



# People Security

## PESEC-2: Ongoing suitability assessment



# Contents

---

<b>About this document</b>	<b>3</b>
<b>Definitions and shortened terms</b>	<b>5</b>
<b>Context</b>	<b>9</b>
<b>Guidance</b>	<b>11</b>
Introduction	11
Required action: Establish suitability and compliance procedures	12
Required action: Manage and support awareness of contractual obligations	17
Required action: Support people who hold a national security clearance	18
Required action: Ensure compliance with requirements of a security clearance	20
Required action: Identify and report non-compliance and matters of concern	22
Required action: Manage inability to meet ongoing suitability requirements	23
<b>References and resources</b>	<b>24</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 – PESEC-2: Ongoing suitability assessment – 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.



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
<b>Security governance</b>	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
<b>Information security</b>	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
<b>People security</b>	10	PESEC-1: Recruiting the right people
	11	<b>PESEC-2: Ongoing suitability assessment</b>
	12	PESEC-3: Managing separating people
<b>Physical security</b>	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 <i>State Service Act 2000</i> ), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	Person/people nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance.
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information, and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.

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

Term	What this means in the context of the TAS-PSPF
principles	<p>Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF.</p> <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> <li>3. Security will be guided by a risk management approach.</li> <li>4. Strong governance ensures protective security is reflected in agency planning.</li> <li>5. A positive security culture is critical.</li> </ol>
protected information	Information which has been assessed and classified as requiring protective markings and protection.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
risk appetite	The risk an agency or Accountable Authority is willing to accept.
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	<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.



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

Acronym/abbreviation	Meaning
ASA	Agency Security Advisor
ASIO	Australian Security Intelligence Organisation



## Context

---

The **PESEC-2: Ongoing suitability assessment** policy and guidance will assist agencies to apply consistent expectations as to the ongoing suitability of people and must be actioned in accordance with the specific agency's risk assessment. The policy and guidance sit within the people security domain of the TAS-PSPF and address core requirement 11 and its supplementary requirements.

### Core requirement 11

The Accountable Authority must ensure the ongoing suitability of their people to access official information and assets, while ensuring compliance with the TAS-PSPF.

### Supplementary requirements

To apply consistent expectations and management of ongoing suitability, the Accountable Authority will:

- a) establish procedures which maintain confidence in the ongoing suitability and compliance of agency people<sup>1</sup>
- b) ensure people are aware of their ongoing obligations according to their engagement contracts and have appropriate management arrangements in place which support these<sup>2</sup>
- c) ensure there are adequate management arrangements which support all agency people holding a national security clearance
- d) ensure any security-cleared people are aware of and comply with the requirements of their clearance
- e) identify and report non-compliance and matters of security concern to the relevant authority
- f) establish policy and process for people who are unable to retain required obligations for ongoing suitability.

---

<sup>1</sup> Such procedures may include refresher training, interval-based compliance checks, and mandated screening updates with position changes (in accordance with statutory requirements or limitations).

<sup>2</sup> Each employment Act or agreement within the Tasmanian Government holds the participating parties to account. Ongoing suitability according to these may include compliance with any code of conduct standards or requirements of certifications, e.g. working with vulnerable people, NDIS endorsement.



People engaged with the Tasmanian Government have access to valuable information and assets which are vulnerable to compromise and harm. Enabling a culture of security, with confidence in the ongoing suitability of people, reduces operating risks to Tasmanian Government agencies. The ability to maintain engagement should be based upon continued compliance with relevant initial suitability screens and vetting.

Application of prescribed and consistent management protocols for people who hold security clearances ensures increased compliance and enhanced trust networks inter-jurisdictionally. The protection of Tasmanian Government information and resources is crucial.

The TAS-PSPF assists agencies to apply consistent expectations to the ongoing suitability of people and must be actioned in accordance with the agency's risk assessment.



