INFOSEC-1

Access to, and management of, official information

What to know

This summary sheet outlines key points from INFOSEC-1: Access to, and management of, official information – 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 ensure information produced and held by Tasmanian Government agencies is protected from compromise and harm. This requires controlled and considered access to, and management of, official information.

Policy INFOSEC-1 sets out how agencies can deliver efficient and effective services while protecting the confidentiality, integrity and availability of official information as required under the TAS PSPF.

Apply the 'need to know' principle

The information that Tasmanian Government agencies produce and hold is a valuable resource. Protecting the confidentiality, integrity and availability of this information is critical. When your agency's information security policies and procedures are well designed and implemented, you reduce the risks of your information being compromised.

Your agency must apply any whole-of-government information management policies and procedures to ensure consistency with commonly accepted industry standards and best practice. In the absence of these, you must work with the Tasmanian Government Chief Information Officer to develop your own agency specific policies.

Awareness of whole-of-government and agency-specific policies not only protects information from compromise and harm; it also strengthens your agency's security culture.

The 'need to know' principle is an important supportive element of information security policies. This principle is about people accessing information only when there is an operational requirement that they do so. It applies to all information, regardless of the classification of the information and the position or seniority of the person seeking access.

With careful management, applying the 'need to know' principle still allows for information to be shared between people or agencies where there is an operational benefit. Examples of good management strategies include applying access controls and auditing capability to all of your agency's information processes.

As well as developing policies and actions that reflect the 'need to know' principle, it is important that your agency supports everyone to become aware of the principle and understand why access to information is restricted.

Tasmanian Government

Require security clearances for certain information

While the 'need to know' principle applies to all information, more protection is needed when it comes to access to sensitive and security classified information or resources. Due to the potential harm associated with compromise of that information, your agency needs a high level of assurance as to a person's integrity. This can be achieved by requiring that every person with an ongoing need to access security-classified information has a valid security clearance to the appropriate level, as shown in the table below.

	Sensitive information		Security classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Security clearance required	Security clearance not required; pre-employment screening is sufficient	Security clearance not required; pre-employment screening is sufficient	Baseline security clearance or above	Negative Vetting 1 security clearance or above	Negative Vetting 2 security clearance or above

Manage access to information

Along with establishing policies that detail who can access what sort of information, your agency must also manage the access itself. To do this, your agency's general and ICT systems need to be well-structured and robust so that people have the right tools to access the information they need to do their jobs.

Some good access management strategies include:

- implementing formal user registration and deregistration procedures for granting and cancelling access to information systems
- establishing processes to uniquely identify and authenticate people each time they seek access
- adopting strong authorisation processes to control access to your agency's ICT systems, networks (including remote access), infrastructure and applications.