Tasmanian Government

Information Management Framework

Information Security Classification Standard

Chief Information Officer

< contact email >

< website URL >

State Archivist

< contact email >

< website URL >

This document is a consultation draft. Once finalised, we will format and apply design elements.

This Standard supports the Tasmanian Government Cybersecurity Policy (2018).

This Standard replaces the Tasmanian Government Information Security Policy (2011).

This is a living document and we will make minor changes as needed. If you notice anything that needs updating, please let us know.

Chief Information Officer and the State Archivist. 2020. Information Security Classification Standard.

Document Development History

Version	Date	Comments
A	4/06/2020	First draft circulated to Digital Strategy and Services, Office of the State Archivist
B	29/07/2020	Exposure draft released

Contents

<Insert table of contents>

Purpose

This Standard describes information security classification requirements to manage risks to official information and to protect government information assets through their life cycle.

Context

This Standard is part of the Tasmanian Government Information Management Framework. The Framework is intended to be a coherent set of information management policies, standards and implementation guidance for Tasmanian public sector bodies. This document describes information security classification labels, processes and controls as part of the Framework.

Benefits

Consistent classification of information helps Tasmanian Government organisations deliver better services for Tasmanians.

Benefits:

- reduced business risks
- make informed and timely decisions to deliver better public services
- operate accountably, effectively and legally
- protect the reputation of your organisation and the government
- support interoperability
- protect government information from cyber-attacks,

Scope

This Standard applies to all Tasmanian Government organisations, as listed in Schedule 1 of the *State Service Act* 2000.

Other organisations may choose to adopt this Standard as good practice.

Implementation

We recommend that you apply a risk-based approach when implementing this Standard. In practice, this means that resource and effort should be directed to high-value, high-risk information. You should follow your organisational risk management processes.

1. Policies and procedures

Develop, implement and maintain authorised information security classification policies and procedures.

Monitor and evaluate policies, systems, procedures and processes, modifying as needed.

2. Responsibilities

Ensure overall information security classification responsibilities are assigned to a senior executive in your organisation.

Assign, document and communicate information security classification responsibilities to appropriate staff, and board members, elected representatives, volunteers and contractors where appropriate. Ensure staff with particular responsibilities, such as senior executives, are aware of their responsibilities.

Your organisation may have outsourced services, activities and/or functions where information security classification should be applied. Ensure this is communicated to relevant staff in your organisation and in the outsourced organisation/s, and clearly documented in outsourcing contracts or agreements.

3. Capability

Provide awareness, tools, training and professional development for managers, information and records professionals and staff to help them meet their responsibilities.

Where appropriate, extend training to board members, elected representatives, volunteers and contractors.

4. Classification labels

Classification Label	Explanation
National Security Information Refer to the Australian Government Protective Security Policy Framework (PSPF)	This Standard does not deal with National Security Information (NSI) that is assessed and classified above Protected level. Follow Australian Government processes described in the Protective Security Policy Framework (PSPF) to support interoperability.
Protected	Protected information requires careful safeguards as compromise or loss could cause serious damage to the State, the Government, commercial entities or members of the public. Protected information must be labelled.
Sensitive	Sensitive information requires additional protection and handling because of its higher confidentiality requirements. Labelling Sensitive information supports good information management practice and reduces the risk of mishandling. You may wish to use additional labelling for internal purposes, for example, Sensitive (Commercial), Sensitive (Legal) or Sensitive (Personal).
Official	Information generated, received, developed or collected by, or for a Tasmanian Government organisation for an official purpose or to support official activities. Official information is day-to-day or routine information. Official information has low confidentiality requirements. Protection and handling of Official information requires security processes and controls aligned with 'business as usual' operating environments. Labelling Official information may be helpful when sharing with other organisations to indicate handling requirements. Using the Creative Commons Licence on Official information indicates the information is Public.
Unofficial	Unofficial information is not related to Tasmanian Government activities. For example, a personal email. Labelling information 'Unofficial' is optional.

Protected

Protected information requires careful safeguards as compromise or loss could cause serious damage to the State, the Government, commercial entities or members of the public. Examples: Cabinet information, Police-specific information.

Labels or markers

Protected information must be labelled 'Protected'

Storage, handling and disposal

Store and handle Protected information based on assessed risk to the information owner.

Consider implementing the controls outlined for Protected information in the current Information Security Manual published by the Australian Signals Directorate.

