Information Management Advice 67 - Tasmanian Government Information Security Policy considerations for Local Government

Introduction

Information is one of your organisation's most important assets: it needs to be protected. Security threats and breaches can affect your organisation's ability to protect personal safety or privacy, to safeguard infrastructure or to comply with its legal and other obligations. Breaches of security can have significant impacts on an agency's ability to do business, including damage to its reputation.

The release of the Tasmanian Government Information Security Policy Manual has mandated Information Security principles and procedures for use by Tasmanian State Government agencies, in response to threats posed by increasing reliance on information and communications technology. Agencies and their information systems face security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, theft, fire or flood. Damage caused by breaches such as computer viruses and computer hacking is becoming increasingly common and sophisticated. Dependence on information systems and services means that agencies are increasingly exposed, and vulnerability to security threats and security issues is heightened during information sharing/exchange between state and local government entities.

What is it?

Information security is 'the preservation of the confidentiality, integrity and availability of information.'

- Confidentiality means ensuring that information is accessible only to authorised users.
- Integrity involves safeguarding the accuracy and completeness of information, and processing methods.
- Availability involves ensuring that authorised users have access to information and associated assets when required.

Other properties such as authenticity, accountability, non-repudiation and reliability can also be considered as part of information security. Information security applies to all forms of information (digital, print or other), and includes the management of the software and/or communications technology systems and networks for storing, processing and communicating information.

In essence, managing information security involves protecting your information assets by implementing controls including policies, procedures, organisational structures and software / hardware functions and undertaking regular reviews.

How does this affect Local Government?

Local Government agencies may already have internal Information Security models and policy in place. These models may not yet have defined specific information assets as part of broader information security. They traditionally focus on:

- physical security and access issues concerning facilities and environment,
- internal access, audit trails and logging of core IT systems and applications, including email, networks, and databases

- security of personnel records and client information in relation to the Personal Information Protection Act

Local Government agencies are reminded that where they are involved in information exchange with Tasmanian Government agencies, the requirements of the Tasmanian Government Information Security policy manual will apply.

Where information is shared, internal security models should be reviewed against the requirements of the Tasmanian Government Information Security policy manual to ensure practices are consistent, and the same levels of access/restriction are applied to information assets in their custody. This review does not necessarily require changing the terms or classification already applied, simply that existing classification/terminology should be 'mapped' to the equivalent Tasmanian Government term to ensure appropriate safeguards are in place. An overview of the Tasmanian Government Information security labels can be found in the attachments.

Who's responsible?

Information security is not just an 'IT problem' –the management of information security in the agency requires a number of stakeholders. Ideally, a management framework should be established to initiate and control the implementation of information security. This includes establishing management accountability, assigning roles, and establishing necessary external liaisons. A multi-disciplinary approach is encouraged, and your agency's information security policy should outline the roles and responsibilities of different personnel who have a business requirement to ensure the appropriate security of information assets.

In particular, Information Managers have a key role to play in the implementation of Information Security Policy because information is one of your agency's most important assets: you need to preserve its confidentiality, integrity and availability. Records and Information Management (RIM) professionals are important stakeholders because they have a comprehensive knowledge of the agency's information assets, and their work already involves maintaining the confidentiality, integrity and authenticity of information.

Where to begin?

As a starting point, Local Government Records and Information Managers should undertake analysis of their business to identify business processes where information is exchanged with Tas Government agencies, in order to ensure that information shared is managed consistently, and in accordance with the Tasmanian Government Information Security Policy requirements. Some examples may include:

- Property ownership enquiries from the State Revenue Office
- Centrelink (e.g. confirmation of previous employment)
- Tasmania Police investigations
- Tasmania Fire Service Evacuation plans approvals
- Statistical reporting to the Australian Bureau of Statistics

A good place to start looking is likely to be your Information Asset register. See *TAHO Advice 39 Developing an Information Asset Register*, and *Advice 40 The role of an Information Asset Owner*, if your council hasn't yet developed one.

