TAHO
Tasmanian Archive + Heritage Office

State Records Guideline No 1

Records Management Principles: Overview

Department of Education
LINC Tasmania

Tasmania
Explore the possibilities

Table of Contents

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
3.0	04-06-2014	Christine Woods	Template	All
2.0	13-07-2014	Samara McIlroy	Revised and updated	All
1.0	13-07-2005	Tina Howard	Initial release	

Amendments in this Release

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

Release for Comment: December 2014

Ross Latham
State Archivist

1 Introduction

1.1 Purpose

This Guideline describes the principles of Records Management. It is intended to assist agencies to develop a strategic approach to records and information management, and introduces some key concepts to promote a culture where agencies value their corporate information as a business asset.

The *Archives Act 1983* requires all relevant authorities to keep proper records of the business of their organisation until they are dealt with through other sections of the Act. This Guideline assists agencies to meet their obligations flowing from this requirement, and includes a checklist to measure compliance which describes the evidence that the agency will need to provide. Regular audits will be conducted by Tasmanian Archive and Heritage Office (TAHO) to measure each agency's compliance with this Guideline.

1.2 Authority

This guideline is issued under the provisions of Section 10A of the *Archives Act 1983*. Guidelines issued by the State Archivist under this Section set standards, policy, and procedures relating to the making and keeping of State records. This section also requires all relevant authorities to take all reasonable steps to comply with these guidelines, and put them into effect.

Keyword	Interpretation
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS RECOMMENDED	The item is encouraged or suggested.

'MUST' and 'MUST NOT' statements are highlighted in capitals throughout the Guideline. Agencies deviating from these MUST advise TAHO of the decision to waive particular requirements.

Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has management approval.

Agencies deviating from a 'RECOMMENDS' or 'RECOMMENDED' requirement are encouraged to document the reasons for doing so.

2 Principles

This Guideline introduces the principles of Records Management and describes the processes and practices that agencies MUST align with to meet their obligations under the Act.

The five principles are:

- Create and Capture Records
- Govern Records
- Store Records
- Access Records
- Dispose of Records

Each principle is supported by mandatory compliance requirements.

Principle 1: Create and Capture Records

- Records must meet legislative, regulatory and administrative requirements
- Records must be captured regardless of format
- Records must be appraised for their value
- Records must be classified, and metadata applied
- Records must be captured into systems with recordkeeping functionality.

Alignment with this principle ensures that the agency creates and captures State records which comply with the Archives Act 1983, have evidential integrity, meet accountability requirements, and mitigate business risks.

Records MUST meet legislative, regulatory and administrative requirements

Aside from their obligations under the *Archives Act 1983*, each agency must determine what additional legislative, regulatory and administrative requirements they MUST meet. If recordkeeping requirements are identified and/or specified in legislative and regulatory obligations, records MUST be created and captured to meet these requirements.

Legislation that may be applicable includes:

- *Corporations Act 2001*
- *Crimes Act 1924*
- *Electronics Transactions Act 2000*
- *Evidence Act 2001*
- *Limitations Act 1974*
- *Personal Information Protection (PIP) Act 2004*
- *Right to Information (RTI) Act 2009*
- *Work Health and Safety Act 2012*

However, agencies MUST undertake their own legislative mapping to identify specific recordkeeping requirements.

Records MUST be captured regardless of format

Records MUST be created and captured irrespective of the technology format or medium. This includes hardcopy formats and electronic records in email systems, websites, social media, business systems and cloud-based applications.

Records MUST be appraised for their value

The agency MUST appraise State records to determine how long the records need to be kept to meet business needs, organisational accountability requirements and community expectations. This appraisal MUST be documented in an approved Retention and Disposal Schedule (see Principle 5 - Dispose of Records for more on records disposal).

Records MUST be classified, and recordkeeping metadata MUST be applied

File and record naming conventions MUST be applied to State records. Classification of records SHOULD be based on functional Business Classification Schemes (BCS) and be systematically applied. Records MUST contain, or be linked to, sufficient metadata to describe record structure, business context, relationships to other records, retention and disposal rules and leave an audit trail.

Systems that keep records SHOULD contain controls (such as monitoring access, verifying users, authorising transfer, destruction and providing security) that protect the integrity of the records. Such systems can be either in an electronic or paper form, and includes information systems, business systems and hardcopy files.

Principle 2: Govern Records

- Overall responsibility for records management must be assigned to a senior officer
- Direct responsibility for records management must be assigned to an appropriately skilled and resourced records officer(s)
- All management, staff, contractors, and volunteers must be responsible for their recordkeeping
- The agency must have a Records Management program that is a framework for:
  - Business analysis to inform the program
  - Records Management Policy
  - Records Management Procedures
  - Records Management Plans - Operational, Strategic, Vital Records and Disaster Management
  - Performance management for reporting
  - Risk analysis
  - Continuous improvement activities
  - Managing multiple sites
  - Outsourcing government business
- The agency's Records Management program must align with:
  - The agency's Risk Management program
  - Internal and External audit and review
  - Disaster Recovery and Business Continuity planning
  - Tasmanian Government Information Security Manual
- The agency MUST participate in recordkeeping audits conducted by TAHO.

Alignment with this principle ensures that the agency has information governance structures, policies, procedures, processes and controls in place to manage State records. This will support immediate and future regulatory, legal, risk, environmental and operational requirements.

