Tasmania's Protective Security Policy Framework

Department of Premier and Cabinet

Tasmanian Government

Document release

This document is Version 2.1 of Tasmania's Protective Security Policy Framework. This is a managed document. Changes will only be issued as complete replacement. Recipients should remove superseded versions from circulation.

Development status

Version	Date	Author	Reason	Sections
1.0	November 2022	A Marshall	Cabinet Endorsed	All
1.1	June 2023	A Marshall	Update to Authority Removal of Acronyms	1.2, 5.2, Figure 2, Definitions
2.0	March 2024	A Marshall	Annual Review	3.4, 7, 8, 9, 10 Definitions
2.1	December 2025	L Grover	Annual Review	1.3, 1.4, 3, 5.2, 5.4, Definitions

Review and evaluation

This document will be reviewed 12 months post implementation and updated as necessary or in the instance of an investigation into any security incident that recommends review and evaluation.

Author: Resilience and Recovery Tasmania

Publisher: Department of Premier and Cabinet

Date: December 2025

© Crown in Right of the State of Tasmania December 2022

Contents

1. Introduction **4**

1.1 Purpose 4

1.2 Authority 5

1.3 Scope and application 5

1.4 Legislation and International Standards 5

2. Statement of requirement **6**

3. Background **7**

4. Structure of the TAS-PSPF **8**

5. Roles and responsibilities within the TAS-PSPF **9**

5.1 Department of Premier and Cabinet 9

5.2 Agencies/Accountable Authorities 9

5.3 People and visitors 9

5.4 Framework governance 10

6. Principles of the TAS-PSPF **11**

6.1 Security is a responsibility of government, its agencies and its people 11

6.2 Each agency is accountable and owns its security risks 11

6.3 Security will be guided by a risk management approach 11

6.4 Strong governance ensures protective security is reflected in agency planning 11

6.5 A positive security culture is critical 11

7. Tasmania's Protective Security Policy Framework **12**

8. Core requirements: Security governance **14**

9. Core requirements: Information security **18**

10. Core requirements: People security **21**

11. Core requirements: Physical security **24**

i. Definitions **26**

1. Introduction

The Tasmanian Government has a responsibility to protect its information, people and assets. In a broad and ambiguous security environment, Tasmania's Protective Security Policy Framework (TAS-PSPF) addresses the need for a central, holistic document which frames consistent protective security principles and coordinates whole-of-government approaches to our security environment. The TAS-PSPF is the mechanism which establishes the minimum protective security standard required to provide protection, enabling resilience to compromise and harm.

To achieve this, the TAS-PSPF establishes a proportionate, risk-based approach to the effective and efficient delivery of government business, services and operations. It also acknowledges that existing practices and procedures have the capacity to be aligned to the TAS-PSPF.

The TAS-PSPF is complemented by a review and evaluation function to remain contemporary with the local threat context, national security interests and, where possible, global standards.

Due to the national and international context of Tasmania's governmental interests, the TAS-PSPF is based on, and consistent with, the principles articulated within the Australian Government's Protective Security Policy Framework and relevant Australian Security Standards.

1.1 Purpose

To establish minimum protective security standards and provide Tasmanian Government agencies with guidance on decision-making and implementation of effective policies. The TAS-PSPF includes core requirements and guiding policies; applying these will improve the protection of Tasmanian Government information, people and assets.

To establish defined roles and responsibilities, providing clarity about the way agencies can deliver the minimum protective security standards.

To introduce a layer of transparency to the protection and security functions of Tasmanian Government agencies' business operations.

To enable information sharing in a consistent and coordinated way, providing confidence regarding information protection across agencies and interjurisdictionally.

To facilitate a focus on whole-of-government protective security issues, trends and challenges. This focus is the foundation of a holistic, strategic and consistent approach to the application of prioritised protective security mitigations across Tasmanian Government agencies.

1.2 Authority

The TAS-PSPF has been prepared as a whole-of-government approach and is maintained by the Department of Premier and Cabinet (DPAC) on behalf of the Tasmanian Government.

The Premier of Tasmania is the formal authority of the TAS-PSPF, a function which is not delegated under this framework.

1.3 Scope and application

Initially, the TAS-PSPF applies to all Tasmanian Government agencies and any subsidiary of those agencies, e.g. Parks and Wildlife Service.

The Accountable Authority of each agency is responsible for ensuring their agency's compliance with the TAS-PSPF, including any Directions issued by the Premier.

The TAS-PSPF informs policies and procedures which promote best practice in achieving consistent security standards across all agencies. The Tasmanian Government requires each agency to demonstrate a continuous cycle of improvement against the TAS-PSPF in the form of annual reporting.

While the TAS-PSPF is currently not binding for private or local government enterprises, the Tasmanian Government encourages these entities to adopt the framework as good practice. Future versions of the TAS-PSPF are likely to expand its application.

1.4 Legislation and standards

The TAS-PSPF is not explicitly legislated, though it is underpinned and supported by existing legislation and Australian and International Standards.

