

How to Manage Records

How to Manage Records

Records Management Services

State of Michigan



Notes:

Welcome to the training module titled, “How to Manage Records.” This training is offered by the State of Michigan, Records Management Services.

Overview

- Common Recordkeeping Problems
- Keeping Records
- Storing Records
- Destroying Records
- Getting Organized



Notes:

This training will address common recordkeeping problems. We will discuss best practices for keeping records, storing records, and destroying records. Then we will provide tips for getting your office organized.

Do you have?

- Disorganized records
- Trouble finding records
- Too much stuff



RTMB



HELP. CONNECT. SOLVE.

Notes:

Does your office have disorganized records? Trouble finding records? Too much stuff? Is that frustrating for you and your co-workers?

Does your desktop look like this?



RTMB



HELP. CONNECT. SOLVE.

Notes:

If records are not managed properly, the result can be chaotic. Hopefully, your desktop does not look like this. These employees may work for offices that have great filing systems. However, these employees are not using it, and are creating problems for everyone else in the office. How would you feel if this was your co-worker?

Are these storage spaces a mess too?

- Email Account
- Network Shared Drive
- Individual Network Drive
- Computer Desktop
- OneDrive
- SharePoint



HELP. CONNECT. SOLVE.

Notes:

Cubicles are not the only space where records can become out of control. Electronic records can also be disorganized and voluminous. Employees need to manage their email accounts, network shared drives, individual network drive and computer hard drive.



Notes:

Common recordkeeping problems include: version control, duplicate records, FOIA and litigation hold requests, disorganized records, retirements and departures, and more.

What words do you think of when you hear the phrase "records clean-up"?



Notes:

What words do you think of when you hear the phrase "records clean-up"? It probably does not make you feel excited and motivated. However, experience shows that people feel better when their work space is clean and organized. Well organized records help with productivity and reduce stress, because it is faster and easier to find the stuff you need.

Did you know ...



RTMB



HELP. CONNECT. SOLVE.

Notes:

Did you know that as a general rule, in every office approximately 30% of the records need to be retained but are not retrieved regularly, and should be moved off-site to low-cost storage; 40% of the records have met their retention requirements and should be destroyed; which makes it a whole lot harder to find the 30% of the records needed on-site for active reference and retrieval. When was the last time your office reviewed its recordkeeping practices?

Records Management Phases



Creation and
Receipt



Maintenance
and Use



Disposition

Notes:

Records are managed in three phases: creation/receipt, maintenance/use, and disposition. We are going to discuss each phase.

Creating and Receiving Records

Phase #1



RTMB

HELP. CONNECT. SOLVE.

Notes:

Agencies create and receive a lot of records. Not all of these records are “official records” that need to be kept. Employees need to determine which records are needed to document the activities of their agency. Then the records need to be named and filed appropriately so they can be retrieved when they are needed.

To Keep or Not to Keep?

Keep

- Records that document the office's performance, services, activities, decisions, and compliance
- Data that is generated or collected to support a business process
- Final versions that document a completed activity
- Messages that contain the full conversation and attachments

Don't Keep

- Publications from outside sources (newsletters)
- Personal documents (family, personal finances, friends)
- Mass mailings (received)
- Drafts replaced by new versions
- Duplicate records
- Records that don't document job duties and responsibilities
- Reminders
- Spam, advertisements, junk mail

Notes:

To keep or not to keep, that is the question... Employees often ask RMS how to know if they need to keep a record. These are examples of which records should be kept.

Keep records if: you are the designated recordkeeper, and the records document the office's performance, services, activities, decisions, and compliance, including data that is generated or collected to support a business process. Recordkeepers should retain final versions that document a completed activity, and messages that contain the full conversation and attachments.

Don't keep records if they are: publications from outside sources (newsletters), personal documents (family, personal finances, friends), mass mailings (received), drafts replaced by new versions, duplicate records, records that don't document your job duties and responsibilities, reminders, spam, advertisements, and junk mail.

Who is the Official Recordkeeper?



Notes:

The official recordkeeper is the employee responsible for filing and maintaining the essential records of a business process or activity. An employee could be the official recordkeeper if any of the following criteria apply. Employees should discuss their recordkeeping responsibilities with their supervisor.

In general, the lead employee or project manager is the official recordkeeper. If multiple employees serve as the lead on assigned projects or activities that are part of the same business process, then each of them should be responsible for filing the records in a shared filing system.

Other employees could be the official recordkeeper, if they are designated by their supervisor or a team, or if they are the only employee with the records.

The records should be stored in the designated "system of record" according to recordkeeping rules established by the office to promote consistency.

Employees who are not the official recordkeeper should delete redundant, obsolete and trivial (ROT) documents to reduce clutter of non-essential documents.

Tip: Organizing Records

- Organized records are easier to retrieve
- Good organization is the responsibility of the office
 - File cabinets and computers do not require that records be organized
- Filing systems should be
 - Easy to use
 - Used consistently
 - Easy to purge, without reviewing individual documents
- Large/Thick Files
 - May need sub-folders to separate document types, such as applications, licenses, case-related correspondence
- [Additional guidance is available from the RMS website](#)



Notes:

Organized records are easier to retrieve. When all of the records of a particular business process are kept together (centralized storage), staff only have to look one place to find the document they need to answer their question. Decentralized storage makes the search and retrieval process more difficult, and it increases the risk that the information found will be incomplete.

Good organization is the responsibility of the office and the user. File cabinets and computers do not require that records be organized.

Filing systems should be easy to use, they should be used consistently, and they should be easy to purge, without reviewing individual documents.

Large or thick files may need to be divided into sub-folders to separate different document types, such as applications, licenses, and case-related correspondence.

These filing tips work for both paper and electronic files. Additional guidance is available from the RMS website.

