



# Security Governance

## GOVSEC-I:

### Establish security governance



# Contents

---

<b>About this document</b>	<b>3</b>
<b>Definitions and shortened terms</b>	<b>5</b>
<b>Context</b>	<b>9</b>
<b>Guidance</b>	<b>11</b>
Introduction	11
Required action: Action roles and responsibilities	11
Required action: Implement the requirements of the TAS-PSPF	13
Required action: Determine the threat context and environment	14
Required action: Determine security risk profile and risk tolerance	14
Required action: Consider aggregate value of decisions across government	15
Required action: Collaborate and share information	16
Required action: Develop governance that allows monitoring and reporting	17
Required action: Develop a security plan	18
Required action: Provide security awareness training	18
Required action: Implement contract security procedures	19
<b>References and resources</b>	<b>21</b>

Author: Resilience and Recovery Tasmania  
Publisher: Department of Premier and Cabinet  
Date: April 2023

© Crown in Right of the State of Tasmania April 2023

## About this document

---

This document – GOVSEC-I: Establish security governance – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF is a whole-of-government approach to the protection of Tasmanian Government information, people and assets from compromise and harm. It establishes minimum protective security standards and makes clear that to continue ensuring the security of our people and assets, Tasmanian Government agencies need 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.

The TAS-PSF sets out 14 core requirements – with each accompanied by supplementary requirements – that define what must be addressed in order to protect our information, people and assets.

The suite of policies and guidance, including those found in this document, ensures that the TAS-PSPF will be applied across Tasmanian Government agencies in a consistent way. It will also assist agencies to achieve the expected outcomes of the following protective security domains under the TAS-PSPF:

- security governance
- information security
- people security
- physical security.

The table below lists all 14 core requirements of the TAS-PSPF and their corresponding policies. The name of the policy and guidance provided in this document is [highlighted](#).

Protective security outcome	Core requirement	Relevant policies and guidance
<b>Security governance</b>	1	<a href="#">GOVSEC-1: Establish security governance</a>
	2	GOVSEC-2: Security advice and responsibilities
	3	GOVSEC-3: Security awareness
	4	GOVSEC-4: Annual reporting
	5	GOVSEC-5: Security planning
	6	GOVSEC-6: Reporting incidents and security investigations
<b>Information security</b>	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
<b>People security</b>	10	PESEC-1: Recruiting the right people
	11	PESEC-2: Ongoing suitability assessment
	12	PESEC-3: Managing separating people
<b>Physical security</b>	13	PHYSEC-1: Protecting assets
	14	PHYSEC-2: Agency facilities

## 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/ies	The person or people responsible for, and with control over, a Tasmanian Government public authority. This includes, but is not limited to, agencies (as defined in the <i>State Service Act 2000</i> ), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	Person/people 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.

Term	What this means in the context of the TAS-PSPF
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'.
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 desired protective security outcomes. Each of the 14 TAS-PSPF policies includes 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 protected 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) responsible for producing information.
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. <ol style="list-style-type: none"> <li>1. Security is a responsibility of government, its agencies and its people.</li> <li>2. Each agency is accountable and owns its security risks.</li> </ol>

Term	What this means in the context of the TAS-PSPF
	<ol style="list-style-type: none"> <li>3. Security will be guided by a risk management approach.</li> <li>4. Strong governance ensures protective security is reflected in agency planning.</li> <li>5. A positive security culture is critical.</li> </ol>
protected information	Information which has been assessed and classified as requiring protective markings and protection.
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.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
risk appetite	The risk an agency or Accountable Authority is willing to accept.
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 culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	<p>A security incident is:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• an approach from anybody seeking unauthorised access to protected assets</li> <li>• an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.</li> </ul>
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.



Term	What this means in the context of the TAS-PSPF
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 protected information; however, this information requires some protections on a 'needs to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's desired protective security outcomes. Each of the 14 core requirements includes supplementary requirements to help implement 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.
vetting	The evaluation of a person's suitability to obtain and maintain a security clearance and access sensitive and protected assets.
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.

