WISCONSIN HISTORICAL SOCIETY

NATIONAL
ARCHIVES
NATIONAL HISTORICAL
PUBLICATIONS
& RECORDS COMMISSION

Best Practices for
Organizing Electronic Records

October 2017

Best Practices for Organizing Electronic Records

CONTENTS

INTRODUCTION

It is important for government employees to understand that they are responsible for the maintenance and care of all public records created as part of their position, including any records created by prior employees. This responsibility pertains to any public record created by the government unit regardless of format. Standards and guidelines for the management of electronic records are outlined in Chapter Adm. 12 to ensure that electronic records remain: accessible, accurate, authentic, reliable, legible, and readable.

The management of electronic documents on agency file shares is a tremendous challenge and often one of the most significant pain-points for staff, agency Records Officers, and IT. Generally, network content consists of records and non-records in numerous file formats. Creating a file organization policy for employees is an important aspect of managing e-records throughout their lifecycle. A good plan helps determine what types of e-records exist, how they are arranged, where they are located, and retention information. Standardization also creates a solid foundation for applying technological solutions like a content management system to help the long term management of e-records. While technology can help, technology applied to the unstructured mess which often makes up our share drives will not solve the underlying problem; it just moves the mess to a new platform.

File organization standards work hand in hand with file naming policies and should be distributed together within an organization. Guidelines around the organization and file naming of electronic records should be well documented for your agency to enable employees to locate and manage the files well into the future. This document provides best practices for the organization of files and folders and may be used to create a file organization policy to be distributed to all staff members.

FILE ORGANIZATION BEST PRACTICES

Centrally locate records in share drives

- When files are used by multiple staff members, it is important to have a central location on a shared network for easy access and management of the records.

- Determine ahead of time who should have permission to access, view, edit, or delete files and folders within a shared drive.

- If there are security concerns for documents/projects that are specifically assigned to a staff position or team, your agency IT team should be able to help you set up restricted areas on a share drive that are only accessible to designated parties. While it may be tempting to keep sensitive records on a personal drive, they run a much higher risk of being lost when a person leaves as well as making it difficult to manage them appropriately according to records schedules.

- Any exceptions to keeping agency records on a shared drive should be discussed and agreed upon with the agency Records Officer. In some unique cases, it may be determined that some records should remain on a personal drive but isolated and clearly labeled so they can easily be located and identified after the individual leaves their position. This should be accompanied by a word document (like a ReadMe file) placed in the departmental shared drive indicating where these files exist, the content contained within the documents and the record schedule associated with it.

Do not store records on your computer's hard drive or personal drives

- Records should never be stored on your computer's C: drive (hard drive). This drive is rarely, if ever, backed up by normal IT processes and records will be lost should your computer fail.

- Records should never be stored on your personal drive. While this is often in a network location that is backed up by IT, records stored on personal drives are inaccessible to other employees and have an increased chance of being lost when the employee leaves their position.

Assign Records Schedules to your folders

- Determine which records schedules apply to your electronic records and how long you should retain those records. It may be helpful to add some combination of information (ex: ADM00001_CR1_des) to folder titles to help you manage the contents over time.

  > *Ex: Folder_ADM00001_CR1_Des*
  > *for a folder containing content that follows General Records Schedule ADM00001 – Routine Activity and Production Reports Created by Individuals or Work Units which has a disposition of Creation + 1 year and destroy*

Use a hierarchical folder structure

- Hierarchical folder structures tend to start very broadly at the topmost folder and become more specific as subfolders are added. Some organizations start with division or section names and then add subfolders by RDA or function. For records that cross divisions it may make more sense to order by record series and/or functions.

- Integrating an RDA number into folder names may help your organization manage records over time and will help provide some rules for the folder content should the records ever be integrated into a content management system.

  > *Root Folder: DivisionNameHere*
  > *Subfolder: CaseFiles_RDA001234*
  > *Subfolders: Individual case name or case number*
  > *Subfolders: Descriptive topic names such as communications, contact information, filings, etc.*

Minimize the depth of the folder path

- Use subfolders to further organize your files, but try to keep structure flattened as much as possible. Long file name/file paths can cause errors when transferring files and folders to other locations. Traditional Windows systems recommend that file path lengths be kept below 260 characters – however it will allow for longer which often renders the file inaccessible. It is also highly likely that file paths at this length will not be usable in other systems you may eventually use to manage your files.

Separate supplemental materials

- Supplemental materials are files that often appear alongside other objects or projects. Examples might be notes, reference information for a report, documents sent from other organizations that are not needed in the understanding of the kept content, or a folder of images that were later embedded in a document. Generally, these are kept for convenience or reference and should be discarded when no longer needed. Storing and tagging these in a separate subfolder will help in disposing of them at the appropriate time.

File copies

- Unless there is a valid business reason for keeping multiple copies of something, do not save more than one copy of a record. Records should be stored in locations that are truly backed up by official IT processes. The additional creation of copies (also often labeled as "backups") across drives by employees makes identifying the item of record difficult. According to Wis. Stat. § 16.61(2)(b), copies maintained only for convenience or reference are not public records. You should be able to do a "keyword search" for the word "copy" or "backup" on the targeted files to quickly locate and eliminate these items.

Versions and drafts of documents

- According to Wis. Stat. § 16.61(2)(b)(5), drafts of documents are not public records. Versions or drafts are often created when a number of people are collaborating on a document. It may be necessary to keep significant versions of important organizational documents which significantly change an organization's procedure or policy, in which case you should review with your records officer. For the vast majority of documents however, only the final version needs to be kept and then rest can be deleted once the final version is complete. Where multiple versions are deemed to be important, they should be clearly labeled to eliminate any confusion as to which is the final item of record.

Leave notes documenting folder contents

- It is perfectly acceptable to leave text documents or ReadMe files in folders that describe its contents. This can include the main subject of the files, any unique file formats that exist in the folder and the software that created them, how it's organized, special file naming conventions, any records schedules that apply to the folders and subfolders and information about who "owns" and manages that data. Notes provide the directions to help groups manage files in a consistent manner over time and provide a contact point for folders that may not have any activity for long periods of time after the records have moved to an inactive state. For records that will eventually be transferred to the State Archives, notes also provide some context for the files and how they should be preserved.

Resources referenced for this document:

Digital Preservation Handbook, 2nd Edition. Digital Preservation Coalition © 2015.

   http://www.dpconline.org/handbook/ (accessed September 2017).

Smithsonian Institution Archives. Managing Active Records. August 31, 2016

   https://siarchives.si.edu/services/managing-active-records (accessed September 2017).