Dispose according to authorised retention and disposal schedules issued under the *Archives Act 1983* (Tas).

Destroy according to requirements in the Information Management Framework.

Sensitive

Sensitive information requires additional protection and handling because of its higher confidentiality requirements.

Examples of sensitive information may include:

- government or agency business that might affect the government's capacity to make decisions or operate, public confidence in government, the stability of the marketplace and so on
- commercial interests, whose compromise could significantly affect the competitive process by providing unfair advantage
- legal professional privilege
- law enforcement operations whose compromise could adversely affect crime prevention strategies, particular investigations or adversely affect personal safety
- personal information, which is required to be safeguarded under the *Personal Information Protection Act 2004* (Tas), or other legislation.

Labels or markers

Labelling Sensitive information supports good information management practice and reduces the risk of mishandling. You may wish to use additional labelling for internal purposes, for example, Sensitive (Commercial), Sensitive (Legal) or Sensitive (Personal).

Storage, handling and disposal

Store and handle Sensitive information based on assessed risk to the information owner.

Dispose according to authorised retention and disposal schedules issued under the *Archives Act 1983* (Tas).Destroy according to requirements in the Information Management Framework.

Official

Information generated, received, developed or collected by, or for a Tasmanian Government organisation for an official purpose or to support official activities.

Official information is day-to-day or routine information. Official information has low confidentiality requirements. Protection and handling of Official information requires security processes and controls aligned with 'business as usual' operating environments.

Labels or markers

Labelling Official information may be helpful when sharing with other organisations to indicate handling requirements.

Using the Creative Commons Licence on Official information indicates the information is Public.

Storage, handling and disposal

Store and handle Official information based on assessed risk to the information owner.

Dispose according to authorised retention and disposal schedules issued under the *Archives Act 1983* (Tas).

Destroy according to requirements in the Information Management Framework.

Unofficial

Unofficial information is not related to Tasmanian Government activities. For example, a personal email, or unsolicited advertising.

Labels or markers

Labelling information 'Unofficial' is optional.

Storage, handling and disposal

Unofficial information should not be stored for long periods in Tasmanian Government information systems.

