Information Security

INFOSEC-1:
Access to, and management of, official information

Contents

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

About this document

This document – INFOSEC-1: Access to, and management of, official information – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

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

- understand the security environment in which they operate
- identify and understand the most critical assets they must protect
- mitigate security vulnerabilities on a prioritised security-risk basis
- anticipate and prepare for emerging security trends which threaten their ability to effectively undertake government business functions
- continue to improve protective security practices through accountability and governance.

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

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

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

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

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

Definitions and shortened terms

Guiding term	What this means in the context of the TAS-PSPF
must/will/required/ responsible for	Any of these terms refer to an essential action that all agencies and Accountable Authorities must take.
must not	This term refers to an action that is prohibited – agencies and Accountable Authorities must NOT take this action.
should/ recommended	Either of these terms refer to an action that agencies and Accountable Authorities ought to take as best practice, unless justifiable circumstances exist.
should not	This term refers to an action that agencies and Accountable Authorities ought to avoid, unless justifiable circumstances prevent an alternative action.
may	This term refers to an action that is optional to agencies and Accountable Authorities.

Term	What this means in the context of the TAS-PSPF
Accountable Authority/ies	The person or people responsible for, and with control over, a Tasmanian Government public authority. This includes, but is not limited to, agencies (as defined in the *State Service Act 2000*), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	The person nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance.
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information, and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.

Term	What this means in the context of the TAS-PSPF
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's required protective security outcomes. Each of the 14 TAS-PSPF policies includes a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, people.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of official information.
integrity	Safeguarding the accuracy and completeness of information and processing methods, i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted, or obtained by an agency.
originator	The instigating individual (or agency) who generated or received the information and is responsible for classifying it.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.
principles	Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF. 1. Security is a responsibility of government, its agencies and its people.

Term	What this means in the context of the TAS-PSPF
	2. Each agency is accountable and owns its security risks. 3. Security will be guided by a risk management approach. 4. Strong governance ensures protective security is reflected in agency planning. 5. A positive security culture is critical.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
Responsible Executive	The person who oversees protective security matters within your agency, they may also be the Chief Security Officer (CSO).
risk appetite	The risk an agency or Accountable Authority is willing to accept.
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security classified	Information that holds a classification of PROTECTED, SECRET or TOP SECRET and must be protected against compromise. Access to the information must be controlled and accessed by appropriately security cleared people.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	A security incident is: • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.
security plan	Central document detailing how an agency plans to manage and address their security risks.

Term	What this means in the context of the TAS-PSPF
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.
security risk management	Managing risks related to an agency's information, people and assets.
security vetting	An authorised vetting agency's assessment of a clearance subject's suitability to hold a security clearance.
sensitive	Information classified as sensitive is not security-classified information; however, this information requires some protections on a 'needs to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's required protective security outcomes. Each of the 14 core requirements includes supplementary requirements to help implement the TAS-PSPF.
threat	The intent and capability of an adversary.
threat actor/adversary	An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security.
visitor	Any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency.
zone	The physical locality, workspaces, and design of areas within an agency that store assets and information, specifically where information is produced, accessed, handled and stored. Security zoned areas range from 1-5, where the security requirements increase with the applicable zone number allocation.

Acronym/abbreviation	Meaning
ASA	Agency Security Advisor
CIO	Chief Information Officer

Context

The **INFOSEC-1: Access to, and management of, official information** policy and guidance will assist agencies to achieve an effective protective security outcome within the information security domain of the TAS PSPF. They address core requirement 7 and its supplementary requirements.

Core requirement 7

The Accountable Authority must adhere to whole-of-government protective security policies and procedures relating to the management of information security.

Supplementary requirements

In adhering to the whole-of-government approach to the management of information security, the Accountable Authority must:

a) promote awareness of whole-of-government protective security policies and procedures relating to the management of information security or ensure development of agency-specific policies as necessary[1]

b) ensure that information is accessed only by people with a legitimate need to know and implement measures to protect sensitive information, through physical and electronic means, from unauthorised access, copy or release

c) ensure people requiring access to security-classified information, or assets, are appropriately security cleared to the correct level and, where necessary, meet additional suitability requirements[2]

d) develop and implement an agreement or arrangement enabling the sharing of sensitive or security classified information external to the Tasmanian Government and its agencies[3]

e) where appropriate, manage access to information systems with unique user identification, authentication and authorisation for each instance of system access.

