



# Physical Security

## PHYSEC-I: Protecting assets





# Contents

---

<b>About this document</b>	<b>3</b>
<b>Definitions and shortened terms</b>	<b>5</b>
<b>Context</b>	<b>10</b>
<b>Guidance</b>	<b>12</b>
Introduction	12
Required action: Identify, categorise and keep records of assets	12
Required action: Implement proportionate physical security measures	15
Required action: Zone work areas	17
Required action: Apply control elements	20
Required action: Separate ICT infrastructure, equipment and facilities	28
Required action: Certify and accredit security zones	30
Required action: Dispose of physical assets securely	32
Required action: Ensure accreditation of worksites away from agency locations	32
<b>References and resources</b>	<b>43</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 – PHYSEC-I: Protecting assets – 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-PSPF 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.



## OFFICIAL

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. <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
	<p>3. Security will be guided by a risk management approach.</p> <p>4. Strong governance ensures protective security is reflected in agency planning.</p> <p>5. A positive security culture is critical.</p>
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	<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.



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
EACS	electronic access control system
PIDS	perimeter intrusion detection system
RE	Responsible Executive
SCEC	Security Construction and Equipment Committee
SEEPL	Security Equipment Evaluated Product List
SL	security level (rating from 1-4)
SAS	security alarm systems
TSCM	Technical surveillance counter-measures



## Context

---

The **PHYSEC-I: Protecting assets** 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 13 and its supplementary requirements.

### Core requirement 13

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

### Supplementary requirements

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

- a) identify, categorise and keep a record of the agency's assets which require any level of physical protection<sup>1</sup>
- b) implement physical security measures proportionate to the identified threat and likely risk scenario, using the assessed business impact of harm or compromise to agency assets - this may include -
  - a. zoning of work areas (e.g. access controls, security screening)
  - b. application of required individual control elements (e.g. secure storage, site locations, perimeter measures, security lighting)
  - c. separated ICT infrastructure, equipment and facilities
- c) certify and accredit all security zones on all premises for which the agency has responsibility<sup>2</sup>
- d) dispose of physical assets securely
- e) implement procedures to ensure appropriate accreditation of proposed worksites outside the office. Provide training to all people, in the correct use and application of the agency's physical security measures.

---

<sup>1</sup> This will be based on the agency risk assessment and business impact levels.

<sup>2</sup> Refer to ASIO Technical Notes to ascertain the requirements of security zones and associated processes. Access is via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.





## OFFICIAL

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

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





## 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, categorise and keep records of assets

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).

Identifying your agency's critical assets enables you to prioritise the application of protections to those assets. Understanding your assets, including their value and sensitivity, is essential to accurately assess your physical security risks.



Physical security measures provide an essential layer of protection that minimises the risks of compromise or harm to your agency's assets – your information, your people, and your physical items.

## Information

Information is a valuable asset and requires protection. The TAS-PSPF policy: Protecting official information (INFOSEC-2) provides guidance relating to the classification, protective marking, transfer, handling and storage requirements of information assets.

The physical security measures applied by an agency, in support of these requirements, will strengthen the protection of information assets, reducing the likelihood of compromise to those assets.

## People

An agency's people are central to its operations and require protection from harm. This policy (PHYSEC-I) reinforces the requirement of the *Work Health and Safety Act 2012* that an agency protects its people and others from harm. This is achieved by minimising exposure to risks and providing support in the event of a harmful or traumatic incident.

It is recommended that agencies implement appropriate physical security measures to ensure the personal security of their people, while working in the office and away from the office, to support compliance with the *Work Health and Safety Act 2012*.

## Physical assets

Physical assets are tangible items that are valuable to an agency and require protection. Protection includes ensuring continued operability and accessibility, as appropriate, and preventing any unauthorised access, use or removal.

Physical assets can be categorised as follows.

Category/Description	Factors to consider
<b>Attractive</b> This category of asset may not always be valuable but is desired.	<ul style="list-style-type: none"> <li>The function of the asset is desirable, i.e. it holds information which may be attractive to an outsider.</li> <li>Portable assets which could be easily removed with limited likelihood of detection, regardless of the information held within.</li> </ul>
<b>Classified</b> This category of asset is classified in its own right or is classified due to the confidentiality requirements	<ul style="list-style-type: none"> <li>The level of the classification of the asset.</li> <li>The mobility and accessibility of the classified asset.</li> </ul>



Category/Description	Factors to consider
of the information held on the asset (e.g. ICT equipment).	<ul style="list-style-type: none"> <li>The assessed business impacts which resulted in the security classification of the asset.</li> </ul>
<b>Dangerous</b> This category of asset considers its likelihood to inflict harm (e.g. weapons or hazardous material).	<ul style="list-style-type: none"> <li>The quantity and type of dangerous assets being stored, e.g. storerooms with large quantities of chemicals that could be weaponised or armoury rooms or disposal holding locations.</li> <li>The level of public awareness/concern about the presence of the assets.</li> </ul>
<b>Important</b> This category of asset considers the significance of the asset's integrity or availability for the agency's operations.	<ul style="list-style-type: none"> <li>The integrity of the asset.</li> <li>The consequences should the asset be unavailable or inoperable when it is needed.</li> </ul>
<b>Significant</b> This category of asset has cultural or national significance, regardless of monetary value.	<ul style="list-style-type: none"> <li>The intrinsic value to the state or national identity.</li> <li>The negative reputational effect of the loss or damage of the asset.</li> </ul>
<b>Valuable</b> This category of asset relates to monetary value.	<ul style="list-style-type: none"> <li>The financial viability and time required to replace or repair the asset.</li> <li>The capability of the agency to operate without the asset or with partial functionality.</li> <li>The level of importance the asset has to the agency's function or capability.</li> </ul>

Table I – Categories of physical assets and factors to consider

## Asset controls

It is recommended that your agency implements asset controls. Asset controls are useful as they identify asset holdings while serving as a mechanism to protect against theft, damage and loss.