File Plans

- File plans provide a hierarchical structure for organizing records
 - **Level 1:** Business Process – all files related to a business process or activity should be stored together
 - **Level 2:** Folders – contain all documents related to an entity or topic
 - **Level 3:** Documents and Data – records that serve as essential evidence of activities
- Useful for both paper and electronic files
- [Additional guidance is available from RMS website](#)

Notes:

File plans provide a logical and hierarchical structure for organizing records.

Level 1 of the file plan is the business process or activity. All files related to a business process or activity should be stored together in the same file cabinet, drawer, Teams or SharePoint site, shared network drive, Electronic Document Management System, or Line of Business application. Employees should only have to look one place, the designated “system of record,” to find the document they need or the answer to their question. The files that are created to support the business process should be linked to the same record series on a retention schedule, either by applying standard operating procedures or by using technology to apply retention.

Level 2 of the file plan is the Folders. Folders contain all documents related to an entity or topic. Retention is applied at this level, so all documents in the folder should be eligible for disposition at the same time to avoid weeding.

Level 3 of the file plan is the documents and data. These records serve as essential evidence of activities.

These filing tips work for both paper and electronic files. Additional guidance is available from the RMS website.

Tip: Filing for Chronological Retention Periods

- Examples
 - RETAIN UNTIL: creation date, fiscal year ends, current year ends
 - PLUS: # days/months/years
- Solution
 - Organize the folders chronologically
 - Create separate folders for each month or year
- Disposition
 - Pull entire folders when the retention period is met
 - Avoid weeding the contents of a folder

Notes:

A chronological retention period is used when records are kept for an amount of time according to when they were created. For example, RETAIN UNTIL: creation date, fiscal year ends, or current year ends; PLUS: a specified number of days, months, or years.

When filing records with a chronological retention period, they should be stored in folders that are organized chronologically. Create separate folders for each month or year. This will allow the office to pull the entire folder when the retention period is met and avoid weeding the contents of a folder.

Tip: Filing for Conditional Retention Periods

- **Examples**

- RETAIN UNTIL: no longer active, event takes place, case is closed, permit expires
- PLUS: # days/months/years

- **Solution**

- Active Files: organize by entity (such as a person, group, location, or project)
- Inactive Files: organize by date file became inactive
- Re-activated Files: pull from inactive files and put in the active files; when they close again, put in the inactive files for the most recent closure

- **Disposition**

- Pull entire folder when the retention period is met
- Avoid weeding the contents of a folder



HELP. CONNECT. SOLVE.

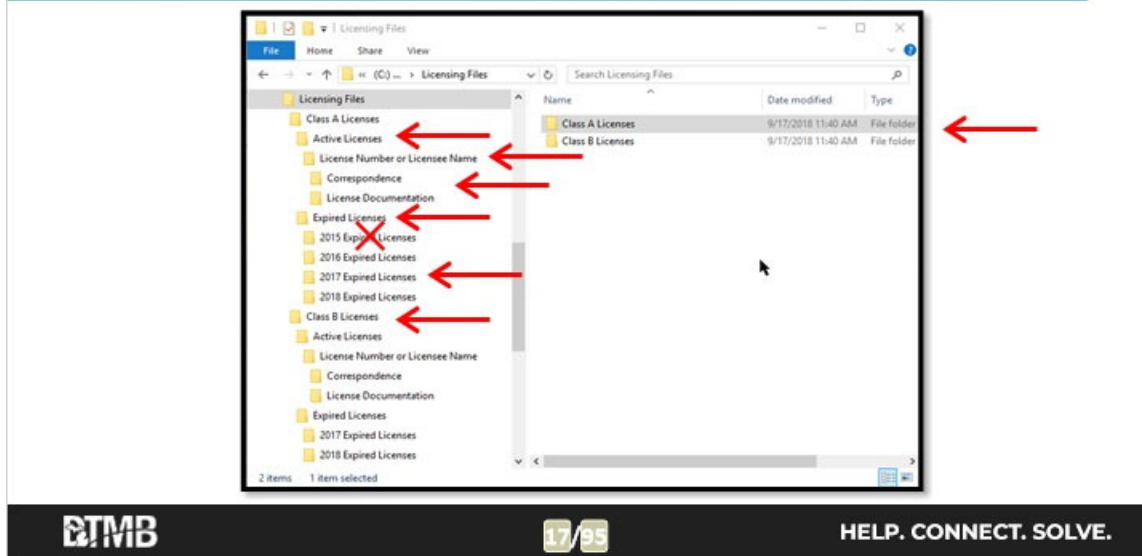
Notes:

A conditional retention period is used when records are kept for an amount of time according to when they are no longer active, because a specific condition rendered them inactive. For example, RETAIN UNTIL: no longer active, event takes place, case is closed, or permit expires; PLUS: a specified number of days, months, or years.

When filing records with a conditional retention period, they should be stored in folders that are organized by entity (such as a person, group, location, or project) when they are active. The inactive files should be organized by the date the file became inactive. If an inactive file is re-activated, it should be pulled from the inactive part of the filing system and put back in the active part of the filing system. Then, when they close again, put them in the inactive filing area for the most recent closure date (not the original closure date).

This filing method will allow the office to pull the entire folder when the retention period is met and avoid weeding the contents of a folder.

Example: File Plan Organization



Notes:

This is an example of an electronic filing system for licensing files.

In this example, the Class A licenses are filed separately from the Class B licenses.

The Class A active licenses are filed separately from the Class A expired licenses. The Class A active licenses could be organized either by license number or licensee name. Within the licensee's file are sub-folders for the correspondence and the actual license documentation. This makes it easier to find specific documents.

The Class A expired licenses are filed according to the year the license expired. The office can simply move the entire licensee folder from the active files to the expiration year folder when the license expires. When the retention period is met for the expired licenses, the folder for that year can be deleted (if there are no legal holds for specific licensees).

The Class B licenses are organized the same way the Class A licenses are organized.

This model file plan could be used for any type of case file, licensing file, permit file, as well as other types of files.