# Guidance

## Introduction

Pre-employment screening plays an important role in recruiting people who present low security concern to your agency. However, people and their circumstances and attitudes can change, either gradually or in response to certain events. This can increase your agency's security risks.

Effective ongoing assessment ensures that employees continue to meet all eligibility and suitability requirements in their current position and also manages the risk of insider threat.

Insider threat is the risk of compromise to Tasmanian Government information and assets from the agency's people; this behaviour can be deliberate or unintentional. Some types of insider threat and examples of harm they can cause are described in this table.

Action/threat	Harm
Theft, fraud and corruption	Financial losses, unauthorised access or dissemination
Information leaks	Reputational damage, loss of intellectual property
Privacy breaches	Compromised client information
Sabotaged systems or equipment	Disruptions to operations
Violent acts or threats	Safety risk

Table 1 – Insider threat examples

Your agency has a responsibility to address any concerns about a person's suitability for continued access to Tasmanian Government information and assets. This policy (PESEC-2) requires you to establish processes to support continued monitoring of people regarding their ongoing suitability, and to manage associated risks. Taking the actions outlined below will assist you to keep your agency's information, people and assets safe from compromise and harm.

## Required action: Establish suitability and compliance procedures

Establishing procedures to regularly assess and collate information regarding the ongoing suitability of your agency's people will assist you to identify and report changes that may signal potential security concerns.

To develop these procedures, you should undertake risk assessments that consider:

- the personnel type of the people engaged with your agency and the nature of their duties (employees and contractors, temporary employees, security clearance holders)
- the access that people have to sensitive or security-classified information and assets
- your agency's tolerance for security risks
- any risks that may be specific to the position that the individual holds
- the individual's personal risk profile.

The table below will assist you in the assessment and management of the ongoing suitability of your agency's people.

Procedure	Uncleared employees	Security-cleared employees
Build people security into performance evaluation	Required	Required
Periodic employment suitability checks	Required <sup>3</sup>	Required
Security incident reporting	Recommended	Required
Annual security check	Recommended	Required
Contact reporting obligations	Recommended	Required
Collecting and assessing information – changes in circumstances	Recommended	Required
Annual review of eligibility waivers	N/A	Required – for waiver holders

<sup>3</sup> As you determine necessary, according to your agency's risk tolerance and threat environment.

Monitoring compliance with clearance conditions	N/A	Required – for conditional clearance holders
Positive Vetting maintenance obligations in accordance with SMSMP-PVG <sup>4</sup>	N/A	Required – for Positive Vetting clearance holders

Table 2 – Required and recommended procedures to assess and manage ongoing suitability

## People security in performance evaluation

As indicated in the table above, your agency is required to embed security considerations into annual performance evaluation. Conducting annual performance evaluations is a mechanism to assess and manage the ongoing suitability of your agency's people.<sup>5</sup>

Security inclusions in annual performance evaluations may include validating the following:

- the individual has reported changes in circumstances
- the individual has reported any suspicious or strange contact with foreign and Australian nationals who are seeking information that they do not need to know, as well as suspicious, ongoing, strange or continual incidents
- the individual has reported any conflicts of interest
- supervisors/managers have no unreported security concerns about the individual.

It is recommended that your agency educates supervisors/managers on how to identify behaviours of concern and engage in effective conversations about security within the context of performance evaluation. Examples may include confirming compliance with security awareness training and ensuring understanding of reportable incidents and contact reporting arrangements.

Central human resource areas may also have knowledge of performance concerns at a high level across business areas, which could indicate personal issues leading to security concerns. Your agency should consider the need for procedures within these areas to identify and report information which could be of relevance to security.<sup>6</sup>

<sup>4</sup> For further information please review the Sensitive Material Security Manual Protocol – Positive Vetting Guidelines (SMSMP-PVG), available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

<sup>5</sup> The connection between performance issues and security concerns is complex. You must not misuse the security clearance process to address performance issues. Where performance issues are being investigated, if there are security concerns, these can be reported to the relevant authorised vetting agency.