Asset control procedures should include:

- recording the location and authorised custodian of the asset/s
- periodic auditing of the asset/s
- reporting requirements for the loss or damage of any asset/s.



## Required action: Implement proportionate physical security measures

The protections required for, and that can effectively be applied to, physical assets will be affected by the category of asset and the business impact level of the compromise or loss of, or harm to the asset. The table below will assist you in defining the business impact level of your agency's physical assets.<sup>3</sup>

<b>Business impact level</b>	<b>1 Low business impact</b>	<b>2 Low to medium business impact</b>	<b>3 High business impact</b>	<b>4 Extreme business impact</b>	<b>5 Catastrophic business impact</b>
Compromise, loss or harm to asset, 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 2 – Business impact levels: compromise or harm to assets

After determining the business impact level of an asset, your Accountable Authority must implement commensurate physical security measures according to the assessed risk.

It is recommended that your agency protects its assets by using a combination of physical and procedural security measures to achieve this outcome.

In determining the physical security measures required to protect your agency's assets, you should consider the cost of security measures, ensuring they are proportionate to the mitigation of the identified threats and likely risk scenario/s.

<sup>3</sup> The coloured areas in the table relate to information classification; for details, refer to TAS-PSPF policy: Protecting official information (INFOSEC-2).



Any physical security measures you take should ideally be capable of achieving all, or at least a combination, of the outcomes listed in the table below.

Outcome	Description
Deter	Measures that cause significant difficulty or require specialist knowledge and tools for adversaries to defeat.
Detect	Measures that identify unauthorised action is being taken or has already occurred.
Delay	Measures to impede an adversary during attempted entry or attack or slow the progress of a detrimental event to allow a response.
Respond	Measures that prevent, resist, or mitigate an attack or event when it is detected.
Recover	Measures to restore operations to normal levels (as soon as possible) following an event.

Table 3 – Protective security outcomes

## Measures to protect agency assets

In applying physical security measures, you can implement various protections to address the risk of assets being made inoperable or inaccessible or being accessed, used, or removed without proper authorisation.

Tables 1 and 2 above will help you to categorise your physical assets and identify the level of business impact of any compromise, loss, or harm to an asset. Knowing these things will in turn help you to determine the physical security measures needed to protect the asset.

Below is an example of this process in action.

### Example:

*Your agency holds a database with comprehensive information relating to your staff. On face value, the information in the database does not warrant security classification as the business impact level of compromise of its confidentiality is assessed as 'medium'. However, the database is determined critical to the business operations of the agency which indicates the categorisation of the database may best be as an 'important' asset. Considering the factors relevant to 'important' assets and the integrity and availability of the database, you may determine the business impact level in relation to compromise of its integrity and availability to be 'extreme'.*

*As a result of this determination, the database is now marked and handled as Official: Sensitive. Due to the 'extreme' business impact level of the database, greater protections are applied to protect the integrity and availability of the database.*



The following physical security measures are considered to provide protection.

CCTV	security alarm systems
electronic access control	secure storage
emergency communication systems	security and trespass warning signs
perimeter security measures	security doors, screens, and keying systems
perimeter intrusion detection systems	security lighting
security screening equipment	

Table 4 – Examples of physical security measures

## Required action: Zone work areas

Your agency may contain various divisions, business areas and alternate sites. These variations are likely to influence the assets held within certain workspaces.

Zoning specific work areas can help you to scale physical security measures based on your security risk assessment.

Security zones are numbered 1-5, with increasing restrictions and access controls as the zone number rises.

Extra physical security measures apply to areas where protectively marked information and other official or valuable assets are processed, handled, and stored. The physical security measures applied to each of these areas are designed to protect the contained items from compromise, either accidentally or maliciously.

Where you identify increased threat levels to your agency's environment, you must consider what additional measures are required to protect assets and whether a change in zone storage is required.

To aid the ongoing management of physical security in your agency, you must:

- certify and accredit all security zones on all premises for which your agency has responsibility<sup>4</sup>
- dispose of physical assets securely

<sup>4</sup> Refer to ASIO Technical Notes to ascertain the requirements of security zones and associated processes. Access is via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.



- implement procedures to ensure appropriate accreditation of proposed worksites outside the office.
- provide training to all people in the correct use and application of your agency's physical security measures.

The different security zones are explained below.

## **Understanding security zones**

### **Zone 1: Public access areas**

Public access areas are unsecured zones and include out-of-office working arrangements. They provide limited access controls to information and physical assets and limited protection for people. Storage, handling, processing and discussion of security-classified information should not be conducted within a Zone 1 area, due to the public access in these areas.

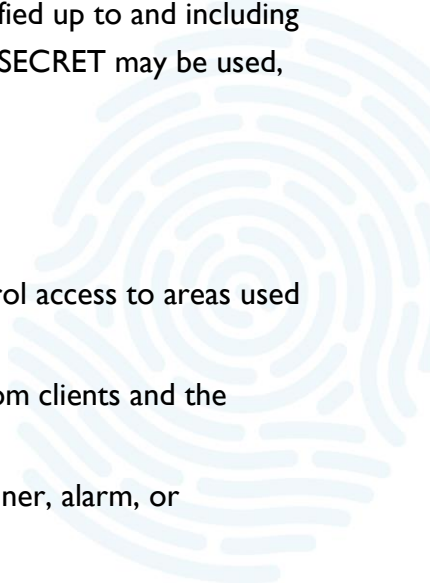
Examples of Zone 1 areas include:

- building perimeters and public foyers
- interview and front-desk areas
- temporary out-of-office work areas where your agency has no control over access
- field work, including most vehicle-based work
- public access areas within multi-building facilities (e.g. cafes).