Tip: Naming Records

- Consistency helps employees find records they did not create
- Names should be unique - avoid confusion
 - Know what the record is without opening it
- Contain information employees know about the content
 - Is an index needed to find the correct record?
- Adopt rules
 - Abbreviations, acronyms, upper/lower case characters, numbering, name changes, etc.
- Electronic Sorting
 - Numbers: Know the maximum number of digits, and use zeros as placeholders
 - Dates: Do not spell out months, format by year-month-day
- [Additional guidance is available from the RMS website](#)



HELP. CONNECT. SOLVE.

Notes:

Employees often have to search for records that they did not create. Proper naming of folders and documents will help people find what they need quickly and easily. File names for folders and documents should be unique to avoid confusion. They should contain enough information, so people know what the record is without opening it. File names should contain information that employees know about the content, or there may need to be an index to help people search by assigned numbers or codes.

Offices should establish business rules, so records are named consistently. Business rules should address the use of abbreviations, acronyms, upper/lower case characters, numbering, codes, and name changes.

Keep in mind that computers often sort numbers before alphabetic characters in a file name. It is also important to know whether the filing system is case-sensitive. If an assigned number will be in the file name, it helps to know the maximum number of digits that will be used, and to use zeros as placeholders. Also, if you are naming by date, do not spell out months. Instead format the date by year, then month, and then day.

Additional guidance is available from the RMS website,
http://www.michigan.gov/documents/dtmb/rms_naming_499766_7.pdf.

3 Elements of a File Name

- **What** is it?
 - Contract, License Application, Complaint, Meeting Agenda, Budget Approval
- **Who** or **what** does it represent?
 - Company, Person, Litigation Case, License File, Project, Group, Agency
- **When** was it created?
 - Specific date (meeting date, filing date), Cycle (calendar year, fiscal year), Version (draft number, final, superseded)



Notes:

Elements of a good file name answer the questions what, who, and when. What is it? Is it a contract, license application, complaint, meeting agenda, budget approval, etc.? Who or what does it represent? Is it about a company, person, litigation case, project, group, agency, etc.? When was it created? Was it created on a specific date, like a meeting date or a filing date? Is it related to a particular calendar year or fiscal year? Or is it a particular version number of the document (draft number, final, superseded)?

Good Names Save Time

- Naming files consistently when they are created saves time later
- User can select order of the 3 elements - be consistent



Minutes.docx

[What]

Minutes – Executive Committee.docx

[What] [Who]

Minutes – Executive Committee 2022-10-07.docx

[What] [Who]

[When]

Notes:

Naming files consistently when they are created saves time later. It is worth the effort. For example, the name “Minutes.docx” does not answer who or when. The name “Minutes - Executive Committee.docx” does not answer when. Whereas, the name “Minutes - Executive Committee 2022-10-07.docx” contains all three elements - what, who, and when. The user can select order of the 3 elements and should be consistent. For example, it is fine to put the date (when) first.

Classifying Sensitive Records

- [Technical Standard 1340.00.150.02 – Data Classification Standard](#)
 - Protect sensitive information from unauthorized access and misuse
 - Reduce risk of security incidents via security controls
- Classification does not impact retention period, but does impact recordkeeping
- Classification Levels
 - Public
 - Internal
 - Confidential
 - Restricted
- Employees should know the level of records they create/use
- [Tip Sheet: Classifying Sensitive Records](#)



HELP. CONNECT. SOLVE.

Notes:

It is very important for Michigan government agencies to protect sensitive information from unauthorized access and misuse. The State of Michigan (SOM) adopted Technical Standard 1340.00.150.02 – Data Classification Standard to address this issue.

Classification is a process that identifies and categorizes information and recordkeeping systems based on their sensitivity, criticality, and risk. The classification level provides a framework for effective management and oversight of security controls. Without classification, there is an increased risk of inadequate security controls that may lead to a security incident. Agencies that experience a security incident can suffer reputational damage, operational downtime, loss of customer or public confidence, and have direct costs associated with managing the incident and notifying the affected parties.

The classification level of a record does not impact its retention period. Records with high classification levels can have short or long retention periods. However, the classification level can have a significant impact on recordkeeping practices, such as the location where records are stored, and security controls for access.

The SOM uses 4 classification levels: public, internal, confidential, and restricted. Employees should know the classification level of all records that they create and use to do their job. Supervisors are responsible for ensuring that their employees know and apply the correct classification level to all email, documents, and data. Microsoft 365 tools (Outlook, Word, Excel, and PowerPoint) require all SOM employees to apply classification levels to the email and documents that they save and send.

Independent vs Shared Filing

Independent Filing	Shared Filing
<ul style="list-style-type: none">• Retrieval: Employees must look multiple places to find records, and may not find everything they need• Volume: Employees hoard non-essential documents, drafts, and duplicates• Turnover: Supervisors don't have time to review individual files maintained by departing employees to find important records• On-boarding: Training new employees can be a challenge if institutional knowledge and records are lost• Security: Confidential or sensitive records may not be securely stored• Legal Liability: Increased volume of records that need to be reviewed and released for FOIA or litigation, because of inconsistent recordkeeping• Disaster Mitigation: Vital records are not identified and protected• Customer Service: Suffers – slower and inconsistent	<ul style="list-style-type: none">• Retrieval: Only one filing system needs to be searched• Volume: Fewer records are retained, which saves resources• Turnover: Records are not lost when employees depart• On-boarding: Institutional knowledge and records are protected• Security: Confidential or sensitive records are protected• Legal Liability: Reduced risk that recordkeeping issues will create problems for FOIA or litigation• Disaster Mitigation: Vital records are protected• Customer Service: Consistent quality control and assurance

Notes:

There are many problems associated with independent filing by employees.

