TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 41 Managing Records on Shared Network Drives

Introduction

If your agency does not have an electronic record document management system (EDRMS), and is not planning to implement one, then this advice will help you by explaining:

- ***The value of managing your shared drives well***
- ***How to improve the management of shared drives for better access to information and more efficient use of ICT resources***
- ***How to ensure that your organisation's recordkeeping requirements are met.***

What are shared drives?

Shared drives, also known as network drives, are used by many organisations to store electronic information, including Word documents, Excel spreadsheets, PowerPoint slides, digital photos, PDF documents and database reports.

Are shared drives recordkeeping systems?

No. While they have a number of business advantages, shared drives are not suitable as recordkeeping systems. While some security measures can be added, most information on shared drives can be easily edited or deleted and there are no audit trails to indicate who has made modifications. Property fields are rarely populated with metadata and there are no contextual links between documents and their business context. As their authenticity can be compromised, records stored on shared drives cannot adequately function as evidence. This causes problems for the agency, including:

- Difficulty finding and retrieving information that is known to exist
- Difficulty authenticating State records
- Documents not providing reliable evidence of actions
- Lack of recordkeeping functionality, for instance:
    - Auditing controls;
    - Security controls able to match whole of Government guidelines; and
    - Retention and disposal rules.

When documents and other information kept on shared drives have been finalised, issued, sent or have otherwise taken part in official business transactions, they should be captured into corporate recordkeeping systems (EDRMS). If agencies do not have an EDRMS then they must introduce some rigor into the use of shared drives by improving their use (see tips below) and by defining business rules for the use of share drives in the agency information management policy.

> **Tip:** in many cases, documents will be emailed as part of business transactions, making the capture of the email with attachments the most sensible option for keeping the records. Otherwise, documents and other information types used for official business should be captured individually if they are needed as evidence of the business being performed.

Organisational recordkeeping policy and business rules should direct staff on when and how to save documents as records

Other problems with shared drives

- Shared drives have often evolved informally with little planning or structure. As a result, directory folders and documents may be poorly organised and titled. In an environment where records are supposed to be shared with a number of users, this lack of rigour will inevitably cause difficulty in locating, retrieving and using information and in managing versions. It also makes it difficult to assign security restrictions to certain parts of the business that may be more sensitive.
- Users of shared drives often do not usually perform regular 'housekeeping' of their shared drives. For example, information accumulates and is rarely deleted, leading to volumes of storage that are costly for the organisation to maintain. Excessive volumes of storage on the drive also contribute to the inability to find and use relevant information.
- Users will often leave the organisation without 'cleaning up' their documents on shared drives, and it is difficult for others to determine what is of value and what has or has not been saved to corporate recordkeeping systems.

How to improve the use of shared drives

There are a number of ways the organisation can improve the management of shared drives. *Advice 42: Structuring Shared Network Drives for Recordkeeping* describes how to structure shared drives. The following strategies will assist in managing the shared drives:

- Consider shared drives as part of your information management strategic framework and include them in your Records management policy
- Have clear policy and procedures for staff regarding the use of shared drives and saving records to corporate recordkeeping systems
- Create (or facilitate the creation of) logical hierarchical structures for information in shared drives. It may be suitable to align the folder titles to the organisation's business classification scheme if there is one that is accepted in the workplace. Structures should be workshopped and piloted within the group. Structures should be flexible and be altered as the business changes. See *Advice 42: Structuring Shared Network Drives for Recordkeeping*

> **Tip:** If an XSL style sheet has been used to produce the organisation's retention and disposal authority, a batch file can be generated to automatically create the same structure in shared drives. See Creating custom XSL style sheets for more information[1]

[1] https://github.com/srnsw/ae/wiki/Creating-custom-XSL-stylesheets

- Define document naming conventions that are easy to use and can be adopted by all staff.

Tip: the Tasmanian Government Communications office has developed MS Office templates for common business formats (such as memos, faxes etc.) and most Tasmanian government agencies have further developed other templates (e.g. agency letterhead), which can be used by staff. These automatically capture a sensible file 'save as' name based on document content. It takes information from bookmarked fields, processes it, and suggests a filename, and also saves metadata into the document properties. The templates are available for anyone in Tasmanian Government to use, and can be downloaded[2] or specific Agency templates may be available from your Agency's intranet.

