People Security

PESEC-3:
Managing separating people

Contents

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

About this document

This document – PESEC-3: Managing separating people – 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
ASIO	Australian Security Intelligence Organisation
RE	Responsible Executive

Context

The **PESEC-3: Managing separating people** policy and guidance will assist agencies to achieve an effective protective security outcome within the people security domain of the TAS-PSPF. They address core requirement 12 and its supplementary requirements.

Core requirement 12

The Accountable Authority must ensure adequate management of all separating people.[1]

Supplementary requirements

To provide secure management of separating people, the Accountable Authority will:

a) ensure access to Tasmanian Government information and assets is withdrawn or modified according to changed government duties.[2]

b) ensure all agency items are returned accordingly – such items may include, but are not limited to, swipe access, ID passes, keys, IT equipment

c) withdraw or transfer sponsorship of security-cleared people, including eligibility waivers and conditional security clearance holders

d) ensure separating people are reminded of their ongoing security obligations

e) share information of security concerns with the appropriate stakeholder/s or authorities – this may be the Agency Security Advisor (ASA), the Security Clearance Sponsor, the authorised vetting agency, or the Australian Security Intelligence Organisation (ASIO)

f) manage any residual risk associated with the employee's departure.[3]

Agencies must apply prescribed and consistent management protocols for separating and transferring people, ensuring all access to agency information and assets is adjusted or terminated accordingly, safeguarding the integrity of Tasmanian Government information and assets. The TAS-PSPF outlines what must be implemented by agencies to protect the integrity, confidentiality and availability of Tasmanian Government information and assets.

[1] Separating refers to people who leave an agency by transfer, resignation, secondment, contract cessation, termination or long-term leave.

[2] In the instance of an internal transfer, secondment or long-term leave.

[3] Deed of confidentiality or similar as required.

Guidance

Introduction

When a person leaves (separates from) your agency, they retain their knowledge of your business operations, intellectual property, official information and security vulnerabilities. Managing departures from your agency may reduce the risk of this knowledge being misused. Separating people have greater opportunity to harm your agency deliberately or accidentally, with fewer consequences than if they were still engaged by your agency, due to the limited ability for you to monitor, manage and support these people.

To limit the risks posed to your information, people and assets, your agency must implement risk-based processes to manage a person's departure from the agency. This includes ensuring that any access, security passes and assets are returned, and that people understand their ongoing obligations.

Separation from your agency includes:

- resignation or end of contract
- transfer to another agency
- termination
- transfer either temporarily or permanently to another state or Australian Government agency
- taking an extended period of leave.

Required action: Withdraw or modify access as needed

Throughout their career, people often move within the Tasmanian Government. Sometimes, this is within your agency or to another agency, through the likes of promotion, secondment or transfer. In these circumstances, you will be required to make a risk-based assessment as to the modifications which are necessary regarding a person's access to all facets of your agency. When considering the person's ongoing access, you must first assess the movement and if it should be considered as a separation under this policy (PESEC-3).

Assessing the movement of your staff is a critical step in ensuring you protect your agency information, people and assets from compromise and harm. When conducting this risk-based assessment, it is recommended you consider the following:

Has the person remained within your agency?	If yes, what physical and ICT access changes are required? Modify access as necessary and cancel any access no longer required.
Has the person separated (by transfer, resignation, secondment, contract cessation, termination or long-term leave)?	If yes, cancel any access immediately upon separation.

Once a person separates from their role or your agency within the Tasmanian Government, their need for ongoing access to official information and resources also concludes. With this in mind, you must remove their access to both physical facilities and resources, including ICT systems. You should also recover any agency property in the person's possession (e.g. credit card/s, key/s, vehicle).

It is recommended that you categorise the removal of access to ensure you maintain the ability to successfully remove all access that a person may have had. The table below provides examples of actions that may be necessary at different phases of separation.

Phase	**Action**
Before separating	• Recover ICT equipment and physical assets. • Recover corporate credit cards/ID and other agency property. • Recover anything in hard copy - originals and/or copies. • Recover uniform/s.
After separating	• Deactivate access to ICT systems, including email, telephone, voicemail and any cloud accounts. Ensure any additional external access has also been disabled. • Remove physical access to facilities and resources – deactivate any access passes. • Change or remove combinations or locks that the separating person had access to.

