TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 54 Records management Toolkit for Local Government

FACT SHEET 3 - Basic Records Management - Access management

Introduction

This Fact Sheet is part of a sub-set of Advice 54, and focuses on the operational procedures of a records management program. Some templates are provided to assist agencies to establish and implement recordkeeping controls and procedures. Agencies with very small records operations, those who do not have dedicated RM resources, and those who have not yet implemented specialised EDRMS software, may find these Fact Sheets particularly beneficial.

Records program operations

Daily operations are the basis for the development of a procedure manual for the records team. This promotes consistency of process, and information sharing, in the event of new staff, volunteers or contractors. Procedure manuals should be regularly reviewed and updated as required to allow for organisational and procedural change. Whether paper or electronic recordkeeping systems are in place, key functions include:

- Record identification
- Record capture
- Registration
- Indexing
- Classification
- File creation and closure
- Distribution & tracking
- Search & retrieval
- Access
- Security
- Storage
- Scheduling, retention & disposal
- Records transfer
- e-discovery & Disposal Freezes
- Vital Records
- Disaster Management
- QA & Auditing
- Monitoring (program, processes and people) & reporting on activities, performance and compliance
- Resourcing

Tools you may need

If your system is paper-based consider:

- Stationery (pencils, markers, paperclips, file ties etc)
- File register (spreadsheet or book)
- Lockable cabinets & key register
- Security register/control document

If your system is electronic or hybrid consider:

- Stationery (pencils, markers, paperclips, file ties, etc)
- Appropriate permissions to manage security within the electronic system
- Security register/control document

Access

Accessibility is an important part of records management and directly impacts business productivity, through use/re-use of information for business decision-making. Records management protocols manage records across the business, helping to avoid data silos and 'lost' information.

Development and implementation of effective record keeping tools whether registers, indexing, keywords, metadata or other control mechanisms, assists records and general staff to identify, locate and retrieve records for later use. This is true of both electronic and paper-based systems, and for this reason, meticulous management of these tools play an important part in the effectiveness of a records management program.

Agencies should develop and document procedures around how access is provided to staff, whether a 'self-help' model applies to an EDRMS system that manages access permissions electronically, or the provision of a 'helpdesk' type service where records staff retrieve hard copy file requests for business units and individuals. These may either be collected from the records section counter, or a set daily delivery time introduced for non-urgent requests.

It is also important that the records control system indicates what level of access restriction applies to the file. This is easy to apply in an electronic records management system where user logon profiles can be used to indicate what access rights they have, and the process of restricting access to electronic records where necessary can be automated.

With a paper-based filing system, files to which access is restricted must be kept securely, e.g. in a safe, locked filing cabinet or room. Note the level of restriction clearly on the file cover. Hand delivery or collection by authorised personnel should be mandated, and restricted files should not be left unattended on desks, or in collection trays as part of the routine delivery run. The location of storage facilities should not impede retrieval requirements.

Managing access to records also includes developing protocols around public access, in the event a customer requests access to information managed by Council, for example ratepayers and animal owners; or a request by a government agency. Access policy in relation to records is also regulated by legislation, including the *Right to Information Act 2009*, and the *Personal Information Protection Act 2004*, and must be developed in accordance with these requirements. Procedures governing external access should be developed which may include:

- Viewing identification to verify clients are who they claim to be

- Asking clients to record name, who they represent, purpose of visit, etc in a Visitors Book on a given day
- Requiring the completion of a request form so there is a documentation of who was issued with what information on a given day. This should include a signature, and a copy provided to the client
- Ensuring access is provided under supervision in a designated area or room to prevent misuse, damage/destruction, removal or unauthorised copying.
- Checking returned documents and returning them promptly to the records storage area

Note this does not include formal requests for information under the *Right to Information Act 2009*, for which separate policy/procedures should be developed.

Security

All records require a basic level of security to ensure their authenticity and integrity, and to prevent improper use. Policy and procedures should dictate the importance of security within facilities and storage areas, the responsibilities of staff and contractors, and access controls. There should be clear protocols around the appropriate use and handling of agency records and information, processes for reporting damage or breaches, and confidentiality clauses included where relevant in Position Descriptions.

Development of an Information asset register assists in planning the implementation of information security across all information assets in an agency in order to ensure consistent application across information and records systems (see TAHO *Advice 39 Developing an Information Asset Register* for further information on developing a register). Records identified as containing critical, sensitive or in-confidence material, should be handled, stored and protected according to these security classifications.

