Physical Security

PHYSEC-2:
Agency facilities

Department of Premier and Cabinet

Tasmanian Government

Contents

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

About this document

This document – PHYSEC-2: Agency facilities – 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	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. 1. Security is a responsibility of government, its agencies and its people. 2. Each agency is accountable and owns its security risks.

Term	What this means in the context of the TAS-PSPF
	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.
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	A security incident is: • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.
security plan	Central document detailing how an agency plans to manage and address their security risks.
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.

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
BCA	Building Code of Australia
RE	Responsible Executive

Context

The **PHYSEC-2: Agency facilities** policy and guidance will assist agencies to achieve an effective protective security outcome within the physical security domain of the TAS-PSPF. They address core requirement 14 and its supplementary requirements.

Core requirement 14

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

Supplementary requirements

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

a) identifying security threats relevant to the facility location, functions and stored assets, in conjunction with any identified accompanying risk[1]

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

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

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

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

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

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

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

Guidance

Introduction

Physical security is a key component of your agency's protective security regime. It is a combination of physical and procedural measures designed to prevent or reduce the risks of compromise or harm to your information, people and assets.

Adopting physical security measures can assist your agency to:

- keep your people, clients and the public safe
- prevent unauthorised people accessing your information, people and assets
- maintain the trust and confidence of the people, agencies and organisations you work with
- deliver services without disruption in the event of increased threat levels.

To do this, you must know what you need to protect. In the physical security space, threats can come from your own people or from outside the agency. Threats are applicable to your information, people and assets when in the office or the usual place of business. Different threats may apply when your people are working away from the office.

Your agency's unique context and potential threats determine the physical security measures you need. Taking a risk-based approach will ensure that the physical security measures you implement are right for your agency's operating environment.

Required action: Identify security threats and accompanying risk

Under the TAS-PSPF, 'assets' refers to an agency's information, people and physical items, including ICT systems, technology and information infrastructure. Identifying assets which are critical to key functionality and ongoing operations is addressed in TAS-PSPF policy: Security planning (GOVSEC-5). GOVSEC-5 also requires agencies to develop a security plan that includes the prioritised application of protective security measures according to the security risks identified for the agency.

It is recommended that you use site-specific risk assessments to help you prepare site-specific security plans and to include security requirements within other site development plans. The physical protective security measures applied by your agency to its facilities and physical assets are vital to minimising risks of harm or compromise.

When you are determining physical protective security measures to be applied, it is important that they be proportionate to the threats you have identified and likely risk scenarios. Understanding threats against your agency will be the result of determining an adversary's intent to cause harm, damage or disruption to your agency's location, function and/or assets.

The physical facilities that house your agency's assets must be able to provide the level of protection required, as determined by risk assessments and the security plan in place for your agency. For this reason, you must incorporate protective security considerations into all processes related to facility design, selection and development, or modification of existing facilities.

Required action: Consider criticality of information, people and assets

TAS-PSPF policy: Protecting assets (PHYSEC-1) requires agencies to identify, categorise and keep a record of the agency's assets which require any level of physical protection.

In support of PHYSEC-1, this policy (PHYSEC-2) requires that when you are assessing risks, you consider the criticality of your agency's stored information, people and assets as relevant to the facility design, selection, development or modification of your agency's facility/ies. For more information about criticality assessments, please refer to TAS-PSPF policy: Security planning (GOVSEC-5).

Security planning also involves identifying the business impact level (BIL) of the compromise or loss of, or harm to, agency assets. BILs provide a consistent and coordinated method to categorising security risks and impacts across government. The BIL scale ranges from 1 (low) to 5 (catastrophic), where the higher the impact, the stronger the agency's protective security measures should be. The table below will assist you in defining the BIL of your agency's assets.[2]

[2] The coloured areas in the table relate to information classification; for details, see TAS-PSPF policy: Protecting official information (INFOSEC-2).

Business Impact Level	**1** **Low business impact**	**2** **Low to medium business impact**	**3** **High business impact**	**4** **Extreme business impact**	**5** **Catastrophic business impact**
Compromise, loss or harm to assets, including physical assets, expected to cause:	Insignificant damage to an individual, organisation or government.	Limited damage to an individual, organisation or government.	Damage to individuals, organisations, the state or national interests.	Serious damage to individuals, organisations, the state or national interests.	Exceptionally grave damage to individuals, organisations, the state or national interests.

Table 1 – Business impact levels: compromise or harm to assets

The protection of information, people and assets is achieved via a combination of procedural and physical security measures.

It is recommended that you use asset control systems to identify, protect, and monitor physical assets. Implementing asset control systems increases accountability and protects against theft, damage, and loss. Asset control procedures should include:

- recording the location and custodian of assets
- periodic auditing of assets
- reporting procedures for the loss or damage of assets.

Required action: Integrate protective security measures

At the earliest possible opportunity, you should consider how your agency will integrate physical security measures into the design, selection, development or modification of facilities.

Protective security measures are more likely to be effective if you address them at the concept and design stages when your agency is planning new sites/buildings, selecting new sites, and planning alterations to existing buildings.

