Security Governance

GOVSEC-4: Annual reporting

Contents

Author: Resilience and Recovery Tasmania

Publisher: Department of Premier and Cabinet

Date: April 2023

About this document

This document – GOVSEC-4: Annual reporting – 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
RE	Responsible Executive
DPAC	Department of Premier and Cabinet
SCEC	Security Construction and Equipment Committee

Context

The **GOVSEC-4: Annual reporting** 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 4 and its supplementary requirements.

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 –

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

   ii. 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.

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.

Guidance

Introduction

The policies of the TAS-PSPF are designed to ensure the security of information, people and assets within the Tasmanian Government. However, the effectiveness of the policies, and how you apply them, depends significantly on the risks identified, the risk environment you operate in, and your agency's risk appetite and tolerance.

The annual self-assessment report provides a mechanism for your agency to provide a level of assurance and demonstrate its level of confidence that it is achieving the overall security outcomes of the Tasmanian Government, while also identifying broader protective security risks or challenges.

The Department of Premier and Cabinet (DPAC) provides a reporting template that will support you in capturing relevant information and meeting all the elements of the core requirement.

The report is intended to provide clear and succinct assessment against TAS-PSPF core requirements, along with protective security capability and maturity indicators.

You must classify the report according to the information contained within and apply the appropriate protective marking.

The report should be completed by your Agency Security Advisor (ASA) and reviewed by your Responsible Executive (RE). As the responsible party to the TAS-PSPF, your agency's Accountable Authority is responsible for approving the report before it is submitted to DPAC. This responsibility cannot be delegated.

The report must be submitted to DPAC by no later than 30 March of each calendar year, reviewing the agency's previous 12 months' protective security performance. The report should be submitted by the RE or their nominated delegate.

At the completion of each reporting period, DPAC will analyse and consolidate all reported data into an aggregated summary record for Cabinet.

Required action: Assess and identify progress against the security plan

As per TAS-PSPF policy: Security advice and responsibilities (GOVSEC-2), you are required to regularly monitor and assess your agency's security capability and risk culture by considering progress against the goals and strategic objectives identified in your agency's security plan.

This element presents as an 'executive summary' of your agency's security program over the preceding 12 months.

It is recommended that you include any highlights from the previous 12 months, for example, milestones or achievements that have been made in developing the security culture or maturity of the agency.

The annual self-assessment report should also include justification/s for any decision to deviate from the TAS-PSPF core and supplementary requirements, and identification of challenges, themes and barriers which have impacted compliance.

Deviating from the TAS-PSPF requirements

As per TAS-PSPF policy: Establish security governance (GOVSEC-1), you must put in place protective security arrangements for your agency that implement the core and supplementary requirements of the TAS-PSPF, unless relevant circumstances prevent you from doing so.

If this is the case, then in the annual self-assessment report, you must:

- detail the exceptional circumstances preventing the implementation of the core or supplementary requirement(s)
- outline the alternative arrangements being implemented, including any justifications based on your agency's security maturity and risk tolerance
- outline actions planned to move toward achieving the requirements of the TAS-PSPF and/or further reducing risk.

Exceptional circumstances may include:

- circumstances beyond the control of your agency
- that the cost of implementation is so prohibitive, it prevents your agency's ability to perform and deliver its core business function

- instances where alternate arrangements have been implemented to achieve equivalent or enhanced security outcomes to those that would be achieved by applying the minimum standard of the TAS-PSPF
- legislative requirements that dictate your agency must address protective security differently to the methods or processes outlined in the TAS-PSPF.

Challenges, themes and barriers to compliance

When completing your annual agency self-assessment report, you should highlight any challenges or barriers that were encountered in achieving your agency's security plan or the requirements of the TAS-PSPF. Sharing challenges and barriers to effective protective security can serve as a useful source of information for broader improvements to the TAS-PSPF and enable useful solutions or risk treatments to be identified from across government.

Challenges or barriers may include:

- financial considerations
- resources
- capability
- legislative restrictions
- external third-party dependencies
- machinery of government
- difficulty assigning appropriate security responsibilities
- low security awareness/understanding of core and/or supplementary requirements.

Where challenges or barriers are identified, you should indicate how your agency plans to address any shortfall in protective security effectiveness or develop strategies to overcome those challenges or barriers in future.

Required action: Assess security maturity against the core requirements

This policy (GOVSEC-4) requires you to develop and implement processes to assess your agency's current security maturity against the TAS-PSPF core requirements and establish maturity targets to work towards.

