Security Governance

GOVSEC-3:
Security awareness

Contents

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

About this document

This document – GOVSEC-3: Security awareness – 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
Security governance	1	GOVSEC-1: Establish security governance
	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
Information security	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
People security	10	PESEC-1: Recruiting the right people
	11	PESEC-2: Ongoing suitability assessment
	12	PESEC-3: Managing separating people
Physical security	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 *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.

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 required 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 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. 1. Security is a responsibility of government, its agencies and its people.

Term	What this means in the context of the TAS-PSPF
	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.
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.
Responsible Executive	The person who oversees protective security matters within your agency, they may also be the Chief Security Officer (CSO).
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 classified	Information that holds a classification of PROTECTED, SECRET or TOP SECRET and must be protected against compromise. Access to the information must be controlled and accessed by appropriately security cleared people.
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.

Term	What this means in the context of the TAS-PSPF
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 'needs 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 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.
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
DPAC	Department of Premier and Cabinet
RTO	Registered Training Organisation

Context

The **GOVSEC-3: Security awareness** 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 3 and its supplementary requirements.

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.

Incorporating agency security awareness is the foundation to supporting staff to 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.

Guidance

Introduction

The Tasmanian Government, its agencies and its people are responsible for a positive security culture. The evolution of that culture is reliant on the adoption of collective attitudes and behaviours 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.

Required action: Deliver agency-specific security awareness during induction

Security awareness training supports implementation of security policies, practices and procedures, and is a critical component of building your agency's security culture and overall security maturity.

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. While you remain responsible for providing security awareness training to all people upon their commencement with your agency, training materials provided through DPAC may be helpful as you develop or update your induction and ongoing training programs.

Under TAS-PSPF policy: Security advice and responsibilities (GOVSEC-2), your Agency Security Advisor (ASA) is responsible for ensuring the development and delivery of agency-specific security awareness training, including enhanced role-specific training where necessary.

Your ASA may determine the appropriate training delivery method that ensures consistency across your agency for all employees, while ensuring all specific training and awareness requirements are met. If your agency elects to use an outsourced training provider to deliver the training, the provider should have sufficient knowledge of the TAS-PSPF and expertise in delivering adult education.

It is recommended that you use your agency's security plan to identify security expectations, targets and risks of most relevance, and then address these in your agency-specific training. Content for agency-specific security awareness training may include:

- an overview of protective security requirements and arrangements within your agency
- a description of your agency's security culture and security objectives
- personal safety and security measures in agency facilities and when people are working away from the office
- individual and line manager security responsibilities
- training or updating information classification and protective marking requirements
- outlining your agency's security risks and threats and notifying of relevant TAS-PSPF or agency-specific policies to address those risks and threats, and the individual employee's responsibilities associated with them
- information control measures, such as the 'need to know' principle and security clearance requirements (if applicable)
- overseas travel safety and security responsibilities
- measures to identify and report unusual or suspicious behaviours
- asset (including information) protection
- reporting requirements and procedures, including –
    - reporting security incidents
    - contact reporting (including the Contact Reporting Scheme)[1]
    - reporting suitability concerns about other employees
    - any other agency-specific reporting requirements including public interest disclosures.
- case studies of reported or investigated security incidents (with information redacted to maintain appropriate confidentiality).

In addition to providing security awareness training, you may consider further enhancing your agency's security awareness and culture through:

- advising people on agency-specific asset management and loss reporting procedures prior to them taking custody of assets, including agency fraud measures

[1] Refer to TAS-PSPF policy: Ongoing suitability assessment (PESEC-2) for information relating to contact reporting obligations.

- a safety handbook for all people that includes emergency response guidelines and contacts, as well as agency-specific safety requirements and procedures
- regular safety exercises and drills for employees
- providing people with specific emergency safety or security roles with regular training, in addition to assessing their ongoing suitability[2]
- targeted security awareness training where your agency has identified a need based on their risk profile, or when the agency has an increased or changed threat environment.