- Establish suitable restrictions and controls for workgroups or folders within shared drives. Consider controls to prevent the unauthorised creation of top or mid-level folders, while allowing more freedom at lower levels.
- Consider whether some folders containing sensitive information may need to be removed from shared drives or secured and hidden from view except to those groups who have the correct levels of authorisation.
- Advise staff regarding security needs for documents they create that may be sensitive.
- Create and implement standard templates which include footers that provide the document name and file path (they are also valuable for capturing essential metadata).
- Assign responsibility for the management of the folder structures in shared drives.

For example, in some organisations it may be suitable for a records or information manager to be responsible for structuring and maintaining organisation-wide shared drives with administrators within each workgroup managing workgroup folders.

- Provide training and assistance for staff with responsibility for structuring or managing folders and for users. Consider change management initiatives that will promote compliance.
- Establish procedures and controls and assign responsibility for managing the deletion of information and records from shared drives. These could include security controls to prevent deletion, reference to your organisation's guidelines regarding what can be routinely deleted and the inclusion of responsibilities in HR exit procedures for staff.
- Deletion of records is 'disposal' and must be recorded in your agency's Register of Records Destroyed. A recommended template for a Register of Records Destroyed can be found on the website
- Set up a transition arrangement for moving from old directory structures or files to the new structure. This might involve, for example, freezing use of the old structure, leaving shortcuts pointing to the new location and gradually moving files into the new structure.
- Audit shared drives regularly to ensure procedures are followed.

[2] http://www.communications.tas.gov.au/templates

Managing existing or legacy data in shared drives

Organisations will need to establish a strategy for dealing with existing unstructured or poorly managed data that is already residing in shared drives.

For example, when new structures are established, staff should be encouraged to:

- Capture records to corporate recordkeeping systems as required if they have not already done so (whether this means printing and filing or capturing digitally)
- Delete unimportant information in accordance with the organisation's guidelines
- Move any documents they are still working on to the new structure.

Records or business unit managers will need to monitor shared drives to ensure that staff are saving records correctly. This may involve speaking to relevant staff in business areas and reviewing drives and what has been captured into recordkeeping systems.

If unstructured or poorly structured shared drives are to be closed off, they should be saved for reference purposes for a period of time prior to deleting them. Set a timeframe for this and make staff aware of it.

If there is an overwhelming volume of information in older shared drives that is legacy information that no one in the organisation is familiar with and it cannot be confidently assumed that records have been saved to corporate recordkeeping systems, it may not be viable to sort them. In this case, organisations may make a risk based decision to close off the shared drive and save the entire drive. The drive will need to be migrated and kept accessible until the retention of all the records likely to be contained in it has expired.

There should be clear and enforced procedures for staff to use new directory structures and guidelines so that this situation does not reoccur.

Sample Procedures for Managing Shared Drives

To manage the network drives, you must firstly establish ownership of content on the drives (see *Advice 39 Developing an Information Asset Register* pg 8 'Information Custodianship' for more information).

TAHO has prepared sample procedures for staff on managing shared drives (see the TAHO website). These are designed to be circulated to staff members of an agency to help them manage their shared drives. Before circulating, Records Managers, in liaison with ICT professionals and business unit managers, should modify the sample procedures so that they are in line with internal business practices and the agency's particular infrastructure and information strategy.

Examples of modifications include:

- A list of the types of shared drives in use in the organisation and their purpose
- Particular details about the business classification scheme or thesaurus to be used in shared drives
- Information on when and how acronyms can be used
- More information about folder administrators' responsibilities
- Organisation-specific examples and links to procedures or guidance
- Advice about infrastructure requirements e.g. size of personal drives, access restrictions or security measures (e.g. password protection)
- Information about particular corporate recordkeeping systems to be used and links to guidance on how to save to them

- Authorisation and high level support for the guidance from a senior manager (in line with organisational procedures)

See TAHO Advice and Guidelines on our website for further guidance on managing digital records.

