TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 34 Implementing Information Security Classification in EDRMS

Introduction

This Advice outlines issues to consider when implementing the Tasmanian Government Information Security Classification markings in Recordkeeping Systems. State records stored in an EDRMS usually have their access described by three attributes: security classification, caveats and access control. This advice describes these attributes and ways to configure EDRMS to manage security..

What is the Information Security Classification Framework?

The Tasmanian Government Information Security Classification Policy sets out guidelines for the appropriate security classification of information assets in agencies. It states that agencies must ensure that:

- the classification of all information is in accordance with Tasmanian Government Information Security Classification Policy - Section 3.3; and
- the control of all security classified information (including handling, storage, transmission, transportation and disposal) is in accordance with Tasmanian Government Information Security Classification Policy – Section 4.3.

Information Security in Context

It is important when trying to implement information security as applied by an EDRMS, to understand the context in which it sits.

The first step in managing information security in an agency is to understand what information assets are. An information asset is information that has value to the organisation. See *Advice 39 Developing an Information Asset Register*.

The information security policy asks agencies to manage their information assets by an agency information security approach that seeks to protect:

- Availability, by ensuring access to information, systems, networks and applications by authorised users.
- Integrity, by ensuring the accuracy and completeness of information is protected
- Confidentiality, by ensuring that information is only access by authorised individuals
- Proportionality, ensuring measures to protect information are relative to the risk of loss or failure of availability, integrity and confidentiality

A variety of methods including physical security, password protection, intrusion detection and prevention, security classification labelling, encryption, security shredding and information security awareness to protect information assets is a part of the implementation of information security policy and developing an information security framework for the Agency.

Recordkeeping practices utilising the functionality of an EDRMS significantly support the implementation of information security in an agency. EDRMS create an auditable security trail throughout the life of the record enabling breaches of security to be managed at their source.

Security and Access in EDRMS

State Records managed in an EDRMS have their access described by three attributes, Security Classification, caveats and access control.

Security Classification

Most electronic document and records management systems (EDRMS) and records management software contain provisions to identify the security classification of a record. The Policy provides a standardised set of information security classifications and treatments to ensure consistency across government agencies.

An information security classification may be applied at the file level or document level. When classifying with physical records, the security classification is normally applied to a file and all documents in the file 'inherit' this classification. In an EDRMS, it is also possible to apply information security classification at the document level. In this situation, either the file will be managed in accordance with the highest classification on it, or access will be restricted or permitted on a document by document basis. The option to inherit security from the file is the default for most agencies and then this is reviewed as required. This option works well where there are both paper and electronic document on the same file.

Table 1 Overview of the Tasmanian Government Information Security Classification Labels

Security Classification	To be used when
PUBLIC	Information has been authorised by the owner/custodian for public access and circulation It is important that agencies maintain the integrity and availability of PUBLIC information. Until public access is authorised, it is common for information to have some access restrictions applied by using a higher level of security classification.
UNCLASSIFIED	Information is released within the organisation on the basis of 'need to know' but is not restricted. Information is not released outside the organisation without the permission of the owner of the information, in which case its classification would change to PUBLIC.
UNCLASSIFIED with Dissemination Limiting Markers Eg: For Official Use Only (FOUO)	Information can only be released to organisations and individuals with a demonstrated need to know and information is to be stored and processed away from public access.

Sensitive: Personal Sensitive: Legal	
X-IN-CONFIDENCE This protective marking includes a notification of the subject matter (X), which alludes to its audience and the need-to-know principle	Used when the compromise of the information it relates to must be considered as possibly causing LIMITED damage to the State, the Government, commercial entities or members of the public. 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.
PROTECTED	Used when the compromise of the information could cause damage to the Government, commercial entities or members of the public compromise could: endanger individuals and private entities, work substantially against government finances or economic and commercial interests, substantially undermine the financial viability of major organisations, impede the investigation or facilitate the commission of serious crime, and/or seriously impede the development or operation of major government policies
HIGHLY PROTECTED	Used when the Information requires a substantial degree of protection as compromise could cause serious damage to the State, the Government, commercial entities or members of the public. Compromise could: threaten life directly, seriously prejudice public order, and/or substantially damage government finances or economic and commercial interests.

The first level of classification is Unclassified, this should be the default. UNCLASSIFIED can be strengthened by the use of a dissemination limiting marker (DLM) . Their purpose is to restrict the release of information to a group of people (Business Unit or Role) for a purpose. For example, a record classified UNCLASSIFIED: Sensitive: Legal is likely to be restricted to people in the Legal Unit.