- *Archives Act 1983* (Tas)
- *Criminal Code Act 1924* (Tas)
- *Electronic Transactions Act 2000* (Tas)
- *Evidence Act 2001* (Tas)
- *Financial Management Act 2016* (Tas)
- *Industrial Relations Act 1984* (Tas)
- *Industrial Relations (Commonwealth Powers) Act 2009* (Tas)
- *Justices Act 1959* (Tas)
- *Ombudsman Act 1978* (Tas)
- *Personal Information Protection Act 2004* (Tas)
- *Police Offences Act 1935* (Tas)
- *Professional Standards Act 2005* (Tas)
- *Public Interest Disclosures Act 2002* (Tas)
- *Right to Information Act 2009* (Tas)
- *State Service Act 2000* (Tas)
- *Work Health and Safety Act 2012* (Tas)
- AS/NZS 4804:2001 – Occupational health and safety management systems – General guidelines on principles, systems and supporting techniques
- AS 4811:2022 – Workforce screening
- AS 8001:2021 – Fraud and corruption control
- ISO 27000 series – Information Security Matters
- ISO 31000:2018 – Risk management – Guidelines
- SA HB 167:2025 – Managing security related risks (Standards Australia Handbook)

2. Statement of requirement

The Tasmanian Government's information, people and assets are valuable and therefore vulnerable to threat actors (an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security) who have the intent to compromise and harm its core business functions and deliverables.

The Tasmanian Government requires its agencies to demonstrate a continuous cycle of improvement in enhancing their security culture, capability and maturity, in order to protect its information, people and assets. Applying consistent protective security principles enables agencies to develop an approach which reflects their individual risk environments and business needs and helps them to mitigate vulnerabilities on a proportionate and priority basis.

Agencies will commence working towards compliance with the TAS-PSPF on a prioritised security-risk basis, addressing the most critical elements across government, on behalf of the community.

Security incidents create a loss of confidence in the Tasmanian Government, particularly public perception and interjurisdictional trust networks as they relate to information, people and assets.

To continue ensuring the security of our assets, the Tasmanian Government expects its agencies to:

- understand the security environment in which they operate
- identify and understand the most critical assets they must protect
- mitigate security vulnerabilities on a prioritised security-risk basis
- anticipate and prepare for emerging security trends which threaten their ability to effectively undertake government business functions
- continue to improve protective security practices through accountability and governance.

3. Background

The minimum security standards of the TAS-PSPF were developed to integrate with practices at state and Commonwealth level, including with the Australian Government's Protective Security Policy Framework.

The TAS-PSPF consists of four key components which provide the methodology and structure required to improve security practices and standards:

- Principles
- Security outcomes
- Core requirements
- Guiding policies.

The TAS-PSPF encourages the adoption of a security culture which recognises the importance of protecting assets the government relies on to fulfil its responsibilities to the community. Accountable Authorities must implement and maintain adequate security for their agency's assets.

Embedding a security culture and applying protective security principles in corporate planning processes enhances an agency's ability to meet business needs, provide a safe working environment and improve relationships with clients and the community.

After completing a criticality assessment, an agency will then undertake a full risk assessment, to help focus on assets identified as being of greatest importance. Security planning and risk mitigation should focus on the agency's areas of most significant, critical risk, allowing priority application of risk treatment strategies which are proportionate to the agency's environment.

4. Structure of the TAS-PSPF

The TAS-PSPF is a document supporting 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.

The TAS-PSPF contains:

- five (5) protective security principles – these apply to all areas of security and are fundamental values to be considered in agency decision-making
- four (4) protective security outcomes – one for each security domain within the framework
- fourteen (14) core requirements – these define what must be delivered by agencies to achieve effective protective security outcomes.

The core requirements are further strengthened through supplementary requirements and guiding policies which aid in the consistent application of the TAS-PSPF across Tasmanian Government agencies.

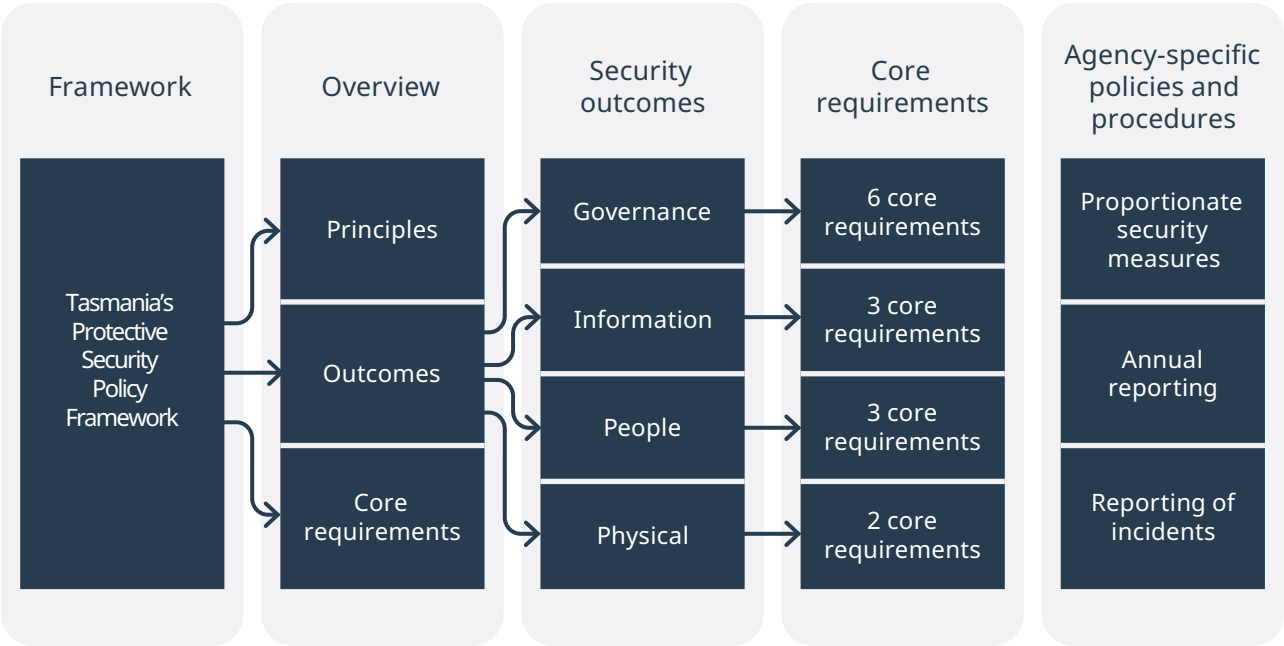


Figure 1: Table showing the structure of Tasmania's Protective Security Policy Framework