Acronym/abbreviation	Meaning
ASA	Agency Security Advisor
BIL	business impact level
CSO	Chief Security Officer
DPAC	Department of Premier and Cabinet
RE	Responsible Executive



## Context

---

The **GOVSEC-I: Establish security governance** policy and guidance will assist agencies to achieve an effective protective security outcome within the security governance domain of the TAS-PSPF. They address core requirement I and its supplementary requirements.

### Core requirement I

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.



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.



# Guidance

---

## Introduction

Establishing a security governance structure, appropriate for your agency, is an important step to embedding protective security in all aspects of your agency outputs. The TAS-PSPF requires you to establish and implement a security governance structure in accordance with your operating environment, which includes consideration of your business functions, services and requirements, and the assessed risk.

Establishing and implementing security governance according to your environment provides risk management opportunities that are integrated and scalable according to the needs of your agency.

## Required action: Action roles and responsibilities

### Role of your Accountable Authority

As defined above, the Accountable Authority, for the purposes of the TAS-PSPF, is the person or people responsible for, and with control over, a Tasmanian Government public authority.

Your Accountable Authority is responsible to their portfolio minister/s and the Tasmanian Government for the protection of their agency's information, people and assets. Your agency must establish minimum protective security standards, based on its risk assessment and tolerance, and in accordance with the TAS-PSPF.

In establishing security governance arrangements, your Accountable Authority must consider:

- your agency's business continuity capability during security incidents, disruptions or emergencies
- the ongoing and continued safety of people
- the protection of information and resources held within your agency.

## Responsibilities of your Accountable Authority

Your Accountable Authority has overall responsibility for your agency's security risk management, which includes determining risk appetite and tolerance. The TAS-PSPF recognises that responsibility rests with Accountable Authorities to ensure appropriate security governance strategies are developed and implemented consistently according to agency-specific criticality and risk assessments.

Your Accountable Authority is required to:

- nominate a Responsible Executive (RE) or Chief Security Officer (CSO) who will oversee protective security matters within your agency, monitoring all security arrangements and performance outcomes, and relevant decision-making
- nominate an Agency Security Advisor (ASA) who regularly reports to the RE or CSO
- develop, implement and maintain protective security policies and plans in accordance with the core and supplementary requirements of the TAS-PSPF, taking into account agency-specific functions and business requirements
- implement risk management strategies applicable to all domains of protective security across your agency
- ensure security awareness and culture is enhanced through continued training, awareness campaigns, and support mechanisms
- adopt review and evaluation processes which assess agency protective security policies and plans, with consideration of the existing threat environment
- complete annual reporting to assess security maturity and provide a copy to the Department of Premier and Cabinet (DPAC) at the conclusion of the review period
- promote a culture that supports identification of security incidents and encourages reporting
- ensure reported security incidents are responded to promptly and with transparency.

## Required action: Implement the requirements of the TAS-PSPF

Your Accountable Authority is ultimately responsible for the adoption and implementation of the TAS-PSPF in accordance with the core and supplementary requirements. To support this, your agency is obliged to action protective security arrangements, unless justifiable and relevant circumstances restrict agency capacity to do so.

Justifiable and relevant circumstances may include:

- circumstances beyond the control of your agency
- the cost of implementation being so prohibitive that it would prevent your agency from performing and delivering its core business function
- instances where alternate arrangements have been implemented to achieve equivalent or enhanced security outcomes than those applied by the minimum standard of the TAS-PSPF
- legislative requirements that dictate your agency must address protective security differently to that outlined in the TAS-PSPF.

Where justifiable and relevant circumstances are proposed, your agency must:

- provide advice to DPAC at the earliest opportunity, to allow any early assistance and support where possible
- identify and adequately record the circumstances that are purportedly preventing the implementation of the core and supplementary requirements
- provide advice to DPAC as to what measures are being actioned as alternate security arrangements, including the justification/s based upon agency security maturity and risk tolerance
- outline to DPAC the measures that are intended to be actioned to support achieving implementation of the TAS-PSPF and reduction in risk
- include a record of all decision-making in your agency's annual report.

## Required action: Determine the threat context and environment

All of your agency's information, people and assets are valuable and vulnerable. Protection of these resources through security risk management is the responsibility of your Accountable Authority. Your agency's security risk management includes identifying, assessing and prioritising risks to information, people and assets. It involves the efficient and coordinated application of protections that minimise, monitor, and mitigate the consequence of risks.