### **Zone 2: Work areas**

Work areas are low-security areas with some controls. This zone is typically the first layer of protection for information, people and assets. Information and assets classified up to and including PROTECTED may be used and stored. Information and assets classified as SECRET may be used, but not stored.

Examples of Zone 2 work areas include:

- normal office environments
  - normal out-of-office or home-based worksites where you can control access to areas used by your agency
  - interview and front-desk areas where your people are separated from clients and the public
  - vehicle-based work where the vehicle is fitted with a security container, alarm, or immobiliser
  - exhibition areas with security controls and controlled public access.
- 



### **Zone 3: Restricted work areas**

Restricted work areas are security areas with higher security controls. They provide access controls to information and assets where a loss would result in a business impact up to extreme. Information and assets classified up to and including SECRET may be used and stored. They provide layered protection for people.

Access to this zone is limited according to 'need to know' and security clearances – all visitors must be escorted, or closely monitored, and have a business need to access the area.

Examples of Zone 3 areas include:

- storage area for highly valuable assets
- secure areas within an agency building that have additional access controls for your people.

### **Zone 4: Security areas**

These are areas with high levels of security. These areas provide access controls to information where any loss would result in a business impact to extreme and assets where any loss would result in a business impact up to catastrophic. They provide layered protection for people.

People with ongoing access must hold a security clearance. Visitors and contractors must be closely controlled and have a business need to access the area.

Examples of Zone 4 areas include:

- secure areas within your agency's building/s that have additional access controls for authorised staff
- storage area for highly valuable assets, with additional asset protection controls.

### **Zone 5: Highly restricted security areas**

These are the highest security zones. They are restricted with dual authentication applied to access controls. These areas are likely to contain information and assets with a business impact of catastrophic. Visitors and contractors must be closely escorted and demonstrate a 'need to know'.

Zone 5 areas include Australian intelligence community facilities.

### **Zoning control elements**

Each of the security zones requires specific control elements to meet the required level of protection. Implementing control elements provides assurance against:



- the compromise, loss of integrity or unavailability of sensitive or security-classified information
- the compromise, loss or damage of sensitive or security-classified assets.

Control elements must be in accordance with ASIO Technical Notes<sup>5</sup> which dictate the minimum requirements to protect sensitive and security-classified information and assets. For more information, refer to Annexure I: Physical protections for security zones.

## Required action: Apply control elements

### Security Construction and Equipment Committee-approved equipment

The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment and determining which products will be evaluated and the priority of that evaluation.

The SCEC then assigns evaluated equipment a security level (SL) rating from 1-4, which is based on the level of security it has been assessed to provide, in increasing order. Products rated at SL1 provide the lowest acceptable level of security for government use.

Approved products are listed in the SCEC Security Equipment Evaluated Product List (SEEPL). This is available to government users via the GovTEAMS Protective Security Policy community.<sup>6</sup>

While it is not a mandated requirement that you use SCEC-approved equipment, it is recommended that you use SCEC-approved equipment for strengthened protection of your agency's assets. Alternatively, you can use suitable commercial equipment as long as it complies with the identified security-related Australian and International Standards for the protection of people, information, and assets.

### Security containers and cabinets

Layering your physical security measures includes using security containers and cabinets. Security containers and cabinets can be used to protect information, portable and valuable assets, and money. You must identify the need for, and the most appropriate type of, security cabinets or containers to secure your agency's assets.

---

<sup>5</sup> Access to ASIO Technical Notes is via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

<sup>6</sup> Access via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.



When choosing the most appropriate security container or cabinet, it is recommended that you consider:

- the type of assets (refer to Table I – Categories of physical assets and factors to consider)
- the quantity or size of information and assets
- the location of the information or assets within your facility
- the structure and location of your facility
- the access control systems
- other physical protection mechanisms, for example, locks and alarms.

It is recommended that you store sensitive and security-classified information and assets in security containers and cabinets separately from physical assets. Ensuring separation decreases the risk of multiple compromises.

For information on selecting security containers to store official information, refer to TAS-PSPF policy: Protecting official information (INFOSEC-2).

## **Managing security containers and cabinets**


If not managed appropriately, security containers and cabinets can be a security risk. It is recommended that keys to security containers and cabinets are secured in key cabinets within an agency's perimeter and where possible, within the security zone where the containers and cabinets are located.

For containers or cabinets secured with a combination setting, it is recommended that the combination is changed:

- every 6 months
- following repairs
- following change of employees
- when there is reason to believe there has been or may have been a compromise.

## **SCEC-approved security containers**

SCEC-approved security containers are for the storage of sensitive and security-classified information and assets. These containers are designed to provide a high level of tamper evidence from covert attack and significantly delay other attacks.





There are 3 levels of SCEC-approved security containers:

- Class A – protect information with a business impact level of extreme or catastrophic when it has been assessed as high risk. These containers are a significant structure and will not always be suitable in premises with restricted floor loadings.
- Class B – protect information with a business impact level of extreme or catastrophic when it has been assessed as low risk. These containers can also be used to store information with a business impact level of high or extreme when it has been assessed as high risk.
- Class C – protect information with a business impact level up to extreme when it has been assessed as low risk. These containers can also be used for information with a business impact level of medium when it has been assessed as high risk.

## **Key cabinets**

You can use manual and electronic key cabinets to secure keys (e.g. keys for Class C containers or internal offices). These should be located within the security zone or near the zone where the security containers or cabinets are located. Some electronic key cabinets may have an automated audit capacity which means you won't need to maintain a key register. Electronic key cabinets may also be integrated into your electronic access control system/s.

