Global Shared Storage Guidelines

August 2014
Version 1

State Archives of North Carolina
NATURAL AND CULTURAL RESOURCES

Contents

Purpose

A shared, or network, drive permits centralized network file storage and sharing, which is especially valuable when a project requires collaboration with multiple users, or when a record of institutional value must be accessible to multiple users. This document is intended to offer guidance regarding the value of managing a shared drive, and provides best practice techniques for more efficient management of a shared drive.

These guidelines encourage use of shared drives in a manner that will create a navigable drive with appropriate restrictions and offers guidance in the following areas:

- Structuring a shared drive
- Techniques for efficient management on a shared drive
- Maintaining continued accessibility of records stored on a shared drive

Compliance with the recommendations laid out in this document will support more efficient document retrieval, free up network space, mitigate migration costs, and improve the agency's ability to respond to public records and e-discovery requests.

What is Shared Storage?

Shared storage is a device or devices that allow multiple users from different computers to access the same documents and work materials. Usually, it consists of a remote server to which users save and share documents with a defined group of people (their workgroup, their division, or their entire agency). Shared storage increases collaboration and improves efficiency among users while reducing the burden placed on email systems. Instead of sending multiple large files via email, users simply copy and paste a file path to the document on the shared storage. Multiple people can access documents in a central location, make edits, comments, or changes and resave them so that others can see them.

Shared storage in state and local government usually exist as part of the intranet system within a given workgroup. Only employees in that workgroup, or administrators, have access to documents on the shared storage, and a central IT organization maintains hardware and software associated with the storage.

Private companies also offer shared drive-like products for individuals to use. These products are most commonly associated with "cloud computing." Examples include Microsoft's OneDrive, Google's Drive, Dropbox, and Apple's iCloud. While cloud computing and shared storage are not synonymous, they act in a similar manner, allowing users to upload documents to remote hardware for sharing with other users.

Cloud Computing

Cloud computing refers to storing data on a remote server for access from anywhere with an internet connection, and is a major driver of shared storage use among the public. Most cloud computing services allow users to designate who can access and edit documents down to the individual level (as opposed to whole workgroups or agencies). This allows collaboration with groups outside of the agency while still maintaining control over their documents.

Clouds come in two major categories: private and public. Private clouds are completely hosted by the organizations that use them, meaning that the organization owns the hardware and software for storing the documents. Third party companies such as Google, Microsoft, Apple, Dropbox, SugarSync, Basecamp, etc. offer public clouds. The term "public cloud" does not mean that the information stored on them is available to the public, only that they offer their services to the public. These companies set their own security and privacy standards that are usually unalterable and non-negotiable. Cloud computing has a number of advantages and disadvantages that are outside of the scope of this document. However, it is important to note areas of concern when using public cloud services.

Concerning storage and retention of government records, public cloud services carry risks not associated with private clouds. Users cannot be confident in the security of any third-party shared storage unless their organization's IT department has reviewed and approved it. If there is a security breach in a third-party cloud service that affects government data or records, the employee that owns the account could face disciplinary action for the disclosure of data if the data was uploaded without permission. Additionally, users should be aware of the potential for losing data if a public cloud provider should fail. If a cloud service shuts down, users can lose all of their data if there is no accessible backup. Users should also be wary of proprietary data-types and vendor lock-in. Cloud services that do not use an open file format standard to create a document or dataset carry a higher risk of data loss.

Ultimately, documents stored with cloud services are subject to the same records and confidentiality laws as any shared storage, computer, or hardcopy record system, and can potentially pose greater risk to the organization. While public clouds provide a great opportunity for collaboration, users should be aware of the risks and disadvantages of using public cloud services. For more information about the risks and advantages of cloud computing, see *State of NC Cloud Computing Strategy* at www.scio.nc.gov/library/pdf/Cloud_Computing_Strategy_v1_0.pdf and *Best Practices for Cloud Computing* at www.ncdcr.gov/Portals/26/PDF/guidelines/cloud_computing.pdf.

Challenges of Shared Storage

Because shared storage is rarely developed and maintained systematically, problems can quickly develop, especially when sharing across a large department. These include:

- Users rarely perform routine housekeeping on documents stored on the shared storage, leaving drafts and other records without institutional value behind. As records accumulate, the storage becomes cluttered, difficult to navigate, and costly to maintain. This unchecked accumulation of records complicates tasks like applying records retention requirements or identifying the official record copy when multiple copies exist.

- Naming of files, folders, and sub-folders may be inconsistent or meaningless. Folders and sub-folders may not be logically organized. File names and file structures lose their meaning with the addition of new employees, the loss and retirement of old employees, and the close of projects.

- Shared storage without any document management software lacks the capability to create audit trails of the records stored on the storage, making it difficult to authenticate them.

- Often, the Information Technology group must manage these records in place of the records' creators. Because IT is not the custodian of the records, these files can exist for long periods, exposing the agency to storage, maintenance, and unnecessary recovery and migration costs.