Records Management and recordkeeping responsibilities MUST be assigned:

- The agency MUST assign overall responsibility for records management to a senior officer.
- Direct responsibility for records management MUST be assigned to an appropriately skilled and resourced records officer(s).
- All management, staff, contractors, and volunteers MUST be responsible for their recordkeeping.
- Responsibility for recordkeeping SHOULD be routinely promoted throughout the agency through inclusion in agency-wide policy and procedures.

The agency MUST have a Records Management program

The Records Management program encompasses the management framework, the people and the systems required within an organisation to manage State records over time. This includes the identification and protection of records with enduring value that may be required as State archives.

The Records Management program MUST include the following:

- **Analyse agency business activities to inform the Records Management program** including conducting research and stakeholder consultation to understand the structure, policies and business operations of the agency. The outcome of this business analysis will recommend business improvements or systems solutions in order to meet records management goals.
- **Records Management policy** adopted at the corporate level. The policy directs that records are made, captured, maintained and disposed of in accordance with the legal, regulatory and business needs of the agency. The policy defines the responsibilities of all personnel who manage records or carry out recordkeeping activities.
- **Records Management procedures** which define business rules and processes to ensure that records are created, captured and stored in authorised agency systems.
- **Records Management strategic plan** in which long and short term records management goals are identified and documented in the planning mechanisms of the agency. The plan SHOULD address training and specialist knowledge requirements and allocation of appropriate resources to achieve records management goals.
- **Records Management operational plan** which turns the broad objectives and strategies from the strategic plan into a detailed plan for action, linking strategic goals to deliverable outcomes.
- **Vital Records plan** that identifies the records essential for the ongoing business of the agency, and the actions required for ensuring the protection of those records, and **Disaster Management plan** for records and recordkeeping systems should be developed, implemented and maintained.
- **Performance management for reporting** on the records management program. These SHOULD be designed so that all aspects of the records management program can be regularly reported on, and reviewed against performance objectives.
- **Risk analysis** to analyse any strengths, weaknesses and risks that may impact on the recordkeeping requirements of the agency.
- **Continuous improvement activities** that identify opportunities for improving the effectiveness, efficiency and quality of records management systems, processes and tools through regular monitoring and review. Agencies SHOULD regularly collect information and gather feedback about the Records Management program, and use this to develop new services or make existing services and tools better.
- **The Records Management program applies across all sites** if the agency operates multiple sites and locations.
- **Outsourcing government business** addresses recordkeeping requirements, in accordance with Guideline 10 - *Outsourcing of government business: recordkeeping issues*.

The Records Management program MUST align with agency processes for:

- **Risk Management** - By aligning the records management and risk management programs across the agency, both business risks and recordkeeping risks will be consistently identified and addressed.
- **Internal and external audit and review** - Any agency audits, such as legal compliance or financial audit programs, SHOULD align with the records management program. Agency self-assessments and internal audit programs SHOULD include assessments of recordkeeping practices across the agency.
- **Disaster Recovery and Business Continuity planning** - The agency MUST include protection and recovery of State records in disaster recovery plans in the event of disaster. Planning for business continuity MUST also include actions to reduce damage to or loss of records from disruptions to business operations.
- **Tasmanian Government Information Security Policy** - the Office of eGovernment's T*asmanian Government Information Security Manual*[1] sets the minimum requirements for information asset security classification. It also provides a standard process to allow agencies to evaluate their information assets and determine the appropriate level of security classification that must be applied, addressing the need for a consistent approach to managing the sensitivity and confidentiality of information assets across the Tasmanian Government.

The agency MUST participate in recordkeeping audits conducted by TAHO

The agency MUST participate in scheduled TAHO audits of recordkeeping practices. The agency will be audited against the requirements in this Guideline. The checklist at the back of the document describes the evidence that the agency SHOULD provide as proof of compliance. These audits will be conducted every two years.

[1] http://www.egovernment.tas.gov.au/standards_and_guidelines/tasmanian_government_information_security_framework

Principle 3: Store Records

- Records must be stored on appropriate media or hardware, and in appropriate formats
- Records must be stored in suitable containers, locations and systems
- The agency must implement storage management strategies including:
  - Disaster Management plans
  - Vital Records plans
  - Digital records management
- The agency must monitor records storage for environmental conditions appropriate to the media, and retention periods
- The agency must store and handle records according to their security status
- Where storage is outsourced, only approved secondary storage providers must be used by the agency.

Alignment with this principle will ensure that the agency has met their obligation under *the Archives Act 1983*, and ensure that:

- Records are stored in the most cost-effective manner possible and risks to records are minimised
- Records are protected, secure and accessible for as long as they are required to meet business and accountability needs and community expectations.
- Permanent value records are stored in the best possible conditions while in agency custody.

Records MUST be stored on appropriate media or hardware, and in appropriate formats
Media or hardware storage MUST be appropriate to the record format, retention period, security protection and storage capacity requirements. Equipment or technology dependant records SHOULD remain accessible for as long as they are required (e.g. audio-visual material and magnetic tapes). This may involve refreshing, converting or migrating stored records into different formats. Permanent records MUST be stored in the best possible conditions while in the custody of the agency to ensure their long-term preservation and access.

