Security Governance

GOVSEC-6:
Reporting incidents and security investigations

Contents

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

About this document

This document – GOVSEC-6: Reporting incidents and security investigations – 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
AGIS	Australian Government Investigations Standards
ASA	Agency Security Advisor
ASIO	Australian Security Intelligence Organisation
DPAC	Department of Premier and Cabinet
RE	Responsible Executive

Context

The **GOVSEC-6: Reporting incidents and security investigations** 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 6 and its supplementary requirements.

Core requirement 6

The Accountable Authority will develop, implement and review processes to support the reporting and investigation of security breaches and incidents.

Supplementary requirements

To assure improvement and enhance security maturity, it is necessary to create an environment that supports investigation. To achieve this, the Accountable Authority must:

a) provide a supportive environment for people to report security breaches and incidents[1]

b) ensure security awareness includes knowledge about actions which constitute security breaches and incidents

c) develop and implement clear processes supporting thorough investigation of reported security breaches and incidents

d) provide adequate security awareness training to assure agency people are cognisant of the TAS-PSPF's protective security requirements

e) ensure corrections are addressed following the conclusion of investigations.[2]

With increased security awareness and enhanced security culture, the identification of and response to security incidents will improve. Accountable Authorities must ensure reporting processes are developed and implemented in accordance with the TAS-PSPF.

While the investigation of security incidents will be based on agency-specific risk tolerance and appetite, the TAS-PSPF provides guidelines to ensure a consistent approach to these investigations.

[1] In conjunction with existing reporting processes, including (but not limited to): Code of Conduct, Integrity Commission, Equal Opportunities Tasmania.

[2] Consider updating security plans, enhancing security training, modifying the security treatment, revisiting the agency risk assessment.

Guidance

Introduction

This policy requires your agency to implement practices and procedures to support the reporting and investigation of security breaches and incidents. Through effective reporting and investigation of security incidents, you can identify vulnerabilities and reduce the risk of future occurrence.

Required action: Provide a supportive environment

Early detection of a security incident, and a timely response, is critical in reducing the consequences from the incident and is essential to effective security risk management.

The TAS-PSPF requires your Accountable Authority to provide a supportive and transparent environment that encourages your people to report security breaches and incidents, contributing to a positive security culture.

To support this requirement, it is recommended that you work to build understanding, trust and confidence in your agency reporting processes among employees.

To help ensure a supportive environment for reporting, you should:

- establish simple, discreet channels for people to report possible or actual security incidents
- actively promote security incident reporting procedures through multiple channels, e.g. agency-specific security awareness training, posters, banners, intranet, desktop shortcuts and computer login prompts
- ensure your Agency Security Advisor (ASA), or other designated security staff, are accessible for your people to discuss security issues or concerns (including sensitive issues to be discussed in confidence)
- include feedback processes to ensure that employees who report security breaches and incidents have their report acknowledged and/or are notified when the issue has been resolved
- provide clear pathways for people to escalate reports to external parties, as appropriate.[3]

[3] In the event employees elect to escalate reports externally, the mechanism and information to do so should be made available. This may include matters relating to police investigation and integrity concerns (Integrity Commission).

While reporting is a common means of detecting security incidents, it is recommended that your ASA consider other security monitoring measures to assist in identifying potential or actual security incidents.

Required action: Ensure awareness of actions constituting security incidents

Agency-specific security awareness training and materials should include relevant examples of reportable security breaches and incidents to complement agency reporting procedures and policies.

The TAS-PSPF defines a security incident as:

- 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 incidents can lead to security breaches, which can have serious consequences for your agency, the community and state or national interests, so it is important that you have robust systems and procedures in place to identify and respond effectively.

Table 1 provides some examples of security incidents and significant security incidents, noting that significant security incidents should be reported to the Department of Premier and Cabinet (DPAC) via your ASA.

Examples of security incidents	Examples of significant security incidents
Criminal actions such as actual or attempted theft, break and enter, vandalism or assault	Espionage or suspected espionage
Loss of personal information that is likely to result in serious harm	Actual or suspected compromise of material at any level, including tampering with security containers or systems
Security-classified material not properly secured or stored	Loss, compromise, suspected compromise, theft or attempted theft of classified equipment

Security-classified material left in inappropriate waste bins	Actual or attempted unauthorised access to an alarm system covering a secured area where security-classified information is stored
Deliberate disregard of implementing TAS-PSPF requirement	Loss of material classified PROTECTED or above, or significant quantities of material of a lower classification
Access passes or identification documents lost or left unsecured	Recovery of previously unreported missing classified material or equipment
Incorrect handling of information that is protectively marked, such as a failure to provide the required protection during transfers or transmission resulting in a data spill on an electronic information network or system	Unauthorised disclosure of official or classified information, significant loss or compromise of cryptographic keying material, or a significant breach of ICT systems
Compromise of keys to security locks, or of combination settings	Continuous breaches involving the same person or work area where the combination of the events warrants an investigation
Sharing computer passwords	Loss, theft, attempted theft, recovery or suspicious incidents involving weapons, ammunitions, explosives or hazardous materials including chemical, biological, radioactive or nuclear
Vandalism	Actual or suspected hacking into any ICT system

Table 1 – Security incidents

Required action: Develop and implement clear processes

Not all security incidents warrant investigation. Your ASA is responsible for assessing the requirement for a formal security investigation or escalating the decision to your Responsible Executive (RE).