The levels of classification impose increasing restrictions on their storage, distribution, copying and destruction. Most agencies will have well over 95 per cent of their records classified as PUBLIC, UNCLASSIFIED or X-IN-CONFIDENCE.

It is important for agencies to review the requirements of each classification level within the policy in regards to storage and access of the records and reflect these requirements in their Access Control Policy.

Caveats

A caveat is a warning that the information has special requirements in addition those indicated by the security classification. It is generally used to limit specific types records to specific roles across an agency such as HR records types to HR roles. When it is used those peoples who need to know about its use need to be involved

and educated. Any caveats should be identified in the agencies access control policy. Areas that you may apply include:

- Human Resource Personnel Records
- Grievance and Investigation Records
- Legal Services records
- Industrial Relations records
- Internal Audit function records
- Specific projects to implement government organisational change

Access Control

Access controls are the most specific level of security applied to records in an EDRMS. Access control is an individual security control and is applied to individual records. Access controls restrict access across a range of properties such as View document, View Metadata, Update Document, Update Record Metadata, Modify Record Access.

Control of access to sensitive records in an EDRMS is often applied through groups linked to user profiles: a user in the system is a member of a particular group (for example "HR staff") and certain records (for example, personnel files) may only be accessible to users in a relevant group.

Information security classification does not replace the need for this type of group-based security. A key principle in the Policy is 'need to know' – for example, a person cannot access all information at a particular classification level, as they also must have a need to access the information, to do their work or for the efficient conduct of business. Group-based access complements information security classification by enforcing this 'need to know' access. As a result, an EDRMS will contain both information security classifications and group-based access controls.

Agencies should develop an access control policy. See Attachment 1 for a sample Policy. The policy maps access to the records in the EDRMS according to roles. The protocols include the default security settings for business units and governance committees as well as identifying caveats - specific business units that are treated as exceptions.

An access control policy combined with information security classification provide sufficiently security control through EDRMS.

Table 2 - Access Control Policy

Information Asset Role or Business Unit	Personal and/or sensitive information	Ministerial information	Executive Management papers	Governance Committee papers	Own branch	Others' branch
Senior Executive Members & admin support	No access unless required	Full access	Full access	Normal access	Full access	Read Only
Ministerial and coordination staff	No access unless required	Full access	Full access	Full access	Full access	Read Only
Governance committee members, & admin support	No access unless required	View metadata	Normal access	Full access	Full access	Read Only
Senior staff to Business unit Managers, and assistants	No access unless required	View metadata Full access to own BU documents	Normal access	Normal access	Full access	Read Only
Branch staff	No access unless required	View metadata	View metadata	Read Only	Full access	Read Only
Records Services Unit	Full Access	Full access	Full access	Full access	Full access	Full access

Note: the records area must have full access as they provide systems administration and support for the EDRMS. They will not be able to fulfil their role to support the system and users of it for example recover access to documents unless they have full access to all records.

EDRMS Feature Configuration

Case Study: Agency example of configuring TRIM for Information Security Classification

There are three features to be configured: record types, profiles recordkeeping (metadata)/locations and classifications. The goal is to determine how to apply a combination of security attributes to each of the objects in a complementary manner.

A review of TRIM objects should be conducted. This should be a staged project that includes an audit of record types, locations and Security and access for individual locations.

Groups and positions should be created in the first instance and individuals' locations assigned to a position, and positions assigned to certain groups to ensure appropriate access to information.

Note: TRIM will not allow duplicate positions to be created, so if creating generic positions in TRIM also add the position number from the SOD which is unique.

Secondly a process for auditing and updating security rights for individual locations in TRIM to reflect the Information Security Classification standards should be undertaken. (e.g. Asset Management and HR staff require an 'In-Confidence' classification to enable them to access Tender Information (Commercial In-Confidence) and Personnel Records (HR In-Confidence). It is a pre-requisite that prior to following this procedure that locations are created and assigned to groups.

Thirdly a procedure for auditing and updating security currently assigned to files in TRIM to reflect the agency's Information Security policy and procedures and the *Tasmanian Government Information Security Policy Manual* should be undertaken. Tools such as a Ready Reference for Information Security Classification and Impact Assessment Matrix ensure a clear understanding of the information security classification guidelines and should be developed prior to commencing this task. See the Tasmanian Government Identity and Access Management Toolkit for assistance with developing these tools. (Refer Attachment 2 and 3).