Security maturity is a meaningful way to demonstrate progress to achieving or exceeding the minimum standards of the TAS-PSPF while factoring in the specific risk environment and risk tolerance of individual agencies.

Security maturity considers how holistically and effectively your agency:

- understands, prioritises and manages its security risks
- responds to and learns from security incidents
- fosters a positive security culture
- achieves security outcomes and core requirements while delivering business outcomes.

To create consistency across the Tasmanian Government, your agency must use the following maturity assessment tool when setting maturity targets and assessing security maturity. Table 1 contains the 4 levels of security maturity of the TAS-PSPF.

Maturity levels	Definition
1	Partial or basic TAS-PSPF implementation. Success is reliant upon individuals, not processes, and protective security is not well understood across the agency.
2	Foundational practices with substantial implementation of the TAS-PSPF. Protective security requirements are not fully implemented into business practices, though the agency is meeting most security outcomes.
3	Complete and effective risk-based security measures are implemented. Protective security requirements are integrated into business practices and the agency is meeting security outcomes.
4	Comprehensive and adaptive operating environment with effective TAS-PSPF implementation. Protective security requirements are proactively integrated into business practices and exceeding security outcomes. The agency is excelling at implementing better-practice and exceeding security outcomes.

Table 1 – Security maturity levels

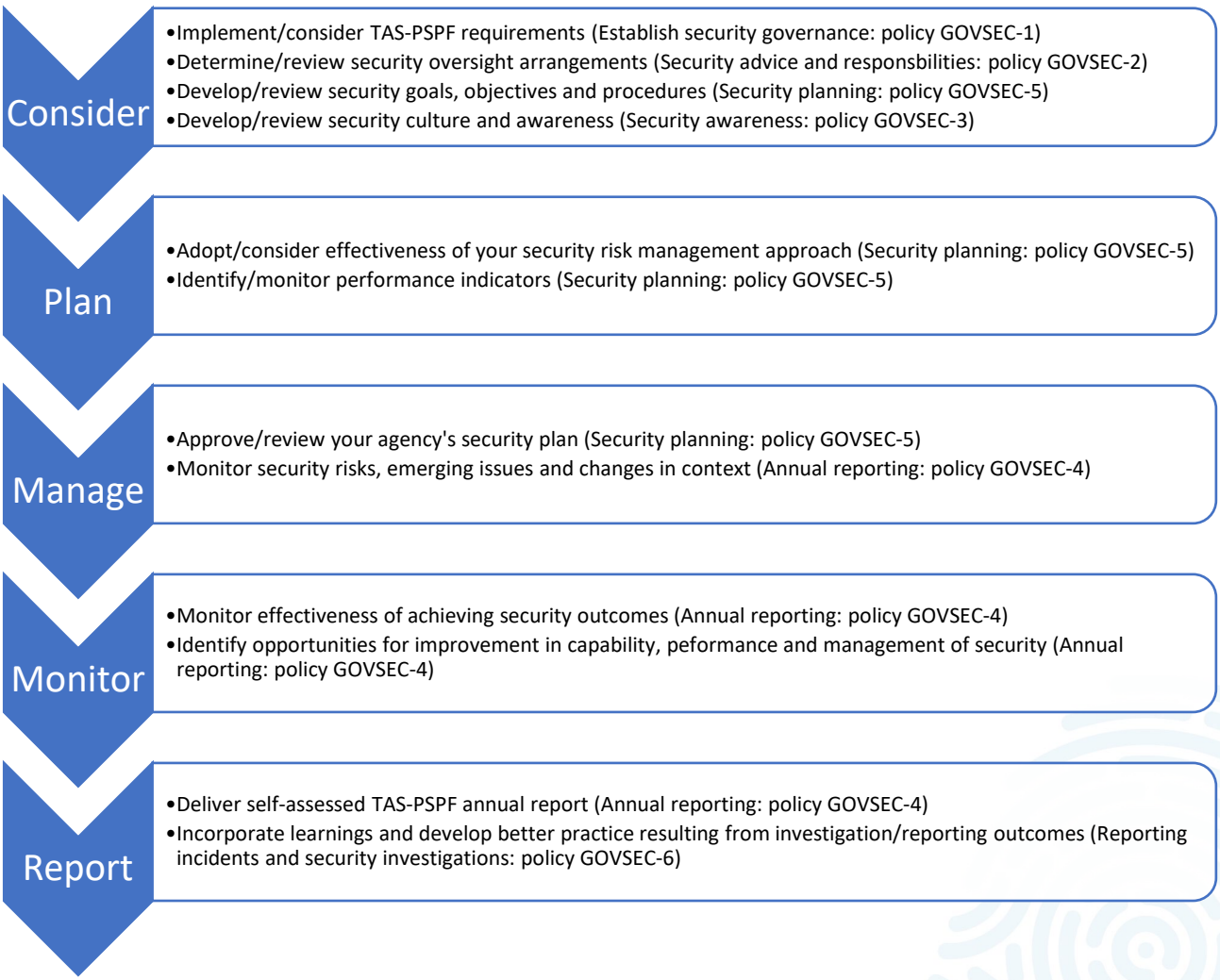
You should review the security maturity indicators in TAS-PSPF policy: Security planning (GOVSEC-5) when setting maturity targets and assessing security maturity.