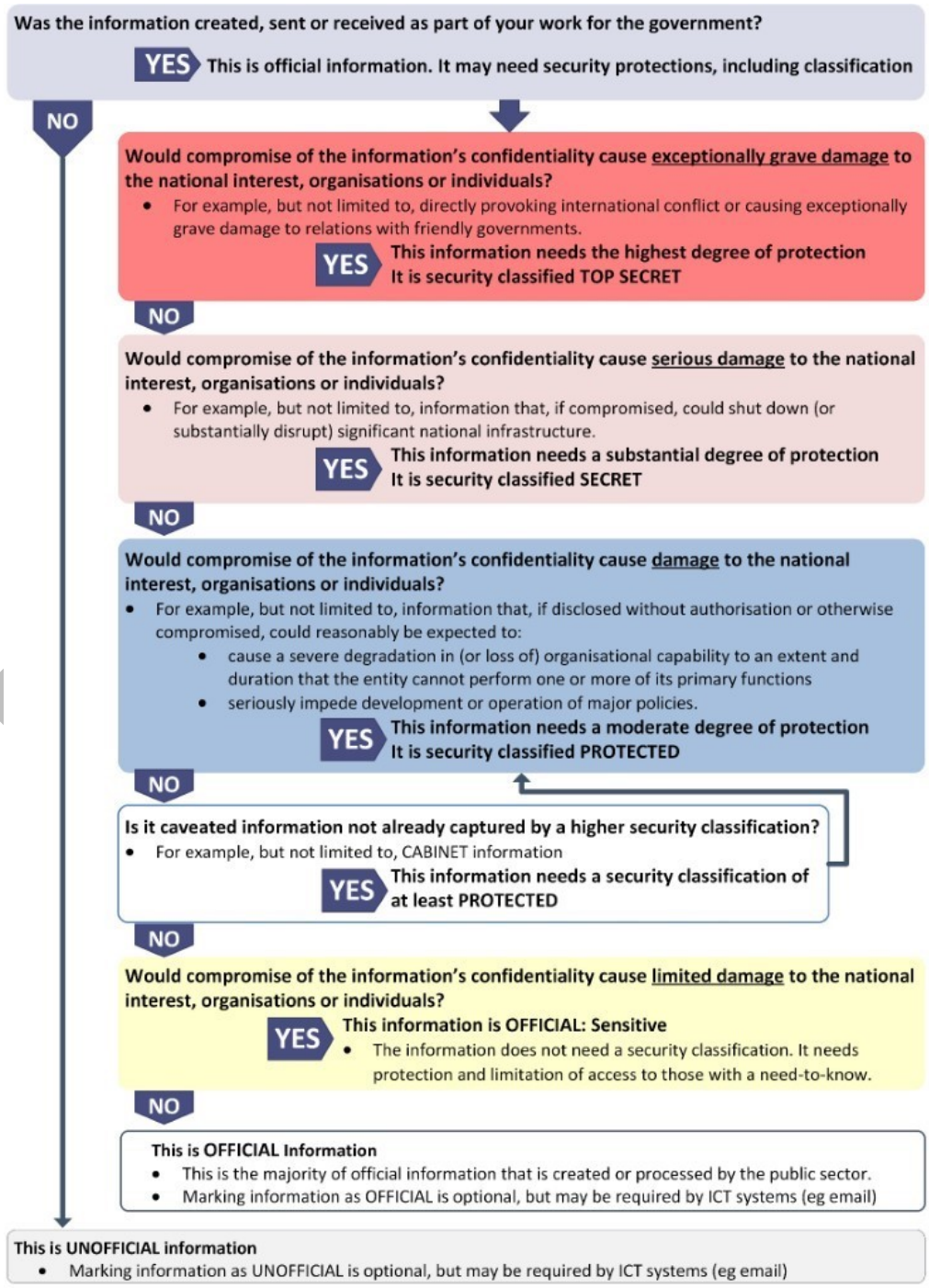
5. Implementation approach

This Standard does not mandate specific processes and controls. You should implement information security classification according to your organisational risk management processes.

Classifying and labelling information

Use the Flowchart below to determine classification label.

[EXAMPLE ONLY]



Protecting information

Choose controls and safeguards that protect the information against confidentiality risks based on the Classification label.

[EXAMPLE ONLY]

Classification Label	Confidentiality Risks	Example Security Controls
National Security Information – refer to Commonwealth PSPF	Very High	• Use the PROTECTED controls outlined in the current Australian Government Information security manual
Protected	High	• Consider the PROTECTED controls outlined in the current Australian Government Information security manual
Sensitive	Medium	• Employment Screening • Additional user permissions required • Audit logging • Store in locked cabinets
Official	Low	• State Service Code of Conduct • Password protected • Store in approved recordkeeping systems

NOTE: This table is an example only. Risk levels should be informed by your agency's risk management framework.

Handling information

To share information safely, information custodians should store and handle information using controls and safeguards agreed to by the information owner.

Definitions

Classification label

Protective markings applied to indicate the value of the information and the minimum level of protection that is required.

Confidentiality (of information)

Limiting access to official information to authorised users for approved purposes. Determine confidentiality requirements based on likely consequences of unauthorised disclosure of official information.

Disposal (includes transferring information to Archives or destroying information)

A range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of records in or from recordkeeping systems. They may also include the migration or transmission of records between recordkeeping systems, and the transfer of custody or ownership of records. (from OSA)

An action concerning the fate of records. Includes destroying, transferring, selling, donating, damaging, abandoning, or the unauthorised amending of records in accordance with an authorised retention and disposal schedule. (from QLD QGCIO)

Information (and Personal information)

A collection of data in any form that is maintained by an agency, or person and which may be transmitted, manipulated, and stored. Records are the subset of information that constitutes evidence of activities. (from OSA)

Personal information

Any information or opinion in any recorded format about an individual whose identity is apparent or is reasonably ascertainable from the information or opinion; and who is alive or has not been dead for more than 25 years; (PIP Act Tas)

Security Controls

Hardware, procedures, policies and physical safeguards that are put into place to assure the integrity and protection of information and the means of processing and accessing it. (from QLD QGCIO)

More definitions can be found in the Tasmanian Cybersecurity Policy

Acknowledgements

Further information

Protective Security Policy Framework: Information: Sensitive and security classified information <insert link>

Information Security Manual, Australian Signals Directorate <insert link>

Appendix 1. Mapping Tasmanian classifications to Australian Government classifications