When considering protective security measures for your agency's facilities, think about:

- the location and size of the site
- ownership or tenancy of the site (e.g. sole occupancy, shared tenancy, multiple agencies/entities)

- collateral exposure (e.g. proximity to other categories of physical assets)
- access needs to the site (e.g. authorised personnel only, public access)
- security classification of information, activities and assets (including ICT assets) to be stored, handled or processed in the facility, or parts of the facility
- the category of other assets stored on the site
- periods of greatest or increased risk (e.g. business hours or out-of-hours)
- protective security measures required for –
    - the site as a whole
    - particular areas within the site (e.g. where a space or floor will hold information of a higher classification than the remainder)
    - storage, handling and processing of security-classified information
    - security-classified and other sensitive discussions and meetings.

Site selection

It is recommended that your Responsible Executive (RE) and Agency Security Advisor (ASA) are involved in the assessment of:

- the suitability of the physical security environment of a proposed site for agency facilities
- whether the facility can be constructed or modified to include the security measures that will provide the appropriate level of protection.[3]

There are several physical security risk factors to consider before a site is selected for your agency. The table below describes some of these factors.

[3] Physical security measures are designed to reduce the likelihood of security events; the site and design must also accommodate normal business.

Factor	Description
Neighbourhood	The neighbourhood may present security-related issues, e.g. local crime activity, risks from neighbouring entities or businesses, suitability of neighbours, and risks associated with oversight of operations.
Standoff perimeter	Standoff perimeters refer to the distance placed between a facility and any identified threat e.g. hostile people and vehicle-borne attacks. It may not be possible to achieve an effective standoff perimeter in urban areas for some threats. It is recommended that agencies seek further advice where specific or known threats have been identified.[4]
Site access and parking	The need and ability to control access of pedestrians and vehicles to the site. This includes the facility itself, parking and the required standoff perimeter.
Building access point	The ability or need to secure all building access and egress points, including entries and exits, emergency exists, air intakes and outlets, and service ducts.
Security zones	Establishing security zones based on – a) agency risk assessments business impact levels security-in-depth at the site.[5]
Environmental risks	Natural disasters and potential mitigation strategies.

Table 2 – Physical security risk factors

Construction of buildings

All building work in Australia (including new buildings and building work in existing buildings) must comply with the requirements of the Building Code of Australia (BCA).[6] The BCA classifies buildings according to the purpose for which they are designed, constructed or adapted to be used. The BCA requirements for commercial buildings, including facilities used by agencies, provide an increased level of perimeter protection as well as protection for assets and information where their compromise, loss of integrity or unavailability would have a business impact level of medium or below.

[4] Where a specific or known threat has been identified, further information (e.g. hostile vehicle mitigations, blast mitigations) is available via the ASIO Outreach website, requiring registration for an account.

[5] Security-in-depth is a multi-layered approach to security, where measures combine to increase difficulty for intruders or authorised people to gain unauthorised access.

[6] Refer to the *Building Act 2016* for relevant state legislation in accordance with the BCA.

You may include additional building elements to address specific risks identified in the risk assessment for your agency where building hardening[7] may provide some level of mitigation. For example:

- blast mitigation measures
- forcible attack resistance
- ballistic resistance
- siting of road and public access paths
- lighting (in addition to security lighting).

TAS-PSPF policy: Protecting official information (INFOSEC-2) requires that agencies using Zones 2-5 for storage of sensitive or security-classified information and assets must construct facilities in accordance with the relevant sections of ASIO Technical Note 1/15: Physical security of zones.[8] It further requires that agencies constructing Zone 5 areas that will store TOP SECRET information or aggregated information – the compromise, loss of integrity or loss of availability of which may cause catastrophic damage – must also use ASIO Technical Note 5/12: Physical security of Zone 5 (TOP SECRET) areas.

Required action: Conduct reviews of physical security measures

Your ASA is responsible for conducting regular reviews of your agency's physical security measures to monitor their efficacy, relevance and use, while confirming they are fit for purpose.

It is recommended that your agency uses a combination of methods, such as monitoring, reporting, reviewing and auditing, to help determine if:

- physical security policies are being followed
- physical security controls are effective
- any new threats or practices have developed.

[7] The process of making a building a less attractive and more difficult target.

[8] ASIO Technical Notes detail protective security mitigations to maintain the confidentiality and integrity of sensitive and security-classified information and assets. Access to the Technical Notes is via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

You should anticipate that your agency's security threats and vulnerabilities will change. Preparing for change will be supported by conducting regular reviews of all protective security measures. Revising your agency's physical security measures as appropriate will enable the contemporary and proactive maintenance of requirements under the TAS-PSPF.

Agencies must communicate changes that affect their people and advise them of any new policies and procedures as they are introduced. The TAS-PSPF policy: Security planning (GOVSEC-5) requires agencies to review their security plans at least every 2 years. However, you should consider your agency's security plan to be a living document that can accommodate the evolving environment and changes which may be required.

References and resources

Australian Government, GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.	
Australian Government, Protective Security Policy Framework, at www.protectivesecurity.gov.au/system/files/2022-09/pspf-policy15-physical-security-for-entity-resources.pdf	
Australian Government, Protective Security Policy Framework, at www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-16-entity-facilities_0.pdf	
ASIO T4 Protective Security, Security Managers Handbook – Introduction to protective security measures, available to authorised people via the GovTEAMS protective security community.	
SA Government, protective security, at www.security.sa.gov.au/documents/SAPSF-PHYSEC1-Physical-security-B463483.pdf.pdf	
Tasmanian Legislation	*Building Act 2016*

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7979

Email:
sem@dpac.tas.gov.au