TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 32
Implementing Information Security for Information Managers

Introduction

Information and Communications Technology (ICT) has fundamentally changed the way in which the Tasmanian Government conducts business. The Government is now dependent on information and communications to deliver services to the Tasmanian public, and to efficiently manage internal Government operations. However, information and communication technology has significant risks, including unprecedented and escalating levels of external threats to information security and privacy.

The Tasmanian Government Information Security Policy Manual (The Manual) provides the common high-level policy and supporting procedures to guide Government agencies. It also includes other resources such as standards, codes of practice and legislation that will assist agencies to implement the policies.

The purpose of this Recordkeeping Advice is to examine how the work you are already required to do as part of the management of your records program can be used to meet information security objectives, including compliance with the Tasmanian Government Information Security Policy and the Australian Standard AS/NZS ISO/IEC 27002:2006. It also suggests options for implementing the mandatory policy principles for records security.

Audience

This Advice is designed for recordkeeping professionals working in the Tasmanian public sector, business unit managers and ICT Professionals.

What is information security?

Information security is 'the preservation of the confidentiality, integrity and availability of information.'[1]

- Confidentiality involves ensuring that information is accessible only to those authorised to have access.
- 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.[2]

Other properties such as authenticity, accountability, non-repudiation and reliability can also be considered as part of information security.[3] 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 and hardware functions and regularly reviewing these.[4]

Why is information security important?

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 vulnerable to security threats and security issues are not always the primary consideration in system design.

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.

What is AS/NZS ISO/IEC 27002: 2006?

Many organisations seek to or have achieved compliance with AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques – Code of practice for information security management. This is available from the standards Australia web site. The Tasmanian government has a whole of government subscription contract the Office of eGovernment at the Department of Premier and Cabinet.

This standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation. It contains best practice guidance concerning a number of areas of information security management.[5]

Who is responsible for information security?

Information security is not just an 'IT problem.' Technical measures need to be designed to meet real business requirements and supported by appropriate training, business rules and assigned responsibilities.

Information security, by necessity, requires a number of stakeholders. The Manual and the Australian Standard recommends that a management framework should be established to initiate and control the implementation of information security. This includes establishing management accountability, assigning roles, establishing necessary external liaisons and monitoring industry trends. A multi-disciplinary approach is encouraged.

Accountability for Information Security

Some of the positions with accountability for information security may include:

- Business managers who need to ensure security responsibilities are addressed at the recruitment stage and monitored during an individual's employment, ensure staff are trained and updated in security policy and procedures and act on incidents affecting security.
- Human resource management staff who need to manage personal information.
- Contract managers who need to deal with in-confidence material.
- ICT staff who need to establish security controls in systems and protect ICT equipment from threats.
- Users of the information service who need to report observed or suspected weaknesses in security or threats to systems or services.
- Facilities staff who need to maintain the physical and environmental security of the building and particular secure areas. [6]

Your organisation's information security policy should outline the roles and responsibilities of different personnel.

Implementation Guide

The implementation of information security for recordkeeping cannot be achieved in isolation and needs to be a part of the development of an agency wide framework for Information Security.

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.

Recordkeeping professionals are important stakeholders in an agency because they have a comprehensive knowledge of your information assets and their work already involves safeguarding their integrity and authenticity. These key staff have many valuable skills to contribute to your information security management framework, and may already have developed tools that will assist in the secure management of information.

Footnotes

[1] Information technology – Security techniques – Code of practice for information security management, second edition, 2.5 Terms and definitions.

[2] Wikipedia. ISO/IEC 27002, available at: http://en.wikipedia.org/wiki/ISO/IEC_27002

[3] Standards Australia/Standards New Zealand, AS/NZS ISO/IEC 27002:2006 ibid., 2.5 Terms and definitions.

[4] Ibid., Introduction, p.vii.

[5] Ibid., 6.1 Internal organisation

[6] Ibid., 6.1 Internal organisation; 7.1 Responsibility for assets

Table 1 Implementation Guide

The following table examines ways records management techniques and skills may assist you in addressing your information security (IS) needs and provides examples from agencies and a list of expected outputs.