You must assess your agency's progress towards achieving the agency maturity target and include any evidence to support that assessment. You should also describe the steps that will be taken to meet – or enhance – your agency's security maturity level over the next 12 months.

Gathering evidence of security maturity

TAS-PSPF policy: Security planning (GOVSEC-5) requires you to regularly monitor and assess your agency's security capability and risk culture by considering progress against the goals and strategic objectives identified in the security plan. Information collected through security maturity monitoring can be used to inform your agency's annual self-assessment report.

Figure 1 below shows possible information collection points during the process of planning, managing and monitoring your agency's path to security maturity, and aligns each point to the most relevant TAS-PSPF policy.



Security maturity can be highly subjective and difficult to compare across business units, let alone agencies of varied size and function, so information that will assist you to assess your agency's maturity may not always be obvious or evident. With this in mind, when you are setting security goals and maturity targets, you must seek, identify and document the best available evidence to support your agency's security maturity assessment.

Information which can contribute to security maturity assessments and monitoring may include:

- engagement with, and decisions on, security risk and risk tolerances
- risk mitigation strategies
- frequency and/or response to security incidents (including learnings)
- employee security behaviours (including security incidents)
- security training programs
- systematic and routine audits of security practices/procedures (including access controls)
- security issues reported (internally or externally)
- internal focus groups or security questionnaires
- horizon scanning for emerging or evolving threats, risks and vulnerabilities
- provision of security advice or services.

You can use the information collected to validate the maturity level of your agency and determine progress toward the maturity targets identified in your agency's security plan. You should use the maturity level indicators described above to guide planning and assessment of maturity.

Required action: Identify current vulnerabilities and key security risks

Your agency's annual self-assessment report includes your consideration of current vulnerabilities and key security risks to your agency's information, people and assets.

An agency's security risks and vulnerabilities may be influenced or changed by factors such as the risk environment, operational priorities, and security incidents. The priority of risks across your agency may change year on year as a result.

Identifying and reporting on the current vulnerabilities and key security risks affecting your agency provides you with invaluable insight and can be used to inform agency and government decision-makers. Analysing this information may highlight:

- risks identified under any of the 14 TAS-PSPF policies
- systemic or emerging risks
- significant risks not sufficiently mitigated
- significant risks that have insufficient protective security policy coverage.

DPAC uses information collected about key security risks to inform policy and develop strategies to mitigate security threats and vulnerabilities across government.

Security risk environment

Your agency's security risk environment is the environment in which it operates and is determined after considering the threats, risks and vulnerabilities affecting the protection of your agency's information, people and assets, including:

- what you need to protect (via your risk assessment), this being the information, people and assets assessed as critical to your agency's ongoing key business functions
- what you need to protect against (via your threat assessment), for example, face-to-face contact with the public, shared facilities)
- how the risk will be managed within your agency.

When determining your agency's risk environment, there are several security risk indicators you may consider, including:

- the sensitivity and security classification of information holdings, including consideration of aggregations of information and the classification of your agency's IT networks; refer to TAS-PSPF policy: Protecting official information (INFOSEC-2)
- the type of information held and the impact level of compromise, e.g. aggregations of personal information[1]

[1] See TAS-PSPF policy: Protecting official information (INFOSEC-2) for advice relating to business impact levels when determining the consequences of compromise or loss of agency information or assets, or harm to your people.

- the type of people (employees and contractors, security clearance holders or uncleared people) within the agency; refer to TAS-PSPF policy: Ongoing suitability assessment (PESEC-2)
- categories of assets held by the agency; refer to TAS-PSPF policy: Protecting assets (PHYSEC-1)
- the physical security zone levels defined in your agency's facilities; refer to TAS-PSPF policy: Protecting assets (PHYSEC-1).