5. Roles and responsibilities within the TAS-PSPF

The Tasmanian Government is responsible for the security of all government assets; individual ministers are responsible for the security of assets within their portfolios. The TAS-PSPF places ownership and responsibility of security risk management on all agency people and visitors. Accountable Authorities are responsible for ensuring strategies are developed and implemented consistently in accordance with the principles and outcomes of the TAS-PSPF.

Security risks are best treated through early identification and management. This requires agencies to strengthen their security culture and awareness, making sure that these activities form part of their day-to-day business activities.

5.1 Department of Premier and Cabinet

The Department of Premier and Cabinet (DPAC) is responsible for whole-of-government implementation of the TAS-PSPF, including the development and promotion of training materials to elevate protective security understanding and awareness across Tasmanian Government agencies.

DPAC is also responsible for ongoing monitoring and assurance of whole-of-government security maturity and reporting to Cabinet. The monitoring function will be facilitated via agencies' annual self-assessment reporting, where collected data will inform review and evaluation.

Following any review, deficiencies, trends and improvements will be identified and addressed where necessary, as often many security risks are shared/ common across Tasmanian Government agencies.

Annual reporting data will also be used to understand the rigour applied to each agency's risk assessment processes, in accordance with international standards (ISO 31000:2018 – Risk management – Guidelines).

While DPAC provides oversight and assurance of security monitoring, individual agencies have flexibility and autonomy to determine how they action the TAS-PSPF.

5.2 Agencies/Accountable Authorities

Accountable Authorities must apply the TAS-PSPF in accordance with their agency risk assessment. The risk assessment must be conducted and maintained in accordance with ISO 31000:2018 – Risk management – Guidelines (supported by SA HB 167:2025 – Managing security related risks) and demonstrate robust consideration of the threat environment relevant to the agency and its functions. When implementing protective security measures, agencies must consider the broader Tasmanian Government operating environment to optimise whole-of-government consistency.

Accountable Authorities must resource and undertake protective security planning and preparedness activities in accordance with risk appetite and individual agency risk plans, which will be validated via annual self-assessment reporting. These plans should be validated for effectiveness to ensure they are robust.

Accountable Authorities hold responsibility for implementing and maintaining adequate protective security using the core requirements of the TAS-PSPF.

Accountable Authorities must adhere to any Direction issued by the Premier under the TAS-PSPF.

5.3 People and visitors

While the Accountable Authority is responsible for the implementation of the TAS-PSPF within their agency, protective security is everyone's responsibility. Agency people and visitors are required to comply with the protective security policies and procedures implemented by their agency, to ensure the integrity of assets.

People and visitors are required to undertake any mandatory training that is deemed necessary by the Accountable Authority in support of the TAS-PSPF. People are encouraged to adopt a culture of respectful challenge in their workplace, 'if it doesn't seem right – query it'.