A threat assessment identifies where the threats to your agency, or its resources, come from, and considers the likelihood that the threats will eventuate. The level of threat is a combination of the intent and capability to cause harm or damage to your agency, the community or the Tasmanian Government. Threats can be either malicious or accidental.

Determining the threat environment applicable to your agency is crucial to efficient security risk management and requires you to understand the criticality of your agency's information, people and assets, along with the intent and capability of any potential threat actor. To assist in determining the threat context and environment for your agency, your RE or ASA should consider:

- conducting site-specific risk assessments where your agency occupies and/or operates on various sites
- engaging Tasmania Police to obtain advice on the local security threat context.

TAS-PSPF policy: Security planning (GOVSEC-5) provides further guidance on determining your agency's threat context and environment.

## Required action: Determine security risk profile and risk tolerance

Risk tolerance is an informed decision to accept risk after risk treatments have been applied. Each agency's level of risk tolerance will vary depending on the level of potential damage from an identified risk. Typically, the level of risk tolerance should decrease as the level of risk increases.

Your Accountable Authority is responsible for making informed decisions on your agency's priorities and balancing the capacity to deliver business objectives while maintaining a secure environment. This is achieved by determining the level of risk your agency is willing, or able, to accept and allows practical application of risk appetite.



While setting the risk profile and tolerance for your agency, your Accountable Authority must also consider the implications of their security risk management decisions on other agencies or whole-of-government security, i.e. the aggregate whole-of-government impact. It is important to consider the broader implications, particularly where consequences may be felt outside of your agency.

When considering your agency's risk profile and risk tolerance, you should assign a business impact level (BIL) to each identified security risk. BILs provide consistent methodology to the agency's risk assessment process and assist with implementing security measures that are proportionate to the agency's identified risks.

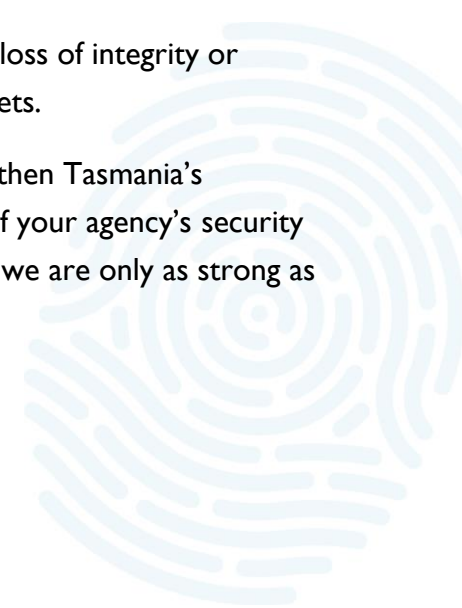
TAS-PSF policy: Agency facilities (PHYSEC-2) contains information that will help you define the BIL of your agency's assets, while TAS-PSPF policy: Security planning (GOVSEC-5) provides further guidance on determining, measuring and monitoring the risk tolerance for your agency.

## **Required action: Consider aggregate value of decisions across government**


While each Tasmanian Government agency is encouraged to take a risk management approach to protective security, it is important to understand that each of your decisions can have a flow-on impact outside your agency. Your risk management decisions have influence across government and for this reason, when determining your agency risk profile and risk tolerance, or assigning BILs, you should consider:

- the potential impact of your agency's security risks and your risk management decisions on other agencies or whole-of-government protective security
- the level of impact resulting from a compromise of confidentiality, loss of integrity or unavailability of both individual and aggregated information and assets.

Tasmanian Government agencies have a collective responsibility to strengthen Tasmania's resilience to existing and emerging security threats. The aggregate value of your agency's security risk management decisions can influence our collective resilience because we are only as strong as our weakest link.







Your risk management decisions should include consideration of the level of impact resulting from compromise of confidentiality, loss of integrity or unavailability of both individual and aggregated<sup>1</sup> information and assets.

Please refer to Annexure 2 in TAS-PSPF policy: Protecting official information (INFOSEC-2) for a list of questions your agency should consider when assessing risks to information.

