INFOSEC-3

Robust technology and information systems

What to know

This summary sheet outlines key points from **INFOSEC-3: Robust technology and information systems** – 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 are all responsible for ensuring Tasmanian Government information is protected from compromise and harm. This can be achieved by our agencies operating secure systems that safeguard data, information and privacy while also supporting the continuous delivery of government business.

Policy INFOSEC-3 sets out how your agency can build and maintain robust and validated technology, information, and infrastructure systems to manage access to information, particularly protected information, as required under the TAS-PSPF.

Apply Tasmanian Government cyber security principles

The Tasmanian Government's Cyber Security Policy is based on a number of cyber security principles and provides a consistent, risk-based approach to protecting Tasmanian Government information, systems and services from cyber security threats.

Considering and applying these principles (outlined in the table below) will be helpful as your agency works to safeguard its ICT systems from cyber security threats.

Awareness	Increased cyber security awareness enables staff at all levels to understand their responsibilities and identify and respond to cyber security risks.
Collaboration	Sharing cyber security knowledge across government improves cyber security capability and maturity.
Enablement	Cyber security is a key enabler for digital transformation.
Integration	Integrating cyber security into business risk management frameworks, policies and procedures improves planning for, and responses to, cyber security incidents.
Privacy and security	Integrating cyber security into all digital systems and services improves privacy and security for consumers of government services.
Risk	Adopting a risk-based approach allows the Tasmanian Government to adapt its cyber security risk management approach based on its risk tolerance.
Standards	Aligning with national and international industry and Tasmanian Government standards provides a consistent, systematic and repeatable approach enabling collaboration across government and the private sector. Applicable international standards are: • AS ISO/IEC 27001 for cyber security management requirements • AS/NZS ISO 31000 and AS/NZS ISO/IEC 27005 for risk management.

Tasmanian Government

Authorise ICT systems and include processes for audit trails and activity logging

Your agency is required to authorise its ICT system/s to a level appropriate to the highest assessed sensitive or security classified information and data it will process, store or communicate. To support ongoing protection, it is important that your agency understands the operating environment of its ICT system/s, as risks of compromise to a system or systems increase where the operating environment is complex.

Your agency is also obliged to protect any Tasmanian Government information and data which is processed, stored or communicated via outsourced managed service providers and/or cloud service providers. This can be achieved by applying the same authorisation process that is applied to internal systems.

Authorisation helps to instil confidence that your agency's ICT systems meet security requirements, address known security vulnerabilities, and remain secure.

Putting measures in place to monitor the accuracy and integrity of information and data captured or held will help you to respond to incidents and to detect unusual, unauthorised or malicious activity. These measures include audit trails and activity logging in applications.

For further information about authorisation, audit trails and activity logging, please refer to the policy.

Ensure ownership and accountability in ICT systems

All systems, including those managed by external providers, must have a business risk owner (system owner) to ensure ownership of, and accountability for, information security risk in ICT systems.

The system owner is responsible for ICT governance processes, ensuring secure operation and that business requirements are met. The owner may be the same for external systems utilised by your agency and for various (or all) internal systems.

System owners have an important role in the ongoing operation and monitoring of your agency's ICT system/s, as well as ongoing authorisation compliance. Activities in these areas may include vulnerability assessments and penetration tests, as well as making sure that any system modifications are made correctly, in line with the system's controls and risk environment.

System owners are also responsible for the development of documentation supporting the safe operation of your agency's ICT systems.