Table 1 – Actions that may be taken to support employee separation

Required action: Ensure all agency items are returned

It is the responsibility of your agency to ensure a separating person returns all property that belongs to the agency. This includes ensuring all identification cards, access passes and keys are returned (including tools that allow remote access to information systems).

If your agency allows transfer of ownership of ICT equipment to separating employees, or the use of personal devices for work purposes, it is recommended that:

- any business-related documents are archived in accordance with your agency's record management procedures
- all agency information is removed
- all agency software applications are removed and access disabled
- if deemed necessary, the content of the device's hard drive is erased entirely.

Refer to Table 1 above for examples of actions that may be required for the removal of access before and after employee separation.

Required action: Withdraw or transfer sponsorship of security-cleared people

Security clearances require sponsorship from an authorised agency in order to be deemed valid and active, in Tasmania the authorised agency is the Department of Premier and Cabinet (DPAC). As highlighted in TAS-PSPF policy: Recruiting the right people (PESEC-1), you must identify the positions within your agency which require an active security clearance – this means that only while a person occupies one of these roles should they have a valid security clearance.

Your Agency Security Advisor (ASA) must review active agency security clearances regularly and provide confirmation to DPAC that those arrangements are to continue according to position requirements. When a person holding a security clearance separates from your agency, you must carry out the following activities, in addition to those mentioned previously:

- conduct an exit interview
- debrief them from any sensitive or security-classified information, which may include caveated and compartmented information

- withdraw authorisation for sponsorship of the security clearance and notify the clearance sponsor[4]
- the clearance sponsor is to advise the authorised vetting agency, who will update the clearance status according to separation circumstances.

If the separating person is transferring, either temporarily or permanently, to another Tasmanian Government agency, you must notify the clearance sponsor and where possible, provide details of the transfer.

Where the security-cleared person is transferring to an organisation external to the Tasmanian Government, you must notify the clearance sponsor that the sponsorship is to be withdrawn. If the security clearance is still required, the person transferring and the receiving entity are responsible for ensuring the sponsorship is transferred correctly.

If your agency receives security-cleared people from another Tasmanian Government agency, you must notify the clearance sponsor as to whether the sponsorship of the security clearance is still required. This will be referenced against the agency's identified positions register and where sponsorship is still required, the ASA must provide confirmation to the clearance sponsor.

There may be circumstances where you receive security-cleared people from sources external to the Tasmanian Government. In doing so, you must ensure sponsorship of the security clearance is transferred to the appropriate security clearance sponsor.

The table below provides additional information regarding managing security clearances and personal security files.

Stage	Actions
Permanent transfer	**Actions for the gaining sponsoring agency** Before personal security file actions commence, the gaining sponsoring agency: • identifies the level of security clearance required and whether the clearance subject has previously held a security clearance (including the agency that sponsored the previous clearance) • obtains the clearance holder's consent to share information where a current or previous clearance is identified

[4] You must notify the clearance sponsor if the separation is the result of any misconduct or security incident or concern, which may impact the integrity of the individual's security clearance. If there is a chance other agencies may be impacted by this outcome, the relevant REs should also be notified.

	• requests permanent transfer of sponsorship of the security clearance – this will trigger the authorised vetting agency to commence permanent transfer of the personal security file.
	Actions for the gaining vetting agency Once it has received a request for the permanent transfer of a security clearance from the gaining sponsoring agency, the gaining vetting agency: • requests the personal security file from the losing vetting agency[5] • confirms the information in the personal security file meets the requirements for the requested level of security clearance, or commences a new vetting process if the sponsoring agency requires a clearance that is higher than the clearance held • identifies and addresses concerns or anomalies in the personal security file at the time of transfer, including determining whether the concerns or anomalies warrant a review for cause • confirm the transfer of the personal security file with the sponsoring agency, including if further actions will be undertaken before the transfer of sponsorship is finalised (i.e. sharing any concerns or conducting a review for cause).
	Actions for the losing vetting agency The losing vetting agency: • facilitates transfer of the personal security file as soon as practicable following receipt of request from the gaining vetting agency[6] • seeks consent from the clearance subject prior to transferring and sharing the personal security file.
Temporary transfer	Only transfer personal security files if necessary, for example: • the position in the gaining sponsoring agency requires a higher security clearance • the clearance expires during the transfer or secondment period.

