UW-Madison Archives and Record Management

2016

UW-Madison Guidance for

Managing Electronic Records in *Information Systems

*Shared Drives, Content Management Systems, Electronic Document Management Systems; Collaborative Tools and Electronic Records Management Systems

Questions:
University Records Officer
recmgmt@library.wisc.edu
Voice: 608-262-3284

This guidance was reviewed and endorsed by the URMAG on September 2, 2016

Managing Electronic Records in Electronic Information Systems

Introduction:

University information in electronic format needs to be managed in a way that ensures it is accessible, available and preserved for as long as it is required. Properly managing electronic records in electronic information systems such as a shared network drive is an important business activity. Do not store official university documents on your desktop, personal drive or personal email folders or removable media such as thumb drives or external hard drives as this limits access and retrieval to official university business.

This guide is one of a series by the records management program to facilitate proper management of electronic records among university departments and/or units. If organized properly, electronic Information systems can be a major asset that documents the transaction of business, provides evidence of decisions, and provides a history of departments and/or units. Compliance with varying state standards and regulations such as Wisconsin Administrative Rule 12 (ADM 12), Wis. Stat. §16.61 and Wis. Stat. §19.32 is also important. ADM 12 was created to specifically to address requirements, standards, and guidelines for state and local electronic records management, while state statutes Wis. Stat. §16.61 and Wis. Stat. §19.32 define public records in Wisconsin.

Use of Electronic Information Systems:

Shared Network Drives are the most common form of an electronic information system in use on the UW-Madison campus. There are many places to manage electronic records such as Content Management Systems, Electronic Document Management Systems, Collaborative Spaces such a UW-Madison Box, but for the purposes of this guideline we will focus on shared network drives. Shared Drives, are also known as network drives, and are typically used to store and share content such as word-processing documents, scanned and photographic images, audio, video, spreadsheets, presentations, and databases. Departments also used shared drives to group and store content by function, project, committee, or other logical category based on their business process. Shared drives are also sometimes referred to by their drive letter, e.g. “M:” drive are typically in organizational disarray, with poor naming conventions and are at inherit risk in lost files, loss of the chain of custody, and records without integrity or authenticity. Shared drives contain both unstructured content such a pdf, Word doc, video, audio and other file formats and structured records such as a relational database.

There are many benefits of a shared network drive.

- It provides a central place for storing university information in electronic format for the department or unit
- It provides a controlled hierarchy of electronic folders and document titles making it easier to retrieve information
- Supports the management of versions, drafts and working documents and reduces duplication by have one central storage space for your department or unit
- It is backed up and supported by the departments or unit IT services

- It prevents loss when staff members leave the department or unit

Shared Drives: Best Practice

Electronic Information Systems and in particular shared network drives, if managed correctly, contain information vital to the interest of the university and day to day university business. Proper management of a shared drive should be in compliance with Records Management Standards such as technical requirements of Wisconsin Administrative Rule 12 for Electronic Records, ARMA International Standard TR 23-2013 Development of Electronic File Structures and best practices such as the 8 Generally Accepted Recordkeeping Principles which are: Accountability, Transparency, Integrity, Protection, Compliance, Availability, Retention, and Disposition.

Filing and Folder Structure:

The availability of information is important to consider when managing electronic records. Users want to be able to find the information they are looking for quickly and easily. They will not want to go through many electronic folders before finding the one they want. The main concern with deciding on how to structure a shared drive is to ensure that it is clear; a simple test would be to consider whether a temporary or new member of staff with a very basic understanding of how the department works would be able to locate a specific document. During this process, evaluate if the department or units folder structure is working. Does it make sense with the department's business process? Since electronic and paper records are sometimes used in conjunction, the structure established in your shared drive should mirror and be cross-referenced to the filing or folder structure of your paper records.

Use of Standard Terms and Naming Conventions:

Once the hierarchal structure of the shared drive has been determined, it is important to ensure that electronic folders and files are appropriately named to reflect what the document or folder is. To decide if files are named appropriately, consider the context of the information contained within the folder or file. Titles should be clear and provide enough information to identify the document should it be misplaced from the file structure. The department or unit should decide on standard terminology and uniform naming conventions to use in folders and document titles. These should be applied constantly to all files and documents in the shared drive.

Access and Security of Information:

It is recommended that each department should designate an individual(s) who are able to provide/restrict access to certain folders within the shared drive. This is generally managed by

the IT department with input from the University's Information Security Department. These individual(s) would have an approval role to be able to approve or denied access to the shared drive. This role would also be accountable for making sure the records on the shared drive are protected and in compliance with policies of the UW-Madison Office of Cybersecurity policies. Users should take care to protect their passwords and logins and avoid leaving their computers unattended.

Organization or Re-organization of the Shared Drive

How to begin organization or re-organize the shared network drive

To begin to assess the shared network drive is a huge undertaking, but an important one.

1) **First know the rules.** Find the Records Schedules and understand the business process for your department or unit. What types of record does the dept. create and manage in the drive?

2) **Pull together a team of subject matter** experts in your area to begin to review and assess the drive.

3) In a separate file create the file structure that will be used.

4) Clean out the ROT (Redundant, Obsolete, and Trivial Files). These files are the Temp files; or system generated files; Personal content; Orphaned content; Duplicates; and other Documents types. This analysis would probably fall to your IT team member.

   Note: Tools available - there are tools that can be purchased or are free to assist with this exercise.