- Documents with digital rights management (DRM) restrictions applied can be permanently lost. Digital Rights Management systems "promote automated distribution of materials while protecting those materials from unauthorized copying or access."[1] DRM is most commonly occurs when an employee protects a folder on the shared storage so that only he or she can view the contents. Issues arise if or when the employee leaves the organization without removing the protection (or granting a supervisor access). IT must then shoulder the burden of finding a way around the folder permissions in order to capture the content of the records themselves. Leaving a shared storage in this way can also mean dealing with "orphan" files or folders and experiencing difficulty in determining which documents need to be retained and which do not. Often, files are

[1] Archivists, Society of American. "Digital Rights Management." Glossary of Archives and Records Terminology. http://www2.archivists.org/glossary/terms/d/digital-rights-management (accessed April 28, 2014).

saved not because a records retention schedule says they should be saved but rather because people cannot delete them.

Tips for Structuring Shared Storage

- Shared storage must be navigable by other users, present and future. To encourage continued accessibility of documents stored on the shared drive, structure the folders and sub-folders logically.

- Rely on the structure of the file system to provide context to individual records. The file path need not be apparent in the file title, assuming the file structure is logical.

- Avoid creating hierarchies more than 4-5 folders deep. This will ensure that documents are not lost in a deep folder and keep duplicate documents off the shared storage (leaving more space for everyone). Deep folder hierarchies also pose challenges when moving content or upgrading a system.

    - Decide early on which documents to file by case and which to file by subject. A good rule of thumb is to follow the file plan created for paper records in organizing digital documents. For more information on creating a file plan, contact an analyst at the Division of Archives and Records (http://www.ncdcr.gov/archives/ForGovernment/ServicesandTraining.aspx)

- File administrative and reference records by subject or function, not by project, as projects do not retain meaning over time.

- If records must be filed by project or case, a good practice is to keep documents in a well-labeled project folder for the project's duration, but transfer the final product to the correct topical folder upon project completion. Remove any records with no retention schedule, such as document drafts or outside research, from the shared drive upon project completion or completion of the final copy. However, filing records by subject and function from the beginning is ideal.

Outlined below is an example of an index of storage locations (drives) accessible to employees that agencies could maintain..

	Drive	Purpose	Capacity
Shared	L:	The main shared storage accessible across the entire Division of Archives and Records.	2 TB
	U:	Accessible across the entire Department of Cultural Resources. Files placed on the U: drives are deleted once they no longer serve collaborative purposes.	1.08 TB
	W:	The drive used to store Web files.	249 GB
Personal	H:	Individual network storage space: Used for work-related records, draft versions, and other documents that do not need to be shared. These drives are not accessible by other employees, but their security is not such that confidential information is safe.	2 TB, shared among all users
	C:	Local hard disk storage. Used for records that need to be stored off the network drive, such as personnel, confidential, or otherwise sensitive data.[2]	Varies

[2] Note: Employees are responsible for the backup of any files stored on the C: drive. This drive is not subject to a backup schedule because it is disconnected from the network.

Shared Storage and Records Management

Shared storage is ***not*** a document management or records management system. Organizational IT departments generally err on the side of open access in order to facilitate collaboration. By design, typical users can easily access, manipulate, or delete records stored on a shared drive. Without strong auditing capabilities, such acts go undocumented. Additionally, shared storage only supports limited security measures, and metadata fields are rarely populated, thus making it difficult to manage, and leaving a contextual void. These aspects of shared storage jeopardize the authenticity and trustworthiness of the records stored on the drive. The following active management techniques can lead to better management of those records stored on shared storage.

File and Folder Naming Conventions

Efficient management of electronic records begins with accurate and meaningful file naming. This requires that file names (as well as folder structures) make sense to everyone, not just their creator. A file, folder, or sub-folder name should be:

- Interpretable by others in the department or agency in which the file resides
- Interpretable by future users of the shared storage
- Distinguishable from files with similar subjects, and from different versions of the same file
- Consistent across the department or workgroup, and in compliance with established naming conventions

Additionally, folder names should not repeat information contained elsewhere. For example:

Instead of: Archives and Records/Archives and Records Policies/Approved Policies/LeavePolicyFinal.doc
Use: Archives and Records/Policies/Approved/LeavePolicyFinal.doc

Define file/folder naming conventions that are consistent, easy to use, and easy to interpret. The following tips will help ensure strong file names:

- Avoid special characters (\/:*?“”<>|[]&$,) as the computer may interpret such characters as specific to a task unrelated to the file name.
- Avoid “floating” folders to the top of alphabetical lists by using symbols or numbers as the first character. For example, use “Projects” instead of “_Projects”. This will avoid losing folders and unnecessary duplication.
    - If necessary, appending folder names is acceptable. For example, Use “Projects” and “Projects_001” or “Projects_Short-Term” when trying to keep a certain set of files separate.
- Incorporate the following elements within the file name:
    - Title descriptive of the document’s content
    - Date of creation or of modification (YYYYMMDD)
    - Version number (v1.0, v2.0)
        - When updating existing documents, use the current version number as a reference for internal changes (e.g. v1 becomes v1.1, v1.2, etc. while being edited internally and v2.0 upon publication).