<sup>6</sup> This decision should be in accordance with agency risk assessments and guidance should be provided to assist any impacted central human resource areas if implemented.

## Periodic employment suitability checks

Pre-employment screening checks are conducted during recruitment, as outlined in TAS-PSPF policy: Recruiting the right people (PESEC-1); however, these checks represent a point-in-time only. Conducting screening checks periodically throughout a person's employment can inform your agency's assessment of their ongoing suitability.

You should determine the frequency of periodic employment suitability checks based on your agency's risk profile as well as specific risks associated with the person's position, any associated enabling legislation, and your agency's operating environment.

Periodic employment suitability checks may include the following.

Check	Description
Updating personal particulars	Relevant changes may include: <ul style="list-style-type: none"><li>• qualifications</li><li>• overseas travel</li><li>• significant changes in circumstances</li><li>• any other changes relevant to the person's employment.</li></ul>
Confirming adherence to employment conditions	Where conditions are pertinent to a person's employment, confirm adherence to or completion of these conditions, e.g. security clearance or citizenship.

Table 3 - Assessing ongoing suitability

## Security incident reporting

TAS-PSPF policy: Reporting incidents and security investigations (GOVSEC-6) requires your agency to develop, implement and review processes which relate to security incidents and consequent investigations.

Managing security incidents and investigations aids your agency in monitoring performance, identifying inadequacies and gaps in existing mitigations, and implementing appropriate treatments.

Where patterns of behaviour from specific or collective agency people result in frequent or recurring incidents of security concern, this should trigger assessment of the suitability to maintain access to Tasmanian Government information and resources.

## Annual security check

All security-cleared people must undergo an annual security check. This check addresses the person's compliance with general security clearance obligations, as well as any specific clearance maintenance obligations.

General obligations include compliance with agency security procedures, in particular:

- reporting –
  - changes in circumstances
  - security incidents
  - suspicious, ongoing, unusual, or persistent contacts
- completion of security awareness training
- identifying and discussing any concerning workplace behaviours.

Conducting an annual security check provides an opportunity to discuss any security-related matters or concerns, reinforces awareness and understanding of security obligations, and enhances your agency's positive security culture.

As with performance management reviews, a person's supervisor/manager is usually best placed to conduct the annual security check as they are likely to have greater oversight and knowledge of the person's performance and behaviour. For further guidance on conducting annual security checks, liaise with your Agency Security Advisor (ASA).

The annual security check can be incorporated into the annual performance management process or exist as a standalone requirement. Conducting an annual security check does not negate your agency's responsibility for assessing the ongoing suitability requirements for all agency people, in accordance with your employment processes.

Should an annual security check raise matters of security concern relating to the person, you must ensure these are reported immediately to your ASA and to the clearance sponsor<sup>7</sup> who must inform the relevant authorised vetting agency who issued the security clearance.

---

<sup>7</sup> The agency or entity that sponsors a security clearance on behalf of an applicant. Sponsorship by the agency or entity verifies the need for the applicant to hold a security clearance. For more information on the role of clearance sponsors, please refer to TAS-PSPF policy: Recruiting the right people (PESEC-1).





## Contact reporting obligations

Tasmanian Government information is valuable and may be attractive to foreign governments; this information does not need to be sensitive or security-classified to be sought after. For this reason, it is essential your agency has clear policies and procedures supporting contact reporting obligations.

Security clearance holders must report any contact with another person or group that they believe is suspicious, unusual, persistent, or where ongoing contact with a foreign national has been established.

Security clearance holders must report any such contact to their agency's ASA and their clearance sponsor. The clearance sponsor is responsible for providing details to the authorised vetting agency and the Australian Security Intelligence Organisation (ASIO) via the Contact Reporting Scheme.

