Australian Government
Department of Home Affairs
Protective Security Policy Framework

Protective Security Policy Framework
Release 24 Overview

The Protective Security Policy Framework (PSPF) sets out Australian Government policy across six security domains and prescribes what Australian Government entities must do to protect their people, information and assets, both domestically and internationally.

PRINCIPLES

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

GOVERNANCE

Establish
- Responsibilities for protective security
- Governance arrangements

Develop
- Security plan

Embed
- Security culture
- Security awareness

Detect & Respond
- Security incidents

Assess & Report
- Security capability

Review & Improve
- Inform improvements

RISK

Adopt
- Enterprise risk management approach
- Risk tolerances

Prioritise
- Prioritise risks
- Security mitigation measures

Implement
- Procurement and contract establishment

Manage
- External suppliers

Recognise & Respond
- Foreign Ownership Control or Influence
- Insider threats

Review & Adapt
- Business continuity and disaster recovery plans
- Respond to emerging threats

INFORMATION

Assess
- Business Impact Levels

Apply
- Security classifications

Protect
- Information compromise

Implement
- Operational controls

Share
- Domestic sharing
- International sharing

Dispose
- Secure disposal

TECHNOLOGY

Define
- Identify systems

Implement
- Systems controls

Authorise
- Systems authorisation

Safeguard
- Cyber-security strategy
- Essential Eight Strategies

Monitor
- Systems monitoring

Retire
- Decommission resources or facilities

PERSONNEL

Screen
- Pre-employment screening checks

Control
- Access (ongoing, temporary and remote)

Clear
- Security vetting and clearance

Ensure
- Security clearance maintenance and revalidation

Share
- Information of security concern

Separate
- Withdrawal of access
- Ongoing security obligations

PHYSICAL

Integrate
- Secure facilities design and construction

Certify
- Physical security zones

Implement
- Security control measures

Monitor
- Facilities and controls

Review
- Effectiveness of arrangements

Retire
- Decommissioning resources or facilities

Dependent Standards and Technical Manuals

- Australian Government Investigation Standard (AFP)

- Commonwealth Risk Management Policy and Procurement Rules (DOF)
- National Terrorism Threat Level Advisory System

- Australian Government Security Caveat Standard (Home Affairs)
- Australian Government Email Protective Marking Standard (Home Affairs)
- Australian Government Record Keeping Metadata Standard (NAA)
- Normal Administrative Practice (NAA)

- Information Security Manual (ASD)
- Australian Government Hosting Certification Standard (Home Affairs)

- Australian Government Adjudicative Standard (Home Affairs)
- TS-PA Standard (ONI/ASIO)

- Technical notes (ASIO)
- Security Equipment Evaluated Products List and Equipment Guides (SCEC)
- Building Code of Australia (ABCB)