



Security advice and responsibilities

What to know

 This summary sheet outlines key points from **GOVSEC-2: Security advice and responsibilities** – 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

We each have a role to play in ensuring the safety and protection of ourselves and the information and assets we work with. Tasmanian Government agencies are required to enhance this via roles that have specific responsibilities in line with the governance of the TAS-PSPF.

One of the ways that every agency must meet this requirement is by nominating an Agency Security Advisor (ASA). The ASA takes a leadership role to ensure ongoing compliance with the TAS-PSPF and its supporting policies.

Policy GOVSEC-2 sets out the ASA's role and responsibilities under the TAS-PSPF.

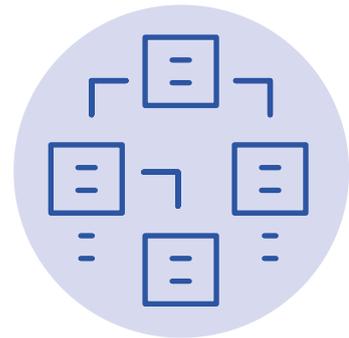
Create effective security procedures and systems

Creating and following protective security procedures and systems enhances your agency's resilience to compromise. Appropriate security policies and procedures that are easily understood and accessible to all agency people also support the achievement of security awareness outcomes.

This policy recommends that your nominated ASA develops security measures, policies and procedures as part of your agency's security and risk planning processes, and that the ASA updates these when significant changes occur in your agency's risk environment.

Induction and staff development programs provide an excellent opportunity to explain security measures, policies and procedures that are in place to support your agency's people in their work.

The value of effective security procedures is that they 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.



Identify and manage security risks

Identifying security risks is crucial to effective security risk management. Good security risk management not only supports your agency's resilience, it also helps to build a positive risk culture.

Knowing your agency's risks means you can make coordinated and informed decisions about managing those risks, as well as identify new opportunities and learn from mistakes. 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 your ASA to monitor and evaluate existing security measures and introduce new measures, where required, to reduce risk to an acceptable level.



Consider security requirements in all planning processes

Embedding a security culture and applying protective security principles in corporate planning processes enhances your agency's ability to meet business needs, provide a safe working environment, and improve relationships with clients and the community.

Including protective security in all plans and policies across your agency also ensures that the protection of information, people and assets from compromise is considered in every aspect of your agency's operations.

Respond to, investigate and report security incidents

Effective investigation processes make it possible to identify vulnerabilities in your agency and reduce the risk of security incidents in the future. Alongside these processes, it is also vital to have procedures in place to manage security incidents.

Incident management procedures should be consistent, appropriate and fair and be applicable to any security incident that may arise. It is the responsibility of your ASA to investigate broad security incidents and where necessary, escalate complex investigations to your agency's Responsible Executive (the person who oversees protective security arrangements in your agency).

When there is a report of a security incident, your ASA makes an initial assessment to:

- confirm it is a genuine security incident and not 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 (including by whom and when).

Sometimes a security incident must be reported to another agency or authority, depending on the nature and severity of the incident. Your ASA is responsible for reporting these incidents as necessary, and for ensuring your Responsible Executive is advised of the incident at the earliest opportunity. Guidance is available to agencies to help them manage this process.