Additionally, your agency should have procedures which support submission of a contact report where a person or group, regardless of nationality, seeks to obtain information they do not need to know.

## Reporting changes in personal circumstances

Changes in personal circumstances<sup>8</sup> can impact a person's suitability to access Tasmanian or Australian Government information and assets. You must develop clear policies and procedures which support reporting changes in circumstances, as early identification and action can reduce or prevent larger issues developing.

Security clearance holders have an obligation to report changes in their personal circumstances and must do so to their ASA and clearance sponsor. The security clearance holder must then formally report the changes to the authorised vetting agency.<sup>9</sup>



---

<sup>8</sup> For further details on changes of circumstances, please refer to ASIO Clearance holder obligations on the ASIO Outreach website.

<sup>9</sup> Where required, the clearance sponsor can provide further information relating to the authorised vetting agency.

## Required action: Manage and support awareness of contractual obligations

As set out in TAS-PSPF policy: Recruiting the right people (PESEC-1), your agency must set clear expectations regarding any employment requirements or obligations, including mentions of these in advertising, statements of duties and any contract/agreement issued. Employees must understand your agency's security policies and practices as soon as possible after commencing engagement, as part of the induction process.

This policy (PESEC-2) supports you to ensure the ongoing suitability of people, which includes engagement obligations such as compliance with any code of conduct standards, requirements of certifications (e.g. working with vulnerable people), contractual obligations (specifications/milestones) and security clearances.

There are 2 important aspects to supporting workplace understanding of, and compliance with, security policies and practices. At an individual level, you must ensure that each person is aware of their ongoing obligations according to their role-specific engagement contract. However, it is equally important that you ensure that there is agency-wide clarity around security expectations and procedures. Addressing these 2 aspects will help you to ensure there is a collective and consistent understanding of obligations and an enhanced culture of security within your agency.

You will first need to consider the types of engagement, roles and requirements that occur across your agency, in accordance with your agency's risk assessment. The measures described below can then provide opportunities for you to address and manage the ongoing suitability of your agency's people.

Security awareness interviews and induction	Interviews conducted before people are provided access to agency assets and information. Induction includes agency-specific security policies and procedures.
Signed confidentiality agreement	Agreement signed where access to sensitive or security-classified information forms part of a person's duties or contract.
Compliance with security policies and procedures	Security awareness training tailored to your agency's security risk environment and the risks identified for specific roles. Compliance incorporated into annual performance review.
Review of suitability in response to changes in a person's risk profile	Management response triggered by a significant change in circumstances, a significant security incident, or any reports of suspicious activity.

Table 4 – Measures to support management of ongoing obligations

## Security clearance revalidations

Revalidations assess a security clearance holder's ongoing eligibility and suitability to hold a security clearance. You must ensure that all of your agency's security clearance holders maintain their clearance for as long as they are required to have one. Under the Australian Government Protective Security Policy Framework policy 13: Ongoing assessment of personnel, it is mandated that authorised vetting agencies ensure security clearances are revalidated at set intervals, depending on the level of clearance.

The checks undertaken at revalidation must cover the duration since issuing the initial clearance or the last revalidation was completed. If periods of time are deemed uncheckable for vetting purposes, or where the vetting agency is unable to provide adequate assurance about a security clearance holder, then an eligibility waiver may be required.<sup>10</sup>

Authorised vetting agencies should provide sufficient notification to security clearance holders and the sponsoring agency, prior to the revalidation date, confirming whether the requirement for a security clearance still remains. The TAS-PSPF requires your agency to ensure that all positions requiring a security clearance are clearly identified and that all employees occupying those roles have a valid clearance at the correct level. This will support management of ongoing obligations and clarification of the ongoing need for a person to hold a security clearance.

