Security Governance

GOVSEC-2:
Security advice and responsibilities

Department of Premier and Cabinet

Tasmanian Government

Contents

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 – GOVSEC-2: Security advice and responsibilities – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

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

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

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

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

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

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

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

Definitions and shortened terms

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

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

Term	What this means in the context of the TAS-PSPF
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's desired protective security outcomes. Each of the 14 TAS-PSPF policies includes a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, people.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of protected information.
integrity	Safeguarding the accuracy and completeness of information and processing methods, i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted, or obtained by an agency.
originator	The instigating individual (or agency) responsible for producing information.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.
principles	Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF. 1. Security is a responsibility of government, its agencies and its people. 2. Each agency is accountable and owns its security risks.

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

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

Acronym/abbreviation	Meaning
AGSVA	Australian Government Security Vetting Agency
ASA	Agency Security Advisor
AFP	Australian Federal Police
CIO	Chief Information Officer
CSO	Chief Security Officer
SCEC	Security Construction and Equipment Committee
RE	Responsible Executive

Context

The **GOVSEC-2: Security advice and responsibilities** policy and guidance will assist agencies to achieve an effective protective security outcome within the security governance domain of the TAS-PSPF. They address core requirement 2 and its supplementary requirements.

Core requirement 2

The Accountable Authority will nominate an ASA.

Supplementary requirements

ASAs have responsibility for components of the security governance structures, including:

a) ensuring the agency achieves the elements of the security plan

b) developing, using and monitoring the effectiveness of security procedures and systems

c) identifying and managing security risks

d) monitoring and assessing the agency's security maturity and capability, including areas of improvement against the security plan/s

e) ensure security requirements are considered in all agency plans

f) responding to, investigating, and reporting security incidents

g) ensuring the Accountable Authority meets all relevant whole-of-government security policy or legislative requirements

h) responsibility for arranging and, where applicable, delivering security briefings

i) ensuring the development and delivery of agency-specific security awareness training, including enhanced role-specific training where necessary.

An Agency Security Advisor (ASA) provides protective security advice and leadership in day-to-day protective security risk management issues. The TAS-PSPF requires an agency to nominate an ASA to lead monitoring of the effectiveness of the protective security system, in accordance with the agency's strategic risk-based protective security plan.

The ASA supports the Accountable Authority with implementation, coordination and ongoing compliance with the TAS-PSPF.

Guidance

Introduction

The TAS-PSPF requires your agency's Accountable Authority to establish and implement appropriate security governance structures to protect the agency's information, people and assets, including appointing an ASA.

Your ASA reports to your agency's Responsible Executive (RE) and/or Chief Security Officer (CSO) on security matters as required.

Your ASA is responsible for:

- managing your agency's implementation of the TAS-PSPF and supporting policies
- performing quality assurance of your agency's protective security functions
- measuring your agency's security maturity and completing the annual self-assessment report
- monitoring and advising on your agency's operating environment, threat context and emerging risks.

Your ASA performs functions in alignment with the 4 protective security domains under the TAS-PSPF: security governance, information security, people security and physical security. Your Accountable Authority is responsible for determining what functions they may delegate to your ASA in addition to the requirements of this policy (GOVSEC-2).

If your agency performs diverse functions or has responsibilities across a range of locations or operational environments, your Accountable Authority may determine it appropriate to appoint additional security advisors to these diverse functions or locations. In these circumstances, it is recommended that any additional advisors are designated 'Deputy ASA'.

It is necessary for your ASA to maintain detailed knowledge of protective security policies protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.

Required action: Ensure success of the agency security plan/s

The TAS-PSPF policy: Establish security governance (GOVSEC-1) requires your agency to develop a security plan. A security plan enables you to review strategic and operational risks, and implement appropriate treatments that manage those risks to an acceptable level.

Security planning involves the use of sound risk management processes to design, implement, monitor and review an agency's protective security arrangements to ensure efficient and effective delivery of government services. All security planning should be based upon achieving a cycle of continuous improvement.