Retrieval: Employees must look multiple places to find records, and may not find everything they need

Volume: Employees hoard non-essential documents, drafts, and duplicates

Turnover: Supervisors don't have time to review individual files maintained by departing employees to find important records

On-boarding: Training new employees can be a challenge if institutional knowledge and records are lost

Security: Confidential or sensitive records may not be securely stored

Legal Liability: Increased volume of records that need to be reviewed and released for FOIA or litigation, because of inconsistent recordkeeping

Disaster Mitigation: Vital records are not identified and protected

Customer Service: Suffers because it is slower and inconsistent

The solution is shared filing systems. The benefits of shared filing systems are the opposite of the problems. They include:

Retrieval: Only one filing system needs to be searched

Volume: Fewer records are retained, which saves resources, especially costs

Turnover: Records are not lost when employees depart

On-boarding: Institutional knowledge and records are protected

Security: Confidential or sensitive records are protected

Legal Liability: Reduced risk that recordkeeping issues will create problems for FOIA or litigation

Disaster Mitigation: Vital records are protected

Customer Service: Consistent quality control and assurance

Shared Filing Systems

- Work records are the property of the office, not individual employees
- Work records should be stored in shared filing systems, instead of individual user accounts or workspaces
- Independent storage of records wastes resources, reduces accessibility, and increases risk
- Supervisors are responsible for designating the filing system

Notes:

Work records are the property of the office, not individual employees. Work records should be stored in shared filing systems, instead of individual user accounts or workspaces. Independent storage of records wastes resources, reduces accessibility, and increases risk. Supervisors are responsible for designating the filing system for the business processes or activities they manage.

Step #1: Choose a Location

- **Questions:**

- Are the majority of the records created as paper or electronic documents? What percentage of the records are email? If formats are mixed, do paper files need to be scanned into digital images, or should electronic be printed?
- Who uses the files to do their job? Where are the users located (central office, district office, field workers)?
- Is special security needed for confidential or sensitive records?
- How often are the files retrieved (by employees, for FOIA requests, for litigation, etc.)?
- What is the retention period?
- Will additional resources be needed for storage and maintenance?

- [Tips: Electronic Records Storage Locations](#)



HELP. CONNECT. SOLVE.

Notes:

The process of converting from independent filing to shared filing will take time. The first step is to choose where the shared files will be stored. When choosing a location to store records, ask the following questions:

- Are the majority of the records created as paper or electronic documents?
- What percentage of the records are email?
- If formats are mixed, do paper files need to be scanned into digital images, or should electronic be printed?
- Who uses the files to do their job?
- Where are the users located (central office, district office, field workers)?
- Is special security needed for confidential or sensitive records?
- How often are the files retrieved (by employees, for FOIA requests, for litigation, etc.)?
- What is the retention period? Will additional resources be needed for storage and maintenance?

The answers to these questions will help identify an appropriate storage location that meets the agency's needs. RMS published a tip sheet about selecting storage locations for electronic records.

Step #2: Identify Essential Documents

- Reduce the clutter within files of non-essential documents
 - Examples: drafts, duplicates, transitory records
- Identify documents needed to comply with state or federal laws and regulations, or the agency's internal procedures
 - Examples: applications with required submission documents, approvals/denials, compliance communications, planning documents, reports, project charters, agreements, financial documents, etc.





Notes:

The second step is to identify the office's essential documents. Try to reduce the amount of clutter within files by eliminating non-essential documents like drafts, duplicates, transitory records.

The essential documents are the ones that need to be in the file to comply with state or federal laws and regulations, or the agency's internal procedures, such as applications with required submission documents, approvals/denials, compliance communications, planning documents, reports, project charters, agreements, financial documents, etc.

Step #3: Select Naming Conventions


- Assemble a team to define how files will be named

Category		
Grammar: noun then adjective	Minutes Web Governance 2021 -12-06.docx	Web Governance Minutes 2021 -12-06.docx
Readability: capitalize every word	Tips - File Naming.docx	tips file naming.docx
Special Characters: dashes or spaces, no underscores or other characters	Tips - File Naming – v02.docx	Λ:*"<> []{}&\$,._ Tips_File Naming_#02.docx
Dates: YYYYMMDD	20211206 2021-12-06	12062021 12-6-2021 December 6, 2021
Versioning: use zeros for single-digit numbers for sorting	v01, v02 Version01, Version 02 Final	v1, v10, v11, v2, v20, v3, v4
Spelling, Abbreviations: be consistent	Minutes Web Governance 2021 -12-06.docx Minutes Web Governance 2021 -12-20.docx	Minutes Web Governance 2021 -12-06.docx Min Web Gov 2021 -12-20.docx

Notes:

Assemble a team of employees who will be using the files to agree on naming conventions that will promote the fast and easy retrieval of information through consistency. The naming conventions should promote good grammar, answering the questions what, who, and when, which means the noun should appear before the adjective. They should promote readability, by capitalizing every word. They should avoid special characters, and format the dates by year, then month, then day. Version numbers should support sorting, and spelling and abbreviations need to be consistent.

Step #4: Check Out/Check In Procedures

- Employees need confidence that the filing system is complete and accurate
- Return records to the filing system by the end of the work day, if possible
 - *Electronic*: delete duplicates or file new versions by the end of the work day to avoid storage issues and confusion
 - *Email*: store in the shared filing system (paper or electronic) when the activity/task/conversation is completed 
 - *Paper*: use out cards when retrieving files or documents

Notes:

The fourth step is to establish check out and check in procedures for the shared files. Employees need confidence that the filing system is complete and accurate, or they may choose to keep their own copies of the records they use. This will create duplicate storage and version control problems for the office.

Employees need to return records to the filing system by the end of the work day, if possible.

If the records are electronic, the employee should delete duplicates or file new versions by the end of the work day to avoid storage issues and confusion.

If the records are email, the employee should store the messages in the shared filing system (paper or electronic) when the activity/task/conversation is completed. Inbox and sent mail folders should be used to remind the employee about incomplete activities/tasks/conversations. Older messages in a conversation string should be deleted when newer messages are sent/received (unless they contain important attachments). Non-essential email (like Gongwer) should be deleted by the end of the work day to avoid clutter.