SCEC have approved various Class B key cabinets; however, these provide the same level of protection as other SCEC-approved Class B cabinets (e.g. filing cabinets and cupboards). SCEC-approved electronic Class C and B key containers are recommended to store keys for Zones 4 and 5, and for Class C containers.<sup>7</sup>

## **Commercial safes and vaults**

Commercial safes and vaults provide a level of protection against forced entry. A vault is a secure space that is generally built in place. A safe may be portable and is typically smaller than a vault. Both safes and vaults provide varying degrees of protection, depending on their construction, use and location. They may both be used to store valuable physical assets.

It is recommended that you seek advice from qualified locksmiths or manufacturers when deciding the criteria to apply to select commercial safes and vaults. Guidance is available in Australian/New Zealand standard AS/NZS 3809-1998 – Safes and strongrooms.

---

<sup>7</sup> For advice, refer to ASIO SEG-013 Electronic Key Cabinets, available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.



## OFFICIAL

The table below may also assist you as you consider commercial safes and vaults for your agency.

<b>Business Impact Level</b>	<b>1 - Low Impact</b>	<b>2 - Low to medium business impact</b>	<b>3 - High business impact</b>	<b>4 - Extreme business impact</b>	<b>5 - Catastrophic business impact</b>
<b>Zone 1</b>	Determined by an agency risk assessment – locked commercial container recommended.	Determined by an agency risk assessment – commercial safe or vault recommended.	AS/NZS 3809-compliant commercial safe or vault.	AS/NZS 3809-compliant high-security safe or vault.	Not to be held unless unavoidable.
<b>Zone 2</b>	Determined by an agency risk assessment – locked commercial container recommended.	Determined by an agency risk assessment.	Commercial safe or vault.	AS/NZS 3809-compliant medium-security safe or vault recommended.	Not to be held unless unavoidable.
<b>Zone 3</b>	Determined by an agency risk assessment.	Determined by an agency risk assessment.	Determined by an agency risk assessment – locked commercial container recommended.	AS/NZS 3809-compliant commercial vault or safe.	AS/NZS 3809-compliant high or very high-security safe or vault recommended.
<b>Zone 4</b>	Determined by an agency risk assessment.	Determined by an agency risk assessment.	Determined by an agency risk assessment.	Commercial safe or vault recommended.	AS/NZS 3809-compliant medium or high security safe or vault recommended.
<b>Zone 5</b>	Determined by an agency risk assessment.	Determined by an agency risk assessment.	Determined by an agency risk assessment.	Commercial safe or vault recommended.	AS/NZS 3809-compliant medium or high-security safe or vault recommended.

Table 5 – Selecting commercial safes and vaults



## **Vehicle safes**

You may consider fitting vehicles used by staff with field safes to carry valuable assets and official information. Vehicle safes provide some protection against theft but only when vehicles are fitted with other anti-theft controls.

## **Secure rooms and strongrooms**

You may consider using secure rooms and strongrooms instead of containers to secure large quantities of official information, classified assets, and valuable assets, where compromise or harm would have a high business impact level.

A secure room is designed to protect its contents from covert attack and has a degree of fire protection, if correctly constructed.<sup>8</sup> Secure rooms are suitable for storage of large quantities of official information and classified assets, while maintaining the levels of protection provided by a Class A, B or C container.

## **Audio security measures**

It is recommended that you implement audio security measures to prevent overhearing in areas where discussions and/or meetings relating to sensitive and security-classified information are held.

Rooms or areas where sensitive or security-classified discussions are held should be acoustically treated so that sound created within the space is inaudible to a person or device outside that area. Appropriate and effective sound insulation is critical to achieving the required level of security for sensitive and security-classified discussions.

If your agency needs to engage in sensitive or security-classified discussions in unsecured areas, it is recommended that you take all available steps to reduce the likelihood that those conversations are overheard.

## **Security alarm systems**

Security alarm systems (SAS) detect unauthorised access to an agency's facilities. SAS are only effective if used in conjunction with layered physical security measures to delay or respond to the detected unauthorised access.

SAS can be broadly divided into 2 categories:

---

<sup>8</sup> For information relating to the construction of secure rooms and strongrooms, refer to ASIO Technical Notes: 7-06, 8-06 and 9-06. Available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.



- perimeter (external) intrusion detection systems (PIDS) or alarms
- internal security alarm systems.

It is recommended that SAS are configured to monitor your agency's high-risk areas (e.g. infrequently accessed areas, roof spaces, inspection hatches and underfloor cavities).

To support the operation of SAS, you must facilitate periodic maintenance and testing via an authorised service provider. It is recommended that maintenance and testing happen at least every 2 years to ensure all systems are operational.

## **Security guards**

Security guards provide a physical presence at agency facilities and a swift response to security incidents. It is recommended that if you are thinking about using security guards, consider:

- the level of threat and/or risk
- if guards need to be onsite or offsite
- security clearance requirements based on the security zone and frequency of access
- confirming that guards hired are licensed in Tasmania.

## **Access control**

Access control measures are designed to limit access to authorised people, vehicles and equipment, while preventing unauthorised access. Measures of access control include:

- security guards located at premises access/egress points
- security guards located in a central area who control access/egress via intercoms, videophones and CCTV
- electronic access control systems (EACS)
- mechanical locking devices – controlled with keys or codes.

## **Electronic access control systems**

EACS are mandatory for Zones 3-5, where no other suitable identity verification and access control measures are active. In managing Zones 3-5, your agency must:

- have sectionalised access control systems and full audit capacity
- regularly review and audit your EACS for unusual or prohibited activity or access.