Your Accountable Authority is responsible for your agency's security plan, supported by the RE and ASA.

This policy (GOVSEC-2) requires your ASA to implement identified strategies and security measures, and to monitor, review and evaluate your security plan to ensure your agency achieves the fundamentals of its security plan.

For further information about developing, implementing and reviewing your security plan, refer to TAS-PSPF policy: Security planning (GOVSEC-5).

Required action: Create effective security procedures and systems

This policy (GOVSEC-2) requires you to develop, use and monitor the efficiency of security procedures and systems, in support of your agency's implementation of the TAS-PSPF. Creating and adhering to protective security procedures and systems will enhance your agency's resilience to compromise and also reflects a level of security maturity within your agency.

Appropriate security policies and procedures that are easily understood and accessible to all your people will also support achievement of security awareness outcomes.

Develop procedures

You must develop procedures which cover all elements of protective security consistent with relevant TAS-PSPF policy and the security outcomes specified in your security plan.

It is recommended that you develop security procedures as part of your security and risk planning processes, and that you update these procedures when significant changes occur in your agency's risk environment.

Using procedures

To support your people to use protective security procedures effectively, it is recommended that you embed the procedures across all outputs of your agency. Doing this will also help you to strengthen people's security awareness and the security culture of your agency.

Security procedures are an enabling factor in your agency's safe and ongoing operation. Your agency's induction and staff development programs provide an excellent opportunity for you to explain security measures, policies and procedures that are in place to support your people in their work. Targeted security awareness training will help your people to understand expectations and assist you to achieve elements of your agency's security plan.

Using security procedures successfully in your agency involves:

- your agency people complying with security requirements and responsibilities
- security requirements being embedded across your agency, including in performance reviews.[1]

Monitoring procedures

Effective security procedures help you to identify changes in the threat environment and allow for adjustments to maintain acceptable levels of risk, balancing the operational and security needs of your agency. Your agency's ASA is responsible for monitoring the effectiveness of security procedures and systems that facilitate the agency's capacity to function.

Further information about developing, using and monitoring the effectiveness of security procedures and systems is available in TAS-PSPF policy: Security planning (GOVSEC-5).

Required action: Identify and manage security risks

Identifying security risks is imperative to effective security risk management. Developing good security risk management supports your agency's resilience and builds a positive risk culture. This is because you know your agency's risks, make coordinated and informed decisions about managing those risks, identify new opportunities, and learn from mistakes.

[1] For more information on security in performance evaluations, refer to TAS-PSPF policy: Ongoing suitability (PESEC-2).

Your ASA is responsible for monitoring and advising on your agency's operating environment, threat context and emerging risks, including identifying site-specific and shared inter-agency security risks. Your ASA's leadership ensures that security risks are considered in agency decision-making and planning, enhancing protection and reducing vulnerabilities.

Continuous engagement with this process allows you to monitor and evaluate existing security measures and introduce new measures, where required, to reduce risk to an acceptable level.

Further information about identifying and managing security risks is available in TAS-PSPF policy: Security planning (GOVSEC-5), which should be considered in conjunction with the Standards Australia Handbook HB167:2006 – Security risk management.

Required action: Ensure security maturity and capability

The term 'security capability' refers to the overall security position of your agency in relation to its specific risk environment, risk tolerances, and the effectiveness of existing security measures. Your ASA's monitoring and assessment of your agency's security maturity on an ongoing basis will help you develop a good understanding of your agency's security capability and give you the opportunity to respond appropriately to any increase or decrease in that capability.

It is important that, as well as highlighting areas for improvement, your agency's monitoring and assessment processes also include acknowledging successes and the effectiveness of the implementation of the TAS-PSPF across your agency.

Security maturity considers how holistically and effectively your agency:

- minimises harm to the government's people, information and assets
- fosters a positive security culture
- responds to and learns from security incidents
- understands and manages its security risks
- achieves security outcomes while delivering business objectives.

