

# Electronic Records Management



**Records Management  
Secretary of State Tre Hargett**

**04.15.20**

# This Training Will Cover:



- Why Electronic Records Management is important
- Guidelines for managing your records
- Safeguarding records while working AWS
- How to organize your agency's shared drive to facilitate better records management
- Maintaining and preserving your agency's shared drive

# Why Get Your Electronic Records Organized?



- Fulfilling Legal Mandates/ Ensuring Compliance with State and Federal Laws
- Facilitating Records Retrieval
- Reduce agency costs from storing obsolete records
- Ensure the creation and management of accurate, reliable records

# Guidelines for Managing Electronic Records



- Electronic Records should be reliably and securely maintained
  - No State records should ever be maintained on an employee's hard drive or personal drive.
  - Your Electronic Record Storage system should include system controls and procedures for measuring the accuracy of your records.

# Guidelines for Managing Electronic Records



- Electronic Records should be retained and disposed of according to their Record Disposition Authorizations (RDAs)
- Your business practices should support your electronic record keeping
  - Scan and verify incoming paper records as they are received
  - Have plans in place for record migration and destruction
  - The file format needs to meet your agency's objectives for sharing and using records.
    - ✦ Ex. If the file format can only be read by specialized hardware and/or software, your ability to share, use, and manipulate the records is limited.

# Guidelines for Managing Electronic Records



- **Electronic Records should be unaltered and secure**
  - Protected from accidental or intentional alteration/destruction for as long as the record must be maintained
  - Access to records should be limited only to authorized and necessary personnel
  - Records should be accessed to the minimum amount needed to perform necessary business functions

# Guidelines for Managing Electronic Records



- Electronic records should be preserved without the loss of any vital information for as long as required by law.
  - Keep your electronic records with an eye towards the future
- Electronic records should be accessible and retrievable in a timely manner throughout their retention period.
  - Electronic records need to be searchable and retrievable for reference purposes and in case of audit or litigation
- Access to electronic records should be controlled through a well-defined criteria established by your agency.

# Work From Home Guidelines



- Do not download State Data onto a personal device.
- Do not maintain official copies of records on your desktop.
- Do not conduct state business via your personal email or messaging apps.



# Work From Home Guidelines



- An employee should get permission from their supervisor before bringing any records from their office to their AWS location.
  - ✦ These records should only be kept for a defined period of time.
  - ✦ The removal should be logged according to your agency's AWS policy.
  - ✦ Any confidential or sensitive information needs to be safeguarded just as it would be in your agency.
  - ✦ Under no circumstances should confidential information be removed in a manner this is not consistent with your agency's policies and guidelines.