5.4 Framework governance

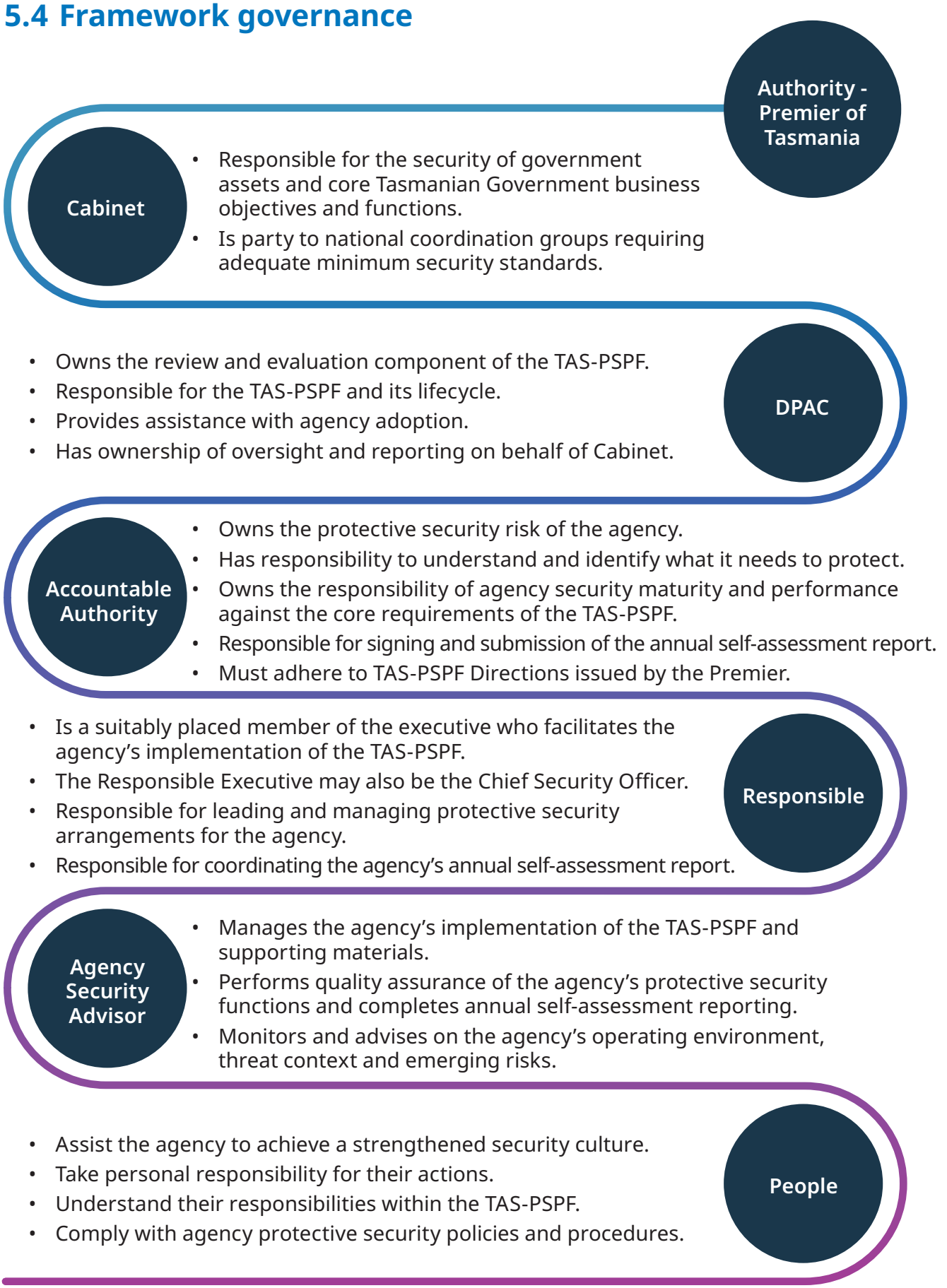


Figure 2: The governance and ownership structure of Tasmania's Protective Security Policy Framework

6. Principles of the TAS-PSPF

There are five principles that form the foundation of the TAS-PSPF and apply to all areas of protective security. These fundamental values should be the basis for informed decision-making within agencies to enable the development of best practice, an enhanced security culture and the protection of assets.

6.1 Security is a responsibility of government, its agencies and its people

All agencies are responsible for security. Protective security takes a layered approach, as it is only as strong as its weakest point and no singular measure is safe from compromise. The Tasmanian Government, its agencies and its people are responsible for ensuring that official information and assets are safe from compromise and harm.

6.2 Each agency is accountable and owns its security risks

Tasmanian Government agencies must have a clear understanding of how to assess their assets, what protections to apply and how to effectively protect them, as guided by the TAS-PSPF. Agencies must recognise the impact of their entity on shared risks across government.

6.3 Security will be guided by a risk management approach

The protection of information, people and assets is maintained by implementing a risk management approach which allows existing risks to be monitored and new risks to be identified and managed. All agencies must develop, implement, maintain and regularly review protective security policies to support a continuous cycle of improvement.

6.4 Strong governance ensures protective security is reflected in agency planning

Each agency should adopt strong leadership and ownership of risk across its protective security governance arrangements, with security measures considered and adopted across all agency outputs. The success of a protective security framework is reliant on the agency's ability to implement effective governance arrangements that appropriately reflect its size, context, individual requirements, and risk.

6.5 A positive security culture is critical

The Tasmanian Government, its agencies and its people are responsible for a positive security culture. The evolution of that culture is reliant on collective attitudes and behaviours adopted in relation to security. The TAS-PSPF, in conjunction with effective security leadership, aims to shift perceptions of security as measures which restrict functionality to security as an enabling feature of effective business. In this positive security culture, security exists intrinsically within an agency's systems and practices in order to enhance security resilience across government more broadly.

7. Tasmania's Protective Security Policy Framework

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

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.

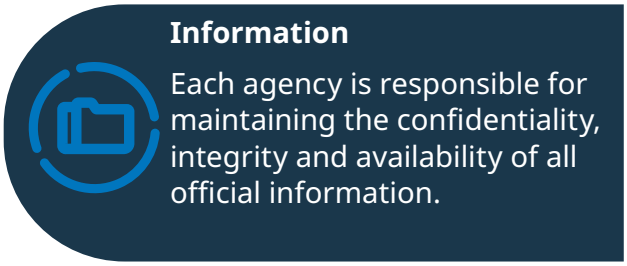
Outcomes outline the end-state results the government expects its agencies to achieve. Core requirements articulate what agencies must do to achieve the government's required protective security outcomes.

Outcome:

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.

Outcome:



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.

Outcome:

People

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.

Outcome:

Physical

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.

8. Core requirements: Security governance

GOVSEC-1: Establish security governance

Context

The TAS-PSPF states that an agency's Accountable Authority has overall responsibility for ensuring there are appropriate security governance structures in place to protect the agency's information, people and assets. This will be achieved through implementation and compliance with the TAS-PSPF.

Establishing a security governance structure appropriate for the agency should be risk-based according to agency-specific business activities and requirements, in accordance with ISO 31000:2018 – Risk management – Guidelines.

Sound security risk assessment and maintenance of an equivalent register will enable the agency to prioritise risk mitigations, improve planning, increase resilience and build a greater security culture.