Security measures relate to classifications, permissions and authorisations – who can access what – but also what they are authorised to do with it once they have access. This is particularly relevant in an electronic environment where various security profiles and rights may be available, from "read only", through to "edit", "print", "distribute" etc.

When using electronic recordkeeping systems, profile and role based security models should be leveraged, with an individual associated with a role, and a role associated to a profile. The profile has the security permissions associated with it, and by default, these permissions filters through to the individual log on. This is much more flexible than traditional methods of maintaining security permissions through individual user profiles, and allows for straightforward transitions when staff commence or resign, act in other positions, etc. Permissions can also be applied to groups, with members of the group inheriting permissions by virtue of being joined.

Records must also be protected against theft. Security measures extend to building and facilities management and physical environments – where the records are housed, and who has access. It is recommended that file rooms and information storage areas are restricted to access by authorised records personnel, ideally using monitored electronic access systems, or locks. Employees, public and other individuals should not be permitted free access to areas housing files and corporate information, and retrieval of information should only be undertaken by staff authorised to be in the storage area. Visitors should be supervised, including contractors undertaking routine maintenance work. This is critical with sensitive, in confidence, or other restricted information, which should be housed in secured locations, and accessible only by authorised staff. For small agencies, this may be able to be managed to some degree with the use of lockable fireproof cabinets (key or pin code access), however it is recommended strong rooms or vaults (where available) are used to store an agencies vital records and those deemed highly confidential.

Records about security measures should be kept including storage plans and assessment reports; access monitoring and logs; incident reports, and procedures which detail appropriate handling and storage of information under different security classifications. For more information, see TAHO *Advice 34 Implementing Information security classification in EDRMS.*

Storage

Section 10 of the *Archives Act 1983*, requires agencies to preserve State records until they are dealt with by the Act. *State Records Guideline 11 - Physical Storage of State records* states clear minimum requirements for the physical storage of records. It aims to ensure:

- storage is cost-effective and efficient
- records are secure, protected and accessible for as long as they are required to meet business and accountability needs, and that\
- records of permanent value which will be transferred to TAHO as State records are stored in the best conditions possible.

In particular, agencies are encouraged to use the minimum requirement checklist provided in *Guideline 11* to assess their current level of risk and areas for improvement.

In practical terms, records should be adequately described and listed before they are stored. Location documentation, including box lists, shelf numbers, etc must be maintained so that records can be found promptly when required. With regard to physical hard copy records, inactive records may require 'secondary storage' areas that may be managed in-house, or outsourced to an Approved Secondary Storage Provider (ASSP). ASSPs meet TAHOs criteria for appropriate records storage, including protection/security measures and insurances. See State Records *Guideline 13 Certification for Secondary Storage Providers* for more information.

In order to assist in the prevention of deterioration or damage to records, establish safe handling practices. (This may be undertaken in conjunction with the development of manual handling procedures for records personnel, after a risk assessment of the records management function and tasks. See Fact Sheet 5 for further information on risk). Steps should be taken to promote the correct handling, use and transport of records. The following should be forbidden in or near records and records storage areas:

- Smoking
- Eating
- Drinking

Records in transit should be secured and protected against weather, light, pollution, unauthorised access, and theft. For example, records should be transported in enclosed and secure vehicles, and loading/unloading should be carried out in covered areas by authorised personnel.

Agencies must also ensure that equipment or technology-dependant records remain accessible for as long as they are required, either for business use, or storage prior to transfer as State archives. Strategies may involve conversion or migration (whether to alternate formats or systems), if a system has been decommissioned/is no longer supported, or if frequent use/fragility demands.

Should damaged records require repair outside of the scope of agency Disaster Recovery manuals, TAHO can assist with advice and access to professional conservation staff. (Refer also TAHO *Advice 26 Disaster Preparedness and Recovery*).