## **Required action: Collaborate and share information**

Collaboration and information sharing is encouraged as a default position of Tasmanian Government agencies. This supports enhanced situational awareness and resilience to existing and emerging security threats.<sup>2</sup> It is important to consider when to share information with other agencies; however, you must share information with those who may be impacted by risk management decisions made within your agency.

Where there are circumstances that limit information sharing, it is recommended that you consider alternative options in the interests of supporting ongoing security awareness and efficient collaboration, for example, sharing partial or redacted information. Should the information be protected by legislative provisions,<sup>3</sup> you can consider adopting formal agreements between your agency and other agencies.

The sharing of information between agencies may help to identify and mitigate threats across government. For example, parties that pose security threats, such as organised crime groups, may target multiple government agencies.

For more guidance on sharing information with other agencies, see TAS-PSPF policy: Access to, and management of, official information (INFOSEC-1). For more guidance on managing shared risks, refer to TAS-PSPF policy: Security planning (GOVSEC-5).

---

<sup>1</sup> Any collections of information are considered to be aggregated information. Aggregated information relates to both physical and ICT collections.

<sup>2</sup> With the exception of circumstances where security, secrecy or privacy limitations exist.

<sup>3</sup> For example, the *Personal Information Protection Act 2004*.

## Required action: Develop governance that allows monitoring and reporting

Under the TAS-PSPF, Tasmanian Government agencies are required to have a security plan which establishes the strategic direction and sets the expectations for efficient and effective security management practices for the agency. For more information about this, refer to TAS-PSPF policy: Security planning (GOVSEC-5).

Your Accountable Authority is responsible for establishing the strategic direction, allocating resources in line with the strategy, and improving the security maturity of your agency.

Planning must incorporate developing practices and procedures that identify, manage, and mitigate security risks, and which enable your agency to continue to deliver effective and efficient government services.

Effective practices and procedures are those that are:

- embedded into day-to-day operations
- well understood by all employees
- demonstrated by senior management.

Effective security processes identify changes in the threat environment and allow for adjustments to maintain acceptable levels of risk, balancing operational and security needs. You should put in place measures to monitor the effectiveness of these procedures and security performance.

Security practices and procedures must be designed to deliver your agency's security plan which can in turn be useful in determining your agency's security maturity and progress in the overall implementation of the TAS-PSPF.

By adopting sound security governance policies, practices, processes and procedures, you will enhance your agency's ability to monitor and report on security risks, increasing your situational awareness. Situational awareness of your operating and threat environment is crucial and these steps will strengthen your resilience and security maturity.

## Required action: Develop a security plan

Your Accountable Authority is responsible for approving your security plan, which should include all protective security measures your agency intends to implement to protect key business functions and assets against identified security risks. Your security plan should outline the approach, responsibilities and resources applied to managing these protective security risks, in line with the core and supplementary requirements of the TAS-PSPF. Your plan should capture how security aligns with your agency's priorities and objectives.

Your security plan should consider:

Ownership	The plan should be owned by a senior member of staff.
Management	The plan should be endorsed by and have support of senior management.
Collaboration	The plan should be developed in consultation with, and including input from, all areas of your agency to ensure all key functions and assets are identified and vulnerabilities assessed.
Confidentiality	The plan should be stored securely and distributed on a strict 'need to know' basis, ensuring protection of vulnerabilities and security treatments.


The TAS-PSPF policy: Security planning (GOVSEC-5) provides further information about the development and implementation of agency security plans.

## Required action: Provide security awareness training

Security awareness training is a critical component of building an agency's security culture and overall security maturity.

You must provide security awareness training to all employees upon commencement in your agency, and annually thereafter (via security awareness refresher training), which outlines their agency-specific obligations and their responsibilities under the TAS-PSPF. Your ASA must determine the appropriate delivery method that ensures consistency across your agency for all employees, while ensuring all specific training or awareness requirements are met.

People in specialist or high-risk positions, positions of trust, security incident investigators or security clearance holders should be provided with specific security awareness training targeted to the scope and nature of their position.



Your security plan should identify the most relevant areas of agency security that need to be addressed in the security awareness training.