Records MUST be stored in suitable containers, locations and systems
Records in all formats are likely to deteriorate if they are not treated correctly, so records MUST be stored in suitable containers and locations. Suitable containers ensure that records are secure, accessible and protected from deterioration. Suitable locations are buildings and facilities which have controlled conditions for environmental, disaster and security reasons. Suitable systems are systems which meet minimum recordkeeping requirements. Records MUST also be stored so that they can be identified, located and retrieved easily. Agencies MUST meet requirements outlined in TAHO Guideline 11 - *Physical storage of State records (2005)*.

The agency MUST implement storage management strategies including:

- Disaster Management plans - Disaster management programs consider records storage so that risks to records are minimised and managed appropriately.

- Vital Records plan - The Vital Records plan MUST address records storage requirements to ensure the protection of those records.
- Digital records management - storage of digital records MUST be controlled and monitored according to Guideline 19 - *Digital preservation formats (2012)*

The agency MUST monitor records storage for environmental conditions appropriate to the media, and retention periods

Monitor temperature, humidity, air quality and light levels in records storage areas. Stored records SHOULD be monitored regularly for mould or pest infestation or any deterioration such as corrosion or physical damage. Digital records storage MUST additionally be monitored for any media decay and to regularly assess on-going viability of file formats and storage media or hardware.

The agency MUST store and handle records according to their security status

In a storage facility all records SHOULD be protected through controlled access to the storage areas, and through a secure physical environment. Access to records in storage SHOULD be restricted to authorised personnel only. Handling procedures SHOULD also be developed for records in transit to ensure they are secured and protected against unauthorised access, theft and other risks. Agencies MUST apply information security procedures to records storage. See the Office of eGovernment's *Tasmanian Government Information Security Manual*[2] for more about risks to information security.

Where storage is outsourced, only approved secondary storage providers MUST be used by the agency.

The agency MUST use only commercial storage providers currently certified as an approved secondary storage provider (ASSP). See Guideline 13 - *Certification for secondary storage providers*. Certified suppliers will be recorded on the TAHO website.

[2] http://www.egovernment.tas.gov.au/standards_and_guidelines/tasmanian_government_information_security_framework

Principle 4: Access Records

- Records access must be monitored for security breaches
- Access must be managed in accordance with:
  - Organisational security policy/model
  - Tasmanian Government Information Security Manual
  - Relevant legislation
  - Organisational change
- Records accessibility must be maintained during and after:
  - System migration
  - Government administrative change
  - Transfer of Custody
- Access to systems, and the records in them, must be maintained for the required retention periods
- Access provisions must be included in outsourcing documentation.

The Archives Act 1983 states that State records MUST be accessible while in agency custody. This includes if the agency has outsourced a function to a commercial provider or if the records are stored in the cloud. Alignment with this principle will mean that agency records and associated metadata can be easily located and retrieved for the required amount of time. Access to and movement of records MUST also be controlled and monitored to protect them from inappropriate use.

Records access MUST be monitored for security breaches.

Any security measures implemented to protect record storage areas and facilities MUST be monitored for unauthorised access. Any security breaches SHOULD be reported to relevant authorities.

Access MUST be managed in accordance with:

Organisational security policy/model

Security threats and breaches can affect the agency's ability to protect personal safety or privacy, to safeguard infrastructure or to comply with legal and other obligations. Applying security classification to records will help safeguard confidential government information. The policy should apply to all agency records, including records stored in cloud-based applications.

Tasmanian Government Information Security Manual

This 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, addressing the need for a consistent approach to managing access to sensitive and confidential information assets.

Relevant legislation

If access to information is specified in legislative and regulatory obligations, records MUST be managed in accordance with these requirements. For example, the Personal Information Protection (PIP) Act governs the management of personal information – its use, protection, retention, and accuracy.

Organisational change

The agency SHOULD manage and maintain accurate and up-to-date registers of authorised users. Access to records SHOULD not be assigned to specific people, but according to organisational roles and functions. If the agency undergoes restructure, access to records MUST be reassigned to appropriate personnel. This includes reassigning access to appropriate personnel to view permanent records held by TAHO. See Guideline 3 - *Managing records of State and local authorities being abolished or amalgamated (2005)* for more about managing records during administrative change.

Records accessibility **MUST** be maintained during and after:

System migration

Planning is required when moving records from one hardware/software configuration to another or from one generation of computer technology to a subsequent generation. The agency MUST ensure that access to records and required metadata is maintained during this process.

Government administrative change

The transfer of a function between Tasmanian agencies will involve the transfer of responsibility for State records relating to that function. This will help the receiving agency to manage the function effectively and with as little disruption as possible. This process may also involve the relocation of staff and records to different premises. Before the records can be transferred a Transfer of Custody authority may be required from the State Archivist.

Transfer of Custody

If the agency is responsible for a function that is to be transferred to another tier of government or being privatised, the management of the affected records MUST be considered. Before the records can be transferred, a Transfer of Custody or Transfer of Ownership authority may be required from the State Archivist, if custody arrangements for the records are not covered in the enabling legislation. For privatisation of government functions, agencies MUST meet requirements outlined in TAHO Guideline 14 - *Privatisation of government business: recordkeeping issues*.

Access to systems, and the records in them, MUST be maintained for the required retention periods

Agency systems and also the records and metadata in these systems MUST remain accessible for as long as they are required. Recordkeeping systems MUST protect records from unauthorised access, alteration, deletion or loss. Any conversion, export or migration of records MUST comply with the reproduction conditions set in Guidelines published by TAHO, such as Guideline 8 – *Digitisation and Disposal of Source Records*.

