




Protecting official information

What to know

 This summary sheet outlines key points from INFOSEC-2: Protecting 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

To protect Tasmanian Government information, we need to first understand our responsibilities and how to classify, mark, transfer, handle, and store information according to its value, importance, and sensitivity.

Policy INFOSEC-2 sets out how your agency can assess the value and business impact of information and apply security protections as required under the TAS PSPF.

Be aware of information protection practices

The Accountable Authority (the person/people with control over a Tasmanian Government public authority) is responsible for ensuring the people within their agency are aware of information protection practices. This includes secure handling and sharing of information, along with maintenance of privacy as required under Tasmanian law.



Demonstrating good security awareness and practices when using sensitive and security-classified information can include:

- remaining vigilant and aware of the environment
- selecting work environments based on their suitability to use the required information
- taking all necessary steps to reduce the risk of unauthorised access, use or removal of information
- appropriate physical handling procedures when information is being carried or is not in active use.

Classify official information

Good management of information enables your agency to continually meet business, government and community needs and expectations. It is important to balance the need to protect information with the need to ensure appropriate access.

Classifying information enables your agency to protect information in a consistent, organised and appropriate way. The information below sets out the approved security classifications for use across all Tasmanian Government agencies.



PROTECTED	This classification indicates compromise of the confidentiality of the information could be expected to cause damage to Tasmania's or the national interest, organisations, or individuals.
SECRET	This classification indicates compromise of the confidentiality of the information could be expected to cause serious damage to Tasmania's or the national interest, organisations, or individuals.
TOP SECRET	This classification indicates compromise of the confidentiality of the information could be expected to cause exceptionally grave damage to Tasmania's or the national interest, organisations, or individuals.

Where compromise of the information's confidentiality would cause limited damage and does not warrant one of the above security classifications, that information is considered sensitive and is treated as OFFICIAL: Sensitive. All other information from your agency's business operations and services requires a routine level of protection and is treated as OFFICIAL.

Sometimes a document has information in it that varies in classification. If this is the case, the document as a whole must be classified at the same level of protection as the information in it that has the highest security classification.

To protect information at the earliest opportunity, your agency must classify information when it is first created or received from sources outside the Tasmanian Government.

The classification must be set at the lowest reasonable level to enable information to be accessed by the highest number of people with an identified 'need to know'. This requirement also helps to reduce over-classification of official information.

The originator (refer to the policy for further information) must clearly identify sensitive and security classified information by using the applicable protective markings.

This policy (INFOSEC-2) does not recognise agency-specific and other protective markings.

A standard set of markings ensures common understanding, consistency and interoperability across systems and government agencies. Creation of markings outside this policy may cause confusion about appropriate handling protections and increase the chance of compromise.

Text-based protective markings are the preferred method to identify sensitive or security-classified information and additional handling requirements

Correctly store and dispose of information

Your agency must store sensitive and security-classified information securely and preserve it in an environment which prevents unauthorised access, duplication, alteration, removal or destruction. This also applies to mobile devices containing sensitive and security-classified information. An example of a simple way to do this is to implement desk, session and screen locking procedures. These measures provide protection from compromise or harm to unattended information or resources.

When protections are no longer required due to changes in the sensitivity or security classification of information, they should be removed.

Creating information doesn't mean that it lasts forever; it depends on the nature of the information and what it is used for. Once information no longer has a business need or value, your agency may not need to keep it. When this happens, the information must be archived, destroyed, repurposed or disposed of in a secure manner.

Tasmanian laws allow for the disposal and destruction of state records when particular requirements are met. Guidance is available to agencies to help them manage this process.

Your agency may use commercial destruction services to destroy classified information, being careful to review the appropriateness of a commercial provider's collection process, transport, facility, procedures and approved equipment when considering engaging their destruction services. Guidance about this is also available to agencies.