The benefits of effective security maturity monitoring include:

- a better understanding of your agency's security risks and risk mitigation strategies
- improved performance of your agency in –
    - implementing the core and supplementary requirements of the TAS-PSPF in relation to its risk environment
    - driving a strong security culture through awareness of expected security behaviours

- identifying and implementing changes that achieve robust security outcomes
- using resources efficiently and effectively to protect people, information and assets

- assurance that –
  - your agency's information, people and assets are adequately protected, consistent with relevant policy
  - security risks are managed appropriately (including security incidents), there are clear lines of accountability, and sound planning and proportionate reporting are undertaken.

Your ASA should develop your agency's security maturity monitoring plan as part of the overarching security plan. The monitoring plan should record progress against the goals and objectives of the security plan, and document and evidence the assessment of your agency's security maturity.

Security maturity monitoring is designed as a continuous improvement cycle to assist your agency to respond to changes in its security environment and emerging security risks. It can help your agency to implement the TAS-PSPF core and supplementary requirements necessary to protect information, people and assets.

Required action: Consider security requirements in all planning processes

Embedding a security culture and applying protective security principles in corporate planning processes enhances an agency's ability to meet business needs, provide a safe working environment and improve relationships with clients and the community. In a positive security culture, security exists intrinsically within an agency's systems and practices in order to enhance security resilience across government more broadly.

Your ASA should work with managers, agency executive members, corporate services branches (for example, human resources, property and fleet, procurement, information technology, communications) and other areas of your agency to ensure appropriate information, people and physical security requirements are considered in the development and review of all agency policies and plans.

Incorporation of protective security in all planning and policies across your agency ensures that the protection of your information, people and assets from compromise is considered in every aspect of the agency's organisation and operations. This encompassing approach provides greater opportunity to address necessary security measures, enhancing your agency's security maturity and capability.

Required action: Respond to, investigate, and report security incidents

Managing security incidents and investigations helps you monitor security performance, identify inadequacies in security procedures, and detect security risks in order to implement appropriate treatments. Through effective investigation processes, you can identify vulnerabilities in your agency and reduce the risk of security incidents in the future.

Your ASA is responsible for reporting and escalating security incidents, as required by this policy (GOVSEC-2).

Responding to security incidents

You must establish procedures for managing security incidents. Incident management procedures should be consistent, appropriate and fair and be applicable to any security incident that may arise. It is appropriate that procedures for responding to security violations are formal. This reflects the significance of these deliberate or reckless actions, particularly regarding the impact they have on security.

The following table provides some recommended elements to consider when developing incident management procedures.

Recommended elements of incident management procedures
A requirement that employees (including contractors) immediately report security incidents to a centralised point, this being the ASA. This requirement and accompanying appropriate arrangements would also be made for employees travelling or working remotely.
Formal procedures and mechanisms to make it easy to report security incidents (including for responding to incidents that occur outside of your agency's premises).
Handling procedures once a security incident has been reported, which would include: • clearly defined roles and responsibilities of people involved in managing and investigating the security incident • clearly defined escalation points, chains of command and communication channels (both internal and external) • time frames for incident response and recovery • assessment and categorisation of the level of harm or compromise • any technical requirements or business continuity arrangements • prioritisation mechanism for multiple or simultaneous incidents • linkages to other procedures, such as business continuity plans or disaster recovery plans • incident reporting to your Accountable Authority and/or RE • testing and review cycles.