Security awareness training is most effective when it:

- informs and regularly reminds employees of their individual and collective security responsibilities and how to raise issues or concerns
- ensures employees with specific security duties receive appropriate and up-to-date training
- briefs security-cleared personnel on the access privileges and prohibitions attached to their security clearance level, either before being issued or during the renewal cycle
- fulfils requirements for security clearance holders.


The TAS-PSPF policy: Security awareness (GOVSEC-3) provides further guidance and information about security awareness training requirements.

## **Required action: Implement contract security procedures**

### **Monitoring and reviewing risk**

Your agency must monitor any active contract/s for changes to identified risks, threats, vulnerabilities or criticalities, as well as the performance of the contractor/sub-contractor in complying with terms and conditions over the lifetime of the contract. You should ensure ownership of contract risks by identifying an appropriate contract manager to be responsible for managing and monitoring each contract.

If your agency's risks are subject to regular change (for example, internal or external security environment changes), a flexible approach to contracts and their management may be required. It is recommended that you:

- develop positive working relationships with contractors/sub-contractors, based on open communication, to help issues be resolved efficiently and effectively
  - ensure contractors/sub-contractors effectively communicate security risks to their employees and all relevant security terms and conditions of the contract that must be followed
  - inspect any premises of the contractor/sub-contractor prior to the contract commencing to verify that protective security measures have been applied to the standard required by the contract, and then reinspect periodically during the contract for any changes and for overall compliance
- 

- ensure all contractor/sub-contractor personnel requirements have been achieved or obtained, such as –
  - security clearances and clearance maintenance requirements
  - legislative or policy requirements
  - conflicts of interest
  - confidentiality or non-disclosure agreements
- test and monitor (through site visits and audits) the contractor's/sub-contractor's processes for handling and storing your agency's information – where required, seek access to vulnerability and risk assessments, business continuity plans and security threat advice that could affect the security of the contract or information.

## **Managing completion or termination of a contract**

Security arrangements governing the completion or termination of contracts helps to prevent the compromise of official government information and damage to your agency. You must put in place arrangements to securely manage the completion or termination of all contracts.

It is recommended that at the completion of a contract, you:

- recover all information (electronic and hard copy) and assets under the control of the contractor/sub-contractor (or ensure the contractor/sub-contractor maintains all security measures if for legal reasons the information or assets cannot be returned)
- require the contractor/sub-contractor to delete all agency information on their ICT systems<sup>4</sup>
- ensure sponsorship of any security clearances is removed and the authorised vetting agency notified (see TAS-PSPF policy: Managing separating people (PESEC-3) for more details)
- obtain formal acknowledgement from contractors/sub-contractors and their employees of their continuing obligations to maintain confidentiality.

---

<sup>4</sup> If security-classified information was held, destruction must be as per the requirements of TAS-PSPF policy: Protecting official information (INFOSEC-2) or the Australian Government Information Security Manual, which is available at [www.cyber.gov.au/acsc/view-all-content/ism](http://www.cyber.gov.au/acsc/view-all-content/ism)

## References and resources

ASIO T4 Protective Security, Security Managers Handbook – Introduction to protective security measures, available to authorised people via the GovTEAMS protective security community.
Australian Government Protective Security Policy Framework, at <a href="http://www.protectivesecurity.gov.au/system/files/2023-04/pspf-policy-1-role-of-accountable-authority.pdf">www.protectivesecurity.gov.au/system/files/2023-04/pspf-policy-1-role-of-accountable-authority.pdf</a>
Australian Government Information Security Manual, at <a href="http://www.cyber.gov.au/acsc/view-all-content/ism">www.cyber.gov.au/acsc/view-all-content/ism</a>
International Organisation for Standardization, Standard ISO31000:2018, at <a href="http://www.iso.org/iso-31000-risk-management.html/">www.iso.org/iso-31000-risk-management.html/</a>
South Australian Government, Security governance, at <a href="http://www.security.sa.gov.au/documents/SAPSF-GOVSEC1-Security-governance-B451752-1.pdf">www.security.sa.gov.au/documents/SAPSF-GOVSEC1-Security-governance-B451752-1.pdf</a>



**Department of Premier and Cabinet**  
Resilience and Recovery Tasmania

**Phone:**  
(03) 6232 7979

**Email:**  
[sem@dpac.tas.gov.au](mailto:sem@dpac.tas.gov.au)