# Work From Home Guidelines

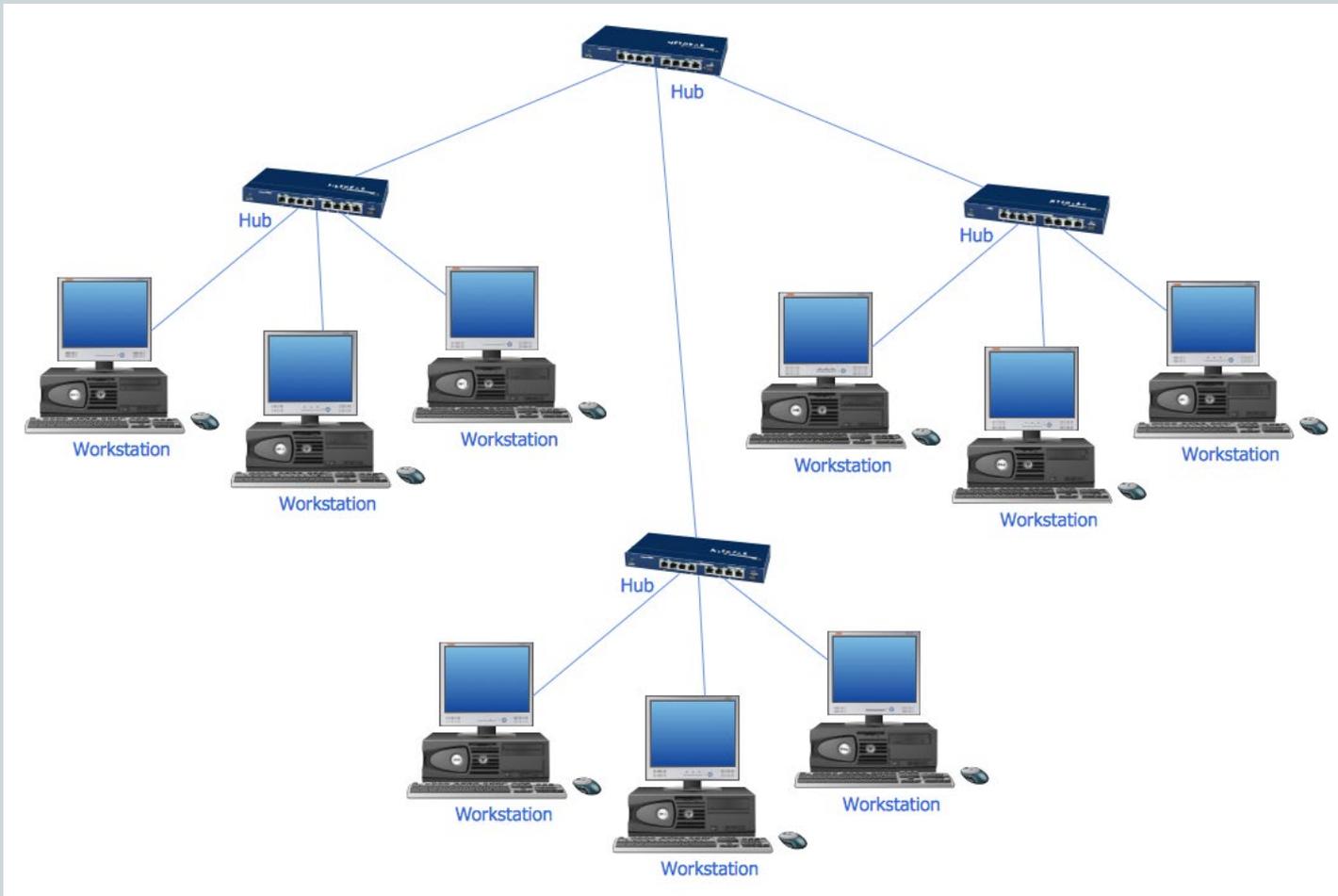


- If you are currently under a litigation hold make sure that your general counsel has cleared the use of instant messaging apps before using them to conduct State business.

**Remember:** Any records that you bring home are still considered State records and any records that you create while working from home are also State records.

- \* For more information please consult DoHR's AWS guidelines, your agency's AWS policy and STS's AWS reference guide.

# Setting up your Shared Drive



# What is a Shared Drive?



- A drive that is shared across all/or selected users on the network.
- Typically used to store and share content such as:
  - Word Documents
  - PDFs
  - Spreadsheets
  - Databases
- For the State, the drive letter *H:* is typically used for an Agency's Shared Drive but any letter can be mapped
- To be useful, agencies must spend time to develop and maintain a structure for their shared drives

# Why utilize your Shared Drive?



- More secure and reliable than storing records on your computer.
  - Records stored on a shared drive won't be lost if an individual computer on the network crashes or is stolen
  - Records kept on your Shared Drive are backed up nightly
- Files can be accessed in your shared folder whenever they are needed and allow multiple users to collaborate and access files simultaneously
- Allows for one centralized copy of a record to avoid duplication of files
- The cost to your agency is significantly less than utilizing an Enterprise Content Management (ECM) system such as SharePoint

# Setting Up and Maintaining Your Shared Drive

## Keys to success:

- Conduct a Records Inventory
- Determine ahead of time who needs access to view, edit, or delete folders within your shared drive and ensure that permissions are set accordingly
- Utilize a standardized naming convention for your records
- Arrange your records according to a hierarchical filing structure
- Once you have set up your Shared Drive ensure that you continue to monitor and maintain the drive



