

TAS-PSPF Tasmania's Protective Security Policy Framework



The Tasmanian Government has a responsibility to protect its information, people and assets. The TAS-PSPF establishes minimum protective security standards required to provide protection and enable resilience to compromise and harm. The TAS-PSPF supports Tasmanian Government agencies to achieve protective security principles and outcomes. These principles and outcomes will be accomplished by complying with core requirements that are underpinned by guiding policies.

Principles

- 1 Security is a responsibility of government, its agencies and its people.
- 2 Each agency is accountable and owns its security risks.
- 3 Security will be guided by a risk management approach.
- 4 Strong governance ensures protective security is reflected in agency planning.
- 5 A positive security culture is critical.

Outcomes



Security governance

Each agency identifies and manages security risks and supports a positive security culture while maintaining a cycle of continuous improvement.

Core requirements:

- The Accountable Authority will establish and implement appropriate security governance for the agency, with specific consideration of the environment in which the agency operates.
- The Accountable Authority will nominate an ASA.
- The Accountable Authority will work to develop a protective security culture within their agency.
- The Accountable Authority will submit an annual self-assessment report, including evaluation of maturity across the TAS-PSPF, using a template provided by DPAC.
- The Accountable Authority will be responsible for adopting protective security planning and monitoring to manage security risks.
- The Accountable Authority will develop, implement and review processes to support the reporting and investigation of security breaches and incidents.



Information security

Each agency is responsible for maintaining the confidentiality, integrity and availability of all official information.

Core requirements:

- The Accountable Authority must adhere to whole-of-government protective security policies and procedures relating to the management of information security.
- Agencies will adopt the Australian Government's Protective Security Policy Framework and related documentation for the classification, protective marking, transfer, handling and storage requirements of information (in any format) relative to its value, importance and sensitivity.
- The Accountable Authority must ensure the security of technology and information assets to safeguard data, information and privacy, and to ensure continuous delivery of government business during all stages of the asset lifecycle.



People security

Each agency ensures its people are suitable to access Tasmanian Government assets and meet the required standards of honesty and integrity.

Core requirements:

- Accountable Authorities must assess the initial suitability, and validate the identities, of people who have access to, or are seeking access to, Tasmanian Government assets.
- The Accountable Authority must ensure the ongoing suitability of their people to access official information and assets, while ensuring compliance with the TAS-PSPF.
- The Accountable Authority must ensure adequate management of separating people.



Physical security

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

Core requirements:

- The Accountable Authority must identify and implement physical security measures to mitigate the risk of harm or compromise to its information, people and assets.
- The Accountable Authority must consider physical security measures and ensure they are adopted and integrated in any proposed facility design, selection, development or modification.