Other collaboration tools

Many organisations are now using other document sharing/collaboration tools, such as SharePoint. This guidance does not address such tools directly. However, it is important to note that if the tool is not compliant with the TAHO Guidelines and Advices on Information Management and Recordkeeping, the documents within these tools should be saved to a recordkeeping system (manually or by integration).

See the following TAHO publications:

- *Advice No 22 Records Management Using SharePoint 2010*
- *Guideline 22 Collaborative Workspaces*

Checklist of steps for managing shared drives

	Policy and Procedure	**Yes**	**No**
1.	Have shared drives been included in the organisation's information strategy and *Records management policy?*		
2.	Are there policy and procedures for staff regarding the use of shared drives?		
3.	Do policies and procedures include rules and instructions for saving records into corporate recordkeeping systems?		
4.	Do policy and procedures include rules and instructions regarding the deletion of information from shared drives eg what defining what short term value records can be deleted in accordance to Disposal Schedule for Short Term Value Records 2157		

	Structures, conventions and templates	**Yes**	**No**
5.	Have folder structures been set up for all corporate drives?		
6.	Have document naming conventions been established and promoted to staff?		
7.	Are standard templates used which include the document name and file path in footers?		

	Security	**Yes**	**No**
8.	Has the organisation considered whether some information is too sensitive to keep on shared drives and, if so, made other arrangements?		
9.	Have appropriate security controls been added to relevant shared drive folders?		
10.	Are staff members aware of security needs for documents they create?		

	Responsibilities	**Yes**	**No**
11.	Has responsibility for managing folder structures been assigned to appropriate people in the organisation and workgroups?		
12.	Have staff responsibilities for managing documents they create in shared drives been documented and communicated to staff?		

13.	Have responsibilities been assigned for the authorised deletion of information from shared drives?		

	Training	**Yes**	**No**
14.	Have all staff members been provided with training appropriate to their roles in managing information on shared drives?		

	Existing or legacy data	**Yes**	**No**
15.	If moving to a new structure for shared drives, have transition arrangements been established?		
16.	Does the organisation have a strategy for managing any unstructured or poorly managed data already residing in shared drives?		

	Monitoring	**Yes**	**No**
17.	Are monitoring arrangements in place to ensure shared drives are being managed in accordance with procedures?		

Further Advice

For more detailed advice, please contac:

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 Heritage and Archives Office (TAHO) wishes to acknowledge that this Advice and the associated document Sample procedures for staff managing shared drives are substantially based on the work by the State Records of New South Wales *Recordkeeping In Brief # 57 – Managing shared drives.*

The following documents were used in the compilation of the State Records of NSW RIB#57:

- Alberta Government, Managing shared electronic workspace: business rules, December 2005, (no longer current)
- Barts and the London NHS Trust, Where to store and how to share electronic documents: guidance for staff, 1 March 2007,[3]
- National Archives of Australia, Can I use shared folders to manage records?[4] available at: http://www.naa.gov.au/records-management/faqs/index.aspx#section11
- National Archives of the UK, Good practice in managing electronic documents using Office 97 on a local area network, (no longer current)
- Queensland State Archives, Public Records Brief: Managing shared drives, October 2005,[5]
- University of Stirling, Managing electronic records in shared network drives – good practice guidance, 24 April 2007, [6]

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

[3] http://www.healtharchives.org/docs/BLT_Where_to_Store_and_How_to_Share_Electronic_Documents.pdf
[4] http://www.naa.gov.au/records-management/faqs/index.aspx#section11
[5] http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/SharedDrives.pdf
[6] http://www.rec-man.stir.ac.uk/documents/ManagingElectronicRecordsInSharedNetworkDrives-V1.pdf

Version	Date	Author	Reason	Sections
2.0	April 2015	Christine Woods	Template	All
1.0	June 2013	Grace Nieuwenhuizen	Initial Release	All

Amendments in this Release

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

Issued: June 2013

Ross Latham
State Archivist