# Records Inventory



- The first step in organizing your shared drive is to identify all of your agency's electronic records. This can be accomplished by conducting a Records Inventory.
- A Records Inventory is a fact finding survey that identifies and describes the characteristics of records created, received, and maintained by an agency.
- Without conducting a records inventory you are likely to have a high amount of unstructured data. This will make it very difficult for you as an agency to follow your retention schedules.
  - Your records need to be categorized and organized in order to be useful

# The Goal is to eliminate Unstructured Data

## **Structured Data:**

- Data that has been organized into a formatted repository

## **Unstructured Data:**

- Any information that has no identifiable organization of any kind



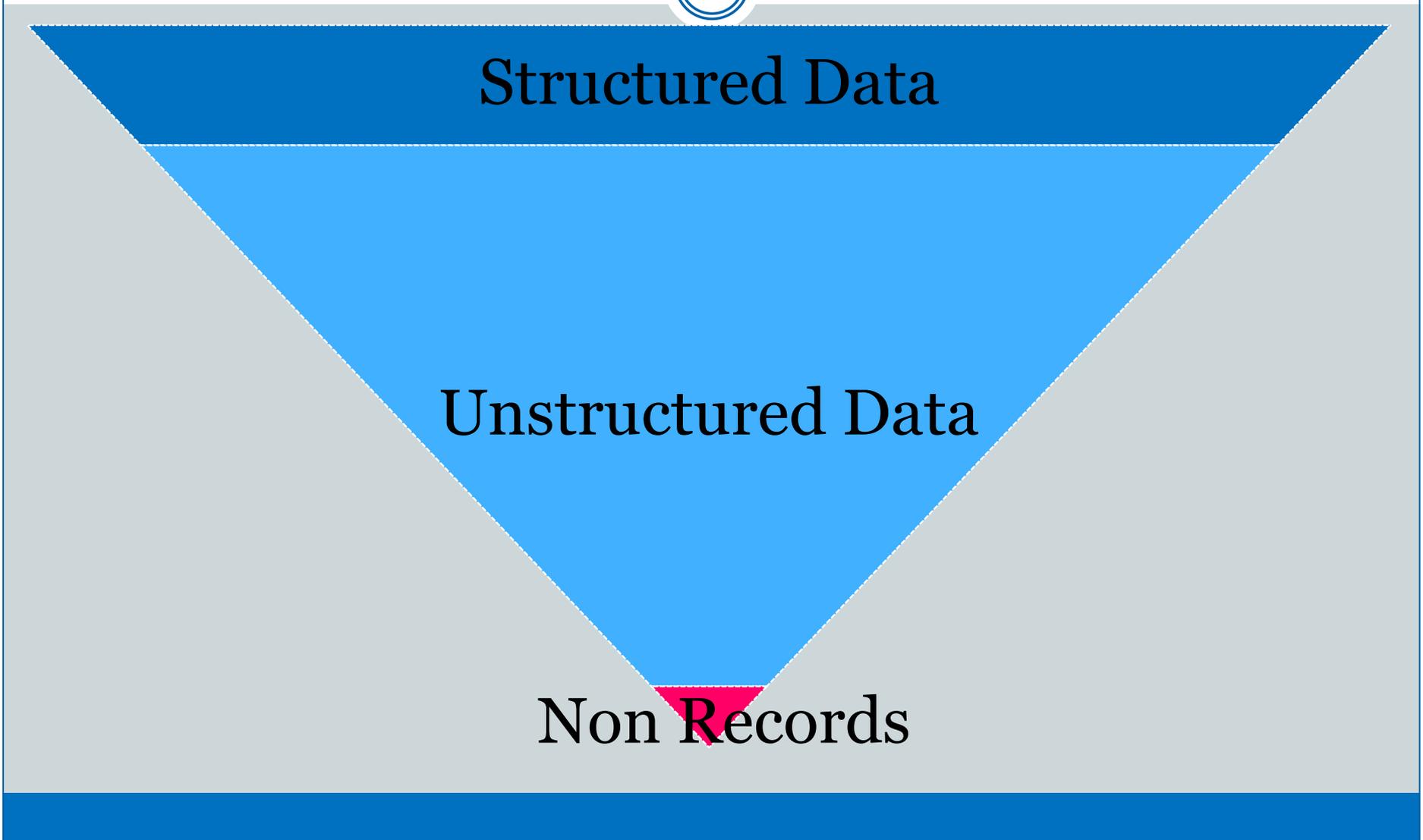
# Records Inventory



Structured Data

Unstructured Data

Non Records



# Records Inventory



Structured Data

Non Records

# Steps to Conduct a Records Inventory



- Every division should inspect all of their files
- Identify whether files are records, reference, personal documents, or non-records
- Identify duplicate, fragmented, and related records
- Determine which files your agency actually needs to keep and maintain
- Match your files to your RDAs



# Determine Access Levels & Permissions



- Determine ahead of time who needs access to view, edit, or delete folders within your shared drive and ensure that permissions are set accordingly.
- *Remember:* These protections exist for a reason and it is critical that your agency follow them.
- Access and permissions should be reviewed routinely and updated as needed.

# Why It Matters



- In 2018 a Nashville Metro Department of Health employee wanted to share HIV/AIDS patient information with the department's epidemiologist.
- The epidemiologist was not one of three metro employees authorized to access the Department's folder that contained the data.
- The employee's solution? To make a copy of the information and place it on the Department's main drive.
- **The Result?**
  - The protected health information for HIV/AIDS positive individuals living in 13 Tennessee counties sat unprotected on the agency's server for 9 months
  - The agency was unable to determine if anyone accessed or copied the information