Document entry forms can be modified to include information security classification in the document metadata. Third party software is available to automatically populate the documents with the protective marking and the TRIM view panes can then be customised to display the information security classification. This is particularly useful when emailing the document from your EDRMS as the document will be security classified.

Security classification can also be applied at domain i.e. Function or file level in the Business Classification System in TRIM, and TRIM templates configured to inherit information security classification from the file/container and documents populated automatically with the protective marking system.

Some Agencies choose to implement Information Security Classification labelling at the document level placing the responsibility on the individual to classify the document as they are saving it into TRIM.

Note in TRIM if you have a caveat on a file then users can only access the file if their access control rights include information with that caveat.

Case Study: Agency Example of implementing Information Security Classification

An information security manual has been developed. This is a complete suite of twenty one policies and guidelines that compliment and reference each other. These policies form the framework for Information Security. These are the high level mandatory rules that are underpinned by the following related framework elements;

- Guidelines
- Technical Standards
- Procedures

The Information security manual covers the following mandatory policy principals of the *Tasmanian Government Information Security Policy*

- Information Security Governance and Management;
- Risk Management;
- Resource Management
- Information Security Classification;
- Physical Environment;
- Information and Communications Technology;
- Identity and Access Management; and
- Business Continuity Management
- Incident Management

The Information Security Committee has been established and will report to the Corporate Management Group (CMG). The Information Security Committee is ensuring that the *Tasmanian Government Information Security Policy* is applied within the agency.

The Information Security Committee has been established and will report to the Corporate Management Group (CMG). The Information Security Committee is ensuring that the Tasmanian Government Information Security Policy is applied within the agency.

An Acceptable Use Reference Guide for Information Resources is being used as a guideline for implementation of the Tasmanian Government Information Security Policy in DPEM. The Acceptable Use Reference Guide is a summary of the DPEM Information Security Manual and collation of user responsibilities that are set out in the Information Security Manual guidelines. Implementing the policies referenced in the Acceptable Use Reference Guide will ensure

- the minimum level of compliance with the mandatory requirements of the Tasmanian Government Information Security Manual;
- delivery of the minimum requirement to ensure that personnel have a basic understanding of their responsibilities in relation to information security;

The Information Security Governance Policy has been approved. The Information Security Governance policy and guidelines defines information security roles and responsibilities within the Department.

Responsibility for setting the classification in a recordkeeping system

Advice 33 Implementing Information Security Classification sets out roles and responsibilities for information security classification. In practice, recommended or default information security classifications may exist for certain types or "domains" of information – for example, all HR paperwork is STAFF-IN-CONFIDENCE or all procurement is COMMERCIAL-IN-CONFIDENCE. Other areas may routinely produce information with a PUBLIC classification. The record classes identified in your agency's Retention and Disposal Schedule may provide a framework for setting security classifications.

Responsibility for applying the correct information security classification in a recordkeeping system depends on the recordkeeping procedures of each agency. For example:

- The end user may be required to select an information security classification when registering a document in an EDRMS, and/or
- Records management staff may apply the information security classification when creating a file.
- Domain level classification will be applied to the BCS by information owners as a part of the implementation of Information Security Classification.

Information security classification prompts and reminders should be built into relevant work procedures, and if end users are responsible for applying the security classification, quality assurance procedures should be in place to ensure consistent and appropriate application.

Relationship between Information Security Classification and recordkeeping metadata

Advice 14 The Value of Recordkeeping Metadata complements the Policy by identifying Security Classification as required metadata. In accordance with the Policy, the Recordkeeping Metadata Advice also allows for "Determination Date" or the date that the classification was made, and a 'Review due date' to trigger a review of the security classification.

As outlined in section 3.3 of the Policy, it is important to limit the duration of security classification, as sensitivity often decreases over time.

Information Security Classification labelling and physical records

Information Security Classification Labelling also applies to physical records. Section 3.3 of the policy details the types of physical controls that must be applied to records of different information security classifications, including markings on file covers, appropriate storage and handling protocols, and methods of destruction. For example, the IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED classifications, require storing physical copies in lockable cabinets of varying specifications.