Effective information management supports business operations and continuity while ensuring integrity, availability and confidentiality of information.

[1] Where whole-of-government policies and procedures are absent, agencies must develop their own in consultation with the Tasmanian Government Chief Information Officer.

[2] Not all office holders are required to hold a security clearance – see exemptions.

[3] This may be in the form of a deed or contract stipulating how the shared information is to be used and what protections must be applied.

The TAS-PSPF supports agencies in the use of tools to appropriately manage information, enabling efficient and timely functions of government business and processes.

Guidance

Introduction

This policy (INFOSEC-1) details security protections which support your agency in the provision of timely, reliable and appropriate access to official information, facilitating efficient and effective delivery of Tasmanian Government services. The availability of information assists in service delivery, business continuity, decision-making and policy development.

While access to information facilitates Tasmanian Government services, it is important for your agency to protect the confidentiality, integrity and availability of the information your people use. The impact of compromise and harm to information can be felt within your agency, other agencies, the community and across the Tasmanian Government. For these reasons, you must apply this policy (INFOSEC-1) to protect the access to, and management of, official information.

Required action: Promote awareness and develop information security policies

Tasmanian Government information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to your agency's business operations. When your information security policies and procedures are well designed and implemented, you reduce the risks of your information being compromised.

Where they exist, your agency must apply whole-of-government information management policies and procedures to ensure consistency aligned to commonly accepted industry standards and best practice. In the absence of these, you must develop your own in consultation with the Tasmanian Government Chief Information Officer (CIO), strengthening our combined approach to information security.

Promotion of these policies and procedures within your agency should be incorporated in induction packages, where practicable. Inclusion in induction provides an opportunity for all people to understand the expectations of your agency and the Tasmanian Government regarding the protection and management of information.

Awareness of agency-specific and whole-of-government policies strengthens security culture and provides information with protection from compromise and harm.

Required action: Ensure that information is accessed on a 'need to know' basis

The 'need to know' principle refers to the access of information based on an operational requirement. It is important to note this principle applies to all information regardless of the classification of the information and the position or seniority of the person seeking access.

Limiting access to information on a 'need to know' basis guards against the risk of unauthorised access, misuse of, and potential compromise to, information. You must apply the 'need to know' principle to all information within your agency; this can be achieved through implementing measures which deter and detect unauthorised access.

The 'need to know' principle is not intended to reduce or limit positive information sharing between people or agencies where an operational benefit exists.

Applying access controls and auditing capability to all information processes will assist you to maintain the 'need to know' principle. You must develop policies to support the management of, and access to, information based on this principle. Applying this principle in agency policies and security practices helps your people understand their responsibilities in the protection of information from compromise.

When applying access controls to information, you can consider restricting access based on the following table.

Action	Limitation
Physical locations	Access based on worksite or work station
File system permissions, including physical documents and files	The ability to create, read, edit or delete
Application or program permissions	The right to run a program
Data and information rights	The right to retrieve, print, update or delete information in a database or system

Table 1 – Information access restrictions

You must communicate the 'need to know' principle within your agency and help people to understand the relevant restrictions your agency has applied to information.

When considering the distribution and sharing of information, it is important that the principle is adhered to, and it is recommended that you consider the following questions:

- Am I allowed to release the information?
- Is the person requesting the information allowed to receive it?
- Is there an operational benefit to sharing the information?
- Does the information or data contain sensitive or security-classified information?
- Are there any other reasons why the information may not be able to be shared, e.g. is there a confidentiality agreement in place?

It may be more difficult to assess whether someone external to your agency has a genuine 'need to know'. In this instance, a trust-based approach can be used between Tasmanian Government agencies.

Required action: Ensure people are appropriately security cleared

In addition to the 'need to know' principle, access to sensitive and security-classified information or assets necessitates a high level of assurance as to a person's integrity. This is due to the potential harm associated with compromise of that information. Any person with an ongoing need to access security-classified information must have a valid security clearance to the appropriate level.

Minimum security clearance levels for access to each information classification level are detailed in the table below.

	Sensitive information		**Security-classified information**		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Security clearance required	Security clearance not required; pre-employment screening is sufficient	Security clearance not required; pre-employment screening is sufficient	Baseline security clearance or above	Negative Vetting 1 security clearance or above	Negative Vetting 2 security clearance or above

Table 2 – Required security clearance to access information

Access to caveated information that involves a codeword[4] requires a briefing and may require a Negative Vetting 1 level, Negative Vetting 2 level, Positive Vetting level or TOP SECRET-Privileged Access security clearance as well as other requirements.