In assessing the incident, your ASA must consider:

- the seriousness or complexity of the incident
- the possible outcomes of the investigation (administrative, disciplinary, civil or criminal)
- if the incident requires referral to another agency or authority
- the resources required to conduct the investigation
- who will conduct the investigation and what support they need

- the investigation process and time frames
- the authorisation needed to undertake the investigation
- the decision-makers and subsequent reporting obligations.

A security investigation is the formal process of examining the cause and extent of a security incident that has, or could have, caused harm to individuals, or another agency or the state or national interest. Security investigations protect the interest of the Tasmanian Government and the rights of the affected individuals.

Investigating security incidents (actual or suspected) may be necessary to resolve an existing breach or vulnerability and reduce the impact or consequences. Security investigations can:

- provide useful information for future risk assessments or reviews
- help determine the effectiveness of existing protective security arrangements within your agency
- monitor security performance (including security maturity and culture)
- identify security risks in order to implement improvements.

Your agency must establish procedures for investigating reported security incidents. It is recommended that these procedures cover:

- the terms of reference and the investigation plan (authorised by your Accountable Authority or RE)
- the responsibilities of the investigator, approving officer and other relevant parties
- qualifications and/or training required for investigators
- procedural fairness and standards of ethical behaviour to ensure impartiality and the absence of any conflict of interest
- actions for handling complaints or allegations (including anonymous or public interest disclosure[4] reports)
- case management procedures to ensure compliance with your agency's procedures
- procedures for undertaking operational practices (such as interviews of affected persons)
- points of referral, escalation or approval, including keeping the RE notified of progress

[4] Refer to the *Public Interest Disclosures Act 2002* for more information.

- points of escalation to law enforcement or the Australian Security Intelligence Organisation (ASIO)
- findings and recommendations
- final report requirements.

It is recommended that, where possible, agencies apply the Australian Government Investigation Standards (AGIS)[5] to maintain a minimum quality standard within investigations.

When investigating, the principles of procedural fairness should be applied, meaning any individuals being investigated or whose interests could be adversely affected should be informed of the case against them and given the opportunity to be heard by an unbiased decision-maker. Procedural fairness should also be applied to any actions taken as a result of the investigation, as well as when considering the security integrity of current or future investigations by your agency, or another agency.

Where a suspected security incident involves major compromise of official information or other resources that originate from, or are the responsibility of, another entity, it is important to seek advice from the originating entity prior to instigating any investigation. The originating entity may have operational security requirements that need to be applied to the investigation.

In some cases, it may be more appropriate that the originating or responsible entity carries out the investigation. TAS-PSPF policy: Security advice and responsibilities (GOVSEC-2) outlines your obligation to report certain security incidents to external entities.

Required action: Provide adequate security awareness training

Your agency is required to take ownership of its maturity and performance against the core requirements of the TAS-PSPF, and work to strengthen agency security culture and awareness.

TAS-PSPF policy: Security awareness (GOVSEC-3) requires you to deliver agency-specific security awareness training during induction. 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.

[5] The Australian Government Investigation Standards are available at www.ag.gov.au/integrity/publications/australian-government-investigations-standards.

Training must ensure all agency people are made adequately aware of their responsibilities under the TAS-PSPF, including:

- assisting the agency to achieve a strengthened security culture
- taking personal responsibility for their actions
- complying with agency protective security policies and procedures.

To support the intent of this policy (GOVSEC-6), agency-specific security awareness training should include security incident reporting procedures, using relevant, practical examples, to assist agency people in understanding when and how to report potential incidents or concerns.

Further information about agency-specific security awareness training, including suggested content, is available in TAS-PSPF policy: Security awareness (GOVSEC-3).

Required action: Address corrections when investigations are concluded

Embedding post-incident learning into incident reports or updated procedures can provide useful insights into opportunities for improvements and emerging issues, vulnerabilities in processes and training, or employee understanding of how to apply their security obligations.

You should apply a process of continual improvement to monitoring, evaluating, responding to, and managing security incidents.

It is recommended that you identify, document, and share learnings internally (i.e. with and between your Accountable Authority, RE and ASA) and externally, where appropriate (i.e. with co-located agencies, agencies with similar risk profiles or through whole-of-government arrangements).

Possible questions to consider once the incident is resolved include:

- Were the procedures adequate to deal with the incident and were all stages of incident management followed?
- Were the right people involved and were escalation points and time frames sufficient and useful?
- Did the incident highlight areas of vulnerability and if so, what action is being taken to address these vulnerabilities?
- Could the incident have been prevented? If so, how?

- Could the incident have been detected earlier, or damage reduced if detected earlier?
- What were the triggers and is there a way to prevent future occurrences?
- Is it a recurring incident or becoming systemic; if so, what additional protection or action is required to prevent further incidents?