If the records are paper, the employee should use out cards when retrieving files or documents, and then return the records by the end of the work day.

Step #5: Standard Operating Procedures (SOPs)

- SOPs ensure that everyone works consistently, and that quality controls are employed
 - Identify business processes within the office
 - Map the high-level steps of the process, and who is responsible
 - Procedures should define how to perform each task
 - Review SOPs annually, and update as needed
- [Additional guidance about recordkeeping rules is available from the RMS website](#)



HELP. CONNECT. SOLVE.

Notes:

The fifth step is to develop Standard Operating Procedures (SOPs) for the business process and the recordkeeping practices. SOPs ensure that everyone works consistently, and that quality controls are employed. The following are tips for developing new SOPs:

- Business Processes - analyze the duties of all employees and define the business processes of the office. This is a group activity. The activity may identify sub-processes of a larger process. Grouping the processes functionally may be helpful. Create a master list of each function and its processes.
- Process Mapping - at a high level, define the tasks involved in each business process from beginning to end, identify decisions that impact the tasks, define who is responsible for each task.
- Procedures - take each task from the process map and define the instructions (down to the click-level, if necessary) to perform the task. Don't leave out any details, this will be used to ensure consistency and to train new employees (assume the reader knows nothing before receiving the document). Identify who is authorized to create records, access records, modify records and destroy records. Identify any quality controls or quality assurance activities that are performed to ensure consistency, accuracy, and accountability. Identify where records are stored, at which step the records are filed (by whom), and if there are any naming conventions used. Identify the applicable Retention and Disposal Schedule that authorizes destruction. Identify who is responsible for each activity, and identify a back-up person, if possible.
- SOP Management - solicit input from all affected employees before adopting the SOP (you may be surprised who can contribute). Review and update the documents at least every 5 years. Use the SOPs to train new employees - this will test accuracy of the instructions.

Additional guidance about recordkeeping rules is available from the RMS website.

Step #6: Follow Retention Schedules

- Retain records according to schedules to reduce costs and legal liability
 - Are the records listed on a schedule (general or specific)?
 - Does the retention period meet the agency's needs?
 - Does the schedule match the organization chart?
 - Does each employee know how long to keep records?
 - Does the office clean up its records regularly?
 - Which employee is responsible for maintaining the shared filing system?
 - Are inactive paper records boxed for off-site storage at the Records Center?
 - Are historical records transferred to the Archives of Michigan?
 - Are confidential and sensitive paper records put in confidential destruction bins?

Notes:

The sixth (and final) step is to ensure the office is following its retention schedules. Retaining records according to schedules will reduce costs and legal liability. Answering the following questions will help with this step:

- Are the records listed on a schedule (general or specific)?
- Does the retention period meet the agency's needs?
- Does the schedule match the organization chart?
- Does each employee know how long to keep records?
- Does the office clean up its records regularly?
- Which employee is responsible for maintaining the shared filing system?
- Are inactive paper records boxed for off-site storage at the Records Center?
- Are historical records transferred to the Archives of Michigan?
- Are confidential and sensitive paper records put in confidential destruction bins?

Strategy for Re-organization

- **Adopting a new filing system will not happen overnight**
 - Assemble a team to develop new business rules and promote adoption of the new filing system
- **New System: Day-forward implementation**
 - Develop business rules for consistent use
 - Pick a start date for the new system
 - Build new recordkeeping habits and refine rules
- **Old System: Clean up is a separate project**
 - Wait 6-12 months to clean up old system
 - Develop new habits first
 - Clean up will be easier



HELP. CONNECT. SOLVE.

Notes:

If the current filing system does not support these principles, supervisors should assemble a team to design and implement a new system. Re-designing a filing system can feel overwhelming and intimidating, and it won't happen overnight. These tips may make it easier, and they will help focus the implementation for long-term success.

First, establish recordkeeping rules (like naming conventions) for how the system will be used. Then, select a start date for the new system and train everyone who will be affected.

Try implementing the new system day-forward first. Give the staff 6 to 12 months to develop new habits using the new system and refine the new recordkeeping rules. Then, when the grace period is over, go back and clean the older files using the new habits that were developed. It should make the clean-up easier. This methodology may temporarily create two different systems for two different timeframes. Eventually, they will be merged.

Email Management



HELP. CONNECT. SOLVE.

Notes:

Let's take a few minutes to discuss email management. Would you keep all of your mail in your mailbox at the curb? Of course not. You review it, and then toss it or act upon it. The same principles apply to email. Unfortunately, many employees let their email stay in their account indefinitely, where they forget about it. We need to improve the ways that email is managed.

50 + Years of Email

- Email was invented in October 1971
 - Technology to support sending electronic messages between computers in different locations
- Email use increased steadily over the past 30 years, and it is a primary tool for business communication
- Today, most employees cannot function effectively at work without email



Notes:

Email technology that supports sending electronic message between computers in different locations was invented in October 1971.

Email use increased steadily over the past 30 years, and it is considered to be the primary tool for business communication today. In fact, most employees cannot function effectively at work without email.

Email Retention Principles

- Purpose of the email system is to send and receive email messages
- Email system is not a record retention/storage tool
- Email should be stored in the office's designated filing system with other records



Notes:

Purpose of the email system is to send and receive email messages. It is not a record retention or storage tool. Email should be stored in the office's designated filing system with other records.

What is the Retention Period for Email?

- There is no single retention period for all email, just like there is no single retention period for all paper
 - Email is a format that a record is stored in
- Retention is based upon the content of the message, and the business process it supports
 - If message is about ...
 - Contracts - keep as long as other contract records
 - Personnel issues - keep as long as other personnel records



Notes:

There is no single retention period for all email, just like there is no single retention period for all paper. Email is a format that a record is stored in.