When implementing EACS, it is recommended that you:



- seek relevant specialist advice during selection and design
- use an appropriate installer recommended by the manufacturer to install and commission the system/s
- regularly audit EACS across all agency security zones and areas, in accordance with your risk assessment and security plan.

## **Identity cards**

Identity cards allow recognition of people across agency facilities. Zones 3-5 require identity cards with personal verification for all people using these facilities.

It is recommended that your agency use identity cards across all facilities, regardless of the level of formal zoning.

Identity cards should only be issued to people who have had their identities validated as per TAS-PSPF policy: Recruiting the right people (PESEC-I).

It is recommended that you use the National Identity Proofing Guidelines<sup>9</sup> to at least Level 3 for people not covered by the TAS-PSPF (e.g. contracted service providers).

Identity card-making equipment and all spare, blank or returned cards should be secured according to the security risk assessment (Zone 2 or higher).

Identity cards should be:

- uniquely identifiable
- worn and clearly displayed by authorised people while on agency premises
- regularly audited in accordance with your agency's risk assessments and security plan.

## **Visitor controls**

A visitor is any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency. All visitors should be issued with visitor access passes which are access controlled according to the visitor need. All passes should:

- be visible at all times
- be collected and disabled at the end of the visit
- audited regularly

---

<sup>9</sup> For further information, please refer to the National Identity Proofing Guidelines on the Department of Home Affairs website at [www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf](http://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf)



- not be shared with other visitors.

## Perimeter measures

Some agencies may require perimeter access control measures, based on agency risk assessments. Perimeter access control measures may be in the form of:

- fences and walls
- pedestrian barriers, ingress/egress points
- vehicle security barriers.

The effectiveness of any perimeter measure is dependent on construction, environmental design and other layered protective security measures. When you are designing and implementing perimeter measures, refer to the relevant Australian Standards and ASIO-T4 documents.<sup>10</sup>

## Security lighting


The use of security lighting can support surveillance of the perimeter and approaches to your agency's buildings and facilities. When applied correctly, security lighting can enhance safety for staff and visitors. Lighting should be placed with consideration to reducing or removing capacity for people to hide or conceal around the buildings and facilities.

When thinking about security lighting for your agency's buildings and facilities, consider:

- the general area and coverage required
- environmental conditions
- site-specific requirements (i.e. ingress/egress, vehicle parking, walkways).

---

<sup>10</sup> Refer to ASIO Security Equipment Guide SEG-003 Perimeter Security Fences and SEG-024 Access Control Portals and Turnstiles, available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community. Also refer to AS 1725.1:2010 Chain link fabric fencing – security fences and gates and AS/NZS 3016:2002 Electrical installations – electric security fences.





## Required action: Separate ICT infrastructure, equipment and facilities

### ICT equipment

Agencies should implement an ICT equipment management policy to ensure that ICT equipment, and the data it processes, stores or communicates, is protected in an appropriate manner.

ICT equipment includes:

- movable physical assets, e.g. computers, photocopiers, multi-function devices, mobile phones, storage media
- system equipment, e.g. hardware and software
- building management systems and security systems.

ICT system equipment is generally operational 24-hours a day and may include:

- servers, e.g. dedicated devices and laptops used as servers
- communication network devices, e.g. PABX systems
- supporting network infrastructure, e.g. cabling, patch panels
- gateway devices, e.g. routers, network access devices.

ICT equipment, as an agency asset, requires specific protection because of:

- the classification of the information held on the asset, the business impact level of compromise or harm to that information, or the classification of the asset itself
- the criticality of integrity or availability of the information held or processed on the asset
- the potential attractiveness of either the information held or the asset in its own right
- the aggregation of information, which may increase the business impact level of the asset's compromise.

It is recommended that to identify the appropriate physical security measures to protect ICT assets and the information held or communicated on them, you base the level of protection required on the highest business impact level that would result from:

- the compromise, loss of integrity or unavailability of the aggregate of electronic information held on the equipment, or
- the loss or unavailability of the ICT equipment itself.



## ICT facilities

It is recommended that you have dedicated ICT facilities to house your agency's ICT equipment and systems. These facilities may include:

- server and gateway rooms
- data centres
- back-up repositories
- storage areas for ICT equipment that holds official information
- communication and patch rooms.

It is recommended that you locate your agency's ICT facilities in security zones dedicated to these facilities and separate to other functions. Remember that you must store sensitive or security-classified information in accredited security zones.

ICT facilities may be housed in a separate security zone, within an existing security zone (i.e. the work area is a Zone 3 and within that Zone 3 is a separate Zone 4 for the ICT facilities). Where ICT equipment is held in one of these separate security zones, the required level of physical security of containers and/or rooms to protect the ICT equipment may be lowered, so long as the security zone is suitable for the aggregation of the information held.

The following table demonstrates storage container requirements for electronic information in ICT facilities.

Business impact level of aggregated electronic information	Security zone of the work area	Security container or secure room ordinarily required	Additional security zone within work area for ICT facility	Security container or secure room required for ICT equipment
<b>1 - Low business impact</b>	Zone 2	Lockable commercial cabinet	No additional zone required	Lockable commercial cabinet
	Zone 1	Lockable commercial cabinet	Zone 2 or above	Lockable commercial cabinet
<b>2 - Low to medium business impact</b>	Zone 2	Lockable commercial cabinet	No additional zone required	Lockable commercial cabinet
	Zone 1	SCEC Class C	Zone 2 or above	Lockable commercial cabinet