  - Numerous potential lawsuits against the department
  - A complaint being filed with the United States Department of Health and Human Services
  - The Metro Health employee at fault being forced to resign
  - Months of negative press coverage

# Standardized Naming Conventions



- The agency should agree upon a set naming convention for all agency records that will be kept on the shared drive
- Naming conventions are a uniform set of rules agreed upon by an agency or division that document what folders/files are to be named on shared drives or other electronic storage

# Standardized Naming Conventions



## Do

- Use descriptive names to identify the purpose of the files
- Include the date of creation or revision in your file name
- Utilize consistent naming patterns for version control. Examples: Final, draft, Revision1, etc.;
- Make sure your naming conventions work for your agency's business needs

## Do Not

- Avoid using spaces in any file names that may be accessed via web browsers. Instead, use hyphens or underscores between words
- Avoid using special characters such as !@#\$%^&\*()
- Avoid using personal names

# How Not To Label Your Files



Name
 Budget Draft Final Final
 Budget Draft Final No More Revisions
 Budget Draft Final
 Budget Draft Final1
 Budget Draft Final2
 Budget Draft Last Version Definitely No More 2
 Budget Draft Last Version Definitely No More
 Budget Draft
 Budget

# How To Label Your Files

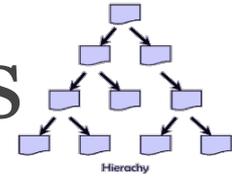


SW18 Budget Papers ▸ 2019

Include in library ▾ Share with ▾ Burn New folder

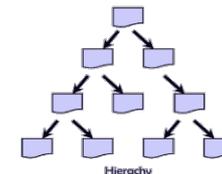
Name	Date modified
 Budget Template	1/17/2019 8:00 AM
 FY2018-2019 Approved Budget	1/17/2019 8:00 AM
 FY2018-2019 Budget Draft	1/17/2019 8:00 AM
 FY2018-2019 Proposed Budget Final	1/17/2019 8:00 AM

# Hierarchical Filing Structures



- We recommend that agencies utilize a hierarchical filing structure to organize their records.
  - Hierarchical folder structures start broadly and then become more specific as more sub folders are added.
  - A common structure is to organize by division and then by RDA or Record type.
  - For records utilized by multiple divisions it might make more sense for an agency to label their top level folders by RDA or record type instead.