Core requirement 1

The Accountable Authority will establish and implement appropriate security governance for the agency, with specific consideration of the environment in which the agency operates.

Supplementary requirements

To achieve security governance structures that effectively manage protective security, the agency must:

a) action the roles and responsibilities as required of the Accountable Authority

b) implement the core and supplementary requirements of the TAS-PSPF

c) determine the threat context and environment in which the agency operates

d) determine and manage the security risk profile and risk tolerance for the agency

e) consider the aggregate value of agency risk management decisions across the Tasmanian Government

f) ensure collaboration and engagement across agencies, to enhance information sharing and situational awareness of security risks

g) develop security governance policies, practices, processes and procedures allowing monitoring and reporting of security risks

h) develop a security plan

i) provide all people with relevant information and security awareness training so they are aware of their protective security responsibilities

j) implement security procedures upon the completion or termination of a contract.

GOVSEC-2: Security advice and responsibilities

Context

An Agency Security Advisor (ASA) provides protective security advice and leadership in day-to-day protective security risk management issues. The TAS-PSPF requires an agency to nominate an ASA to lead monitoring of the effectiveness of the protective security system, in accordance with the agency's strategic risk-based protective security plan.

The ASA supports the Accountable Authority with implementation, coordination and ongoing compliance with the TAS-PSPF.

Core requirement 2

The Accountable Authority will nominate an ASA.

Supplementary requirements

ASAs have responsibility for components of the security governance structures, including:

a) ensuring the agency achieves the elements of the security plan

b) developing, using and monitoring the effectiveness of security procedures and systems

c) identifying and managing security risks

d) monitoring and assessing the agency's security maturity and capability, including areas of improvement against the security plan/s

e) ensure security requirements are considered in all agency plans

f) responding to, investigating, and reporting security incidents

g) ensuring the Accountable Authority meets all relevant whole-of-government security policy or legislative requirements

h) arranging and, where applicable, delivering security briefings

i) ensuring the development and delivery of agency-specific security awareness training, including enhanced role-specific training where necessary.

GOVSEC-3: Security awareness

Context

Incorporating agency security awareness is the foundation to supporting staff understand their role in protecting the agency and its assets from harm. Enhanced security awareness develops and supports improved security culture, which is a baseline protection against the exploitation of agency vulnerabilities.

The TAS-PSPF requires the Accountable Authority to develop agency-specific security awareness and promotion of positive security measures.

Core requirement 3

The Accountable Authority will work to develop a protective security culture within their agency.

Supplementary requirements

Enhancing security awareness and culture will be achieved through:

a) enhancing induction to the agency through delivery of agency-specific security awareness module/s

b) providing refresher, and targeted, training to ensure contemporary knowledge of emerging trends and security measures

c) promoting positive security measures across the agency, including awareness of collective responsibility to foster a positive security culture

d) providing specific training for people in roles that involve emergency, safety and security functions

e) using effective communication methods to improve security culture.

GOVSEC-4: Annual reporting

Context

The TAS-PSPF states annual reporting will be conducted by the Accountable Authority to provide assurance of commitment to continuous improvement and an indication of security maturity across Tasmanian Government agencies. This reporting will be forwarded to DPAC for collation, review and further reporting to Cabinet as necessary.

The adoption and implementation of the TAS-PSPF will vary between agencies, based on individual risk assessments, the business environment and functions undertaken, and the accepted risk appetite and tolerance of the agency. This will capture maturity variations within reporting.

Core requirement 4

The Accountable Authority will submit an annual self-assessment report, including evaluation of maturity across the TAS-PSPF, using a template provided by DPAC.

Supplementary requirements

To support security maturity and ensure improvements against the security plan are being met, the agency must:

a) assess and identify progress against the strategic objectives of the agency's security plan, including:

   ii) justification/s for any decision to deviate from the TAS-PSPF core and supplementary requirements

   iii) identification of challenges, themes and barriers which have impacted compliance

b) assess the agency's security maturity against the TAS-PSPF core requirements

c) identify current vulnerabilities and key security risks to information, people and assets

d) identify treatment strategies which have been considered and/or applied.

GOVSEC-5: Security planning

Context

Adequate security planning and preparedness will support and enable business objectives while protecting vulnerabilities. The TAS-PSPF outlines best practice in the application of risk management across protective security planning.

The adoption of protective security planning will improve agency-specific resilience appropriate to risk appetite and tolerance.

Core requirement 5

The Accountable Authority will be responsible for adopting protective security planning and monitoring to manage security risks.

Supplementary requirements

To identify and manage security risks, the Accountable Authority will:

a) conduct a criticality assessment to identify the agency's key functionality and assets

b) identify agency-specific, and shared intergovernmental, security risks

c) consider site-specific security risk assessments where necessary[1]

d) determine the risk tolerance for the agency, which is subject to measuring and monitoring

e) plan and determine priority application of protective security measures to manage identified agency security risks and capture decisions which deviate from, or alter, the agency security plan

f) Review and evaluate the security plan as necessary or when risks or circumstances change.[2]

GOVSEC-6: Reporting incidents and security investigations

Context

With increased security awareness and enhanced security culture, the identification of and response to security incidents will improve. Accountable Authorities must ensure reporting processes are developed and implemented in accordance with the TAS-PSPF.

While the investigation of security incidents will be based on agency-specific risk tolerance and appetite, the TAS-PSPF provides guidelines to ensure a consistent approach to these investigations.