Required action: Provide refresher and targeted training

To remain contemporary with the security landscape in which your agency, or the Tasmanian Government operates, it is necessary to perform regular refresher training in respect to security awareness. It is recommended this training is conducted annually to adequately address any changes, while maintaining confidence in the ongoing suitability and compliance of agency people.

Your ASA should determine what form (e.g. in person, online), scope of coverage and content is required for the refresher training to meet the security needs of the agency and the minimum requirements of the TAS-PSPF.

Your agency refresher training should consider emerging trends and security measures[3], as well as the agency's current threat or risk environment, goals and objectives of the agency's security plan and any inadequacies of previous trainings or recurring security incidents.

A valuable tool for growth includes incorporating post-incident learning into incident reports or updated procedures which can provide useful insights into opportunities for improvements to your security awareness training.

People with specific emergency, safety or security roles should also be provided with regular training targeted to the scope and nature of their position which may include employees in high-risk positions, positions of trust, security incident investigators or security clearance holders.

Training for people with security clearances may include briefings or targeted training modules which outline the day-to-day responsibilities of being a clearance holder and information relating to reporting obligations (see TAS-PSPF policy: Ongoing suitability assessment (PESEC-2) for further information).

[2] See TAS-PSPF policy: Ongoing suitability assessment (PESEC-2) for further information.

[3] Relevant information may be obtained via ASIO Outreach for authorised subscribers, at www.asio.gov.au/.

Training for those in high-risk positions[4] should include security awareness specific to the risks associated with the focus or scope of the position.

Required action: Promoting a positive security culture

Fostering a positive protective security culture where people value, protect and use agency information and assets appropriately is critical to achieving security outcomes. Through a robust security culture, the threat to an agency and its assets can be significantly decreased.

In addition to keeping an agency and its people safe, a strong and healthy security culture helps to increase internal and external trust, embed consistent positive behaviour and support people to engage productively with risk.

Your agency should aim for a security culture where leadership and employees:

- comprehensively understand your agency's security risks
- understand their collective and individual security responsibilities
- proactively manage the security risk relevant to their work environment
- embed good security practices in their day-to-day activities
- use risk management to inform decisions which might affect the agency's security
- promote good security practices both internally and externally of the agency.

You may implement a range of tools to promote positive security measures across your agency, including:

- security awareness training that provides an understanding of protective security requirements under the TAS-PSPF and addresses relevant areas of agency security
- security campaigns that address ongoing agency security needs and the specific needs of sensitive areas, activities or periods of time
- security instructions and reminders via publications, electronic bulletins and visual displays such as posters

[4] High-risk positions may include those involved in:
- sensitive or priority negotiations or policy work
- controlling access to valuable or attractive assets (including information)
- work in remote or dangerous locations
- liaising or sharing information with foreign officials.

- incorporating protective security competencies into employee selection processes and performance management programs
- drills and exercises.

The importance of a positive security culture is reflected in TAS-PSPF Principle 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.*

For this reason, your agency must be able to demonstrate a continuous improvement cycle in enhancing the security culture.

Required action: Provide role-specific training

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. As mentioned above, such positions may include:

- sensitive or priority negotiations or policy work
- responsibility for, or access to, valuable or attractive assets
- working remotely or in dangerous conditions
- being required to liaise with foreign officials, or regularly share information with foreign officials.

The aim of role-specific training is to enhance awareness of the requirements and risks associated with the identified position, ensuring a more in-depth approach to your agency security. This may include highlighting any existing or emerging trends relevant to the position.

It is recommended that at a minimum, security awareness training programs or briefings for security-cleared people should:

- ensure that people who have access to security-classified resources understand and accept their day-to-day security responsibilities and reporting obligations (e.g. changes of circumstances, and suspicious, ongoing, unusual or persistent contacts)
- remind clearance holders of their responsibilities at regular intervals
- for people with access to sensitive compartmented information, include training and briefings from or in consultation with compartment owners.