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
4.1 Records Management Procedure				
Policy & Procedures	An information security policy provides management direction and support for the security objectives of your business. Recordkeeping professionals can provide input into the policy's development and review and may be assigned specific responsibilities. Recordkeeping professionals are already required to develop policy and procedures on the management of records in all formats. They may produce additional policies e.g. on email management, access to records or the use of media formats. These often incorporate responsibilities relating to information security. Include statements in Agencies Information Management Policy Framework about Information Security. This could be a separate document or incorporated into other corporate policies. Make sure the policy statements include an 'authority' statement saying who issued the policy, e.g. the Board, the CEO, the Secretary, a senior manager, and that it is made available to all staff.	Agency developed an information security plan which consists of establishing a framework comprising security policies, guidelines, standards and procedures. Framework structure The framework states information security is important, defines what has to be done to secure communications and information technology resources, how security rules are to be implemented and who is responsible for their implementation. Information Security Plan Framework has policy categories that include: ➢ Information Security Governance ➢ Records Security ➢ Information Security Classification System ➢ Physical Security ➢ Asset Control ➢ Personnel Security Policy ➢ Information Facilities and systems Operations ➢ Database security ➢ Network and communications management ➢ Security of Computerised Communications Systems ➢ Electronic Information Transfer ➢ Access control management ➢ Security Audit and Logging ➢ Information systems Acquisition,	**TAHO Guidelines and Advice:** ➢ Advice 35 Information Security Governance ➢ Advice 53 Implementing a Records Management Program ➢ Advice 33 Implementing Information Security Classification ➢ Advice 50 Information Management Policy ➢ Template: Information Management Policy ➢ Guideline 1 Records Management Principles Available from the GISU website **Other Sources** Records Management Checklist - Victorian Auditor-Generals Office (VAGO) See: http://www.audit.vic.gov.au/reports__publications/reports_by_year/2008/20080730_records_checklist.aspx	➢ Gap analysis of Agency Policy Framework to identify policies for development ➢ Records management Policy ➢ Acceptable Use Policy for Agency Information Resources

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
	Make it clear in the policy that all employees are responsible for information security and that they must be familiar with Agency polices and use procedures. Incorporate in the policy definition the responsibilities of staff appropriate to their roles.	Development and maintenance ➢ Business Continuity management ➢ Information Technology Media Handling and management ➢ Cryptography ➢ Malicious and Mobile Code Control ➢ Monitoring for Compliance ➢ Information Security Incidents ➢ Information security Risk Management Other Policies Include: Acceptable Use References Guide for Records		
Customer access	The analysis of requirements undertaken by recordkeeping professionals can be used to determine what information can be released to the public under access legislation, and what should not be released. EDRMS or other recordkeeping systems can indicate which records have been made publicly available. Access policies can be implemented within EDRMS.	Agency developed policy on: ➢ Access Control and Management ➢ Security and Audit Logging ➢ Information Technology Medial Handling and Management ➢ Malicious and Mobile Code Control Agency Developed Acceptable Use Guidelines for: ➢ Access Control and Management ➢ Information Technology Medial Handling and Management ➢ Malicious and Mobile Code Control	➢ Tasmanian Government Identity and Access Management Toolkit	➢ Agency Identity and Access Management Policy ➢ Acceptable Use Policy ➢ Release of Information procedures/policy ➢ Risk Assessment Policy ➢ Conduct risk assessment on possible information security incidents, e.g. Possible disclosure of confidential information ➢ Information Security Incident Management Policy
Applying metadata	Organisations need to ensure business information is described with adequate metadata to be effectively and accountably managed, secured and retrieved by authorised users. Recordkeeping professionals can contribute to the development of metadata schemas that meet statutory requirements and promote the	Agency conducted a review of BCS/Disposal Schedule and apply Info Security Classification at Domain Level where possible.	➢ TAHO Advice: 14 Metadata	Minimum Metadata standards defined for the Agency incorporates Information security classification and access control requirements of the Agency Information Security Policy Gap analysis of compliance to agency metadata standard incorporated in Information Asset