Permanent records MUST be maintained in a useable form for the benefit of present and future generations. As a minimum requirement, all permanent value records MUST be stored in a recordkeeping system. The onus is on the agency to manage access to records appropriately, during system upgrades, including meeting preservation requirements in Guideline 19 - *Digital preservation formats* to ensure access is maintained until they can be transferred to TAHO.

Access provisions MUST be included in outsourcing documentation.

Before outsourcing business functions the agency MUST consider records access as part of records management provisions. Any records management responsibilities that the agency has will extend to the records in the custody of the contractor. Any service level agreements with providers MUST cover the retrieval, handling and return of records. See Guideline 10 - *Outsourcing of government business: recordkeeping issues* for more guidance on outsourcing.

Principle 5: Dispose of Records

- Records disposal must be approved by the State Archivist
- The agency must develop and maintain an approved Retention and Disposal Schedule, covering all unique agency-specific functions
- Records destruction must be secure, documented and appropriate to the media
- The agency must have an active disposal program
- Custody of records must be appropriately managed during Government administrative change
- Disposal of source records must meet TAHO requirements
- The agency must not decommission or migrate business systems without consulting TAHO
- Permanent records must be retained in the agency for no longer than 25 years and then transferred to TAHO (unless an exemption has been granted by the State Archivist).

Alignment with this principle will mean that agencies are compliant with the *Archives Act 1983*, which stipulates that, unless the record has been lawfully destroyed, it MUST be delivered to the State Archivist to be readily available for public use or reference. Disposal, which includes both the destruction and transfer of records, applies to records in all formats. The prompt, secure and lawful disposal of non-current records is essential to support accountable and efficient records management.

Records disposal MUST be approved by the State Archivist

The *Archives Act 1983* stipulates that no government employee, or any other person, may dispose of records of any type without the written authority of the State Archivist. This can take the form of either:

- Implementing disposal actions identified in Disposal Schedules which have been authorised and issued by the State Archivist, or
- For records which are not covered by a Disposal Schedule, obtaining written authorisation from the State Archivist.

Disposal of agency records MUST meet requirements outlined in TAHO Guideline 2 - *Retention and disposal of State records*.

The agency MUST develop and maintain an approved retention and disposal schedule, covering all unique agency-specific functions

Agencies MUST develop a records Retention and Disposal Schedule for all records created in the process of undertaking agency business. This is a detailed inventory of the agency's unique functional records, identifying the appropriate disposal action based on regulatory, business and accountability requirements. This MUST be formally authorised by the State Archivist. This process is covered more fully in TAHO's *Guideline 6 - Developing a functional records disposal schedule*

Records destruction MUST be secure, documented and appropriate to the media

The destruction method chosen for records MUST be appropriate to the media and format of the record. It is the responsibility of the agency to ensure that the identified records are actually destroyed and that this process is confidential and secure.

The agency MUST have an active disposal program

Disposal of records SHOULD be supported in the design and implementation of any recordkeeping system. Records disposal MUST be planned, documented and routinely carried out. The agency's Register of Records Destroyed MUST be maintained for inspection by TAHO staff as part of scheduled Recordkeeping Audits. Records disposal decisions SHOULD be monitored and regularly reviewed.

Custody of records MUST be appropriately managed during Government administrative change

In the event of Government administrative change, agencies MUST ensure that any changes to the custody of records are appropriately managed with minimal disruption to business continuity and service delivery.

Disposal of source records MUST meet TAHO requirements

The destruction of source records after copying, conversion or migration is authorised by the State Archivist provided the records meet all requirements set by TAHO's Guideline 8 – *Digitisation and Disposal of Source Records*.

The agency MUST NOT decommission or migrate business systems without consulting TAHO

The agency MUST assess any ongoing business requirements for the information held in any business systems prior to decommissioning or migrating to a new system. The agency MUST consult TAHO to determine if the system contains permanent State records and decide on a suitable management/preservation/disposal strategy before decommissioning or shutting down the system.

Permanent records MUST be retained in the agency for no longer than 25 years and then transferred to TAHO (unless an exemption has been granted by the State Archivist).

State records retained in the agency for 25 years MUST be transferred to TAHO to be made available for public use or reference. An exemption from transfer may be obtained from the State Archivist for records more than 25 years old that are required for ongoing business.

The agency can require an access restriction when transferring records to TAHO as set out in Guideline 4 - *Agency determination of access restrictions*. Any access restrictions set out in the Transfer and Access Agreement MUST be approved by TAHO and signed by the relevant authority. Access cannot be made more restricted after this.

3 Definitions

Advice - issued by the State Archivist to agencies on current recordkeeping issues.

Agency - is used in this guideline to refer to all agencies, authorities, statutory offices, departments, councils and other organisations that are subject to, and defined in, the *Archives Act 1983*.

Appraisal - The process of evaluating business activities to determine which records need to be captured and how long the records need to be kept to meet business needs, organisational accountability requirements and community expectations.

Business analysis - Processes used in conjunction with stakeholder consultation which analyse the structure, policies and business operations of the agency in order to recommend actions or solutions to achieve agency goals.[3]

Business system - Business systems (e.g. e-commerce, client-relationship management, or finance systems, etc.) create or manage agency data to support business activities and typically do not have inbuilt recordkeeping functionality. Business systems are typified by containing dynamic data that is commonly subject to constant updates (timely), able to be transformed (manipulable) and holds current data (non-redundant).