Core requirement 6

The Accountable Authority will develop, implement and review processes to support the reporting and investigation of security breaches and incidents.

Supplementary requirements

To assure improvement and enhance security maturity, it is necessary to create an environment that supports investigation. To achieve this, the Accountable Authority must:

a) provide a supportive environment for people to report security breaches and incidents[3]

b) ensure security awareness includes knowledge about actions which constitute security breaches and incidents

c) develop and implement clear processes supporting thorough investigation of reported security breaches and incidents

d) provide adequate security awareness training to assure agency people are cognisant of the TAS-PSPF's protective security requirements

e) ensure corrections are addressed following the conclusion of investigations[4].

1 Such circumstances may include multi-site agencies or complex and varied agency sites etc. Where site-specific plans are actioned, there must still be an overarching agency security plan.

2 For example, where the agency functions vary, certain functions are relocated, or new or evolving threats are identified.

3 In conjunction with existing reporting processes, including (but not limited to) Code of Conduct and those related to the Integrity Commission, Office of the Anti-Discrimination Commissioner, etc.

4 Consider updating security plans, enhancing security training, modifying the security treatment, revisiting the agency risk assessment.

9. Core requirements: Information security

INFOSEC-1: Access to, and management of, official information

Context

Agencies must protect assets from compromise and harm. Effective information management supports business operations and continuity while ensuring integrity, availability and confidentiality of information.

The TAS-PSPF supports agencies in the use of tools to appropriately manage information, enabling efficient and timely functions of government business and processes.

Core requirement 7

The Accountable Authority must adhere to whole-of-government protective security policies and procedures relating to the management of information security.

Supplementary requirements

In adhering to the whole-of-government approach to the management of information security, the Accountable Authority must:

a) promote awareness of whole-of-government protective security policies and procedures relating to the management of information security or ensure development of agency-specific policies as necessary[5]

b) ensure that information is accessed only by people with a legitimate need to know and implement measures to protect sensitive information, through physical and electronic means, from unauthorised access, copy or release

c) ensure people requiring access to security-classified information, or assets, are appropriately security cleared to the correct level and, where necessary, meet additional suitability requirements[6]

d) develop and implement an agreement or arrangement enabling the sharing of sensitive or security-classified information external to the Tasmanian Government and its agencies[7]

e) where appropriate, manage access to information systems with unique user identification, authentication and authorisation for each instance of system access.

5 Where whole-of-government policies and procedures are absent, agencies must develop their own in consultation with the Tasmanian Government Chief Information Officer.

6 Not all office holders are required to hold a security clearance - see TAS-PSPF policy: Access to, and management of, official information (INFOSEC-1) for more information.

7 This may be in the form of a deed or contract stipulating how the shared information is to be used and what protections must be applied.

INFOSEC-2: Protecting official information

Context

Agencies have varied operating environments and associated risks which influence agency risk appetite and tolerance. The TAS-PSPF states agencies must apply protections to information, based on assessed value and business impact levels to ensure consistent application.

Accountable Authorities should consider the value of their information as an aggregate when applying mitigations and upholding compliance with the TAS-PSPF.

Core requirement 8

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.

Supplementary requirements

To achieve the standards required relating to the classification, protective marking, transfer, handling and storage requirements of information, the Accountable Authority will:

a) implement processes that ensure information is assessed, marked and managed in alignment with policies and protocols or the assigned security classification

b) provide and regularly promote awareness of information protection practices, including secure information sharing and handling expectations, along with privacy obligations

c) determine appropriate information classification based on assessment of the information and/or technology assets holding that information, applying relevant controls, protections, processes and handling standards

d) when assessing sensitivity and security, the classification should be set at the lowest reasonable level to protect its confidentiality, integrity or availability from compromise or harm

e) ensure all information (including emails) is clearly identified with the correct protective markings[8]

f) adopt the Tasmanian Information and Records Management Standard, particularly in the creation of metadata, when records are created or captured, and ensure metadata reflects any protective markings[9]

g) when transferring, migrating or transmitting sensitive or security-classified information, ensure adequate processes exist to deter and detect any form of compromise to that information

h) manage and report breaches or security incidents to the ASA[10]

i) comply with storage requirements for sensitive and security-classified information, ensuring appropriate secure containers and zones are applied as necessary

j) ensure compliance with secure disposal of sensitive and security-classified information.

8 According to the assessed value and business impact of any compromise to the information as determined necessary.

9 See link for access to Tasmanian Information and Records Management Standard: https://osa.tas.gov.au/wp-content/uploads/2024/05/Information-and-Records-Management-Standard-v1.1.pdf

10 Types of breaches include but are not limited to: information privacy and all data, cyber, electronic and physical information breaches/incidents.

INFOSEC-3: Robust technology and information systems

Context

Access to information requires controls to ensure that confidentiality and the integrity of Tasmanian Government information, assets and business operations are maintained. As the business operations and environment of each agency vary, levels of access and associated controls will be based on agency-specific security planning and risk assessments.

Limiting unintended or unauthorised access to protectively marked information relies on robust and validated technology, information and infrastructure systems, complemented by enhanced security governance.

Core requirement 9

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 life-cycle.

