Information Management Advice 33 Implementing Information Security Classification

Part 4: Establishing Accountability for Classification

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. A clear accountability regime for all personnel will be important to ensure the protection of government information assets.

Part 4 of this Advice presents an accountability framework for information security classification within agencies. More detailed advice on establishing Information Security Governance is outlined in Advice 35: Implementing Information Security - Part 3: Information Security Governance, and Advice 40: The Role of an Information Asset Owner.

Deputy Secretary

Deputy Secretaries are responsible for government records generally. Specifically, the Deputy Secretary is responsible for:

- defining, documenting and implementing reasonable measures to prevent unauthorized access to and the inadvertent release, destruction or damage of government records; and
- safeguarding records in their custody or under their control, including records which are in the custody of third parties under alternate service delivery arrangements.

Agency Chief Information Officer

The agency's Chief Information Officer is responsible for establishing the agency's security policy and standards for electronic information and information technology assets. The agency's Chief Information Officer is responsible for:

- reviewing, understanding and applying the information security classification standard to electronic information and information technology assets;
- liaising with the agency's Senior Records Officer and information management program on the application of the security classification to recorded information in other media;

- developing agency security policies and standards that are consistent with the corporate Security Policy;
- recording all security breaches and violations discovered by the agency;
- managing the response and actions taken within their agency to breaches, violations, audits, investigations and security reviews;
- reporting these security breaches and violations along with actions taken to the Security Officer and other appropriate personnel;
- ensuring that implementation of the security classification system is appropriately coordinated agency-wide;
- guiding and assisting program managers in the assessment of their information security needs and information security classification;
- assisting staff in the identification, design and implementation of reasonable security measures;
- assisting program managers in determining if the security measures in place meet their program needs; and
- providing guidance and assistance to employees in implementing this standard.

Managers

Managers are responsible for:

- reviewing, understanding and ensuring applicable legislation, policies and guidelines relating to the security of information are followed in their program area;
- developing and maintaining internal procedures that support the requirements for the effective handling and security of information;
- ensuring that information under their control is classified appropriately;
- ensuring that all information resources under their immediate control have appropriate retention periods to meet their business needs, and the legal retention and disposition schedule is understood and applied by staff;
- ensuring that information under their custody or control is protected from physical damage and from unauthorized access, alteration, removal or destruction;
- ensuring that staff are aware of, trained in, and understand legislation, applicable directives and procedures relating to the security classification of government information assets; and
- reporting all actual and suspected security breaches and violations to the agency Chief Information Officer.

Right to Information /Personal Information Protection Coordinator

The Coordinator is responsible for:

- reviewing records to determine whether any exemptions or exclusions apply when requests are received under Right to Information or the Personal Information Protection Acts, for records that have a security classification. Note The application of a security classification to a record does not determine whether a record is exempt from access under RTI; and
- taking required action related to privacy breaches.

Records Manager

The agency's Records Manager is responsible for:

- reviewing, understanding and applying the information security classification standard to physical records in the custody or under the control of the agency;
- assisting the agency's CIO in implementing security classification for electronic information and supporting program managers and staff in applying security classifications to information holdings in a consistent manner;
- recording all security breaches and violations discovered by the agency;
- managing the response and actions taken within their agency to breaches, violations, audits, investigations and security reviews;
- reporting these security breaches and violations along with actions taken to the Corporate Chief Security Officer and other appropriate personnel;
- guiding and assisting program managers in the assessment of their information security needs and information security classification;
- assisting staff in the identification, design and implementation of reasonable security measures;
- assisting program managers in determining if the security measures in place meet their program needs;
- providing guidance and assistance to employees in implementing this standard;
- providing secure locked storage facilities for protected, confidential and restricted information holdings; and
- ensuring records retention and disposition schedules are created for all information holdings under the custody and control of the agency.

All agency staff and staff of corporate partners and contractors

All agency staff, and staff of corporate partners and contractors, are responsible for:

- reviewing, understanding and applying the information security classification standard to information assets they create, receive, use, transmit, or store;
- meeting their obligations under the *Right to Information Act 2009* and *Personal Information Protection Act 2004*, to protect any information under their control or custody from unauthorized disclosure to any person or organization;
- ensuring that information under their custody or control is protected from physical damage and from unauthorized access, alteration, removal or destruction according to the security and access standard; and
- reporting all actual and suspected security and privacy breaches and violations to their Manager.

Security classification roles – owner and user/editor

This section provides additional guidance on information security classification roles. It should be read in conjunction with *Advice 40 The Role of an Information Asset Owner*.

Information owner

The information owner is the recognised officer who is identified as having the authority and accountability under legislation, regulation or policy for one or more information assets. Information owners define the policy which governs the information assets of an agency, including determining the security classification of information assets.

In order to ensure due attention is able to be applied to this role, it is standard practice for CEOs to further delegate the responsibilities and authority of their role as information owner to another senior staff member, or members. When this occurs, it is important that the scope of delegated responsibilities should be clear and formally documented so that accountability and audit requirements are able to be met, and confusion as to who is the appropriate delegated information owner is avoided [1] Information ownership should generally be assigned as part of a role, rather than being personally assigned to a particular individual. In this way, the responsibility is continued when individuals move roles.

Where information ownership is to be delegated to more than one individual, it is advisable that individuals have clear domain responsibilities. For example, the Director of Human Resources may be assigned as information owner for all human resource related information assets. If at any time an information asset is not able to be clearly assigned to a delegated information owner, the CEO will be required to make the security classification determination.

The security classification responsibilities of an information owner include:

- ensuring agency policy and procedures are in place to support security classification of information assets
- setting and ratifying any security classifications for information assets or domains of information assets [2]
- conducting an annual review of security classified information assets
- ensuring information asset security domain classifications are reviewed at least annually, or when changes have occurred to the internal controls used to protect the information assets
- ensuring that Service Level Agreements or Operating Level Agreements between agencies, and/or private entities managing agency information assets, include appropriate service levels and targets relating to information being accurately security classified and managed in accordance with the controls described in this framework and/or other relevant agency policy
- providing resources to support agency security classification and control requirements
- approving classifications or re-classifications of information assets as recommended by custodians [3]

[1] Within this Advice, references to 'information owner' can be read as including 'delegated information owner'
[2] Domain classifications cover a group of similar information – for example, HR information may default to being classified as 'in-confidence'. If domain classifications are used, they should be approved by the owner.

Information Asset Custodian

Information asset custodians are responsible for implementing and maintaining information assets according to the rules set by the owner to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility, including the application of information security classifications and controls.

In some cases, the custodian will be required to make an initial information security classification recommendation for an information asset. However, the information owner retains the approval responsibility for classifying the information.

[3] Information assets that are classified as PUBLIC, X-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED incur substantial management and control costs. Their classification should be ratified by the owner to ensure resources and support is available to manage the assets appropriately and minimise the risk of inappropriate exposure.

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

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

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