<b>3 - High business impact</b>	Zone 3 or above	SCEC Class C recommended for Zone 3. Lockable commercial cabinet for Zones 4 and 5	No additional zone required	SCEC Class C recommended for Zone 3. Lockable commercial cabinet for Zones 4 and 5
	Zone 2	SCEC Class C	Zone 3 or above	Lockable commercial cabinet
			Zone 2	SCEC Class C
<b>4 - Extreme business impact</b>	Zone 4	SCEC Class C	Zone 3 or above	Lockable commercial cabinet
			Zone 2	SCEC Class C
	Zone 3	SCEC Class B	Zone 4 or above	Lockable commercial cabinet
			Zone 3	SCEC Class C
			Zone 2	SCEC Class B
<b>5 - Catastrophic business impact</b>	Zone 5	SCEC Class B	Compartment (certified by Chief Security Officer)	SCEC Class C

Table 6 – Storage container requirements for electronic information in ICT facilities

## Access control to ICT equipment and facilities

Agencies must control access to ICT facilities in line with the relevant security zone. In circumstances where the business impact is lower than catastrophic, agencies may consider the following controls to limit access to ICT facilities:

- a dedicated section of the SAS or an EACS
- people physically administering access to authorised people.

When not in use or unattended, ICT equipment must be secured appropriately according to the classification or business impact level of the stored information or asset.

## Required action: Certify and accredit security zones

Information sharing is crucial to government business and requires a level of confidence between Tasmanian Government agencies, interjurisdictional and national counterparts. Certification and



accreditation of security zones are a means to strengthen the level of confidence in the ability of agencies to share, access and protect information according to classification.<sup>11</sup>

## Certification

Certification of security zones establishes compliance with the minimum physical security requirements to the satisfaction of the relevant certification authority.

Implementation and operation of control elements in Zones 1-4 may be certified by your agency's Responsible Executive (RE) or delegated Agency Security Advisor (ASA).

Annexure 2 provides a summary of the certification authorities for the relevant control measures.

## Accreditation

Accreditation of security zones involves compiling and reviewing all applicable certifications and other deliverables for the zone to determine and accept the residual security risks. Approval for each security zone to operate at the desired, or required level, is only granted for a specified time. For your agency's Zones 1-5, the RE (or delegated ASA) is the accrediting authority when the controls are certified as meeting the requirements summarised in Annexure 2.

## Recertification and reaccreditation

Your agency's facilities must be recertified and reaccredited by circumstances including:

- expiry of the certification –
  - a. Zone 2: 10 years
  - b. Zones 3-5: 5 years
- changes in the business impact level associated with the sensitive or security-classified information or assets stored within the zone
- significant changes to architecture of the facility or the physical security controls used
- any other conditions stipulated by the accreditation authority, such as changes to the threat level or other environmental factors of concern.

---

<sup>11</sup> Refer to ASIO Technical Notes 1/15 and 5/12 to ascertain the requirements of security zones and associated processes. Available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.



## **Required action: Dispose of physical assets securely**

When your agency's building, facilities, information, or assets are no longer needed, you must consider the security implications during the decommissioning and disposal phase.

You must ensure that the disposal of your agency's physical assets is secure and minimises risk to the Tasmanian Government.

Prior to the decommission or disposal of physical assets, such as containers, cabinets, vaults, strongrooms, and secure rooms, it is recommended that you:

- reset combination locks to the original settings
- visually inspect and remove all contents from physical assets.

You should refer to the Australian Government Information Security Manual<sup>12</sup> for information on how to sanitise ICT equipment and media before disposal. In some instances, ICT equipment cannot be sanitised and must be destroyed.

## **Required action: Ensure accreditation of worksites away from agency locations**

Working away from the office covers all work undertaken by agency people away from the agency's facilities and physical locations. When developing working-away-from-the-office policies and procedures, you should consider the security risks of the environments in which your agency's people operate, the type of information used and how that information will be accessed.

You must consider the security measures required to enable your agency's people to work securely when they are working away from the office.

### **Mobile computing and communications**

Mobile computing and communications occur when people are provided access to your agency's systems and information from locations outside of your agency's control, using portable devices. Most areas being used for mobile computing and communications (i.e. work from home or mobile work arrangements) are public areas with few, or no, protective security measures in place, and would therefore be rated no greater than a Zone 1 secure area. For this reason, you should implement controls to minimise any residual risk, such as requiring people to carry portable devices at all times; that is, that they are not to be left unattended.

---

<sup>12</sup> For further information, please refer to the Australian Cyber Security Centre website at [www.cyber.gov.au/acsc/view-all-content/ism](http://www.cyber.gov.au/acsc/view-all-content/ism)



Due to the inherently low security surrounding mobile computing and communications, it may not be possible to implement appropriate zoning requirements away from the office. In these circumstances, you should consider ICT logical security controls to protect your agency's information and assets. You can find advice on suitable logical controls in the Australian Government Information Security Manual.

## **Protecting resources while working away from the office**

The TAS-PSPF requires agencies to protect their people, information and assets in accordance with the assessed business impact level of compromise or harm. This includes while working away from the office. Your agency should accredit proposed worksites outside of the office in line with the type of work expected to be undertaken.

In determining the feasibility of work away from the office, you must consider:

- if sensitive or security-classified information can be appropriately secured
- if the work area can be independently secured
- if the work area can be protected from oversight or overhearing by other people
- if the ICT equipment being used can be secured or segregated from the agency's ICT system.

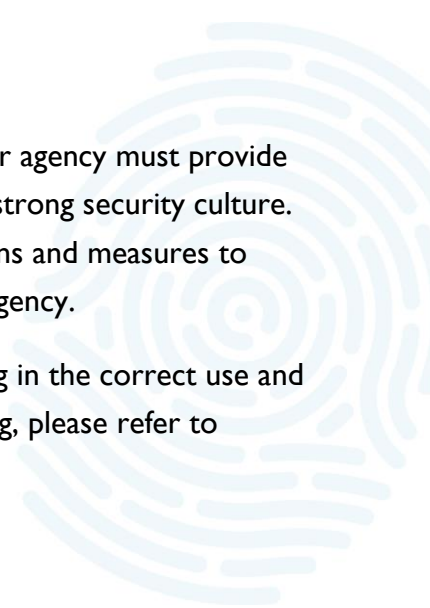
It may be difficult to secure an agency's information when the working environment is not controlled or managed by the originating agency. This situation may present when information is stored or used at commercial facilities, private residences or a service provider's premises.

