GOVSEC-5

Security planning

What to know

This summary sheet outlines key points from **GOVSEC-5: Security planning** – 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 all have a responsibility to be aware of our role in the protection of information, people and assets within our agency. To support this, Tasmanian Government agencies are required to develop a security plan to inform their people of necessary protective security practices and procedures relating to the agency and its threat environment.

Policy GOVSEC-5 sets out and explains the risk management processes your agency should follow to guide its protective security planning and the development of a security plan as required under the TAS PSPF.

Conduct a criticality assessment and a risk assessment

Applying risk management practices within your agency starts with identifying your agency's most critical assets – those that are essential to its ongoing operation and service delivery. Performing critical asset identification and understanding your agency's operational risk environment aids prioritised application of proportionate risk treatment strategies.

With this in mind, your agency's assets that are identified as being critical should have the greatest protections assigned to them, in priority order.

In support of your criticality assessment, identifying security risks is crucial to effective security risk management. Good security risk management enhances your agency's resilience and builds a positive risk culture.

Following analysis, security risks must be evaluated to work out if those risks are acceptable (tolerable, within existing controls) or unacceptable (intolerable, in need of additional treatments or prohibited).

Tasmanian Government

Determine risk tolerance

Your Accountable Authority is responsible for determining and managing your agency's security risks, which includes determining your agency's risk appetite and risk tolerance.

Risk appetite reflects an agency's attitude to risk, and how much risk the agency is willing to accept.

Risk tolerance is the level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk. It is an informed decision to accept risk.

Risk tolerance is often specified for relevant identified risks. These risks can be expressed as acceptable/tolerable or unacceptable/intolerable and are subject to measuring and monitoring. The risk tolerance for your agency can be affected by modifications in evaluation criteria and your appetite for risk.

Plan protective security measures and capture decisions

Your agency's security plan must outline the approach, responsibilities and resources that will be applied to manage protective security risks in line with the core and supplementary requirements of the TAS-PSPF. Your security plan enables the review of strategic and operational risks and the implementation of appropriate treatments to manage those risks to an acceptable level.

The security plan should take a risk-management approach to protective security and address threats, risks and vulnerabilities across all areas of security in your agency (security governance, information security, people security and physical security).

When risk treatments are applied, they should be balanced and proportionate to the identified risk rating. It is likely that not all treatments are possible or cost-effective, however, the most appropriate or effective treatments must be implemented.

This policy recommends treating your agency security plan as a 'living document' that can be adjusted as needed to address new or changing risks. If it does happen that the plan is adjusted, the TAS PSPF requires the documentation of any decisions which led to altering of the security plan, including justifications and alternative risk treatments that are implemented.