Supplementary requirements

To achieve this, the Accountable Authority will:

a) ensure application of the Tasmanian Government Cyber Security Policy cybersecurity principles providing safeguarded maintenance of the confidentiality, integrity and availability of information[11]

b) only process, store or communicate information on ICT systems that the Accountable Authority has authorised to operate, based on acceptance of residual security risk associated with its operation

c) ensure ICT systems incorporate processes for audit trails and activity logging in applications to ensure the accuracy and integrity of data captured or held

d) develop and regularly test a Business Continuity Plan to manage the assessed risks and business impact associated with loss of critical information, personnel, facilities and ICT infrastructure

e) ensure ownership of, and accountability for, information security risk in ICT systems, including cloud and outsourced services, by nominating a business risk owner for every system, who is responsible for ensuring the secure operation of their system[12]

f) in combination with the 'People Core Requirements', ensure the effectiveness of physical controls and application of secure zones at any location where storage of information (in any form) is performed

g) ensure consideration of supply chain security is applied at all stages of contracted supply.

11 See link for access to Tasmanian Government Cyber Security Policy – cybersecurity principles: www.dpac.tas.gov.au/divisions/digital_strategy_and_services/resources/Tasmanian-Government-Cyber-Security-Policy-V1.1.pdf

12 The business risk owner may be the same for various (or all) systems.

10. Core requirements: People security

PESEC-1: Recruiting the right people

Context

Access to Tasmanian Government assets need to be protected. Agencies must apply a risk-based approach to employment processes, ensuring the suitability of its people, and external providers, to access these assets. The TAS-PSPF describes how the suitability and validation of agency people should be applied through pre-employment screens and security vetting where required.

Core requirement 10

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.

Supplementary requirements

To determine that the agency is recruiting the right people, the Accountable Authority will:

a) conduct pre-employment screens in accordance with any statutory requirements and limitations, which may include:[13]
   a. verification of identity and eligibility
   b. reference checks, as necessary, to ensure a person's suitability to access Tasmanian Government assets

b) identify specific roles and positions which may require additional certifications/checks which may include:[14]
   a. working with vulnerable people
   b. drug and alcohol testing
   c. relevant police checks
   d. psychometric assessments
   e. security clearances.

13 This will be based on type of engagement and the agency, along with any relevant state based award/agreement and legislation.

14 If such action is identified as necessary, seek appropriate approvals for associated Statement of Duties and/or advertising.

PESEC-2: Ongoing suitability assessment

Context

People engaged with the Tasmanian Government have access to valuable information and assets which are vulnerable to compromise and harm. Enabling a culture of security, with confidence in the ongoing suitability of people, reduces operating risks to Tasmanian Government agencies. The ability to maintain continued employment should be based upon continued compliance with relevant initial suitability screens and vetting.

Application of prescribed and consistent management protocols for people who hold security clearances ensures increased compliance and enhanced trust networks inter-jurisdictionally. The protection of Tasmanian Government information and assets is crucial.

The TAS-PSPF assists agencies to apply consistent expectations to the ongoing suitability of people and must be actioned in accordance with the agency's risk assessment.

Core requirement 11

The Accountable Authority must ensure the ongoing suitability of their people to access official information and assets, while ensuring compliance with the TAS-PSPF.

Supplementary requirements

To apply consistent expectations and management of ongoing suitability, the Accountable Authority will:

a) establish procedures which maintain confidence in the ongoing suitability and compliance of agency people[15]

b) ensure people are aware of their ongoing obligations according to their engagement contracts and have appropriate management arrangements in place which support these.[16]

c) ensure there are adequate management arrangements which support all agency people holding a national security clearance

d) ensure any security-cleared people are aware of and comply with the requirements of their clearance

e) identify and report non-compliance and matters of security concern to the relevant authority

f) establish policy and process for people who are unable to retain required obligations for ongoing suitability.

15 Such procedures may include refresher training, interval-based compliance checks, and mandated screening updates with position changes (in accordance with statutory requirements or limitations).

16 Each employment Act or agreement within Tasmanian Government holds the participating parties to account. Ongoing suitability according to these may include compliance with any code of conduct standards or requirements of certifications e.g. working with vulnerable people, NDIS endorsement.

PESEC-3:
Managing separating people

Context

Agencies must apply prescribed and consistent management protocols for separating and transferring people, ensuring all access to agency information and assets is adjusted or terminated accordingly, safeguarding the integrity of Tasmanian Government information and assets.

The TAS-PSPF outlines what must be implemented by agencies to protect the integrity, confidentiality and availability of Tasmanian Government information and assets.

Core requirement 12

The Accountable Authority must ensure adequate management of all separating people.[17]

Supplementary requirements

To provide secure management of separating people, the Accountable Authority will:

a) ensure access to Tasmanian Government information and assets is withdrawn or modified according to changed government duties[18]

b) ensure all agency items are returned accordingly – such items may include, but are not limited to, swipe access, ID passes, keys, IT equipment

c) withdraw or transfer sponsorship of security-cleared people, including eligibility waivers and conditional security clearance holders

d) ensure separating people are reminded of their ongoing security obligations

e) share information of security concerns with the appropriate stakeholder/s or authorities – this may be the Agency Security Advisor, the Security Clearance Sponsor, the authorised vetting agency or Australian Security Intelligence Organisation

f) manage any residual risk associated with the employee's departure.[19]

17 Separating refers to people who: leave an agency by transfer, resignation, secondment, contract cessation, termination or long-term leave.