The retention period for an email message depends upon the content of the message, and the business process it supports. For example, if message is related to a contract, it needs to be kept as long as all other contract records. If message is related to a personnel issue, it needs to be kept as long as all other personnel records.

You are Effectively Managing Your Email If...

- Messages that are still in your email account (inbox and sent mail):
 - Have not been read yet, or
 - Are related to tasks awaiting further action
- Messages that are records are filed with other records that document the business process, either electronically or in paper form
- Messages that are not records are deleted



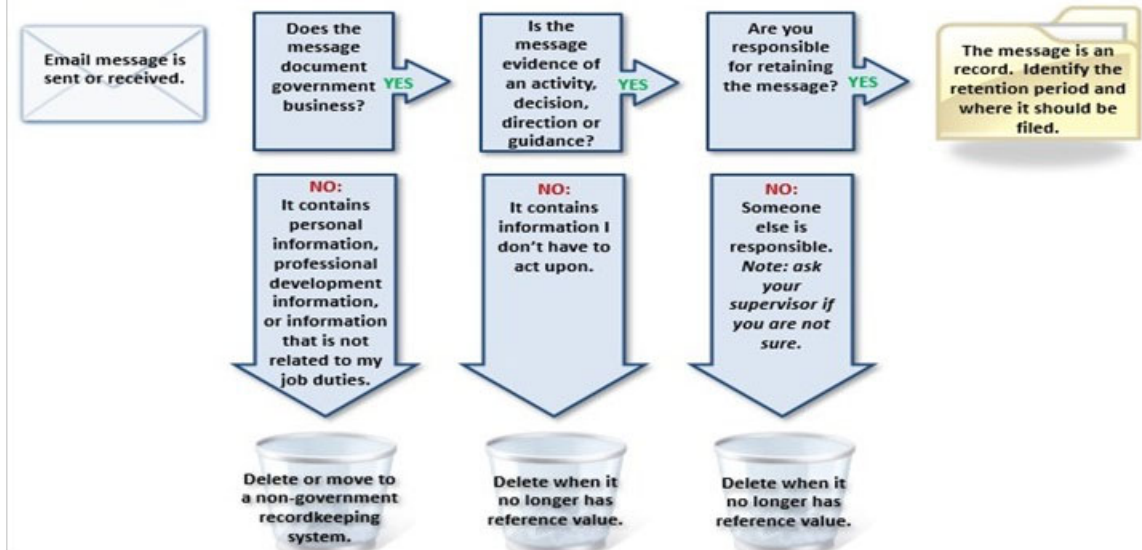
Notes:

You are effectively managing your email if...messages that are still in your email account (inbox and sent mail) have not been read yet, or are related to tasks awaiting further action.

Messages that are records are filed with other records that document the business process, either electronically or in paper form.

Messages that are not records are deleted.

Do I need to retain this email message?



Notes:

How can you determine if you need to keep a particular email message? When you send or receive a message, as yourself these questions:

Does the message document government business? If yes, go to the next question. If no, delete it.

Is the message evidence of an activity, decision, direction, or guidance? If yes, go to the next question. If no, delete it.

Are you responsible for retaining the message? If yes, file it. If no, delete it. If you don't know, ask your supervisor.

Tips: Cleaning Email Accounts

- **Don't Wait:** make retention ASAP
- **Conversations:** only keep the last message, if it includes the content (including attachments) of all the previous messages
- **Don't Keep Duplicates:** rely upon the designated file, so there is less confusion about drafts and versions
- **Calendars:** retain appointments for 2 years (GS-ADM-0103)
- **Trash:** empty deleted items and junk mail often (remains in the Microsoft Cloud for additional 30 days)
- **Mass/Bulk Cleaning:** know your longest retention period, organize all email by year, and annually delete oldest messages



Notes:

Tips for cleaning up email accounts:

- Don't wait, make retention decisions as soon as possible. The longer you wait, the harder it will be to remember which are important, and which are junk. Only keep what you are responsible for filing.
- Only keep the last message in a conversation, if it includes the content (including attachments) of all the previous messages.
- Don't keep duplicates. Rely upon the designated file, so there is less confusion about drafts and versions.
- Retain calendar appointments for 2 years per GS-ADM-0103.
- Empty deleted items and junk mail often. Be aware, deleted email remains in the Microsoft Cloud for 30 days after the trash is emptied.
- Know the longest retention period for the records that you are responsible for retaining. Organize all email by year, so you can do an annually delete the oldest messages with a single click, instead of reviewing each message.

Celebrate the Little Victories

- Deleting the non-records, transitory records and personal records is easy
- Most messages will have the same retention period--even if you have a lot of records
- Start developing new habits today--it feels good!
- Smaller email accounts are less overwhelming



Notes:

Celebrate the little victories at work! Deleting the non-records, transitory records and personal records is easy. Most messages will have the same retention period--even if you have a lot of records, so it should not be difficult to figure out what you need to keep. Start developing new habits today--it feels good! Smaller email accounts are less overwhelming.

Manage Your Email

10 minutes/day – 3 simple steps

Step #1: Delete It

Delete spam, mass mailings, and messages with no reference value

Step #2: File It

File email that needs to be kept, but requires no action, into Outlook folders or the designated filing system

Step #3: Act On It

Remaining messages require action - when done, go to steps 1 or 2



HELP. CONNECT. SOLVE.

Notes:

Managing your email does not need to be time consuming and complex. It will take most people less than 10 minutes a day to follow 3 simple steps.

Step #1: Delete It - Delete spam, mass mailings, and messages with no reference value.

Step #2: File It - File email that needs to be kept, but requires no action, into Outlook folders or the designated filing system.

Step #3: Act On It - Remaining messages require action (such as sending a reply or waiting to receive a reply) - when you are done, go to steps 1 or 2.

Maintaining and Using Records

Phase #2



RTMB

HELP. CONNECT. SOLVE.

Notes:

Once an employee decides to keep the records, those records will be maintained and used until their retention period ends and they become eligible for disposition.

