applications.

10 Safeguarding information from cyber threats

Each entity must mitigate common and emerging cyber threats by:

a) implementing the following Australian Signals Directorate (ASD) *Strategies to Mitigate Cyber Security Incidents*:

i. application control

ii. patching applications

iii. restricting administrative privileges

iv. patching operating systems, and

b) considering which of the remaining *Strategies to Mitigate Cyber Security Incidents* you need to implement to protect your entity.

11 Robust ICT systems

Each entity must ensure the secure operation of their ICT systems to safeguard information and the continuous delivery of government business by applying the Australian Government Information Security Manual's cyber security principles during all stages of the lifecycle of each system.

12 Eligibility and suitability of personnel

Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).

Entities must use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the Personnel Security Vetting Standards.

13 Ongoing assessment of personnel

Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.

14 Separating personnel

Each entity must ensure that separating personnel:

a) have their access to Australian Government resources withdrawn, and

b) are informed of any ongoing security obligations.

15 Physical security for entity resources

Each entity must implement physical security measures that minimise or remove the risk of:

a) harm to people, and

b) information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

16 Entity facilities

Each entity must:

a) ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets

b) in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes, and

c) accredit its security zones.

1. **Alternative arrangements are available for entities with fewer than 100 employees.**

Core requirements are supplemented by supporting requirements and guidance intended to facilitate a standardised approach to security implementation across government. Refer to www.protectivesecurity.gov.au