Feedback processes to ensure all relevant parties are notified of results once an incident has been resolved.
Record keeping arrangements developed and maintained by your ASA to collect data about reported incidents and other security incidents, with this data analysed on a regular basis to identify trends or systematic issues. Recording security incidents creates a valuable source of data to assess an agency's security environment and performance. For example, multiple minor security incidents could indicate poor security awareness and could alert you to the need for increased security training and education. Relevant and useful information to collect could include: • the time, date and location of the security incident, including how the incident was detected • the type of official resources involved • a description of the circumstances of the incident, including any personnel or locations involved • the nature or intent of the incident, e.g. deliberate or accidental • an assessment of the degree of compromise or potential or realised harm • whether it is an isolated incident or part of a broader reoccurring issue • a summary of immediate action taken (including containment or eradication) and any long-term action taken (including post-incident activities).

Table 1 – Recommended incident management procedures

Investigating security incidents

It is the responsibility of your ASA to investigate broad security incidents and where necessary, escalate complex investigations to your RE or CSO.

Upon reporting of a security incident, your ASA is required to make an initial assessment to:

- confirm it is a genuine security incident rather than a false alarm or vexatious complaint
- determine the type of incident and scale of harm resulting from the incident
- decide what further action is required to address the incident (by whom and when), for example –
    - no further action
    - amendments to agency procedures, systems or training
    - containment, recovery or eradication action
    - training or performance management activities with the individual/s involved in the incident
    - a security investigation
    - escalation to the RE, CSO, Accountable Authority or responsible minister
    - external reporting or referral to appropriate authority.

Further information about developing incident investigation processes is available in TAS-PSPF policy: Reporting incidents and security investigations (GOVSEC-6).

Reporting security incidents

There are circumstances where a security incident must be reported to another agency or authority, depending on the nature and severity of the incident. Table 2 below outlines your agency's obligations to report particular security incidents, and to whom they must be reported. Non-reporting of these incidents is considered a security breach.

Your ASA is responsible for reporting these incidents as necessary, and for ensuring the RE or CSO is advised of the incident at the earliest opportunity.

Reportable incident	Details	Reportable to
National security incidents	Security incidents or situations that have, or could have, an impact on national security,[2] including suspected: • espionage • sabotage • politically motivated violence • promotion of communal violence • attacks on Australia's defence system • acts of foreign interference • serious threats to Australia's territorial and border integrity.[3] You must observe the 'need to know' principle in relation to any details of a major security incident, until the Australian Security Intelligence Organisation (ASIO) advises otherwise.	ASIO at – Email: asa@asio.gov.au Internet: www.asio.gov.au Phone: 13 ASIO (13 2746) (24hrs) For advice on whether the incident needs to be reported, contact: National Security Hotline Phone: 1800 123 400
Cyber security incidents	Agencies must notify the Tasmanian Government Chief Information Officer (CIO) of actual or suspected cyber security incidents as per the Tasmanian Government Cyber Security Incident Management Arrangements.[4]	Digital Strategy and Services, Department of Premier and Cabinet Email: cybersecurity@dpac.tas.gov.au Phone: 1800 255 505

[2] As defined in the *Australian Security Intelligence Organisation Act 1979* (Cth).

[3] ASIO will assist your agency to conduct an initial assessment of any potential compromise and will either recommend your agency continue with its own investigation and advise of the outcome, or take over the investigation in close consultation with your agency.

[4] Refer to the Tasmanian Government Cyber Security Incident Management Arrangements at www.dpac.tas.gov.au/__data/assets/pdf_file/0010/123004/Tasmanian_Government_Incident_Management_Cybersecurity_Standard.pdf.