It is recommended that you consider all areas outside of your agency's control as Zone 1 unless you can confirm and certify security measures.

## **Training in physical security measures**

In accordance with TAS-PSPF policy: Security awareness (GOVSEC-3), your agency must provide security awareness communications, training and support to help create a strong security culture. It is important that your agency communicates physical security expectations and measures to your agency people, visitors and anyone who performs work within your agency.

Where specific physical security measures exist within your agency, training in the correct use and application is a requirement of this policy (PHYSEC-1). For all other training, please refer to TAS-PSPF policy: Security awareness (GOVSEC-3).





## Annexure I: Physical protections for security zones

Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
<b>Building construction</b>	In accordance with agency risk assessment.	<p>In accordance with applicable sections of ASIO Technical Note 1/15: Physical security of zones.</p> <p><u>When only used during business hours</u></p> <p>Normal construction to the Building Code of Australia.</p> <p><u>When also used out of business hours</u></p> <p>Normal construction and:</p> <ul style="list-style-type: none"> <li>a) slab-to-slab construction or</li> <li>b) tamper-evident ceilings or</li> <li>c) applicable sections of ASIO Tech Note 1/15: Physical security of zones.</li> </ul>	<p>In accordance with applicable sections of ASIO Technical Note 1/15: Physical security of zones.</p> <p>For protection of valuable physical assets, recommend aligning building construction with level 4 (or above) of the Australian Standard 3555.1. In such cases, construction will be considered to meet minimum security zone protections mandated by this policy.</p>	As for Zone 3.	<p>Construction complies with –</p> <ul style="list-style-type: none"> <li>a) ASIO Technical Note 1/15: Physical security of zones</li> <li>b) ASIO Technical Note 5/12: Physical security of Zone 5 (TOP SECRET) areas.</li> </ul>



Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
<b>Perimeter doors and hardware</b>					
a) Doors	In accordance with agency risk assessment.	Constructed in accordance with ASIO Technical Note 1/15: Physical security of zones.	As for Zone 2.	As for Zone 2.	Constructed in accordance with ASIO Technical Note 5/12: Physical security of Zone 5 (TOP SECRET) areas.
b) Locks	In accordance with agency risk assessment. May use commercial locking systems.	As for Zone 1.	Minimum SCEC-approved SL3 locks and hardware.	As for Zone 3.	As for Zone 3.
c) Keying systems	Recommend SCEC-approved SL1 or SL2 keying system.	As for Zone 1.	SCEC-approved minimum SL3 keying system.	As for Zone 3.	As for Zone 3.
<b>Out-of-hours security alarm system (SAS)</b>	In accordance with agency risk assessment.	In accordance with agency risk assessment. In an office environment, recommend Class 3-4 SAS <sup>13</sup> hard wired in the zone.	Type 1A SAS, or Class 5 SAS <sup>13</sup> hard wired in the zone. If no SAS, guard patrols performed at random intervals, within every 4 hours required.	Use in accordance with the Type 1A SAS transition policy: a) for new or significantly expanded sites, SCEC-approved Type 1A SAS with SCEC-approved	As for Zone 4.

<sup>13</sup> For guidance on alarm systems see Australian Standard AS/NZS 2201.1:2007 – Intruder alarm systems.



Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
				<p>detection devices (designed and commissioned by SCEC-endorsed security zone consultants)</p> <p>b) for existing sites, SCEC-approved Type I SAS with SCEC-approved detection devices.</p>	
a) Detection devices	In accordance with agency risk assessment.	Hard wired within the zone. Recommend SCEC-approved SL2 or SL3 detection devices.	As for Zone 2.	SCEC-approved SL3 or SL4 detection devices.	As for Zone 4.
b) SAS contractor clearance requirements	In accordance with agency risk assessment.	Contractors who maintain these systems provided with short-term access to security-classified resources <sup>14</sup> at the appropriate level for the information stored within the zone.	As for Zone 2.	Contractors who maintain these systems cleared at the appropriate level for the information stored within the zone.	As for Zone 4.

<sup>14</sup> Refer to TAS-PSPF policy: Access to, and management of, official information (INFOSEC-I) for guidance on short-term access to security-classified resources.



OFFICIAL

Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
c) Management of SAS	In accordance with agency risk assessment.	As for Zone 1.	Control of alarm systems directly managed by the agency.  Privileged alarm systems operators and users appropriately trained and security cleared to the level of the security zone.  All alarm system arming and disarming personal identification numbers are secure.	As for Zone 3.	As for Zone 3.
d) Monitoring and response	All alarm systems monitored and responded to in a timely manner.  Response capability appropriate to the threat and risk.	As for Zone 1.	As for Zone 1.	As for Zone 1.	As for Zone 1.
<b>Interoperability of alarm system and other building management system</b>	In accordance with agency risk assessment.	In accordance with agency risk assessment. If a separate SAS and EACS are used, ensure the alarm cannot be disabled by the access control system.	Ensure the alarm cannot be disabled by the access control system.	Ensure limited one-way interoperability in accordance with Type IA SAS for Australian Government—Product Integration specification.	Ensure limited one-way interoperability in accordance with Type IA SAS for Australian Government—Product Integration specification.