This policy (GOVSEC-6) states that you must ensure your agency addresses corrections identified throughout the investigation process. Corrections may be in the form of updates to the security plan, targeted security awareness training, modifications to processes and procedures or agency-specific policies.

Addressing corrections provides confidence to your people and enhances your resilience to future incidents of the same nature. When considering your agency's cycle of continuous improvement with regards to the TAS-PSPF, it includes being adaptive to your environment and strengthening your capability of deterrence, detection, response and recovery.

Useful resource: Steps to conduct security investigations

Step 1 – Appoint an investigator

In the interests of procedural fairness, it is important that the investigator be impartial and not have an actual or apparent conflict of interest in the matter being investigated.

Your agency is strongly encouraged to provide relevant and appropriate training for investigators, as determined by your agency. The AGIS provides guidance on recommended training or qualifications for investigators. Where insufficient power to collect available or required evidence is identified, or if a conflict of interest is identified, the investigator is encouraged to refer the investigation to another person or agency with the necessary powers.

An investigator's key responsibilities include:

- understanding the incident being investigated and the terms of reference
- identifying the relevant law, policy or procedures that apply
- making sufficient inquiries to ascertain all relevant facts
- ascertaining whether an offence or incident has occurred, based on the relevant facts
- reporting the findings and identifying the reasons for the findings
- making relevant recommendations.

Investigators assess:

- applicable legislation that may determine the nature of, and set the framework for, the investigation
- the nature of the incident
- how serious the incident is and therefore the possible level of harm it has for the agency, or more widely for the government
- whether the incident indicates the existence of a systemic problem
- whether it is part of a pattern of conduct
- whether it may breach any Australian law, especially any criminal provision.

Step 2: Develop an investigation plan

The investigation plan identifies:

- the issues to be investigated
- any relevant legislation, particular provisions of a code of conduct, agency policy and procedures, particular standards and guidelines
- required evidence
- methods and avenues to collect the evidence
- legal requirements and procedures to be followed in collecting evidence
- the allocation of tasks, resources and timings
- arrangements in case the terms of reference or investigation plan need to be modified during the investigation.

Terms of reference

It is recommended that the RE approve the terms of reference, objectives and scope for all security investigations. The terms of reference could include:

- the background
- resources allocated
- time frames
- the types of inquiries to be conducted
- the extent and limit of powers of the investigating officer during the investigations to collect evidence by:
    - obtaining information from people about policies, procedures and practices
    - accessing relevant records and other material
    - interviewing witnesses and suspects
    - search and surveillance
    - the format of progress reporting and the final report
    - any special requirements or factors specific to the investigation.

Step 3: Gather evidence

The investigator identifies, collects and presents information or evidence that goes to proving or disproving any matters of fact relating to an incident. In an investigation, the types of evidence are:

- physical
- documentary (records)
- verbal (recollections)
- expert (technical advice).

Evidence gathered in a security investigation may not comply with the rules of evidence and therefore may not be satisfactory in a criminal investigation, or where legal proceedings might arise in relation to the incident.

Step 4: Record and store evidence

It is recommended that investigators maintain a separate file for each investigation. This is a complete record of the investigation, documenting every step, including dates and times, all discussions, phone calls, interviews, decisions and conclusions made during the course of the investigation.

Investigators are encouraged to store this file and any physical evidence securely to prevent unauthorised access, damage or alteration. This is to maintain confidentiality and ensure continuity of evidence. It is important that the record includes the handling of physical evidence and any tampering with the file or physical evidence.

Step 5: Prepare the investigation report

At the conclusion of the investigation, the investigator produces a findings report for the RE, commissioning body (e.g. the agency security governance committee) or the relevant decision-maker.

The report must include reasons for the findings according to the terms of reference, using supporting material, and recommendations that could include:

- disciplinary action
- dismissal of a disciplinary charge following a constituted hearing
- referral of a matter to an external agency for further investigation or prosecution
- changes to administrative or security policies, procedures or practices.

Standard of proof

In drawing conclusions regarding administrative investigations, whether conducted for security or other reasons such as disciplinary purposes, the decision-maker needs to be satisfied that the allegations are proved 'on the balance of probabilities'.

Step 6: Close the investigation

The investigation is considered closed when all reports are completed, and evidence is documented and filed. It is better practice for an independent person, preferably more experienced than the investigator, to review the closed investigation.

This allows an impartial assessment of the investigation that may identify future improvements to investigation practices.

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

ASIO T4 Protective Security, Security Managers Handbook – Introduction to protective security measures, available to authorised people via the GovTEAMS protective security community.	
Australian Government Protective Security Policy Framework, available at www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf	
Australian Government Investigations Standards, available at www.ag.gov.au/integrity/publications/australian-government-investigations-standards	
South Australian Government, Security governance at www.security.sa.gov.au/documents/SAPSF-GOVSEC1-Security-governance-B451752-1.pdf	
Tasmanian legislation	*Public Interest Disclosures Act 2002*

Tasmanian Government

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au