For more information, consult the Department of Cultural Resources publication, *Best Practices for File Naming*: www.ncdcr.gov/Portals/26/PDF/guidelines/filenaming.pdf and State Library YouTube videos on file naming: youtu.be/Hi_A4Ywn4VU.

Similarly, users should name folders semantically and arrange them logically. Name each folder in a way that accurately reflects the content of the folder or the function of the documents contained within. Do not name folders using individuals' names or titles, as titles and the people who hold them can change over time. If choosing to organize documents according to who will use them, name folders according to the office instead of the person or position.

Instead of: Jane Smith/Jane's Policies/Approved Policies/LeavePolicyFinal.doc
Use: Archives and Records/Policies/Approved/LeavePolicyFinal.doc

Saving Documents Correctly

Employees should save documents to the correct location the first time. This reduces the amount of work involved when identifying records and organizing storage drives later. Each drive has different documents that are appropriate and inappropriate. Employees should not save documents of a personal nature (vacation photos, personal emails, etc.) on any shared storage. These items make it more difficult to find relevant information ,create a significant burden for IT systems to back up, and use resources and storage for information that is unrelated to work. Additionally, these items could potentially become subject to a public records request or e-discovery.

In addition to saving documents in the correct location the first time, users should avoid placing duplicate documents on a shared storage. When a document is ready for placement on shared storage, place it in the appropriate existing folder or create the requisite folder.

Examples of documents saved to different drives:

Personal storage	Workgroup storage	Organizational storage
Information **relevant only to the individual**: • Résumés • Professional/career information • Copies of training and development records • Draft documents not ready for sharing	Information that can be **shared with the workgroup**: • Research, drafts and final versions of documents, reports, minutes, etc. for a project carried out within the workgroup • Administrative matters associated with the workgroup or business unit (e.g. time sheets)	Information that can be **shared with the whole organization**: • Research, drafts and final versions of documents, reports, minutes, etc. for projects or business initiatives that involve staff across workgroups • Organization-wide policy and procedures

Active Housekeeping

Unless responsibility for a folder has otherwise been delegated, each user of the shared storage is responsible for the folders and documents he or she creates. Users should regularly audit their documents to determine which records to retain and which to delete from the storage. If placing a document on shared storage on a specific drive for someone else to quickly pick up, users should remove those documents immediately after they retrieve them.

Managers and IT staff should schedule an annual (or more frequent) cleanup day, to ensure periodic cleansing of unnecessary files and folders. Documents and folders to consider for deletion include:

- Draft versions of finalized documents
- Documents and folders that no longer serve a purpose after sharing with someone
- External documentation (e.g. research, downloaded files) after project completion
- Duplicates and redundant files
- Documents that no longer have administrative or reference value or which have met their retention requirements. For more information regarding records retention and disposition schedules, please visit http://www.ncdcr.gov/archives/ForGovernment/RetentionSchedules.aspx.
- Empty folders

Employee Separation

Each agency should have a policy in place regarding the records of employees who leave or are separated from employment. Best practices call for employees to share files with the supervisor of that position so that the supervisor can determine what to retain. Ideally, supervisors will review employee files and shared drives before an employee leaves and make determinations about the files. To avoid confusion about files, an employee should describe his or her files and folder structure to a supervisor prior to leaving the agency or include a .txt or MS Word document with a detailed description of its organization.

The file description should also include files that are in third-party cloud platforms. Even if they exist on a personal cloud account, any document relating to the transaction of public business is a public record must be managed. Employees should pull records down from the cloud and provide them to their supervisor, or they should hand over login information for the account to the supervisor. Please consult your agencies' policies and procedures regarding former employees' files and adhere to them as closely as possible.

Sensitive and Confidential Information

Keep confidential information off the network storage or, at minimum, place appropriate restrictions on folder access. Records that are subject to confidentiality restrictions include but are not limited to:

- Personally identifiable information as defined in G.S. §§132-1.1, 1.2, §125-19, §§126-22, 24, and others.
- Data protected by state or federal statutory law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Family Educational Rights and Privacy Act of 1974 (FERPA), the Gramm-Leach-Bliley Act of 1999 (GLB), and G.S. §130A-476.
- Some administrative information related to personnel functions and financial matters

For more information about public records that may be subject to confidentiality requirements, consult the publication *Laws Relating to Confidential Records Held by North Carolina Government*, located at www.ncdcr.gov/Portals/26/PDF/gov_lists/confidentialitystatutes.pdf.

Education and Training

Employees are responsible for their own records, and bear full responsibility for folder system management. It is crucial that they understand their responsibilities as users of the shared storage and custodians of the public record. Lack of knowledge about proper procedures is the main cause of shared storage issues. We strongly encourage agencies to train new employees on proper use of shared storage and good file naming conventions. More information regarding records management and public records can be found at **http://www.ncdcr.gov/archives/ForGovernment.aspx** . More information about digital files can be found at **http://www.ncdcr.gov/archives/ForGovernment/DigitalRecords.aspx** or **www.digitalpreservation.ncdcr.gov**

References

State Records New South Wales. “Sample procedures for staff: managing shared drives.” 2010. Retrieved 9/16/2013 from: http://goo.gl/8Ps7x5