TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 33 Implementing Information Security Classification

Part 3: Implementing Security Classification Controls

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.

Implementing information security classification will mean that agencies will need to consider and implement appropriate practices related to:

- labelling information;
- storing information;
- transmitting information;
- disposing of unneeded information;
- protecting the integrity of information;
- allowing appropriate access and disclosure; and
- establishing accountability.

This Part provides examples of practices to be considered in each of these areas. The practices identified are not intended to be prescriptive. Rather, they are identified here as a guide to agencies.

It is unlikely that agencies will implement security classification to all information assets at the same time. Rather, the timing of applying information security classification will be based on the result of a risk assessment.

The actual practices that are implemented will depend on the business reason for applying security classification as well as established administrative protocols (in the case of print information assets) and information technology protocols (in the case of electronic information assets).

NOTE: Information that has been classified in the national interest by the Australian Government will require specific practices related to labelling, storing, transmission and use.

Department of Education
LINC Tasmania

Tasmania
Explore the possibilities

Labelling information assets

The actual labelling procedure will vary depending on the medium in which the information is stored. Table 1 identifies some common labelling methods for various types of information assets.

Table 1 Sample Labelling Methods

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level may be needed to mark hardcopy documents received from outside the organization.
Electronic mail	Identify security classification in subject line of e-mail, if classified as confidential, or restricted.
Electronic documents	Identify security classification in document metadata. If the electronic document is to be printed or viewed in .pdf format, the security classification should appear on every page, including the cover page (this can be done by including the classification in the header/footer or by use of a watermark which is automatically applied by the EDRMS when the document is printed or viewed). Information about the ministry or department which created the document and date of creation should be included.
Data, databases and business applications	Identify classification in system/application metadata. Security labels may be required for online screen displays and reports generated by IT systems.
Other media	The security classification may be identified on adhesive labels applied to other media such as CDs, DVDs, and tapes. A message with the classification label should be displayed when the information stored on the media is accessed.

Storing Information

Depending on the security classification, information assets will need different types of storage procedures to ensure that the confidentiality, integrity, accessibility, and value of the information are protected.   Table 2 identifies storage procedures for printed and electronic information in the various classification categories.

Table 2 Sample Storage Procedures Classification

Classification	Print/Hard Media	Electronic Files
PUBLIC	No specific requirements.	Electronic Preparation/storage in disk drive, web content management system, or document and records management system with restricted access is desirable. Electronic publication: web content management system, electronic register or equivalent with access restricted to authorised personnel is essential. Audit logging: logging access to electronic publication systems is essential, ie login, logout, failed login attempt, modify, create and delete.

Classification	Print/Hard Media	Electronic Files
UNCLASSIFIED	May be stored in unsecured cabinet in a room for authorised personnel	Access by authorised personnel only. Regular back-ups to ensure availability and integrity
X–IN-CONFIDENCE	Secure location with restricted access in a lockable cabinet or room when unattended. See Section 3.3.3 of the manual – Physical Environment. Agencies may implement Clean desk policy – see below	Restrict logical access based on need to know. (e.g., authorized access and authenticated access)
PROTECTED	In a lockable container in a secure or partially secure environment when unattended. See Section 3.3.3 of the manual – Physical Environment	Restrict logical access based on need to know. (e.g., authorized access and authenticated access)
HIGHLY PROTECTED	In a lockable container in a secure area when unattended. See Section 3.3.3 of the manual – Physical Environment Agencies may also consider: Clean desk policy Audit trail for all access points (e.g., signatures)	Restrict logical access based on need to know (e.g., single or double authentication, encrypted data, audit and monitoring)

Clean Desk Policy

Some agencies may implement a clean desk policy. A clean desk policy directs all your agency employees to clear their desks at the end of each work day. This not only includes documents and notes, but also post-its, businesses cards, and removable media (CDs, floppy disks, memory sticks).

Following a clear desk policy will help your agency reduce the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible in plain view.

A clean desk policy and a clear screen policy, that is always locking your screen when not at your workstation work hand-in-hand to safeguard your organization's information.

Transmitting information

When transmitting information that is protected, confidential or restricted, special procedures will be needed. Examples of these procedures are identified in Table 3.

