TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 33 Implementing Information Security Classification - Part 1: Overview

Introduction

This Advice outlines issues to consider when implementing the Tasmanian Government Information Security Classification Framework. It is intended for use by information management professionals within Agencies to assist them in establishing effective security classification practices.

About this Advice

This Advice presents a common approach to security classification, and guidance for Agencies on its use. It is intended for use by information management professionals within agencies to assist them in establishing effective security classification practices.

- **Part 1** provides an overview
- **Part 2** outlines the process for security classification
- **Part 3** identifies a range of practices that are needed to implement the policy. These practices relate to labelling, storing, and transmitting information assets that have been classified, as well as practices related to ensuring appropriate access to information, and protecting the integrity of information.
- **Part 4** presents a model accountability framework for information security.

Purpose

This Information Security Classification advice has been developed by TAHO to assist agencies in establishing effective security classification practices. The objectives of the guideline are to:

- ensure personal information and confidential information are protected from unauthorized use and disclosure;
- protect the intellectual property of the Government of Tasmania;
- facilitate the identification of information to support routine disclosure and active dissemination of information;
- facilitate the sharing of information with other jurisdictions to support e-government and integrated service delivery; and
- ensure information shared between the Federal Government and Tasmanian Government Agencies is adequately protected.

What is the Information Security Classification?

The Tasmanian Government Information Security Procedure for Information Security Classification sets the minimum requirements for information asset security classification. It also provides a standard process to allow agencies to evaluate their information assets and determine the appropriate level of security classification that must be applied, addressing the need for a consistent approach to dealing with the sensitivity and confidentiality of information assets across the Tasmanian Government.

By providing a standard approach to information asset security classification, the policy facilitates improved interoperability and consistency within Tasmanian Government agencies. The implementation of electronic service delivery has accelerated the need for a consistent approach to security classification, particularly as agencies seek to integrate services and information.

Why security classification is important

There are several reasons why agencies should be concerned about information security classification. These include:

- **Protection of personal information**. The Personal Information Protection (PIP) Act governs the collection, use and disclosure of personal information. It also governs the management of personal information – its protection, retention, and accuracy. Security standards support the effective application of the Act in the conduct of day-to-day business.
- **Protecting confidential information from unauthorized access**. In the normal business of government, certain information must remain confidential. Examples of such information include the annual Budget, human resources files, case management files, Cabinet documents and investigation files in many agencies. Applying proper security classification and practices can safeguard against unauthorized access to confidential government information.
- **Supporting routine disclosure and active dissemination**. Security classification of information assets is a critical component in identifying and facilitating the disclosure of information to the public. It can also help identify information that needs to be protected, but might be combined with unrestricted information.
- **Facilitating intergovernmental cooperation and integrated service delivery**. More and more work of the government is carried out in partnership with other service providers and other levels of government. Moreover, secure information sharing and access is needed in an electronic service delivery (ESD) and electronic business (E-business) environment. When information is shared with individuals outside the agency who are not aware of the value or sensitivity of an information asset, it becomes essential that the sensitivity level be established so that information requirements can be quickly understood, communicated and acted upon.
- **Protecting information that supports public security and law enforcement**. Many agencies routinely receive information from the Federal Government related to public safety and law enforcement. This information must be adequately protected to ensure continued sharing of this information.

Definitions

'the Framework' – refers to The Tasmanian Government Information Security Framework

'the Manual' – refers to the Tasmanian Government Information Security Policy Manual

'ISC" – refers to Information Security Classification

Further Advice

For more detailed advice please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

This document is largely based on:

- Queensland Government Information Security Classification Framework, ICT Policy and Coordination Office, Department of Public Works
- Information Security Classification Government of Alberta

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	March 2015	Christine Woods	Template	All
1.0	March 2014	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template

Issued: March 2014

Ross Latham
State Archivist