Recommended Reading

State Records *Guideline 11 – Physical Storage of State Records*

State Records *Guideline 13 – Certification of Secondary Storage providers*

State Records *Guideline 19 – Digital preservation formats*

TAHO *Advice 7 – Information Rights Management*

TAHO *Advice 11 – Short term retrieval of State Records*

TAHO *Advice 37 – Keeping Digital Records accessible*

TAHO *Advice 39 – Developing an Information Asset Register*

TAHO *Advice 46 – Treating records with Mould*

NAA - Standard for the storage of archival records. [1]

Appendices:

Template - Offsite storage policy (Appendix 1)

Template - Internal Storage request form (Appendix 2)

[1] http://www.naa.gov.au/Images/standard_tcm16-47305.pdf

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

- National Archives of Australia *Standard for the Physical Storage of Commonwealth Records*
- Australian Standard AS ISO 15489.1 & Guidelines 15489.2 [2]
- NSW State Records Guideline 11 – *Solutions for Storage*. [3]

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	May 2015	Christine Woods	Template	All
1.0	March 2014	Sam Foster-Davies	Initial Release	All

Amendments in this Release

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

[2] http://www.saiglobal.com/Standards/
[3] http://www.records.nsw.gov.au/recordkeeping/advice/storage-and-preservation/solutions-for-storage/solutions-for-storage

Issued: June 2014

Ross Latham
State Archivist

Appendix 1 – Sample Policy

OFFSITE STORAGE OF CORPORATE RECORDS

Policy Manual Number <REPLACE WITH POLICY MANUAL NO>

Council Minutes Ref: <REPLACE WITH REF AFTER COMMITTEE MEETING>
File Ref: Corporate Policies
Author:
Department:

Background

The *Archives Act 1983* outlines legislative requirements in relation to the storage of corporate information. The Records program within [business unit name] ensures that [agency name] complies with these legislative requirements, including specific guidelines from the Tasmanian Archives and Heritage Office (TAHO) with regards to what constitutes "appropriate storage". Records staff will allocate appropriate retention periods to council information and records in accordance with the Disposal Schedule [for functional records of agency name (DAXXXX)]. The allocation of the schedule reference determines the timeframe that the information is required to be stored prior to either secure destruction, or transferred to TAHO as a State archive.

Historically, departments often transferred records for storage to [agency name] owned sites such as [enter examples]. The Records area has assumed control of these unapproved secondary storage areas and has been systematically transferring residual off-site storage to [agency name]'s approved storage provider. To avoid the potential for information loss, and to ensure compliance with record keeping standards, Records staff should be notified in the first instance if departments require transfer of corporate information and records to off-site storage.

The process of preparing information for transfer can be quite resource intensive due to the requirement for sentencing in preparation for eventual archiving/destruction, and formatting of information in order to ensure timely identification and retrieval. For this reason the Records program has prepared a template for departmental staff to complete when requesting transfer of items to secondary storage. This template also assists Records staff to subsequently locate and retrieve items from secondary storage as required.

Policy Statement

All corporate records/information requiring transfer to secondary storage will be submitted to the Records program for review prior to transfer, in accordance with the following procedure.

Procedure for processing records for transfer to secondary storage.

1. Contact Records to advise of requirement for secondary storage. Arrange a time for Records staff to view information and determine the status of the information in accordance with the disposal schedule, ie. Temporary value, whether suitable for immediate secure destruction, etc.
2. Box in approved storage cartons in accordance with packing instructions, and prepare contents listing on approved storage spreadsheet template (sourced from Records).

3. Once information is adequately prepared and template completed, Records staff will sentence accordingly, and make arrangements for the collection and ongoing secure storage of this information.
4. Provide account number for item lodgement, secondary storage charges, retrievals, etc (new users only).

If information is not prepared for storage appropriately, Records staff will advise of any discrepancies to assist with the suitable preparation of the information to aid in future identification and retrieval. From time to time, Records staff will circulate destruction listings produced by the secondary storage provider, in order to arrange for secure destruction of [agency name] records that have surpassed their legislated storage requirements, and minimise unnecessary storage costs to departments.

Should an officer require a retrieval of information that has been sent offsite, an email to the Records group clearly identifying the information sought will assist the Records team to initiate a retrieval request.

References:

State Records *Guideline 11 Physical Storage of State Records*

State Records *Guideline 13 Certification for secondary storage providers*

The *Archives Act 1983*[4]

Archives Regulations 2004[5]

[4]http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=ALL;doc_id=76++1983+AT@EN+20050519150000;histon=;prompt=;rec=;term=archives%20act
[5]http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=+86+2004+AT@EN+20050104120000;histon=;prompt=;rec=;term=

Appendix 2 – Internal Storage request template

Start Date	End Date	Description	File No*	Vol*	Temp Box No	Box type	Retention Code	Period	Archive / Destruction Due	Storage Provider ref no	Responsible Business Unit/owner

Columns with **black** text headings for officers to complete - columns with **red** text headings for Records staff to complete.
*If applicable fields - otherwise leave blank