18 In the instance of an internal transfer; secondment or long-term leave.

19 Deed of confidentiality or similar as required.

11. Core requirements: Physical security

PHYSEC-1: Protecting assets

Context

Agencies must identify the information, people and assets that require protection from compromise and harm. Vulnerabilities will be identified in the agency-specific risk assessment and managed according to the risk appetite and tolerance of each agency. Implementing layered physical security elements between the public and Tasmanian Government information and assets will enhance protection of the information and the public.

The TAS-PSPF describes how to mitigate identified risks to assets through best practice physical security measures.

Core requirement 13

The Accountable Authority must identify and implement appropriate physical security measures to mitigate the risk of harm or compromise to its information, people and assets.

Supplementary requirements

To implement appropriate physical security measures to mitigate the risk of harm or compromise to its information, people and assets, the Accountable Authority must:

a) identify, categorise and keep a record of the agency's assets which require any level of physical protection[20]

b) implement physical security measures proportionate to the identified threat and likely risk, using the assessed business impact of harm or compromise to agency assets – this may include:

   a. zoning of work areas (access controls, security screening etc)

   b. application of required individual control elements (secure storage, site locations, perimeter measures, security lighting etc)

   c. separated ICT infrastructure, equipment and facilities

d) certify and accredit all security zones on all premises for which the agency has responsibility[21]

e) dispose of physical assets securely

f) implement procedures to ensure appropriate accreditation of proposed work sites outside the office and provide training to all people in the correct use and application of the agency's physical security measures.

20 This will be based on the agency risk assessment and business impact levels.

21 Refer to ASIO Technical Notes to ascertain the requirements of security zones and associated processes.

PHYSEC-2: Agency facilities

Context

Access to Tasmanian Government assets by unintended and/or unauthorised people places these assets, and those accessing them, at significant risk.

Early identification and adoption of physical security measures provide protection through separation and isolation of information, people and assets. Consideration of these is critical in agency planning and facility design, selection, development and modification. The early identification and integration of physical security measures will allow agencies to address specific risks with proportionality according to the identified threat and operating environment.

The TAS-PSPF must be applied in conjunction with, and complementing, any work health and safety statutory requirements.

Core requirement 14

The Accountable Authority must consider physical security measures and ensure they are adopted and integrated in any proposed facility design, selection, development or modification.

Supplementary requirements

To ensure physical security measures are adopted and integrated in facility design, selection, development or modification, the Accountable Authority is responsible for:

a) identifying security threats relevant to the facility location, functions and stored assets, in conjunction with any identified accompanying risk[22]

b) considering the criticality of the agency's information, people and assets when assessing risks

c) ensuring any protective security measures are integrated to protect against the highest business impact level, in accordance with the agency security risk assessment

d) conducting regular reviews of the agency's physical security measures to ensure ongoing suitability or modifications as necessary.

22 Noting proportionality and cost effectiveness as considerations. These must also comply with any Treasurer's Instructions relevant to building/facility design, selection, development or modification.

i. Definitions and shortened terms

Guiding term	What this means in the context of the TAS-PSPF
must/will/required/ responsible for	Any of these terms refer to an essential action that all agencies and Accountable Authorities must take.
must not	This term refers to an action that is prohibited – agencies and Accountable Authorities must NOT take this action.
should/ recommended	Either of these terms refer to an action that agencies and Accountable Authorities ought to take as best practice, unless justifiable circumstances exist.
should not	This term refers to an action that agencies and Accountable Authorities ought to avoid, unless justifiable circumstances prevent an alternative action.
may	This term refers to an action that is optional to agencies and Accountable Authorities.

Term	What this means in the context of the TAS-PSPF
Accountable Authority	The person or people responsible for, and with control over, a Tasmanian Government public authority. Including, but not limited to, agencies (as defined in the *State Service Act 2000*), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	The person nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.

Term	What this means in the context of the TAS-PSPF
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third-party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's required protective security outcomes. Each of the 14 TAS-PSPF policies include a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, People.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of official information.
integrity	Safeguarding the accuracy and completeness of information and processing methods i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted or obtained by an agency.
originator	The instigating individual (or agency) who generated or received the information and is responsible for classifying it.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.
principles	Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
Responsible Executive	The person who oversees protective security matters within an agency. They may also be the Chief Security Officer (CSO).
risk appetite	The risk an agency or Accountable Authority is willing to accept.

Term	What this means in the context of the TAS-PSPF
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security-classified	Information that holds a classification of PROTECTED, SECRET or TOP SECRET and must be protected against compromise. Access to security classified information requires an appropriate security clearance and a 'need to know'.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	A security incident is: • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.
security plan	Central document detailing how an agency plans to manage and address their security risks.
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.
security risk management	Managing risks related to an agency's information, people and assets.
security vetting	An authorised vetting agency's assessment of a clearance subject's suitability to hold a security clearance.
sensitive	Information classified as sensitive is not security-classified information; however, this information requires some protections on a 'need to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's required protective security outcomes. Each of the 14 core requirements include supplementary requirements to help implement the TAS-PSPF.

Term	What this means in the context of the TAS-PSPF
TAS-PSPF maturity rating	The level to which an entity has addressed and implemented the core and supporting requirements in the TAS-PSPF.
threat	The intent and capability of an adversary.
threat actor/ adversary	An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security.
visitor	Any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency.
zone	The physical locality, workspaces and design of areas within an agency that store assets and information, specifically where information is produced, accessed, handled, and stored. Security zoned areas range from 1-5, where the security requirements increase with the applicable zone number allocation.

Tasmanian Government

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Email:
taspspf@dpac.tas.gov.au

Website:
www.security.tas.gov.au