## TOP SECRET-Privileged access clearances

For information on the ongoing assessment and management of TOP SECRET-Privileged access clearance holders, please refer to the Australian Government Protective Security Policy Framework policy 13: Ongoing assessment of personnel.<sup>11</sup>

## Required action: Support people who hold a national security clearance

People who apply for a national security clearance are subject to scrutiny when their suitability to hold a security clearance is assessed, with their suitability determined through overall integrity.<sup>12</sup> When people are determined to be suitable to hold a security clearance, the relevant details are forwarded to the applicant and clearance sponsor; keep in mind that the security clearance is issued based on an assessment at a point-in-time.

---

<sup>10</sup> Refer to TAS-PSPF policy: Recruiting the right people (PESEC-1) for further information on eligibility waivers.

<sup>11</sup> Access the Australian Government Protective Security Policy Framework at [www.protectivesecurity.gov.au](http://www.protectivesecurity.gov.au).

<sup>12</sup> Determined by the relevant authorised vetting agency.

To help set expectations from the start, your agency must advise security clearance holders that they will be assessed regularly as their suitability to hold a clearance can change over time.

It is important for your agency to support security-cleared people to remain suitable to hold their clearance. Managers/supervisors play an important role in providing this support, as well as in helping to build and maintain your agency's culture of security.

The table below contains guidance which may assist managers/supervisors in their role.<sup>13</sup>

Ensure security-cleared staff understand their responsibilities	<p>For example:</p> <ul style="list-style-type: none"><li>• locking computers when away from them</li><li>• storing sensitive and security-classified material correctly</li><li>• observing clear desk policies</li><li>• understanding ongoing suitability requirements and reporting arrangements.</li></ul>
Practice the 'need to know' principle	<p>A security clearance gives a clearance holder access to information up to a certain level – where the 'need to know' exists. However, a clearance does not give the holder the right to access information. Your agency's people must understand what information they require to perform their duties and only access this information according to their demonstrated 'need to know'.</p>
Monitor your staff	<p>You must be observant and aware of your security-cleared people; this will enable you to intervene early if you notice changes in attitudes and behaviours. Some things you might observe include:</p> <ul style="list-style-type: none"><li>• changes in work habits</li><li>• significant changes in appearance</li><li>• instances of living beyond means</li><li>• access to information which is not on a 'need to know' basis.</li></ul>

---

<sup>13</sup> For further information, please see ASIO's Managing clearance holders – A supervisor's guide, available through subscription to ASIO Outreach via its website.

Ensure your staff hold the appropriate security clearance	<p>Critically assess the roles and positions requiring security clearances in your agency and determine the required clearance level of people who perform duties in those roles and positions.</p> <p>Do not seek clearances higher than required to conduct duties and where a clearance level is no longer required for the duties performed – advise your ASA to ensure the clearance is downgraded as necessary.</p>
Lead a culture of security	<p>Demonstrating a strong culture of security within your agency is critical to success. As a leader, you should be aware of security at all times and make a concerted effort to incorporate it in all your actions.</p>

Table 5 – Management strategies to support security clearance holders

Managers and supervisors are expected to exercise a duty of care for their people, which includes supporting those with a security clearance. Effective management in these circumstances is also a crucial tool in mitigating associated risks to your agency.

## Ongoing security obligations after leaving a role


Under legislation, security clearance holders have ongoing security obligations, even after they leave a position. Your agency must ensure that separation activities for security clearance holders begin when they leave a position or when they transfer to a role where their access to sensitive or security-classified information ceases or varies.

For further information, please refer to TAS-PSPF policy: Managing separating people (PESEC-3).

## Required action: Ensure compliance with requirements of a security clearance

You should ensure that your agency's people understand and acknowledge their specific responsibilities if they are a national security clearance holder. On appointment, all security-cleared people should be briefed by their manager/supervisor on the security requirements specific to their role, associated risks and mitigating security controls.<sup>14</sup>

<sup>14</sup> Where the manager/supervisor is unsure, your ASA can provide further information.