Retention Periods

- Retention Period: amount of time that the official recordkeeper maintains records to support administrative, fiscal, and legal requirements
- Some retention periods are short, and some are long
- Length of the retention period can influence how the records will be maintained



Notes:

The Retention Period is the amount of time that the official recordkeeper maintains records to support administrative, fiscal, and legal requirements. Some retention periods are short, and some retention periods are long. The length of the retention period can influence how the records will be maintained.

Storage Options

- Cabinets
- Shelving
- Closets
- Cubicles
- Electronic storage
- Off-site storage
- Secret places nobody wants to admit exists...



Notes:

Records can be stored in a lot of places, such as cabinets, employee cubicles, closets, electronic storage (including shared drives, email accounts, SharePoint and other EDM, cloud, hard drives, external devices, etc.), off-site storage, and secret places nobody wants to admit exists...

Nobody has unlimited funds or storage space

- There is no “one size fits all” solution
- Different records and processes have unique needs
- Understand the total cost of ownership



Notes:

However, nobody has unlimited funds or storage space. There is no “one size fits all” solution for storing records. In fact, different records maintained by the same office may need different storage solutions, because they may have unique needs. Their volume, format and usage may be different. It is important to understand the total cost of owning a storage solution, from acquisition to implementation to maintenance.

Cost of Recordkeeping

- Costs are different for each type of recordkeeping system
- Cost factors include:
 - Employees
 - Volume of records
 - Method of record creation and modification
 - Storage and security
 - Frequency of access, and type of access needed



Notes:

Costs are different for each type of recordkeeping system. Cost factors include: employees, volume of records, method of record creation and modification, storage and security, frequency of access, and type of access needed.

Conduct a Needs Analysis

- Define your problem
- Analyze your current processes
 - How/why records are created
 - Storage (volume, location, security)
 - Indexing
 - Retrieval activity (who, how often, where)
 - Workflow and record modifications
 - Retention
- Identify all potential solutions
- Compare the costs of the solutions



Notes:

When choosing a recordkeeping system, you need to define your problem, your current processes, and identify all potential solutions. Then you can analyze and compare the costs of the potential solutions.

Comparing Options

- Cost of initial implementation
- On-going maintenance and storage costs
- Impact of changing how the office does business
- Cost of new staff and equipment
- Timelines for implementation
- Training time for employees



Notes:

When comparing these various storage options, you need to consider the cost of initial implementation, on-going maintenance and storage costs, the impact of changing how the office does business, the cost of new staff and equipment, timelines for implementation, and training time for employees.

Successful Solutions

- Technology alone cannot solve recordkeeping problems
- Consistent recordkeeping by all employees is crucial to success
- Dangers
 - Undefined business rules
 - Improper use of the system



Notes:

Keep in mind that regardless of which option you choose, technology alone cannot solve recordkeeping problems. Consistent use of the recordkeeping system is crucial to the success of the solution. The dangers that threaten the success of the solution include undefined business rules that lead to inconsistent usage, and improper use of the system by employees. It is important to recognize that employees may resist change, and to have a plan to address the situation.

Protecting Records

- Agencies are responsible for managing and protecting their records
 - Records must remain accessible and usable for the entire retention period
 - Maintain good recordkeeping systems
 - Adopt a disaster plan for records
- **Damaged Records:** agency is responsible for recovering records not past retention
 - Vendor that specializes in disaster response or record restoration may need to be hired
 - Agency is responsible for all restoration and recovery costs
- **Destroyed Records:** document what/when/how they were destroyed
 - Keep documentation until retention period is met

Notes:

Agencies are responsible for managing and protecting the records they own and keeping them accessible and usable for their entire retention period. Agencies should identify which of their records are vital and need to be protected in case a disaster occurs. A disaster plan is helpful to define how the agency will try to prevent disasters and respond to disasters.

If records are damaged (but not destroyed) during a disaster, the agency is responsible for recovering those records that have not met their retention period yet. This may require them to hire a vendor that specializes in disaster response or record restoration. The agency is responsible for all restoration and recovery costs.

If government records are totally destroyed during a disaster and are not recoverable, the agency should document which records were destroyed, and when/how the destruction occurred. This information should be kept until the destroyed records' retention period is met.

An online guide is available to assist with disaster preparedness and response.

Off-site Storage

*State Records Center
and
Service Providers*



HELP. CONNECT. SOLVE.

Notes:

Off-site storage may be an option for some records, if the agency does not have the space or resources needed to maintain records in-house or on-site. Paper records can be stored at the State Records Center. Electronic records may be stored with service providers, such as DTMB-IT or vendors.

Why use off-site storage?

- Paper
 - Office space is limited
 - Off-site warehouse storage is cheaper than office storage
 - Boxes are cheaper than file cabinets
 - Shared labor and overhead costs are lower per unit
- Electronic
 - IT resources and skills are not available in-house
 - Cloud storage may be cheaper
 - Vendor may be contracted to create and store SOM records



HELP. CONNECT. SOLVE.

Notes:

Why should an agency consider off-site storage an option?

Office space is limited for paper storage, especially for offices that are moving to new space that is often smaller than their previous space. Off-site warehouse storage is cheaper than office storage for paper. The 2017 rates for space in state office buildings in downtown Lansing was \$13 per square foot per year. This is compared to Records Center costs of \$4 per box per year. Boxes are cheaper than file cabinets. Finally, there is an economy of scale; shared labor and overhead costs are lower per unit. Bottom line, off-site storage is a good solution for records with low retrieval activity, such as closed files.

If the records are electronic, the agency may not have the IT resources and skills that are needed in-house to maintain the IT application. In addition, cloud storage is often a low-cost option, if appropriate security is applied. Also, many agencies contract with vendors to create and then store records that are owned by the State of Michigan.