Security clearance exemptions

Some Australian office holders do not need a security clearance to access security-classified information while exercising duties of their office. Australian office holders who do not require a security clearance are:

- Members and senators of the Commonwealth and state parliaments and territory legislative assemblies
- Judges of the High Court of Australia, the Supreme Court, Family Court of Australia, the Federal Circuit Court of Australia, and magistrates
- Royal commissioners
- The Governor-General, state governors, Northern Territory administrator
- Members of the Executive Council – at federal and state and territory levels
- Appointed office holders with enabling legislation that gives the same privileges as the office holders already identified, e.g. members of the Administrative Appeals Tribunal.

It is important to note that staff of the above office holders do not have an exemption from holding a security clearance.

Caveated information

All information must be assessed to determine its sensitivity or security classification, which is performed by the originator (this could be your agency or an individual who created or received the information). Some information may require additional protections as determined by the originator, which may be in the form of caveats.

Your agency is responsible for and must manage caveated material in accordance with the originator's special handling requirements.

The originator may impose additional access or suitability requirements on top of the security classification. In these circumstances, the people accessing caveated information must meet all the clearance and suitability requirements imposed by the originator.

[4] Refer to TAS-PSPF policy: Protecting official information (INFOSEC-2) for more details regarding caveats and codewords.

Some caveats limit access to information based on citizenship. Further information about caveats can be found in TAS-PSPF policy: Protecting official information (INFOSEC-2).

Temporary access to classified resources

There are some circumstances which may require facilitation of temporary access to security-classified information. However, such instances must only be permitted when a correct risk assessment has been undertaken and the access required is not greater than SECRET.

Temporary access to security-classified information may include:

- short-term[5] access, where the person does not hold a clearance at the appropriate level though has satisfied a genuine 'need to know' for operational benefit and the risks can be mitigated. This may include:
    - new people
    - people undertaking short-term projects
    - people who are reasonably expected to have only incidental or accidental contact with security-classified information (e.g. security guards, cleaners, external IT personnel, researchers and visitors such as children who do not have an ability to comprehend the classified information).
- Provisional[6] access, where the person has commenced a clearance process by providing all relevant details for assessment by an authorised vetting agency. The type of temporary access can be changed from short term to provisional once the authorised vetting agency has confirmed that the completed security clearance package has been received and advises your agency there are no initial concerns regarding the applicant.[7]

You must supervise all temporary access, which may include:

- escorting visitors in premises where security-classified information is being stored or used
- management oversight of the work of people who have the temporary access
- monitoring or audit logging contact with security-classified information.[8]

[5] Short-term is considered a combined maximum of 3 months in any 12-month period, across all agencies.

[6] Provisional access may be granted to people up until their security clearance application is granted or denied.

[7] This information is available via your agency clearance sponsor, who will liaise with the authorised vetting agency.

[8] Monitoring and audit logging are key measures to control access to ICT systems and the information held on those systems. For further information, refer to TAS-PSPF policy: Robust technology and information systems (INFOSEC-3).

Temporary access to TOP SECRET information must only be granted to people with an existing, valid Negative Vetting 1 security clearance.

Temporary access to caveated information must only be granted where all suitability requirements are also satisfied.

When you assess risk for temporary access to security-classified information, it is recommended that you consider the following:

- the need for temporary access – can the need be filled by someone already holding the necessary clearance?
- confirmation from the authorised vetting agency that the person has no identified security concerns or a clearance that has been cancelled or denied
- what is the business impact of compromise to the information?
- how access to the security-classified information will be supervised, including how access to caveated or compartmented classified information will be prevented
- other risk mitigations, such as pre-employment screening checks, character assessments and/or knowledge of personal/work history.

Where you determine temporary access is suitable, it is recommended that you consult with the originator/owner of the information. Where appropriate, you can use confidentiality or non-disclosure agreements to reinforce the requirements to protect the information.

Required action: Develop or implement agreements to protect information

Risks may arise when you share information outside of the Tasmanian Government and its agencies, because the TAS-PSPF only applies to Tasmanian Government agencies and their subsidiaries. For this reason, when your agency shares information externally, you should consider the need for written agreements which address how the information is to be used and the necessary protections that must be applied to it.