Your register is a centralised location that can identify the kinds of records, the responsible business owner, and the relevant system/s in the council that may contain affected information. (It is also a good place to record any Information Security requirements or adjustments that may need to be incorporated). If you don't have an Information Asset register, reviewing the current agency Information Security policy and practices may be the ideal opportunity to undertake the necessary investigative work. Importantly, Information Asset registers also provide a centralised location to manage currency of information security classification status, as information sensitivity may decrease over time. One example of this may be intellectual property information labelled ‘commercial in confidence’ during a procurement exercise. Once the relevant contract has been formally accepted, such information may require re-classification.

Information Security Assessment Checklist

Issue	Considerations	Activities
What information is affected?	Identify processes where information is exchanged with Government agencies. Understand your business – engage stakeholders to assist with the identification of records affected. Review Information Asset register, retention & disposal schedule, Business classification scheme, Vital Records registers to help identify likely candidates.	Develop Information Asset register (if none exists). Consider value/sensitivity of information, likelihood of access to determine priority of any issues identified.
Where is it located?	Consider all formats, all systems, electronic and paper. Don’t overlook cloud technologies (eg. Dropbox, Docs on tap), network drives, web, mobile devices (tablets, ipads, etc). **Hint:** Disaster recovery models may assist. Also check Information Asset register, Information architecture (or database relationship modelling) documentation, business systems, network drives.	Incorporate this information in the Council Information Asset register and/or Records and Information Management Disaster recovery planning (if not already documented).
Tools	What is the capacity of information systems to apply additional layers of classification/labelling? Can existing practice be extended to include new labelling? What are the currently implemented security models and classifications (if any)? Is there capacity for automation rather than reliance on manual intervention from users?	Development of manual processes (e.g. labelling of physical assets, legacy hardcopy files), introduction of classification tools. Build into new (and existing) systems where capability permits.
Contractors, volunteers, suppliers, vendors, etc.	Do current contracts, agreements and outsourcing terms reflect legislative requirements and include (where applicable): • confidentiality clauses • information classification requirements • permissible distribution/access • copyright considerations, etc.	Review existing contracts and agreements to ensure adequate coverage of required information management practices

Issue	Considerations	Activities
Governance	What is the current governance framework in place for information security? Is this currently considered an IT function? Are there robust policies and procedures in place to support the agency practices with regards to the security of information? Is there an existing committee – who are the stakeholders? Consider legislative requirements - what are the access implications (Right to Information, Personal Information protection, etc.)? What are the issues (if any) with respect to intellectual property, copyright, etc?	Establish committee, identify business owners/custodians, etc. Develop additional policies (where required), procedures/processes. 'Appropriate use' policies should consider: • Use of corporate information/records • Use of ICT resources (email, business systems, mobile devices, portable drives, etc.) • Use of Social Media • Provision of agency information - including hard copy file access - to external parties (whether public, other agencies, vendors, suppliers, etc.).
Security models	How can the Tasmanian Government information security classification be incorporated into current practices? Review existing security models for EDRMS, Business systems, network, email, etc.	Develop and document Security/Access procedures for physical records (on-site), and identify/document those of storage providers. Map Tasmanian Government information security classification requirements against current practices and models. Highlight discrepancies for corrective action and devise strategies to manage.

Further Reading

- Cloud Computing Information Security Considerations (2014: Advice 44)
- Developing an Information Asset Register (2013: Advice 39)
- The Role of an Information Asset Owner (2013: Advice 40)
- Implementing Information Security Classification - Part 3: Implementing Security Classification Controls (2014: Advice 33)

Agencies may also refer to the Australian Standard *AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques – Code of practice for information security management*

Attachments

Overview of Tasmanian Government Information Security Classification labels

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

- Tasmanian Government Information Security Policy Manual
- Standards Australia/Standards New Zealand, AS/NZS ISO/IEC 27002:2006
- Implementing Information Security Classification - Part 2: The Security Classification Process (2014: Advice 33)
- Implementing Information Security for Information Managers (2013: Advice 32)

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
1.0	October 2014	Sam Foster-Davies	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
		This is the first release of this document.

Issued: November 2014

Ross Latham
State Archivist

Table 1 Overview of 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	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. UNCLASSIFIED is strengthened by the use of a dissemination limiting marker (DLM). The purpose of the DLM 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.
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.