OFFICIAL

Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
					The alarm system may disable access control system when activated.
<b>Access control systems</b>	In accordance with agency risk assessment.	In accordance with agency risk assessment. Recommend using identity access card in office environments.	Use identity card and sectionalised access control systems. Use electronic access control systems where there are no other suitable verification and access control measures in place. Verify the identity of all personnel, including contractors, issued with EACS access cards at the time of issue (using the National Identity Proofing Guidelines to a minimum level 3). Regularly audit EACS.	As for Zone 3, with full audit trail of access control systems. Directly managed and controlled by the entity. Maintained by appropriately cleared contractors Privileged operators and users are appropriately trained and security cleared to the level of the security zone. Regularly audit EACS.	As for Zone 4, with full audit trail of access control systems and dual authentication.
<b>Technical surveillance counter-measures (TSCM)</b>	No requirement.	No requirement.	In accordance with agency risk assessment.	As for Zone 3.	TSCM and audio security inspection: a) for areas where TOP SECRET discussions are regularly held, or the compromise of



OFFICIAL

Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
					<p>other discussions may have a catastrophic business impact</p> <p>b) before conferences and meetings where TOP SECRET discussions are to be held</p> <p>c) refer to ASIO Technical Note 5/12: Physical security of Zone 5 (TOP SECRET) areas.<sup>15</sup></p>
<b>Visitor control</b>	In accordance with agency risk assessment.	In accordance with agency risk assessment.	<p>Visitor and contractor access only for visitors with a 'need to know' and with close escort. Recommend providing receptionists and guards with:</p> <p>a) detailed auditable visitor control and access instructions</p>	As for Zone 3 and visitor and contractor access with a 'need to know' and with close escort with constant line of sight.	As for Zone 4.

<sup>15</sup> Available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.



**OFFICIAL**

Control element	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
			b) secure method of calling for immediate assistance if threatened.		



## Annexure 2: Summary of control measures and certification authority

Control measure	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
<b>Agency-specific threat assessments</b>	RE (or ASA) if the need is identified in the risk assessment.	RE (or ASA) if the need is identified in the risk assessment.	RE (or ASA) if the need is identified in the risk assessment.	RE (or ASA) if the need is identified in the risk assessment.	RE (or ASA) if the need is identified in the risk assessment.
<b>Agency security risk assessment</b>	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)
<b>Site security plan</b>	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)
<b>SCEC-approved Type 1A SAS</b>	N/A	N/A	N/A	SCEC-endorsed security zone consultant <sup>16</sup> (regular servicing by authorised provider required).	SCEC-endorsed security zone consultant (regular servicing by authorised provider required).
<b>SCEC-approved Type 1 SAS</b>	SCEC-endorsed security zone consultant <sup>16 17 18</sup> (regular servicing by authorised provider required).	SCEC-endorsed security zone consultant <sup>16 17 18</sup> (regular servicing by authorised provider required).	SCEC-endorsed security zone consultant <sup>16 18</sup> (regular servicing by authorised provider required).	SCEC-endorsed security zone consultant <sup>16</sup> (regular servicing by authorised provider required).	SCEC-endorsed security zone consultant <sup>16</sup> (regular servicing by authorised provider required).
<b>Commercial alarm system</b>	Suitably qualified system installer or designer <sup>17</sup>	Suitably qualified system installer or designer <sup>17</sup>	Suitably qualified system installer or designer <sup>17</sup>	N/A	N/A

<sup>16</sup> SCEC-endorsed security zone consultants design and commission SCEC Type 1A SAS in accordance with the requirements of the Type 1A SAS Implementation and Operation Guide.

<sup>17</sup> Inclusion of an alarm system or EACS in Zones 1 and 2 are at the agency's discretion.

<sup>18</sup> If out-of-hours guard patrols or commercial alarm systems are not used instead.



**OFFICIAL**

Control measure	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5
	(regular servicing by authorised provider required).	(regular servicing by authorised provider required).	(regular servicing by authorised provider required)		
<b>Electronic access control systems</b>	Suitably qualified system installer or designer (current software patches and no obsolete components required).	Suitably qualified system installer or designer (current software patches and no obsolete components required).	Suitably qualified system installer or designer (current software patches and no obsolete components required).	Suitably qualified system installer or designer (current software patches and no obsolete components required).	Suitably qualified system installer or designer (current software patches and no obsolete components required).
<b>Other zone requirements</b>	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)
<b>Certification (including site inspection)</b>	RE (or ASA)	RE (or ASA)	RE (or ASA)	RE (or ASA)	ASIO-T4



## 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	
	Removal of reference to TI alarms – these have been phased out	



## 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, Australian Cyber Security Centre website at <a href="http://www.cyber.gov.au/acsc/view-all-content/ism">www.cyber.gov.au/acsc/view-all-content/ism</a>	
Australian Government, Department of Home Affairs, at <a href="http://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf">www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf</a>	
Australian Government, Protective Security Policy Framework, at <a href="http://www.protectivesecurity.gov.au/system/files/2023-08/policy-16-entity-facilities.pdf">www.protectivesecurity.gov.au/system/files/2023-08/policy-16-entity-facilities.pdf</a>	
SA Government, protective security, at <a href="http://www.security.sa.gov.au/documents/SAPSF-PHYSEC I - Physical-security-B463483.pdf.pdf">www.security.sa.gov.au/documents/SAPSF-PHYSEC I - Physical-security-B463483.pdf.pdf</a>	
Tasmanian Legislation	<i>Work Health and Safety Act 2012</i>



OFFICIAL



Tasmanian  
Government

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

**Phone:**

(03) 6232 7770

**Email:**

[taspspf@dpac.tas.gov.au](mailto:taspspf@dpac.tas.gov.au)

OFFICIAL