Agency Security Advisors

The TAS-PSPF requires agencies to nominate an ASA to support the Accountable Authority with implementation, coordination, security monitoring and compliance with the TAS-PSPF.

Many functions of an ASA involve specialised skills. It is recommended ASAs demonstrate comprehensive knowledge or technical competencies in:

- the TAS-PSPF and supporting technical guidance, for example ASIO Technical Notes and the Australian Government Information Security Manual[5]
- the application of security measures relevant to the ASA's functions (e.g. professional certifications)
- managing security risk assessments.

Relevant knowledge, competencies and skills can be attained through on-the-job training, prior experience in a related field or formal qualifications (e.g. tertiary qualifications such as the Certificate IV or Diploma in Government Security or equivalent qualification). Where your agency provides training towards formal qualifications for ASAs, this training should be delivered by a Registered Training Organisation (RTO). RTOs are accredited training providers that offer nationally recognised training courses.[6]

[5] The Australian Government Information Security Manual is available at www.cyber.gov.au/acsc/view-all-content/ism

[6] A list of RTOs is available from www.training.gov.au.

Required action: Improve security culture through effective communication

A well-developed culture of security encourages information sharing by people about risks to themselves and their colleagues. In turn, effective communication and reporting of security incidents and breaches can contribute to a positive security culture.

Many potential security incidents are observed by your agency's employees. It is important that all employees, including contractors, understand how and when to report potential incidents or concerns.

To help ensure timely reporting and improve security culture, you should:

- establish simple channels for people to report security incidents or suspected incidents
- include security incident reporting and consequences, including practical examples, in agency-specific security awareness training
- actively promote agency security measures and employee responsibilities through multiple channels, e.g. posters, banners, intranet, desktop shortcuts and computer login prompts
- communicate security-related information across your agency, including sharing threat-related information with employees when required
- ensure the ASA, or other designated security personnel, is accessible for employees to discuss security issues or concerns (including sensitive issues to be discussed in confidence)
- include feedback processes in reporting and incident management procedures to ensure all relevant parties are notified of results once an incident has been resolved.

To holistically understand the performance of your agency security culture, it is recommended that you identify, document and share learnings internally with relevant security staff and executives, and externally where appropriate (e.g. with co-located agencies, agencies with similar risk profiles or through whole-of-government arrangements).

Security email address

To prevent agency security from becoming siloed, it is recommended that a central security email address be established for agency security-related matters, which can be monitored by your Accountable Authority, ASAs and other security people as required. This enables a greater flow of security-related information within your agency while also creating a central contact within your agency for external communication with other agencies.

It is recommended that your agency's security email address be generic in nature and take the form of security@[agency].tas.gov.au or security.advisor@[agency].tas.gov.au (or similar).

You should provide your agency's security email address to Resilience and Recovery Tasmania[7] and other relevant agencies to facilitate collaboration and communication.

If your agency is unable to create a generic email address for security-related matters and relies on an individual's email address, it is recommended that the email address be transferred to or be monitored by other staff during extended periods of absence.

If required, you may wish to establish multiple security-related email addresses to control the flow of specific information.

[7] Email Resilience and Recovery Tasmania at taspspf@dpac.tas.gov.au.

Version control and change log

First publication	April 2023	
Revision	February 2024	
Next review date	December 2024	
Change Log	Policy issued	V1.0 April 2023
	Definition: ‘core requirement’ updated	V2.0 February 2024
	Definition: ‘originator’ updated	
	Definition: ‘protected information’ removed and replaced with ‘security classified’	
	Definition: ‘Responsible Executive’ added	
	Definition: ‘supplementary requirement’ updated	

References and resources

Australian Government, management structures and responsibilities, at www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf
Australian Government, Information Security Manual, at www.cyber.gov.au/acsc/view-all-content/ism
ASIO Outreach, at www.asio.gov.au/
SA Government, security governance, at www.security.sa.gov.au/documents/SAPSF-GOVSEC1-Security-governance-B451752-1.pdf

Tasmanian Government

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au