   - **Directory Lister Pro** (around $29.00 http://www.krksoft.com/
   - **Cathy** which is freeware http://download.cnet.com/Cathy/3000-2248_4-10057376.html
   - **Advanced Renamer:** This product will work excellent for renaming files with date modified in front of file name. It has many other features as well, mostly related to bulk renaming. https://www.advancedrenamer.com/
   - **Auslogics Duplicate File Finder:** Good for finding unnecessary duplicate files. One thing to consider with this product is that it can only find duplicates that are of the same format. If you have two files named the same, but have different formats, such as PDF and DOC., it will most likely miss these files. There are plenty of freeware programs like this one in case you want variety http://www.auslogics.com/en/software/duplicate-file-finder/
   - **Remove Empty Directories:** Does exactly what the title states. It removes empty directories/folders from the drive.

https://sourceforge.net/projects/rem-empty-dir/

- **Fixity:** This freeware creates a manifest of files stored in directories identified by the user, documenting file names, locations, and checksums. The user can then schedule regular reviews of the directories to monitor for any changes to files that may point to data corruption or loss. These reviews can also be scheduled to be sent by email as a report to whoever is designated as the recipient. I have never used this one, but could see it being helpful in situations where departments/units want to keep a record of files that were deleted per the RDA. https://www.avpreserve.com/avpsresources/tools/

5) The Second Pass should include reviewing case and project files to make sure that these are not duplicates, eliminate drafts and versions and be sure that "final" folders follow the new folder structure or taxonomy.

6) Check for electronic folder dates that have exceeded retention.

7) Set up a review schedule for ongoing maintenance. Organization of a shared drive takes a lot of time and effort up front and the organization should be maintained going forward.

Ongoing Maintenance of the Department or Unit Shared Drive:

There are a number of steps and actions that can be taken to continually maintain and even improve the functionality of a shared drive. It must be noted that as a department expands, changes, and alters, so too does its records. Therefore, it is necessary to continually maintain shared drives for proper records management. Below are a few areas to consider while maintaining shared drives.

Staff Responsibility:

There should be staff assigned who have accountability for consistent management and oversite of the Shared Drive organization. Staff responsibility is important for continual maintenance. All staff should understand the importance of maintaining the structure of the shared drive and how to create and name files in them. If unsure of how to maintain the shared drive, the individual(s) in charge should consult both the file plan and retention schedules for their department records and should contact the University Records Officer for consultation.

File Plan:

It is recommended that every department have a file plan for how the department's records are managed for transparency. A good file plan will assist with: documenting the department activities effectively, identifying records consistently, retrieving records quickly, retaining and disposing of records in the normal course of business, and meeting legal and organizational

requirements. For assistance in creating a file plan, please consult the Records Management website for more information on the creation of file plans.

Retention and Disposing of Documents:
These would be documents such as duplicates and working drafts and should be deleted as part of maintenance. Once or twice a year the disposition process should occur. This varies on the campus depending on the department or unit and whether they function on the Yearly, Academic or Fiscal calendar.

Once the retention schedule states that records within the shared drives are ready for disposition, the appropriated records schedule should be used. It is recommended to document the destruction of both paper and electronic records using a destruction log to demonstrate compliance with schedules.

Below is a Glossary of terms used in this guideline.

Glossary of Terms:

*from ARMA Int'l Glossary of Records and Information Management Terms, 4th edition (ARMA TR 22-2012)

Classification*	The act of analyzing and determine the subject content of a document and then selecting the subject category under which it will be filed and/or indexed. Note: this is not to be confused with assigning a security value (e.g., classified) to a record based on its content).
Disposition*	Final stage of the lifecycle of a record where records are eligible for destruction or transferred to University Archives per the records retention policy.
Naming Conventions or File Naming Policy	A uniform set of rules that department/units decide based on their business process that document what folders/files are to be named in the shared drive or other electronic storage.
Retention Schedule (for records)*	A comprehensive list of records series titles, indicating for each series the length of time it is to be maintained. May include retention in active office areas, inactive storage areas, and when and if such series may be destroyed or formally transferred to another entity, such as an archives for historical preservation.
ROT(Redundant, Obsolete, and Trivial Files)	These are the types of records that reside in a shared drive that need to be reviewed and removed. This could include instances of: files

	with the same content, but multiple file types, personal files that are not business related, etc.
Records Series*	A group of related records filed/used together as a unit and evaluated as a unit for retention purposes, e.g., a personnel files consisting of an application, reference letters, benefit forms etc.
Unstructured Information*	Any information that has no identifiable structure of any kind (e.g. unstructured text, audio, or video files).
Structured Information *	Any information ordered in a defined and previously known format so humans and /or applications handling that information know exactly where to find it. Note: An example is a relational database with tables, data fields, and relations amount fields in different tables.

For more information:

See accompanying job aids for more specific information:

- **Job Aid 1: Setting up or Cleaning up a Shared Network Drive**
- **Job Aid 2: Keeping your Shared Drive Organized**
- **Video on Clean up Shared Drives**

Resource used in creating the introductory guide include:

University of Tasmania Information Sheet 11. Storing Records In Shared Drives. INT11/3595. Jan 7, 2016 http://www.utas.edu.au/__data/assets/pdf_file/0018/132462/RMU-Information-Sheet-11-Storing-Records-in-Shared-Drives.pdf Accessed June 16, 2016

University of Sterling – Records Management. Managing Electronic Records in Shared Network Drives – Good Practice Guidance. http://www.rec-man.stir.ac.uk/good-practice/documents/ManagingElectronicRecordsInSharedNetworkDrives-V1_1.pdf Accessed June 16, 2016

If your department and/or unit is interested in more information about managing your shared drives, please contact University Records Officer at recmgmt@library.wisc.edu.