Table 3 Sample Transmission Procedures Classification

Classification	Print/Hard Media	Electronic Files
PUBLIC	Within the Tasmanian Government: no specific requirements Outside the Tasmanian Government: no specific requirements Receipting: no specific requirements	Data transmission: may be passed unencrypted over Tasmanian Government or public networks. Portable media/devices: no specific requirements. Email, instant message: no specific requirements. Fax: no specific requirements. Receipting: optional.
UNCLASSIFIED	Within the Tasmanian Government: uncovered by hand or by internal mail in a use-again envelope. Outside the Tasmanian Government: Passed by external mail in an opaque envelope. Receipting: no specific requirements.	Data transmission: may be passed unencrypted over Tasmanian Government or public networks. Portable media/devices: password-protected, eg USB drive, CD ROM, smart phone. Email, instant message: no specific requirements. Fax: no specific requirements. Receipting: optional.
X–IN-CONFIDENCE	Within the Tasmanian Government: single opaque envelope indicating classification. Uncovered by hand in discrete office environment. Outside the Tasmanian Government: single opaque envelope that does not indicate classification. Receipting: at discretion of information owner/custodian.	Data transmission: may be passed unencrypted over Tasmanian Government or public networks. Portable media/devices: password-protected eg USB drive, CD ROM, smart phone. Email, instant message: no specific requirements. Fax: someone to attend the receiving facsimile to receive the material. Encryption desirable. Receipting: at discretion of information owner/custodian
PROTECTED	Within the Tasmanian Government: single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. To remain in personal custody during transmission. Outside the Tasmanian Government: double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); inner envelope is to be sealed with an Australian Government Security Construction and Equipment Committee-endorsed tamper-proof seal. To remain in personal custody during transmission. Receipting: required.	Data transmission: to be encrypted over public networks. Encryption is desirable over Tasmanian Government networks. End-to-end encryption is desirable, eg PC to PC. Portable media/devices: to be encrypted, eg USB drive, CD ROM, smart phone. Email, instant message: information to be a separate and encrypted attachment. Fax: someone to attend the receiving facsimile to receive the material. Encryption required. Receipting: required See Section 3.3.4 – Information and Communications Technology in the Manual.

Classification	Print/Hard Media	Electronic Files
HIGHLY PROTECTED	Within the Tasmanian Government: single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. To remain in personal custody during transmission. Outside the Tasmanian Government: double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); inner envelope is to be sealed with an Australian Government Security Construction and Equipment Committee endorsed tamper-proof seal. To remain in personal custody during transmission. Receipting: required	Data transmission: to be encrypted over public and Tasmanian Government networks. End-to-end encryption is desirable, e.g. PC to PC. Portable media/devices: to be encrypted e.g. USB drive, CD ROM, smart phone. Email, instant message: the last resort for distribution unless the information is a separate and encrypted attachment. Fax: someone to attend the receiving facsimile to receive the material. Encryption required. Receipting: required See Section 3.3.4 – Information and Communications Technology. Section of the Manual

Protecting the integrity of information

Integrity refers to the fact that information is current, complete, and only authorized changes are made to it. The integrity of information processed by and stored in information systems can be addressed by assigning the appropriate rights (e.g. read only, modify). If the threat to the integrity of information is significant, electronic files should be saved as read only files with changes to be made only by the author (this may be handled by access rights based on user account, work group or physical access to a specific device). In these cases, procedures should be in place for transfer of rights when the author leaves the organization. In some cases, stronger control such as encryption may be required.

Allowing appropriate access and disclosure

Certain types of information will require controlled access and logs to track access and disclosure activities. The following table outlines the access restrictions and any special audit trail that should be maintained.

Table 4 Allowing Appropriate Access and Disclosure

Classification	Access Restrictions	Audit/Activity Files
PUBLIC	Official information needs to be specifically classified as PUBLIC before it is released into the public domain.	None

Classification	Access Restrictions	Audit/Activity Files
UNCLASSIFIED	UNCLASSIFIED information may need to be protected and controlled and is not to be considered PUBLIC information. As a minimum, UNCLASSIFIED information requires only minimal confidence in the identity of the individual accessing the information (Access Assurance Level 1). Available to and all employees, contractors, sub-contractors and agents on a need to know basis.	Periodic audits to show protection is in fact occurring
X-IN-CONFIDENCE	Limited to individuals in a specific function, group or role with X-IN-CONFIDENCE access. Examples include: STAFF-IN-CONFIDENCE: includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personnel files, recruitment information, grievance or disciplinary records. EXECUTIVE-IN-CONFIDENCE: information associated with executive management of the entity that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial reports, strategic plans, government matters, staff matters etc. COMMERCIAL-IN-CONFIDENCE: procurement or other commercial information such as sensitive intellectual property. For example, draft requests for offer information, tender responses, tender evaluation records, designs and government research.	Pre-clearance based on position or contractor, sub-contractor or agent relationship. Log of access/actions. Periodic audits of adequate protection Includes documented breaches & demonstrated risk mitigation activities implemented as a result. Also includes the maintenance of a security matrix demonstrating access rights within systems.
PROTECTED	Authorized access (employees, contractors, sub-contractors and agents) on a "need-to-know" basis for business related purposes Generally, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED. Includes Cabinet submissions and decisions to be marked CABINET-IN-CONFIDENCE	Periodic audits to show protection is, in fact, occurring includes documented breaches & demonstrated risk mitigation activities implemented as a result. Also includes the maintenance of a security matrix demonstrating access rights within systems.

Classification	**Access Restrictions**	**Audit/Activity Files**
HIGHLY PROTECTED	Limited to named individuals (positions)	All access or actions will be logged and subject to non-repudiation processes as appropriate. Includes documented breaches & demonstrated risk mitigation activities implemented as a result. Also includes the maintenance of a security matrix demonstrating access rights within systems.

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 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