Reportable incident	Details	Reportable to
Significant security incidents	As required under TAS-PSPF policy: Reporting incidents and security investigations (GOVSEC-6), significant security incidents must be reported to the TAS-PSPF team in addition to relevant authorities or affected agencies. You are required to include significant security incidents in the agency annual self-assessment report (refer to TAS-PSPF policy: Annual reporting (GOVSEC-4) for more detail).	Tasmanian Protective Security Policy Framework team Email: sem@dpac.tas.gov.au
Tasmanian Cabinet material	Any security incidents, suspected or actual, involving Tasmanian Cabinet material.	Cabinet Office Email: cabinet.office@dpac.tas.gov.au
Contact reporting	Under the Australian Government Contact Reporting Scheme, employees are required to report a contact, either official or social: • with embassy or foreign officials[5] within Australia • with foreign officials and foreign nationals outside Australia • when contact seems suspicious, persistent or unusual in any respect, or becomes ongoing • when a person or group, regardless of nationality, seeks to obtain information they do not need to know for the responsibilities of their job.	Office of Security and Emergency Management Department of Premier and Cabinet (DPAC) Email: sem@dpac.tas.gov.au DPAC will then forward a Contact Report to ASIO.
Incidents involving security clearance holders	In addition to the requirements for contact reporting, security incidents involving security clearance holders must be reported to the Australian Government Security Vetting Agency (AGSVA) or the authorised vetting agency, at the appropriate time, where the incident may affect a person's suitability to hold a security clearance. The appropriate time will depend on the incident, whether an investigation is ongoing,	Your agency's ASA, who will advise the Tasmanian Security Clearance Sponsor, who will then provide notification to AGSVA Tasmanian Security Clearance Sponsor Email: clearances@dpac.tas.gov.au

[5] Foreign officials could include trade or business representatives.

Reportable incident	Details	Reportable to
	and an assessment of people security risks. If one of your people is unsure about what should be reported, they should talk to your ASA, their manager, the Tasmanian Security Clearance Sponsor, or contact AGSVA.	
Potential criminal/serious incidents	Some incidents may constitute a criminal offence. Depending on the type of offence, your agency may need to report to the Australian Federal Police (AFP) or to Tasmania Police. Refer to the AFP website[6] for advice on the type of criminal incidents that are reported to Commonwealth or local police.	Tasmania Police for state crimes Phone: 131 444 Crime Stoppers to anonymously provide information about a crime Phone: 1800 333 000 AFP for Commonwealth crimes Phone: 02 6131 3000
Critical incidents involving public safety	For critical incidents requiring immediate response, in particular where lives are at risk, your agency must call emergency services on triple zero (000). Other critical incidents that may affect public safety and require a coordinated response from the Tasmanian and/or Australian governments may include: • assault, including armed or military-style assault • arson, including suspected arson • assassination, including suspected assassination • bombing, including suspected use of explosive ordnance or improvised explosive devices • chemical, biological or radiological attack, including suspected attacks • attack on the National Information Infrastructure or critical infrastructure • violent demonstration involving serious disruption of public order • hijacking, including suspected hijacking	Emergency services Triple zero (000) Tasmania Police Phone: 131 444

[6] The AFP website is at www.afp.gov.au.

Reportable incident	Details	Reportable to
	• hostage situation, including suspected hostage situation • kidnapping, including suspected kidnapping • mail bomb, including suspected mail bomb • white powder incident, including real or significant hoax incidents.	
Correspondence of security concern	Correspondence received by your agency may be of security concern if it contains: • threat to use violence to achieve a political objective • warning of imminent threats to specific individuals, groups, property or buildings.	Tasmania Police Phone: 131 444 Crime Stoppers to anonymously provide information about a crime Phone: 1800 333 000 National Security Hotline Phone: 1800 123 400
Incident affecting another agency	Security incidents or unmitigated security risks that affect another agency's people, information or assets, particularly where agencies are co-located or are providing services to another agency.	Accountable Authority of the agency whose information, people or assets may be affected.
Security-classified equipment and services	Incidents involving Security Construction and Equipment Committee (SCEC) and ASIO approved destruction services.[7]	SCEC Email: scec@scec.gov.au Report: SCEC courier incident report[8]
Unauthorised foreign entity access to security-classified information or assets	Inappropriate or unauthorised sharing of security-classified information or assets with a foreign national or international entity, without the protection of an agreement or arrangement.	Your RE or CSO (in line with internal agency reporting procedures, the incident may need to be reported externally, as per the other categories in this table).
Compromise of foreign entity information or assets	Failure to safeguard sensitive or security-classified information of a foreign government or entity covered by an international agreement or arrangement.	Your RE or CSO (your agency must notify the originating foreign entity as soon as practicable).