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
	management and Security of business information.			Register
Asset identification and management	Recordkeeping professionals carry out inventories of systems and repositories containing business information. This information can inform the development of an information asset register.	An agency developed a comprehensive information asset register which included an Information systems Ownership and Custodianship Register. It identified every information asset of every type, identified the business owner, custodian responsible for ensuring that the information asset complied or was working towards compliance to Information Security framework of policies	➢ Advice 39 Developing an Information Asset Register ➢ Information Asset Register Template	➢ Information Asset Register ➢ Business process for annual review of the Asset Register ➢ Apply Information Security Classification to all assets in accordance with Information Security Classification Policy
Long term accessibility	Business information needs to be protected from loss and be available for use for as long as required. Recordkeeping professionals can determine how long records need to be kept, advise on suitable formats and contribute to system design and migration strategies to ensure records remain accessible and useable.	Agency has an up to date approved disposal schedule and an active archiving and disposal program.	➢ Advice 37 Keeping digital information accessible ➢ Guideline 19 Digital Preservation Formats ➢ Advice 41 Managing Records on Shared Network Drives ➢ Advice 68 Migrating Documents from Network Drives to EDRMS ➢ Advice 14: Metadata ➢ Advice 50 Information Management Policy **Other Sources** International Council on Archives, Principles and Functional Requirements for Records in Electronic Office Environments, 2008 Available online at: http://www.adri.gov.au/products/ICA-M3-BS.pdf	➢ Ensure that a Disposal Program and records migration is part of your Information Management Plan

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
Physical security and handling:	Recordkeeping professionals have experience in how to physically secure critical or sensitive business information. They may have existing rules and guidance for staff regarding physical security measures, including the management of particular media such as removable media.	Agency developed a comprehensive Acceptable Use Policy that includes: ➢ Classification of Information ➢ Authorised access disclosure and use of information ➢ Physical Security ➢ Clear Desk Policy ➢ Storing Information on non-Agency premises ➢ Home Based Work Environments ➢ Mobile Based Work Environments ➢ Information Resources ➢ Personal Responsibilities ➢ Downloading Data ➢ Internet and Email ➢ Access Control ➢ Password Management ➢ Use of Information Technology Media ➢ Responsibility for Use ➢ Malicious and Mobile Code Control ➢ Compliance with Agency Policy, Legal and Contractual Obligations ➢ Security Incident Responsibility		➢ Agency Identity and Access Management Policy ➢ Acceptable Use Policy ➢ Ensure that Physical Security information is included in your Information Management Policy and Procedures and update in your Information Management Plan ➢ Develop procedures for marking and manual handling of physical files and documents.
Business continuity management:	As part of their responsibilities, recordkeeping professionals need to identify business information that is vital to the organisation and identify and manage risks in the context of broader business continuity planning.	Agency Developed a policy on Business Continuity Management	➢ Advice 26 Disaster Preparedness and Recovery ➢ Advice 52 Vital Records	➢ Vital Records Plan ➢ Business Continuity Plan ➢ Information Security Risk Assessment
Training	Recordkeeping professionals are regularly involved in cross-organisational induction and training. They can promote security awareness and procedures in relation to the use, classification, handling and	Deliver communication to raise awareness within the agency, may include posters, presentations at team meetings, Divisional Management Group Meetings, District Training Days, Intranet Content.	➢ TAHO Introduction to Records Management Training ➢ NAA Keep the Knowledge Make a Record	➢ Induction Training includes Records Management and Information Security Awareness ➢ Exit Procedure includes

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
	destruction of business information.	Customise to suit the audience, provide specific examples of information security incidents as they relate to records services		process for all staff to manage information correctly ➢ Include IM and IS responsibilities as part of Agency Statements of Duties
4.2 Legislation				
Defining Requirements	Organisational requirements should be defined so that appropriate controls can be applied and risks can be reduced to an acceptable level. Recordkeeping professionals undertake an analysis to define the business, legal and community requirements that apply to business activities and the records required. The analysis includes the identification and definition of requirements for access and security.	Agency has an up to date approved disposal schedule	➢ Advice 36 Legislative Mapping for Information Management ➢ Advice 39 Developing an Information Asset Register and Information Asset Register Template Available from the GISU website	➢ Information Asset Register
Incorporating requirements into systems	Business information needs to be captured into systems that can support context, security, access and long term management. Systems need to incorporate appropriate metadata to support integrity and authenticity. Recordkeeping professionals can assist to identify requirements for the design and implementation of new business information systems and can assess whether existing systems enable requirements to be met.	Security markings to be included in system generated report pro-formas Agency also developed a Role based Access Policy for EDRMS For Example: ➢ Administrator ➢ Information Manager ➢ Information Worker ➢ Records Officer ➢ Enquiry User ➢ Custom User	➢ Advice 39 Developing an Information Asset Register ➢ Information Asset Register Template Available from the GISU website Other Sources: International Council on Archives, Principles and Functional Requirements for Records in Electronic Office Environments, 2008 Available online at: http://www.adri.gov.au/products/ICA-M3-BS.pdf	➢ Information Asset Register ➢ Information Security Policy compliance Implementation Plan for Agency Business Systems ➢ Develop a Role Based Access Policy for EDRMS ➢ System Access Banners for systems to alert users to the information security classification eg, in-confidence, protected etc, - particularly for legacy systems that do not have the capability of applying role based access.