Table 2 – Recommended actions regarding personal security files

[5] Some entities have legal restrictions on the transfer of personal security files. For example, the Department of Defence cannot transfer the personal security files of current and former Regular or Reserve Australian Defence Force personnel and ASIO can only transfer personal security files to other AIC entities. ASIO can only provide a statement of clearance to other vetting agencies. Psychological assessments may only be transferred to another appropriately qualified psychologist and only with the specific consent of the clearance holder.

[6] In some instances, it may not be possible to transfer personal security files immediately. This includes where people are still employed by the losing agency, are under investigation for a security breach or violation, are being revalidated, or are undergoing a review for cause.

Required action: Advise regarding ongoing security obligations

Your agency must advise separating employees of their ongoing security obligations associated with their former position. It is especially important that you remind separating employees about these obligations in relation to intellectual property[7] and where relevant, legislation.[8]

In circumstances where your agency identifies a higher risk associated with a specific position or person, it is recommended that this is managed through an exit interview where you can learn why a person is leaving or reaffirm any ongoing confidentiality agreements or obligations.

People who may have had access to sensitive or security-classified information must be debriefed prior to their separation from your agency. This is particularly relevant in circumstances where the person had access to caveats or compartmented information which require additional briefing and debriefing.[9]

Required action: Share information of security concerns

Sharing of information relating to security concerns is an important component to the protection of Tasmanian Government information, people and assets. Further, it is the responsibility of your agency to identify who may need to be made aware of such information outside of your agency.[10]

The ASA must be notified of any proposed termination of employment resulting from misconduct. It is recommended that in these circumstances, separation procedures are implemented on the basis of a risk assessment and may include:

- immediate suspension of duties
- immediate removal of access to the agency and facilities
- escorting the person from the premises.

[7] Any intellectual property invented or created as a result of an individual's employment will remain the property of the Crown, unless otherwise agreed in writing between the Accountable Authority and employee.

[8] For example, *Criminal Code Act 1995*

[9] As ongoing access to such information is strictly 'need to know', employees no longer requiring access must be debriefed by the caveat or compartment owner.

[10] Within legislative boundaries.

If any risk to another agency has been identified as a result of an incident, termination or during separation, you must notify the RE of the other agency if their interests or security arrangements could be affected.

If the separating person is transferring, either temporarily or permanently, to another state, territory or Australian Government agency, you must provide any relevant information of security concern to the new agency. This action assists combined efforts to ensure the right people have access to government information, people and assets.

In circumstances where there is information of security concern relating to a security clearance holder in your agency, you must provide this to the ASA who must in turn report to the clearance sponsor. The clearance sponsor will report to the authorised vetting agency, which will enable the clearance holder's suitability to be re-assessed.

The clearance sponsor or authorised vetting agency may report information of security concern to ASIO, where required.

Required action: Manage residual risk associated with departure

In addition to their broader function, exit interviews provide the opportunity to remind the departing person of their obligations to protect your agency's information. At the exit interview, ensure all confidential information and devices have been returned and deactivate all access codes and passwords.

Exit interviews provide a good opportunity for you to:

- discuss the person's reason/s for leaving
- enable the separating person to confidentially express any security concerns relating to your agency procedures or colleagues
- glean the person's attitude to your agency and people
- receive any agency property they hold.

In certain circumstances, employees will depart your agency without completing all required separation activities. This may be due to unforeseen circumstances or where the person refuses to participate.

In circumstances where requirements of the separation process are incomplete, you must undertake a risk assessment for any aspects of the person's employment that have not been resolved.

If separation activities are incomplete, your agency must ensure all other requirements of this policy (PESEC-3) are applied, for example, removal of access to systems and facilities or cancelling of security clearance sponsorship.

For the purposes of this policy (PESEC-3), separation includes employees taking long-term leave. There is no defined period of time considered 'long-term leave'. It is recommended that you take a risk-based approach to determine a period of long-term leave based on the risk tolerance and operational requirements of the agency, as well as the nature of the position.

Version control and change log

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

References and resources

Australian Government, security clearances, at www.defence.gov.au/security/clearances	
Australian Government, Protective Security Policy Framework, at www.protectivesecurity.gov.au/publications-library/policy-14-separating-personnel	
New Zealand Government, personnel security, at https://protectivesecurity.govt.nz/personnel-security/	
South Australian Government, people security, at www.security.sa.gov.au/protective-security-framework/personnel-security	
Legislation	*Criminal Code Act 1995*

Tasmanian Government

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au