Table 2 – External reporting obligations

[7] Refer to TAS-PSPF policy: Protecting assets (PHYSEC-1) for more information on SCEC-endorsed equipment and services.

[8] Complete the SCEC courier incident report available at www.scec.gov.au/system/files/documents/2016%20Security%20Incident%20report%20template.pdf

Required action: Meet other relevant security policy and legislative requirements

To support Tasmania's collective capability against compromise and harm, it is important that your agency not only implements the TAS-PSPF but also meets the requirements of any other relevant whole-of-government security policies and legislation.

The policies of the TAS-PSPF have been developed with the view of consistency with existing Tasmanian Government security policy and in accordance with legislation. If you identify discrepancies or conflicts between the requirements of the TAS-PSPF or other relevant security policy or legislation, you must notify the TAS-PSPF team.[9]

While the TAS-PSPF is underpinned and supported by existing legislation and Australian and International Standards, there are also pre-existing whole-of-government policies which focus on security, for example, the Tasmanian Government Cyber Security Policy.

Your ASA should maintain an up-to-date understanding of relevant security policy and legislative requirements that exist in addition to the TAS-PSPF – these policies and legislation will complement your agency's protective security. You must remain aware of any agency-specific legislation that relates to the execution of official duties, noting that the TAS-PSPF does not override this.

Your ASA should ensure that your agency's security plan, strategic goals and objectives consider legislative implications and that all systems are operated in accordance with the law, as well as Tasmanian and/or Australian government policies.

Required action: Deliver security briefings

Your ASA is responsible for arranging and providing briefings and advice to agency employees, including briefings to employees located or travelling overseas.

Security briefings should form part of your agency's security communication strategy, as they raise awareness and ensure that people in high-risk positions, security clearance holders, or staff in security roles are aware of the current trends, risks and challenges facing your agency.

[9] Notify the team via email sem@dpac.tas.gov.au.

Face-to-face briefings allow you to provide current security information to your agency people in a proactive manner. It is recommended these briefings are completed at regular intervals and included in relevant agency training. [10]

Incident briefings

In the event of a security incident, your ASA should arrange or, where applicable, deliver regular briefings to relevant supporting security staff, agency executives, and agency, cross-agency or whole-of-government working groups to ensure situational awareness.

Briefings conducted in these scenarios must be delivered on a 'need to know' basis and, in circumstances where your ASA is not conducting these briefings, it is important for them to be included for security and situational awareness purposes.

Pre-travel briefings

Any people travelling overseas, for work-related purposes, must follow necessary application and approval processes required by your agency. This includes compliance with the Tasmanian Government Overseas Travel Policy and Guidelines.

People in high-risk positions, security clearance holders and security staff traveling overseas for any reason, should notify your ASA in accordance with your agency's security plan.

Your ASA should facilitate any pre-departure or post-travel obligations required by your agency. This can include activities such as:

- recording the details of the overseas travel in a security register[11]
- advising people to monitor the Department of Foreign Affairs and Trade (DFAT) Smarttraveller website, for up-to-date Australian Government advice on physical security
- providing travel briefings/debriefings, as necessary.

---

[10] High-risk positions may include those involved in:

- sensitive or priority negotiations or policy work
- controlling access to valuable or attractive assets (including information)
- work in remote or dangerous locations
- liaising or sharing information with foreign officials.

[11] In accordance with the Tasmanian Government's Overseas Travel Policy and Guidelines.

Pre-travel briefings should include advice on:

- potential physical and information security risks and vulnerabilities, both general and specific to the destination[12]
- any relevant Foreign Intelligence Services threat environment of the destination
- requirements for use of work and personal devices before, during and after travel
- handling of gifts received
- debriefing and reporting requirements upon return.