# Hierarchical Filing Structures



- Folders should be named for Record Series title or Major function/activities. Ex. SW 12 Contracts or Audits.
- Integrating RDA numbers into your folder names will help you organize your records and provide clear rules for the records retention.
- Subfolders should reflect secondary activities. Ex. programs, grants, or projects
  - *Remember:* Folder names should be self-explanatory
- Subsequent folders should be organized by calendar or fiscal years to facilitate the destruction or transfer of records to TSLA.

# Sample Folder Layout



Top Level Folder

Records  
Management  
Division

Sub Folder

Records

Archive

Reference

Subsequent  
Folders

1769 Record  
Center Files

1768 RDA  
Files

T.C.A

Public  
Records  
Laws

2019

2018

2019

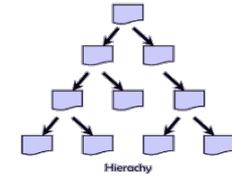
2018

Signed forms

Signed  
Forms

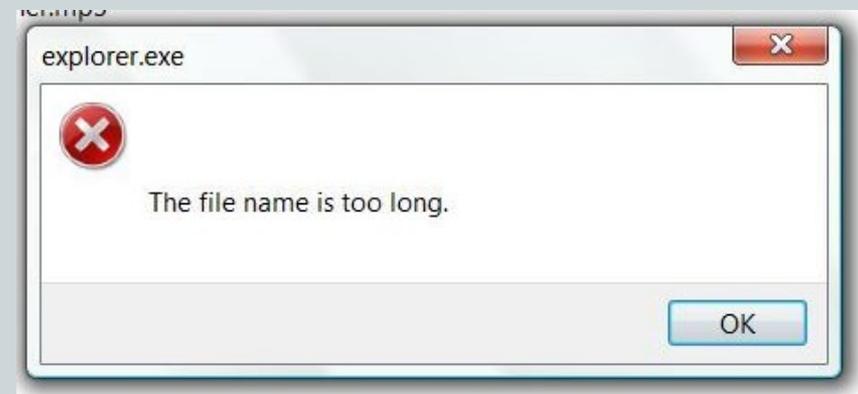


# Hierarchical Filing Structures



To get the most out of your filing structure:

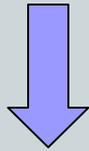
- Include a copy of your agency's RDA or file plan in your top level folders
- Avoid Folder Creep
  - This can cause the records to become inaccessible
  - Adds unnecessary complexity and confusion.
  - Try to have no more than 4 pathways to access a record.