Disposal - A range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of records in or from recordkeeping systems. They may also include the migration or transmission of records between recordkeeping systems, and the transfer of custody or ownership of records.

Guideline - a defined set of Standards for recommended practice, issued by the State Archivist, which agencies must comply with. It is the duty of the relevant authority to take all reasonable steps to ensure that the guidelines are complied with.

Metadata - Recordkeeping metadata is data that describes the context, content and structure of records and assists with the management of records over time. Metadata is attached to records when they are created, and added to as a result of processes such as sentencing and disposal.

Record - Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[4]

Recordkeeping system - A framework to capture, maintain and provide access to evidence of transactions over time, as required by the jurisdiction in which it is implemented, and in accordance with common business practices. Recordkeeping systems can be either in an electronic or paper form, and can include information systems, business systems or hardcopy files that meet the minimum recordkeeping requirements set by TAHO.

Relevant authority - The Secretary or head of a Government department or agency, or the person directly responsible to the Minister concerned for the administration and direction of that department, service; or body. It means, in relation to a State authority or a local authority that is incorporated, that authority; or in relation to a State authority or a local authority that is unincorporated, the secretary, clerk, or other principal executive officer of that authority.

Retention period - The period of time, usually based on an estimate of the frequency of current and future use, and taking into account statutory and regulatory provisions, that records need to be retained before their final disposal. Sometimes also used to indicate the length of time records are to be retained in offices before being transferred to secondary storage.

---

[3] [3]Adapted from A Guide to the Business Analysis Body of Knowledge® (BABOK® Guide), Version 2.0 International Institute of Business Analysis, Toronto, Ontario, Canada <http://www.iiba.org/babok-guide/babok-guide-online/appendix-a-glossary.aspx>
[4] Australian Standard AS ISO 15489 Records Management Part 1 Clause 3.15 Part 1: General. Standards Australia, Sydney

Sentence - The process of identifying and classifying records according to a retention and disposal authority and applying the disposal action specified in it.

Transfer - The process of changing the physical custody of archives, generally without changing the legal title of the material.

Vital Records - Records that are essential for the ongoing business of an agency, and without which the agency could not continue to function effectively.

4 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

- Standards Australia - HB 278-2009 Handbook: Recordkeeping compliance (2009)[5]
- Queensland Government Chief Information Office - Information Standard: Recordkeeping (IS40)[6]
- State Records NSW - Standard on full and accurate records (2004)[7]

[5] www.saiglobal.com
[6] https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2637-recordkeeping-toolbox

[7] http://www.records.nsw.gov.au/recordkeeping/rules/standards/standards

5 Checklist of minimum requirements

1. Create and Capture Records		Requirements	Evidence / Documentation
1.1	Records must meet legislative, regulatory and administrative requirements	• Legislative mapping	☐ List of legislation specific to agency in policy ☐ Legislative mapping of recordkeeping requirements
1.2	Records must be captured regardless of format	• Complete an Information Asset Register • Develop procedures for capturing all records formats into Agency Recordkeeping System	☐ Information Asset Register ☐ Documented procedures that cover capture of records in all formats, for example: o EDRMS o Business systems, o Email & messaging technologies, o Web records, o SharePoint, o Shared drives, o Portable devices, BYOD o Other records outside formal recordkeeping systems
1.3	Records must be appraised for their value	• Records staff undertake appraisal using functional and general Retention & Disposal Schedule (R&DS)	☐ Current functional R&DS OR ☐ Agency-specific R&DS

1. Create and Capture Records		Requirements	Evidence / Documentation
1.4	Records must be classified, and recordkeeping metadata must be applied	• Develop an agency-specific Business Classification Scheme or Taxonomy and implement in recordkeeping systems • Implemented agency-wide Recordkeeping System (e.g. EDRMS) which complies with minimum metadata standards • Develop agency-wide business rules and/or procedures for classifying and applying metadata to records	☐ Business Classification Scheme and/or Taxonomy and/or File Plan ☐ Technical documentation of EDRMS or other software application used for recordkeeping that shows metadata ☐ Published business rules and/or procedures for classifying and applying metadata to records

2. Govern Records		Requirements	Evidence / Documentation
2.1	Overall responsibility for records management must be assigned to a senior officer	• Senior officer's position description includes Records Management accountability	☐ Senior officer's position description (SOD) defines Records Management responsibilities
2.2	Direct responsibility for records management must be assigned to an appropriately skilled and resourced records officer(s)	• Records Officer has a position description which defines Records Management responsibilities • Records Officer has attended (at a minimum) the following TAHO training courses: o Records Management Introduction o Disposal Procedures	☐ Records Officer's position description (SOD) defines Records Management responsibilities ☐ Training attendance records
2.3	All management, staff, contractors, and volunteers must be responsible for their recordkeeping	• Defined and published business rules and/or procedures for recordkeeping • All position descriptions, volunteer roles statements and outsourcing documentations include recordkeeping responsibilities • Induction program for new staff and training for staff and volunteers when new processes and procedures are introduced. • Exit checklists or procedures when staff leave.	☐ Generic position description (SOD) and volunteer agreement which defines recordkeeping responsibilities ☐ Outsourcing agreements / contracts include recordkeeping responsibilities ☐ Procedure documents ☐ Staff Induction/Training program documentation ☐ Exit checklists/procedures