Examples of threats, vulnerabilities and risks

Threats	Malicious action by trusted insider/s Malicious software attack (malware, ransomware, spyware) Cyber extortion (such as a distributed denial of service attack) Abuse of privileged access control Exploited customer data through secondary targeting
Vulnerabilities	Unpatched or uncontrolled portable devices Ineffectual security training or awareness Low resilience to natural disasters Poorly secured personal information Lack of effective cyber security monitoring Ineffective service provider/third party contracts Aggregated data not managed appropriately Inadequate firewalls Poor security culture Weak security clearance management Incomplete application control
Risks	Data breaches and spills Compromise of official/protectively marked information Incorrectly granting security clearance waiver Low resilience to natural disasters Poorly secured personal information Exploited customer data through secondary targeting

Required action: Identify treatment strategies

Your agency's annual self-assessment report should include details of the specific measures you have taken, or considered, to mitigate identified security risks and meet identified improvement opportunities, commensurate with your agency's risk profile.

For each core requirement, the TAS-PSPF reporting template will require you to provide:

- evidence of policy and procedures implemented to support the current assessed maturity level of your agency
- details of planned strategies and implementation activities you have identified to meet or enhance the maturity target for the following 12 months.

Useful resource: Examples of useful evidence when assessing security maturity

Outcomes	Relevant policies	Evidence examples
Security governance: Each agency identifies and manages security risks and supports a positive security culture while maintaining a cycle of continuous improvement.	GOVSEC-1: Establish security governance GOVSEC-2: Security advice and responsibilities GOVSEC-3: Security awareness GOVSEC-4: Annual reporting GOVSEC-5: Security planning GOVSEC-6: Reporting incidents and security investigations	• Security reports, plans, assessments, and reviews of security risk tolerances, measures and mitigations • Correspondence with relevant entities or bodies regarding security risks • Minutes from security risk management meetings • Annual reviews of security procedures • Register of people and security clearances, briefings and training requirements • Risk registers and threat assessments • Incident management procedures • Assessments and reviews of the agency's security plan • Critical assets and business continuity registers • Annual maturity assessment and records of alternative mitigations or variations of TAS-PSPF requirements
Information security: Each agency is responsible for maintaining the confidentiality, integrity and availability of all official information.	INFOSEC-1: Access to, and management of, official information INFOSEC-2: Protecting official information INFOSEC-3: Robust technology and information systems	• Register of key information holdings and ICT systems/controls, including details of legacy systems • Educational materials and campaigns on information security • Security breach logs, policies and frameworks, and register of remedial actions • Register of information sharing and agreements/arrangements for disclosures outside of government • Information reviews and audits, including of ICT system controls • Register or asset list or a software catalogue of approved applications • Patching plans and risk mitigation decisions • Register of ICT systems and determining authority
People security: Each agency ensures its people are suitable to access Tasmanian Government assets and	PESEC-1: Recruiting the right people PESEC-2: Ongoing suitability assessment	• People security register of employees, including contractors • Correspondence with authorised vetting agency • Security roles register • Suspicious and unusual contact register or log

Outcomes	Relevant policies	Evidence examples
meet the required standards of honesty and integrity.	PESEC-3: Managing separating people	• Signed agreements relating to security clearances, briefs, confidentiality and Australian Government policies • Training materials on people security • Performance management programs • Notifications to RE or security advisors on relevant cessations of employment • Records of exit interviews • Register of people risk assessments for separating employees
Physical security: Each agency provides a safe and secure physical environment for their information, people and assets.	PHYSEC-1: Protecting assets PHYSEC-2: Agency facilities	• Register of physical security measures, including security zones and assessments • Register of critical information, people and assets • Register of internal and external security risks • Register of Security Construction and Equipment Committee (SCEC) evaluated products and suitability assessment • Emergency security plan test • Visitor register • Physical safety/concern log • Register of contractors with regular access • Technical surveillance counter-measures inspection reports • Certifications and accreditations

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, Protective Security Policy Framework, at www.protectivesecurity.gov.au/resources/australian-government-and-international-resources
Australian Government, Reporting on security, at www.protectivesecurity.gov.au/system/files/2023-08/policy-5-reporting-on-security-pspf.pdf
SA Government, annual security attestation, at www.security.sa.gov.au/documents/SAPSF-GOVSEC4-Annual-security-attestation-B461278.pdf

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au