Agreements detailing information disclosure requirements provide a level of assurance that your external stakeholders understand their obligations to protect government information. The following factors may be relevant when considering whether a written agreement is necessary before sharing information:

- whether the nature of the work requires access to information protected by the *Personal Information Protection Act 2004* – if so, you should include contractual measures to ensure the principles of the Act are upheld
- if the information is subject to any legislative secrecy provisions
- whether the aggregation of information to be shared increases the business impact level of potential compromise
- what type of access is being granted and the level of supervision and control that your agency will have over the personnel granted access.

To support information protection when involving external stakeholders, it is recommended that you implement regular monitoring of the security controls, service definitions and delivery levels that are included in any deed or contract agreement. This may be in the form of contractual milestone obligations, regular reviews, and audits of services.

Required action: Manage access

Once your agency has established appropriate policies and procedures surrounding access to information, you must manage any access granted, where necessary. To do this, your information and technology systems need to be well-structured and robust, providing your people with the right tools and access to conduct their duties.

When providing access to your agency's networks, operating systems, applications, and information, you should consider the following methods for control:

- establishing a clear understanding of the information held on the system/s
- effective user identification and authentication practices.

User identification, authentication and authorisation practices

To adequately protect your agency's information, you should know who is accessing it and when. It is important to mitigate the risks of unauthorised or inappropriate access to and use of information; to do so, you must establish formal user registration and deregistration procedures for granting and revoking access to information systems.

Your people who access information systems must be authenticated on each occasion they seek access to the system. Establishing uniquely identifying user processes for your agency will ensure greater accountability that the information is being accessed appropriately.

You can authenticate access by using various methods, including:

- passphrases or passwords
- biometrics
- cryptographic tokens
- smart cards.

You may reduce the risk of user accounts being compromised by:

- using multi-factor authentication (2 or more authentication methods) where users provide something they know, like a passphrase; something they have, like a physical token; and/or something they are, like biometric data
- increasing the complexity of single authentication methods (such as passphrases or passwords) by increasing the minimum password length and using a mix of alphanumeric and special characters.

Some user and system/s access can be associated with greater risk due to the nature of such access, for example, system or network administrators and managers, database administrators, privileged users, positions of trust, and remote access users.

High-risk users should be required to access relevant systems using multi-factor authentication to confirm their identity on each occasion of access.

Authorising access to ICT systems

Adopting robust authorisation processes will help you control access to your agency's ICT systems, networks (including remote access), infrastructure and applications. It is recommended that you implement measures to manage authorised access to any system holding your sensitive and security-classified information.

The following table depicts recommended authorisation measures.

Type of access authorisation	Recommended measures
User access management	Ensure that systems for managing passwords are interactive and require users to follow good security practices in the selection and use of passwords or passphrases.
Authorised network access	Consider the use of automatic equipment identification as a means to authenticate connections from specific locations and equipment. Control physical and logical access to diagnostic and configuration ports. Restrict the ability of users to connect to shared networks, including those that extend across agency boundaries. Segregate groups of information services, users and information systems, based on an agency risk assessment. Implement routing controls for networks to ensure computer connections and information flows do not breach other relevant access management measures.
Authorised operating system access	Control access to operating systems through a secure log-on procedure. Restrict and tightly control the use of utility programs that may be capable of overriding system and application controls. Display restricted access and authorised use only (or equivalent) warnings upon access to all agency ICT systems and shut down inactive sessions after a defined period of inactivity. Consider restricting connection times to provide additional security for high-risk applications.
Application and information access	Afford sensitive systems a dedicated (isolated) computing environment, in accordance with your risk assessment.
Mobile computing and communications	Adopt security measures to protect against the risks of using mobile computing and communications facilities.

Table 3 – Recommended access authorisation measures

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	
	Original supplementary requirement 'b' removed - (duplication of footnote at supplementary requirement 'a')	
	Updated supplementary requirement 'c' – replaced 'protected information' with 'security-classified information'	

References and resources

Australian Government, reporting on security, at www.protectivesecurity.gov.au/system/files/2023-08/policy-5-reporting-on-security-pspf.pdf	
SA Government, information security, at www.security.sa.gov.au/protective-security-framework/information-security	
Tasmanian Government, Information and Records Management Standard, at https://osa.tas.gov.au/wp-content/uploads/2023/08/Information-and-Records-Management-Standard.pdf	
Tasmanian legislation	*Personal Information Protection Act 2004*

Tasmanian Government

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au