2. Govern Records		Requirements	Evidence / Documentation
2.4	The agency must have a Records Management program which includes: • Business analysis to inform the program • Records Management Policy • Records Management Procedures • Records Management Plans - Operational, Strategic, Vital Records, Disaster Management • Performance management for reporting • Risk analysis • Continuous improvement activities • Multiple sites and locations • Outsourced records	• Core business activities have been analysed (See Advice 17 - Implementing better records and information management) • Records Management Policy adopted at corporate level • Records Management Procedures • Records Management Plans - Operational, Strategic, Vital Records, Disaster Management • Performance management for reporting • Continuous improvement activities • Plans are reviewed periodically according to internal planning cycle • SWOT and other recordkeeping risk analysis conducted and recordkeeping risks are recorded • Regular reports on recordkeeping performance sent to appropriate managers • Performance agreements incorporate conformance with the organisation's recordkeeping policy • Records Management program applies across all sites and locations • Outsourcing includes recordkeeping requirements in accordance with Guideline 10 - Outsourcing of government business: recordkeeping issues.	☐ Records Management Program documentation ☐ Records Management Policy approved and adopted at corporate level ☐ Business Classification Scheme ☐ Functional R&DS ☐ Workflow mapping for automation ☐ Procedure documents ☐ Strategic Recordkeeping Implementation Plan (SRIP) endorsed by CEO ☐ Operational Recordkeeping Implementation Plan (ORIP) ☐ Vital Records Plan & Disaster Management Plan ☐ Records Management performance reporting ☐ Continuous improvement documentation (e.g. KPIs for service delivery, customer feedback systems, internal communications program) ☐ Up-to-date Information Risk Register/Information risks in Corporate Risk Register/Recordkeeping risk assessments ☐ Complete list (index or inventory) of all records in all locations ☐ Tender documents and

2. Govern Records		Requirements	Evidence / Documentation
2.5	The agency's Records Management program must align with: • The agency's Risk Management program • Internal and External Audit and review • Disaster Recovery and Business Continuity planning • Tasmanian Government Information Security Manual	• Recordkeeping and information risk is recorded in the Corporate Strategic Risk Register • Key compliance requirements are tracked and improvements measured over time via internal and/or external audit processes • Corporate information and recordkeeping risks are included in Disaster Preparedness and Business Continuity Plans (See Advice 26 - Disaster Preparedness and Recovery) • Implement Tasmanian Government Information Security Classification (see Advice 32 - Implementing information security for Information Managers)	☐ Corporate Risk Register ☐ Audit review process/procedure ☐ Sample audit documents ☐ Disaster Preparedness/Recovery Plan ☐ Business Continuity Plan ☐ Information Security Policy

3. Store Records		Requirements	Evidence / Documentation
3.1	Records must be stored on appropriate media or hardware, and in appropriate formats	• Defined and published business rules and/or procedures for storing records • Records media and hardware storage is included in Records Management program • Formats and media are regularly inspected for signs of deterioration	☐ Permanent records migration plan/strategy which covers hardcopy and digital records ☐ Digital records preservation/ continuity plan
3.2	Records must be stored in suitable containers, locations and systems	• Records storage is included in Records Management program • Records storage is compliant against Guideline 11 - Physical Storage of State records	☐ Digital records preservation/continuity plan (e.g. file formats are monitored for obsolescence) ☐ Site inspection
3.3	The agency must implement storage management strategies	• Disaster Management plans include records storage • Vital Records plans address records storage • Digital records storage is compliant with Guideline 19 - Digital preservation formats	☐ Disaster Management plan ☐ Vital Records plan ☐ Digital records preservation / continuity plans
3.4	The agency must monitor records storage for environmental conditions appropriate to the media, and retention periods	• Regular checks for mould and pest infestations • Fire and other disaster monitoring • Monitor storage as per requirements outlined in Guideline 11 - Physical Storage of State records	☐ Site inspection

3. Store Records		Requirements	Evidence / Documentation
3.5	The agency must store and handle records according to their security status	• Storage facilities must be secure and accessed only by authorised personnel • Procedures for handling should consider security protection • Implement Tasmanian Government Information Security Manual	☐ EDRMS security model/ reporting or EDRMS user access matrix ☐ Sign-out process for hardcopy files ☐ Appropriate use policy/procedures for storage ☐ Confidentiality agreements
3.6	Where storage is outsourced, only approved secondary storage providers must be used by the agency	• Only approved secondary storage providers featured on the IPSU website are used for storing agency records	☐ Storage outsourcing contracts and documentation

4. Access Records		Requirements	Evidence / Documentation
4.1	Records access must be monitored for security breaches	• Security measures must be monitored and security breaches reported to relevant authorities	☐ System monitoring practices (verbal evidence) ☐ EDRMS security audit module/reporting ☐ Documented sign-out process for hardcopy files ☐ Procedure for handling and providing access by the public to agency information
4.2	Access must be managed in accordance with: • Organisational security policy/model • Tasmanian Government Information Security Manual • Relevant legislation • Organisational change	• Organisational security classification policy/model is applied to all records including cloud-based applications (Advice 44 - *Cloud Computing Information Security Considerations*) • Tasmanian Government Information Security Manual is implemented • Access to records is in accordance with Privacy legislation, for example • Access to records is managed during and after organisational change	☐ Cloud-based application risk assessments ☐ Tasmanian Government Information Security Policy mandate/alignment ☐ Appropriate use policy, and access procedures for public/external agencies •