You should be satisfied that security-cleared people understand their security responsibilities and the consequences of not meeting them, for example, it is important that security clearance holders know that their continued employment is conditional on them maintaining their clearance.

## **Security briefings**

Your ASA or the relevant manager/supervisor can conduct security briefings to assist your people maintain compliance with their security clearance obligations. A briefing should outline a security clearance holder's responsibilities, along with information about measures to protect the Tasmanian Government's information and assets, particularly in relation to information and assets held by your agency.

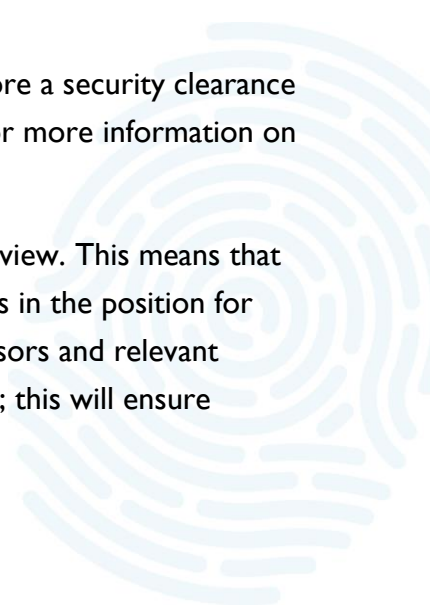
Topics covered in security briefings may include:

- overseas travel briefings and debriefings
- briefings and debriefings for accessing TOP SECRET information
- briefings and debriefings to allow access to specific protectively marked information
- specific location briefings or briefings about high-risk destinations
- briefings tailored for specific categories of employment, e.g. information technology
- briefings tailored to contractors, temporary employees and visitors
- briefings tailored to a person's particular security needs as part of an ongoing management plan
- risk management and protective security briefings.

## **Annual review of eligibility waivers**

All security clearance eligibility waivers must be reviewed annually and before a security clearance is revalidated. See TAS-PSF policy: Recruiting the right people (PESEC-1) for more information on eligibility waivers.

Eligibility waivers are role-specific, non-transferable, finite and subject to review. This means that the waiver only applies while the relevant security clearance holder remains in the position for which the clearance was issued. It is important to inform managers/supervisors and relevant colleagues of the limitations and conditions of the issued security clearance; this will ensure awareness and effective management of eligibility waivers.







## **Specific clearance maintenance requirements**

There may be circumstances where a conditional security clearance is issued by an authorised vetting agency. This occurs in instances where there are concerns about a person's suitability to hold a security clearance, but those concerns are not sufficient to deny issuing a clearance.

In these circumstances, conditions placed on the security clearance must be adhered to by the security clearance holder. Non-compliance with any special/specific conditions must be reported to your agency's ASA and the clearance sponsor, who must provide this information to the vetting agency that issued the clearance.

You must develop policies and procedures supporting the management of any risks related to a conditional security clearance.

## **Security clearance holders on secondment or temporary assignment**

Your agency must determine all security clearance requirements or arrangements for employees seconded, or on temporary assignment, prior to their commencement in the position. Your agency must notify the clearance sponsor of the role change and the expected duration of the secondment or temporary assignment, so that the relevant authorised vetting agency can be notified.

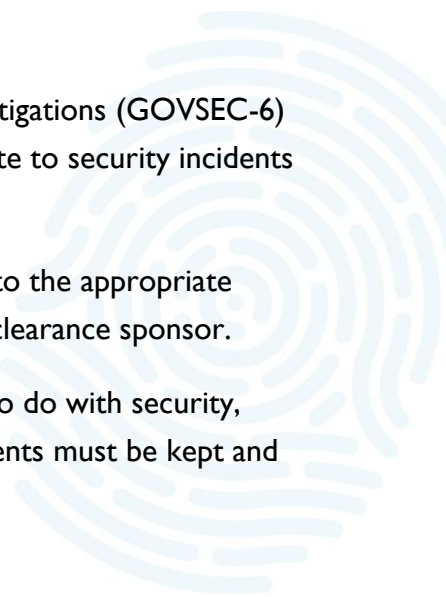
Information about a security concern regarding the security clearance holder must be shared between the relevant agencies to ensure any existing security risks can continue to be managed. This information must also be shared with the clearance sponsor.

