GOVSEC-6

Reporting incidents and security investigations

What to know

This summary sheet outlines key points from **GOVSEC-6: Reporting incidents and security investigations** – a policy under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF supports Tasmanian Government agencies to protect their people, information and assets from compromise and harm.

To read the TAS-PSPF or to find other summaries, policies and resources, go to **www.security.tas.gov.au**

To help protect ourselves and each other, as well as our agency's information and assets, we should all be security aware and understand what a security incident is and how to report it. It is also important that people who investigate these incidents follow proper processes to ensure thorough investigations lead to improvements and lessons learned.

Policy GOVSEC-6 sets out and explains the processes and procedures necessary to create an agency environment that supports the reporting and investigation of security incidents required under the TAS PSPF.

Provide a supportive environment

The TAS-PSPF requires the Accountable Authority (a person/people with control over a Tasmanian Government public authority) to provide a supportive and transparent environment that encourages people to report security breaches and incidents, contributing to a positive security culture.

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

Awareness of actions constituting a security incident/breach

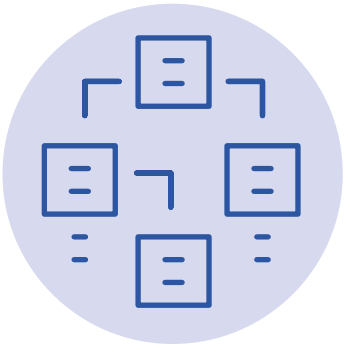
The TAS-PSPF defines a security incident as:

- an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures, and 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 your agency has robust systems and procedures in place to identify and respond effectively.

Some examples include compromise of keys to security locks, or of combination settings, security classified material not properly secured or stored, or access passes or identification documents lost or left unsecured.

Develop and implement clear processes



Your agency must establish procedures for investigating reported security incidents.

Not all security incidents will warrant investigation. Your Agency Security Advisor (ASA) will assess whether an incident requires a formal security investigation or whether that decision should be escalated to your Responsible Executive (the person who oversees protective security arrangements in your agency).

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 interests of the Tasmanian Government and the rights of affected individuals.

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

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.

Address learnings and make corrections

Capturing post-incident learnings will give your agency useful insights into opportunities for improvements and emerging issues, vulnerabilities in processes and training, or agency people's understanding of how to meet their security obligations.

This policy recommends that learnings are identified, documented and shared internally and externally where appropriate. It is important that a process of continual improvement is applied to monitoring, evaluating, responding to, and managing security incidents.

Following an investigation, addressing learnings and making any needed corrections will give confidence to agency people and enhance your agency's resilience to future incidents of the same nature.

These corrections might be in the form of updates to your agency's security plan, targeted security awareness training, or modifications to processes and procedures or agency-specific policies.