4. Access Records		Requirements	Evidence / Documentation
4.3	Records accessibility must be maintained during and after: • System migration • Government administrative change • Transfer of Custody	• All system migrations maintain access to records and metadata • Access to records is maintained during and after administrative changes in Government • Transfer of Custody arrangements comply with Guidelines set by TAHO for access	☐ Procedures for accessing records during system upgrades, media refreshes, migration (e.g. duplicate data prior to commencing migration, access to records during cutover, limit access to new system until QA processes complete) ☐ List of records transferred ☐ Procedures for custody and management of hardcopy and digital legacy records during Government administrative change
4.4	Access to systems, and the records in them, must be maintained for the required retention periods	• Migration and reproduction of records must comply with Guideline 8 - Management of source records that have been copied, converted or migrated • Permanent records must be maintained in recordkeeping systems until they are transferred to TAHO in accordance with Guideline 19 - Digital Recordkeeping Formats	☐ Permanent records migration plan/strategy which covers hardcopy and digital records ☐ Digital records preservation/continuity plan
4.5	Access provisions must be included in outsourcing documentation.	• Access to records must be included in contracts or service level agreements as required in Guideline 10 -Outsourcing of government business: recordkeeping issues	☐ Storage outsourcing contracts and documentation

5. Dispose of Records		Requirements	Evidence / Documentation
5.1	Records disposal must be approved by the State Archivist	• Disposal of records meets Guideline 2 (Records retention and disposal) requirements	☐ Current functional R&DS ☐ One-off Disposal Authority
5.2	The agency must develop and maintain an approved retention and disposal schedule, covering all unique agency-specific functions	• Develop an agency-specific Retention & Disposal Schedule	☐ Agency-specific R&DS
5.3	Records destruction must be secure, documented and appropriate to the media	• Destruction must be confidential and secure • Digital records must be destroyed using secure and appropriate processes	☐ Destruction certificates
5.4	The agency must have an active disposal program	• Disposal of records should be planned and routinely carried out • The Register of Records Destroyed must be maintained for inspection by TAHO	☐ Register of Records Destroyed ☐ Screenshot or visual evidence of disposal class on record/file in EDRMS ☐ Records policy/ procedures for disposal
5.5	Custody of records must be appropriately managed during Government administrative change	• Notification and lists of records to be destroyed or transferred should be sent to the State Archivist	☐ Procedures for management of hardcopy and digital legacy records during Government administrative change ☐ List of records transferred

5. Dispose of Records		Requirements	Evidence / Documentation
5.6	Disposal of source records must meet TAHO requirements	• Reproductions of records must comply with Guideline 8 (Source records) before destruction can be carried out	☐ Scanning procedures (separate Permanent and Temporary) ☐ Screenshot or visual evidence of scan settings ☐ If scanning was outsourced, requirements in documentation
5.7	The agency must not decommission or migrate business systems without consulting TAHO	• Develop a suitable management strategy for the records before turning off legacy systems	☐ List that shows legacy business systems ☐ Completed checklist from Advice 18 - Managing Records in Business Systems ☐ Decommissioning procedures include TAHO consultation
5.8	Permanent records must be retained in the agency for no longer than 25 years and then transferred to TAHO (unless exempted).	• Exemptions from transfer may be obtained from the State Archivist for records more than 25 years old that are required for ongoing business	☐ Transfer procedures for permanent records or exemption documentation

Appendix A - TAHO Guidelines and Advice mapped to the Principles

TAHO Guidelines and Advice are intended to act as a framework for all aspects of creating, managing, and disposing of state records. The table below maps all of TAHO's Guidelines and Advices to the Records Management Principles in this Guideline to assist agencies to implement the Principles and prepare for recordkeeping audits.

<table>
<tr><th colspan="2">1. Create and Capture Records</th></tr>
<tr><td rowspan="2">Records must meet legislative, regulatory and administrative requirements
Records must be captured regardless of format
Records must be appraised for their value
Records must be classified, and recordkeeping metadata must be applied</td><td>Guidelines
Guideline 7 - Managing electronic communications as records
Guideline 15 - Recordkeeping strategies for websites and web pages
Guideline 18 - Managing Social Media Records</td></tr>
<tr><td>Advice
Advice 2 – All About Appraisal
Advice 4 - Managing electronic communications as records
Advice 6 – Information Classification tools
Advice 7 - Information rights management
Advice 14 - Recordkeeping metadata standard
Advice 18 - Managing records within business systems
Advice 21 – Plan before you Scan
Advice 22 - Records management using SharePoint - Considerations
Advice 27 - Managing email
Advice 30 - Digitisation dilemmas
Advice 31 - Managing Records of Projects
Advice 36 - Legislative Mapping for Information Managers
Advice 39 - Developing an Information Asset Register
Advice 56 - Digital Record keeping on a Shoestring
Advice 58 - Managing your agency's photographs
Advice 66 - Classification Scheme Considerations</td></tr>
<tr><th colspan="2">2. Govern Records</th></tr>
</table>

- Records Management and recordkeeping responsibilities must be assigned
- The agency must analyse their business activities to inform the Records Management program
- The agency must have a Records Management program, which includes:
    - Business analysis to inform the program
    - Records Management Policy
    - Records Management Procedures
    - Records Management Plans - Operational, Strategic, Vital Records, Disaster Management
    - Performance management for reporting
    - Risk analysis
    - Continuous improvement activities
    - Multiple sites and locations
    - Outsourced records
- The agency's Records Management program must align with:
    - The agency's Records Management program must align with:
    - The agency's Risk Management program
    - Internal and External Audit and review
    - Disaster Recovery and Business