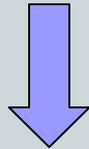
# Controlling Folder Creep



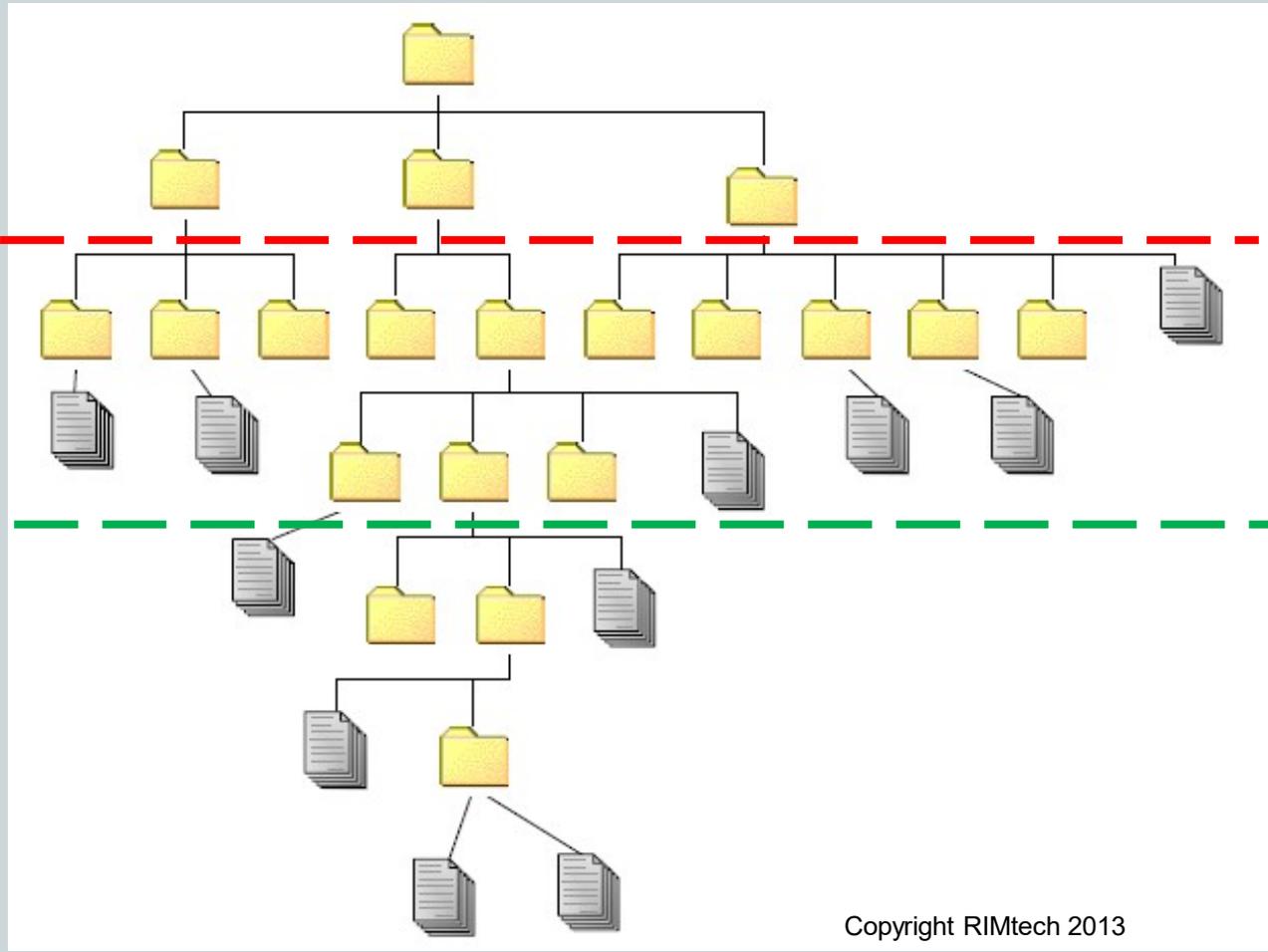
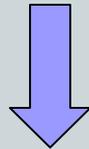
**STS**



**Agency  
Directors &  
Supervisors**



**End Users**



# Maintenance and Preservation



- Agencies should assign individuals or teams to periodically review their shared drives to ensure that records are being retained and disposed of in accordance with their RDAs.
- Agencies should look for records that are duplications, redundant, obsolete, unwanted, or misfiled.
- Agencies should ensure that all file names follow agency's preferred naming conventions.
- Work with STS to ensure plan is in place to dispose of records that reach the end of their retention.