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
Compliance monitoring	Recordkeeping professionals already monitor compliance with security and access requirements such as the security of recordkeeping systems and physical controls in records management programs. Incorporate IS procedure into standard operating procedures for different parts of the Agency as appropriate. Regularly report on compliance of the agency to IS policies or progress toward implementing at senior executive level.	Agency developed procedures for monitoring compliance to Information Security Policy Framework Information Security Incident Management Policy Agency developed a process for reporting and managing information security incidents relating to records and information management. Including inappropriate access to information, disclosure and release of information, visitor access breaches, destroy damage or delete official documents/records, fail to maintain confidentiality.		➢ Reports to the Whole Of Government (WOG) Information Management Committee ➢ Incorporate IS procedure into standard operating procedures for different parts of the Agency as appropriate ➢ Regularly report on compliance of the agency to IS policies or progress toward implementing at senior executive level. ➢ Develop a process for reporting and managing information security incidents relating to records and information management.
4.3 Retention disposal and transfer				
Classifying information	Recordkeeping professionals may have developed business classification schemes or business process maps, both of which can provide a framework for analysing the security requirements of information assets. Their definition of business requirements can also assist you to identify information that requires particular labelling, system controls, supporting business rules or special handling and can assist in the declassification of information, including when it is made publicly available.	Agency developed an information Security classification system policy included: ➢ Need-to-know principle ➢ Definitions of information security classifications ➢ Information requiring increased security protection ➢ Non-national security classifications ➢ National security classifications Developed a Ready Referenced for Information Security Classification for staff and awareness training Developed an impact assessment Matrix as a tool to assist in information security classification	➢ Advice 33 Implementing Information Security Classification	➢ Information Security Classification Implementation plan ➢ Audit of objects in EDRMS eg. Locations, Files, Record Types

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
		Established procedures for implementation of information security classification within the EDRMS, and business systems, records in storage		
Information disposal	Security measures for business information need to include provisions for secure disposal. Recordkeeping professionals can establish and manage disposal programs that accountably manage the destruction of records in compliance with legal and best practice requirements. Ensure that the agency has an up to date disposal schedule and that staff are trained in scheduling and disposing of records.	Agency has defined guidelines, standards and procedures for information technology media handling and management Agency has acceptable use guidelines for disposing of media Agency has an up to date approved disposal schedule	TAHO Guidelines and Advice ➢ Advice 28 Getting Started on developing an Agency Functional Disposal Schedule ➢ Advice 22 Records Management using SharePoint – Considerations ➢ Advice 13 Writing Disposal Classes ➢ Advice 12 Preparing Records for transfer to the Archives Office ➢ Advice 10 Disposal of un-scheduled records and checklist ➢ Advice 9 Disposal of Scheduled records ➢ Guideline 2 Retention and Disposal of State Records ➢ Guideline 6 Developing a functional records disposal schedule Available from the GISU website	➢ Information security policy framework that includes arrangements for information disposal ➢ Approved Agency Disposal Schedule ➢ Register of Records Destroyed ➢ Ensure all relevant staff are trained in the scheduling and disposal of records
Third party agreements and cloud computing	When a business function is outsourced, it is vital that requirements for information are conveyed to the service provider. Recordkeeping professionals can advise on what business information to create, records that require additional security controls and formats for the return of business information as well as recordkeeping considerations in cloud	Agency has standards and procedures for information systems acquisition, development and maintenance that cover third party agreements and cloud computing	➢ Guideline 10 Outsourcing of government business: recordkeeping issues ➢ Guideline18 Managing Social Media records	➢ Information security policy framework that includes arrangement for third party agreements and cloud computing ➢ Set up protocols so that IM staff are consulted about ANY outsourcing undertaken by the

IS Policy Manual section	How your Records Manager can Assist	Example from an Agency	Further Guidance	Minimum Expected Outputs
	computing arrangements.			Agency, including Cloud Computing

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
- Information Security Future Proof State Records NSW
- Thanks to Angela Males and the Department of Police and Emergency Management for description of how to implement an agency wide information security framework

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	July 2013	Allegra Huxtable	Initial Release	All

Amendments in this Release

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

Issued: July 2013

Ross Latham
State Archivist