Guidelines

Guideline 1 - *Records Management Principles: Overview* (this Guideline)
Guideline 3 - *Managing records of State and local authorities being abolished or amalgamated*
Guideline 5 - *Certification of copies of State archives*
Guideline 10 - *Outsourcing of government business: recordkeeping issues*
Guideline 14 - *Privatisation of government business: recordkeeping issues*
Guideline 17 - *Managing the recordkeeping risks associated with cloud computing*
Guideline 22 - *Collaborative workspaces*
Guideline 25 - *Risk Management*

Advice

Advice 1 - *Government employees responsibilities in relation to State records*
Advice 5 - *Australian Standard AS ISO 15489 - Records Management*
Advice 16 - *Legal acceptance of records*
Advice 20 - *Change management issues in EDRMS implementation*
Advice 26 - *Disaster Preparedness and Recovery*
Advice 32 - *Implementing Information Security for Information Managers*
Advice 38 - *Information Custodians and Digital Continuity*
Advice 40 - *The Role of an Information Asset Owner*
Advice 49 - *Recordkeeping for Local Government Councillors*
Advice 50 - *Developing an Information Management Policy*
Advice 54 - *Records Management toolkit for Local Government*
Advice 55 - *Change Management - Preparing for Change*
Advice 61 - *How to review your records holdings*
Advice 65 - *What to do if your Agency is Closed or Privatised*

Continuity planning ▪ Tasmanian Government Information Security Manual	
3. Store Records	
• Records must be stored on appropriate media or hardware, and in appropriate formats • Records must be stored in suitable containers and locations • The agency must implement storage management strategies including: o Disaster Management plans o Vital Records plans o Digital records management • The agency must monitor records storage for environmental conditions appropriate to the media, and retention periods • The agency must store and handle records according to their security status • Where storage is outsourced, only approved secondary storage providers must be used by the agency.	**Guidelines** Guideline 11 - *Physical storage of State records* Guideline 13 - *Certification for secondary storage providers* Guideline 19 - *Digital preservation formats* Guideline 23 - *Certification for Places of Deposit of State archives* **Advice** Advice 3 - *Day batching of source records* Advice 8 - *Microfilm reproductions of State records* Advice 24 - *How to manage 3 1/2 and 5 1/4 inch discs* Advice 25 - *Management of backups* Advice 41 - *Managing records on shared network drives* Advice 42 - *Structuring shared network drives for recordkeeping* Advice 46 - *Treating records with mould* Advice 52 - *Identifying and Managing Vital Records*
4. Access Records	

<table>
<tr>
<td>

- Records access must be monitored for security breaches
- Access must be managed in accordance with:
  - Organisational security policy/model
  - Tasmanian Government Information Security manual
  - Relevant legislation
  - Organisational change
- Records accessibility must be maintained during and after:
  - System migration
  - Government administrative change
  - Transfer of Custody
- Access to systems, and the records in them, must be maintained for the required retention periods
- Access provisions must be included in outsourcing documentation.

</td>
<td>

Guidelines

Guideline 4 - *Agency determination of access restrictions*
Guideline 12 - *Short term retrieval of State archives*
Guideline 16 - *Managing inter-agency transfer of personnel records*
Guideline 20 - *Records required for legal proceedings - Implications for Tasmanian Government Agencies*

Advice

Advice 11 - *Short term retrieval of State records*
Advice 15 - *Transfer and provision of access to Cabinet records*
Advice 23 - *Government agencies using records in the History Room*
Advice 33 - *Implementing Information Security Classification - Part 1: Overview*
Advice 34 - *Implementing information security classification in EDRMS*
Advice 35 - *Implementing Information Security - Part 1: A Step by Step Approach to your Agency Project*
Advice 37 - *Keeping Digital Records Accessible*
Advice 44 - *Cloud Computing Information Security Considerations*
Advice 62 - *Help We're Moving*

</td>
</tr>
<tr>
<td colspan="2">

5. Dispose of Records

</td>
</tr>
</table>

• Records disposal must be approved by the State Archivist • The agency must develop and maintain an approved Retention and Disposal Schedule, covering all unique agency-specific functions • Records destruction must be secure, documented and appropriate to the media • The agency must have an active disposal program • Custody of records must be appropriately managed during Government administrative change • Disposal of source records must meet TAHO requirements • The agency must not decommission or migrate business systems without consulting TAHO • Permanent records must be retained in the agency for no longer than 25 years and then transferred to TAHO (unless an exemption has been granted by the State Archivist).	**Guidelines** Guideline 2 - *Retention and disposal of State records* Guideline 6 - *Developing a functional records disposal schedule* Guideline 8 – *Digitisation and Disposal of Source Records* Guideline 9 - *Managing Ministerial records* Guideline 21 - *Approved destruction methods for State records* **Advice** Advice 9 - *Disposal of scheduled records* Advice 10 - *Disposal of un-scheduled records* Advice 12 - *Preparing hard copy records for transfer to the Tasmanian Archive & Heritage Office (TAHO)* Advice 13 - *Writing disposal classes* Advice 28 - *Getting started on the development of an agency functional disposal schedule* Advice 29 - *Advice for Agencies on Managing Legacy Records* Advice 63 - *Part 1 - Management of Records during Administrative Change Handbook* *Part 2 - Government Administrative Change Advice for Senior Management*