## **Required action: Identify and report non-compliance and matters of concern**

As indicated above, TAS-PSPF policy: Reporting incidents and security investigations (GOVSEC-6) requires your agency to develop, implement and review processes that relate to security incidents and consequent investigations.

Your agency must report non-compliance and matters of security concern to the appropriate authorities, which includes managers, human resources, your ASA and the clearance sponsor.

You must monitor security clearance holders' behaviour for any concerns to do with security, poor performance or unacceptable conduct. Records of the following incidents must be kept and reported, as necessary:





- security infringements, including breaches of your agency's policies and procedures that lead to compromise
- security breaches, such as an accidental failure to observe the requirements for handling classified information or assets
- security violations, including a deliberate action that results in, or could result in, a compromise of classified information or assets.

## **Required action: Manage inability to meet ongoing suitability requirements**

Your agency must establish a clear policy and process to manage people who are unable to meet required obligations for ongoing suitability. Where a person's ongoing suitability is under question, it may be necessary to consider the reassigning of duties, a pause/cease to a contract, a cease to a secondment, and so on.

### **Suspending access**

If your agency is investigating a person on the basis of non-compliance or a security concern, your ASA must be notified. The ASA may suspend the person's access to sensitive or security-classified information, assets or work locations until the investigation (which may include a review for cause<sup>15</sup>) is complete.

### **Removing sponsorship of a security clearance**

Where your agency has cause for ongoing or significant concerns regarding a person's security infringements, breaches or violations, due to frequency or nature, the clearance sponsor must be advised.

The clearance sponsor must report these concerns to the authorised vetting agency; however, they can also remove sponsorship for the security clearance should there be sufficient concern regarding the individual's ongoing suitability to maintain a security clearance.

### **Managing departure**

When/if a security clearance holder leaves your agency, there are minimum requirements to manage their departure. For more information about this, please refer to TAS-PSPF policy: Managing separating people (PESEC-3).

---

<sup>15</sup> For information on a review for cause, please refer to the Australian Government Protective Security Policy Framework.

## References and resources

AS 4811:2022 – Employment Screening
Australian Government Department of Defence at <a href="http://www.defence.gov.au">www.defence.gov.au</a>
Victorian Government, 'Protecting and securing Victorian Government information and assets: I. Personnel security', available at <a href="http://www.vic.gov.au/protecting-and-securing-victorian-government-information-and-assets/personnel-security">www.vic.gov.au/protecting-and-securing-victorian-government-information-and-assets/personnel-security</a>
New Zealand Government protective security requirements, available at <a href="http://www.protectivesecurity.govt.nz/personnel-security/managing-insider-risk/recruiting-the-right-person/">www.protectivesecurity.govt.nz/personnel-security/managing-insider-risk/recruiting-the-right-person/</a>
Employment New Zealand at <a href="http://www.employment.govt.nz/workplace-policies/tests-and-checks/drugs-alcohol-and-work/">www.employment.govt.nz/workplace-policies/tests-and-checks/drugs-alcohol-and-work/</a>
Australian Government Protective Security Policy Framework, available at <a href="http://www.protectivesecurity.gov.au/publications-library/policy-12-eligibility-and-suitability-personnel">www.protectivesecurity.gov.au/publications-library/policy-12-eligibility-and-suitability-personnel</a>
HMG Baseline personnel security standard, available at <a href="https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf">https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf</a>



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

**Phone:**  
(03) 6232 7979

**Email:**  
[sem@dpac.tas.gov.au](mailto:sem@dpac.tas.gov.au)