# Maintenance and Preservation



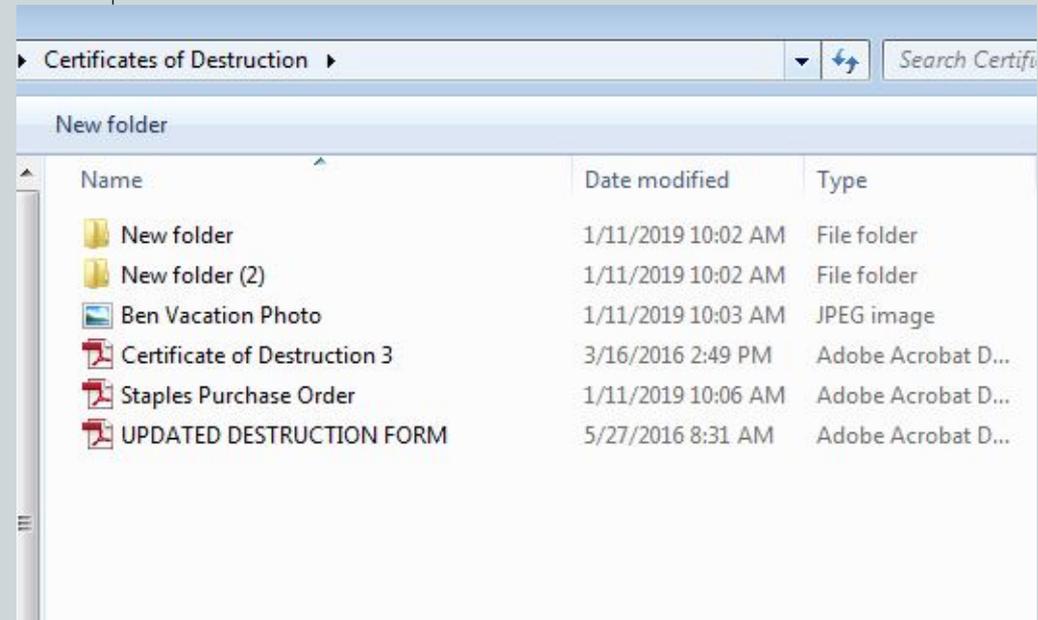
- Your agency should continually review and update their RDAs as laws and business needs change.
- Include copies of relevant RDAs/File Plans in all top level folders to help employees know proper retention and storage for your records.
- Ensure that records are maintained and disposed of in accordance with your RDAs.
- Agencies should make sure that digital records are regularly backed up to protect against accidental deletion or loss
- Agencies should document destruction by filling out and submitting CRDs.

# Maintenance and Preservation

## A Shared Drive That is Not Maintained



- Subfolders are not labeled and do not reflect agency records or activities
- File names do not follow any clear set naming conventions
- The vacation photo is personal content and should never be kept on an agency drive
- The Staples Purchase Order has been miscategorized and should not be filed under Certificates of Destruction

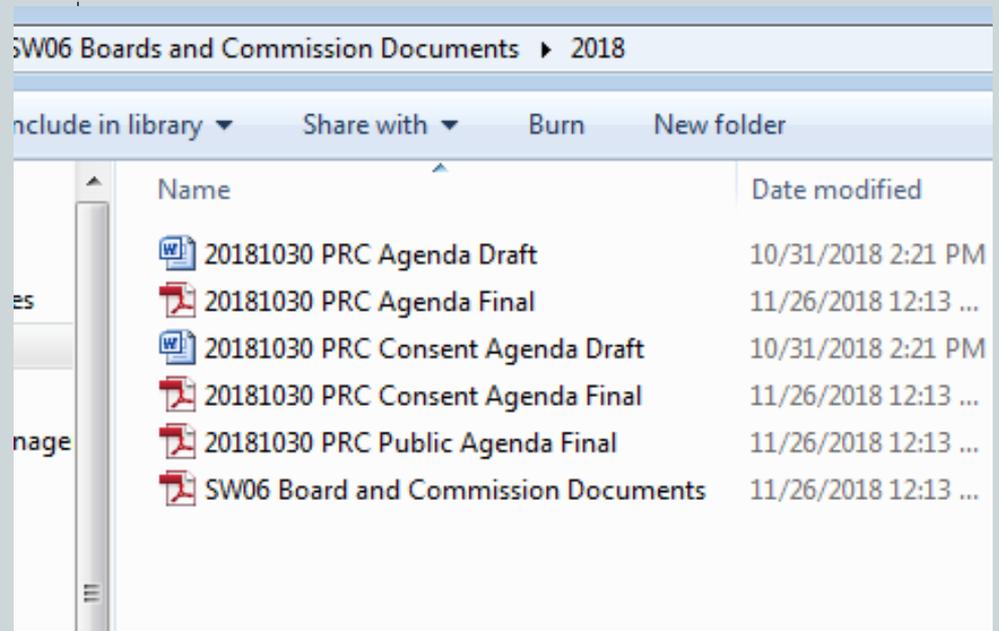


# Maintenance and Preservation

## A Well Maintained Shared Drive



- Versioning control
- Set naming conventions
- All files are related to their containing folder
- A copy of the RDA is included in the folder to provide retention guidance
- There are no duplicate copies of files or unnecessary drafts



# Questions?