When travelling, employees should only take the devices they require and consider leaving personal electronic devices at home. In addition, it is recommended that pre-paid, disposable devices are used for travel. Your agency may consider including, in your agency's security plan, reporting requirements where personal devices containing work-related information are lost or stolen during travel.

Storage of any sensitive and security-classified information on personal electronic devices should be avoided.[13]

Briefings for security clearance holders

The ASA must arrange and, where applicable, deliver briefings or training to ensure security clearance holders in your agency understand their day-to-day responsibilities and reporting obligations (e.g. changes of circumstances, and suspicious, ongoing, unusual or persistent contacts).

Where security clearance holders have access to sensitive compartmented information,[14] this engagement with your ASA should include training and briefings from, or in consultation with, relevant compartment owners.

For further information regarding briefings for security-cleared people, please refer to TAS-PSPF policy: Ongoing suitability assessment (PESEC-2).

---

[12] The DFAT smartraveller website at www.smartraveller.gov.au provides travel advisories (including an advice level) for 170 overseas destinations.

[13] For further information, refer to www.acsc.gov.au or www.cyber.gov.au.

[14] Refer to TAS-PSPF policy: Protecting official information (INFOSEC-2) for more information relating to compartmented information.

Required action: Deliver security awareness and role-specific training

TAS-PSPF policy: Security awareness (GOVSEC-3) requires you to provide security awareness training to all people upon commencement in the agency. Security awareness training supports implementation of security policies, practices and procedures, and is a critical component of building your agency's security culture and overall security maturity.

DPAC is responsible for developing and promoting introductory security awareness training materials to elevate protective security understanding and awareness across Tasmanian Government agencies.

Your ASA is responsible for ensuring the development and delivery of agency-specific security awareness training, including enhanced role-specific training where necessary. Your ASA will determine the appropriate training delivery method that ensures consistency across your agency for all employees, while ensuring all specific training or awareness requirements are met.

Targeted security awareness training should be provided to all agency people where the agency has identified a need based on the agency's risk profile, or when the agency has an increased or changed threat environment. You should use your agency's security plan to help you identify the security expectations, targets and risks of most relevance that should be addressed in your agency-specific training.

People with specific emergency safety or security roles should be provided with regular training, in addition to assessment of their ongoing suitability.[15]

Further information about developing agency and role-specific training is available in TAS-PSPF policy: Security awareness (GOVSEC-3).

[15] See TAS-PSPF policy: Ongoing suitability assessment (PESEC-2) for further information.

References and resources

ASIO T4 Protective Security, Security Managers Handbook – Introduction to protective security measures, available to authorised people via the GovTEAMS protective security community.
Australian Government, Department of Foreign Affairs and Trade (DFAT) Smartraveller website, at www.smartraveller.gov.au/
Australian Government Protective Security Policy Framework, at www.protectivesecurity.gov.au/system/files/2021-08/PSPF-policy-2-Management-structures-and-responsibilities.pdf
Australian Government Protective Security Policy Framework, at www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-4-security-maturity-monitoring.pdf
New Zealand Government, Personnel security, at https://protectivesecurity.govt.nz/assets/Personnel-security/2f0251f728/Travel-advice-for-government-officials-travelling-overseas-on-business.pdf
New Zealand Government, Personnel security, at https://protectivesecurity.govt.nz/assets/Personnel-security/01659feef8/Travel-Advice-Electronic-Devices.pdf
South Australian Government, Security governance, at www.security.sa.gov.au/documents/SAPSF-GOVSEC1-Security-governance-B451752-1.pdf
South Australian Government, Security governance, at www.security.sa.gov.au/documents/SAPSF-GOVSEC3-Security-monitoring-B460718.pdf
Tasmanian Government, Overseas Travel Policy and Guidelines, at www.dpac.tas.gov.au/__data/assets/pdf_file/0025/23947/Overseas_Travel_Policy_2011.pdf

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7979

Email:
sem@dpac.tas.gov.au