Implementation Plan

Prerequisites to implementing information security classification in your EDRMS include:

- Identify Information Assets
- Identify information asset owners
- Develop and Identify and Access Management Policy

Implementation Step	***Responsibility***	***Further advice***
Carry out domain level information classification on the BCS in your EDRMS at the function level	Information Manager IS Project Manager	
Introduce procedures to implement information security classification on document and file metadata in EDRMS	Information Manager	
Records staff training in applying IS classification when new files are created	Information Manager IS Project Manager	
Awareness raising with staff about setting IS classification on new document metadata	Information Manager IS Project Manager	
Apply IS classification labelling to existing files according to domain level classification for files containing digital and paper records	Information Manager	

Overuse of Security and Access Controls

The most common issue with the application of security policy in an EDRMS is the over-classification of records and the over-use of access controls.

Over-classification results in unnecessary, administrative arrangements that remain in force for the life of the record. The volume of security classified information becomes too large for an organisation to protect adequately. Over-classification brings security classification and associated security procedures into disrepute. This often leads to security classifications being devalued or ignored by organisation employees.

The default security level should be UNCLASSIFIED. The default access control for all records should preferably be the whole organisation. The vast majority of records should be viewable by anyone in the organisation. This is rarely the case. Higher classifications should be used sparingly and only when the record meets the requirement of the classification. Most agencies, for example, will have very few, if any, HIGHLY PROTECTED records as defined in the Tasmanian Government Classification Policy.

Information Security Policy

Agencies should develop and Information Security policy which is endorsed by the senior executive.

Security is not a popular topic in most organisations. Spend time and effort to make people aware of the policy for applying additional security and the need to abide by the policy and to follow the procedures. Ensure emphasis is given to the procedure for applying for permission for others to have access if necessary.

Awareness Raising

Make sure people are aware of how security works in your EDRMS and what is happening when they apply it. Telling people how to apply security is insufficient. Educate people in the difficulties that result when incorrect security and access options are applied.

Have people experience the difficulty in finding a record if view metadata access has been denied, or a caveat is applied. Be proactive about managing the situation, rather than reactively adjusting access record by record as requests come in and expect that education is ongoing.

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

- Queensland State Archives Public Records Brief Implementing the Information Security Classification Framework in Recordkeeping Systems
- Access Denied – Navigating the digital information security maze, Michelle Linton and Kevin Dwyer, The RIM Quarterly, Volume 29, Issue 1, February 2013
- Template Access Control Policy, Queensland Government Information Standards
- Thanks to Angela Males and the Department of Police and Emergency Management for implementation advice on configuring EDRMS for implementing information security classification and agency example of how to implement information security classification in TRIM

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	May 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

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

Issued: May 2013

Ross Latham
State Archivist

Attachment 1 Sample Access Control Policy

1. Purpose

2. Scope

3. Policy

1.1. Access control policy

Who and how is authorisation for access to systems and business applications granted?

1.2. User access

How is access to information systems to be granted (eg passwords etc)?

Who is responsible for monitoring and reviewing access rights?

Who is responsible for removing and notifying of redundant User IDs and accounts and what is the process?

Who is responsible for granting access to systems utilities and privilege management?

How is access and use of systems utilities monitored?

1.3. User responsibilities

How are users to be educated and made aware of access responsibilities?

What are users" responsibilities for access and passwords?

1.4. Network access

Who is responsible for authorising network access (both internally and external connections)?

What is the process for enforced network paths, user authentication for external connection, Node authentication, use of remote diagnostic ports?

How will network domains and groups be segregated?

What network connection controls will be in place – eg. times, type and size of file transfers to external source?

1.5. Operating system access

How is automatic terminal identification used to authenticate connections to specific locations and portable equipment?

What is the secure logon and logoff process for access?

Are there restrictions on connection times in place?

How will passwords be issued and managed – what are the rules for passwords?

How will systems utilities" use be controlled?

1.6 Application access

What is the process for authorising access to information when systems share resources, eg. two separate systems are integrated to form a third application or system?

1.7. Monitoring system access

What system events will be logged, e.g. date, IP address, User-IDs, unsuccessful logins, alerts from intrusion detection systems (firewall)?

When and who will review and monitor system logs? And where are they stored?

1.8. Mobile computing and telecommuting

Outline Agency policy for each type of mobile device – eg. physical storage, personal usage, protection of information held on the device, access mechanisms (eg password), virus protection, backup.

Policy on use of computer equipment for telecommuting, eg. authorisation process, system access, physical security, etc.