State Records Center

- Services
 - Temporary storage for inactive physical records in boxes
 - Open shelf (unboxed) storage for active paper records
- Security
 - Records are accessible to authorized individuals
 - Fire and theft protection



Notes:

The State Records Center that is operated by RMS provides for the temporary storage of inactive physical records in boxes for state agencies. The State Records Center recently added a fee-based service called “Open Shelf” for unboxed storage of active physical records in boxes. This service is optional for agencies that do not have space in their offices. Agencies are not required to send items to the Records Center. If agencies find paper records in their offices that already fulfilled their retention period, they can destroy the records themselves at their offices.

All records stored at the Records Center remain the property of the creating agency. Records can be retrieved when they are needed, but can only be accessed by authorized individuals. Agencies can pick up records at the Records Center for urgent retrievals. Normal retrieval is 1-3 business days. The building also has fire and theft protection.

Records Center Database

- User accounts are authorized by departmental Records Management Officers (RMO)
- Used to:
 - Submit records to Records Center and Archives of Michigan
 - Retrieve records from Records Center
- Manages Records Center destruction and Archives transfer



Notes:

The Records Center database manages the boxes that are stored at the State Records Center. User accounts are requested by RMOs. To protect the security of the records, it is important that employees do not share user accounts. Temporary employees and students can get their own user account. The database is accessed using the State of Michigan's intranet. It is used to submit records to Records Center and the Archives of Michigan, and to retrieve records from Records Center. All boxes and many files are barcoded. Each container is linked to Retention and Disposal Schedules, so the State Records Center can generate destruction notices and Archives transfer notices for boxes that have met their retention period.

Records Center Boxes

- Records Center shelves are designed to hold specific boxes
 - Boxes can be ordered by your agency's authorized office supplies purchaser
- Do not over-stuff boxes
- Assemble boxes correctly
- See [tip sheet](#) for instructions



Notes:

Records Center shelves are designed to hold specific boxes. The approved boxes can be ordered by your agency's authorized office supplies purchaser. It is very important to not over-stuff the boxes, so they fit on the shelf. Also, boxes need to be assembled correctly. RMS has a tip sheet available online that contains instructions.

Records Center Destruction

- Boxes are linked to a schedule and have an assigned destruction date upon arrival
 - Active files should not be sent to the Records Center
 - Closed files that re-open should be permanently checked out and returned to the active filing system
- Records are destroyed at the box level
 - Individual files are not destroyed separately
 - All files in a box must have the same destruction date
- Frequency: twice annually
 - Destruction notices are sent to RMOs for approval
 - Legal holds are tracked
 - All boxes are destroyed confidentially



Notes:

Records Center Destruction: Boxes at the Records Center are linked to a schedule and have an assigned destruction date upon arrival. Active files should not be sent to the Records Center, because the appropriate destruction date is not known if the file is still open.

Closed files that re-open should be permanently checked out from the Records Center and returned to the active filing system. These files should be stored in a new box with a new destruction date when they close again.

Be aware, that all records at the Records Center are destroyed at the box level. Individual files are not destroyed separately, so all files in a box must have the same destruction date.

Records Center destruction is conducted twice annually. Destruction notices are sent to RMOs for approval before boxes are destroyed. RMOs distribute the notices to their liaisons throughout the department for review. Boxes can be held beyond the destruction date if they are still needed for a legal hold or a schedule revision. All boxes are destroyed confidentially.

More Records Center Information

- Records Center Procedures and User Instructions
 - [Available online](#)
 - Topics: sending records, retrieving records, returning records
- Customer assistance
 - 517-335-9132
 - recordscenter@michigan.gov



Notes:

The Records Center Procedures and User Instructions are available online at inside.michigan.gov/recordsmanagement. They contain information about sending records, retrieving records, and returning records.

State employees who need assistance can call the Records Center at 517-335-9132, or send an email to recordscenter@michigan.gov.

Service Providers

Include

- DTMB-IT Agency Services
- DTMB-RMS: Content Manager EDM
- Cloud storage
- Vendors contracted to create and maintain SOM records



Notes:

There are a lot of different types of service providers who can be maintaining records for a SOM agency. They may include: DTMB-IT Agency Services, DTMB-RMS: Content Manager EDM, cloud storage providers, and vendors contracted to create and maintain SOM records.

Contracts or Agreements

- Legal document should define the terms of the service provided
 - Clarify that the records are owned by the SOM agency
 - Address security and access to protect confidential information
 - Refer to the schedule that approves the retention period
 - Describe the disposition process
 - Disposition method
 - Frequency
 - Activating, tracking and de-activating legal holds
 - Review and approval of records to be disposed of during each cycle
 - Ensure destroyed records cannot be recovered/reconstructed/
released
 - Quality controls and quality assurance

Notes:

SOM agencies should have contracts or other types of agreements, like charters, with the service provider that documents the terms of the service. These legal documents should clarify that the records are owned by the SOM agency, address security and access to protect confidential information, refer to the Retention and Disposal Schedule that approves the retention period, and describe the disposition process. The disposition procedures should cover the disposition method, frequency, activating, tracking and de-activating legal holds, review and approval of records to be disposed of during each cycle, ensuring that destroyed records cannot be recovered/reconstructed/released, and quality controls and quality assurance.

Disposing Records

Phase #3



HELP. CONNECT. SOLVE.

Notes:

Once the retention period ends, records need to be disposed of in a defensible manner to ensure that no legal issues arise.

Defensible Disposition

“The effective disposal of physical and electronic information that does not need to be retained according to an organization’s policies when the data is not or no longer subject to a legal requirement for retention, be it statutory or as part of a litigation.”

–*The Sedona Conference Glossary*

Notes:

Defensible disposition is “The effective disposal of physical and electronic information that does not need to be retained according to an organization’s policies when the data is not or no longer subject to a legal requirement for retention, be it statutory or as part of a litigation.” – The Sedona Conference Glossary (The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition, 21 SEDONA CONF. J. 263 (2020).)

Defensible Disposition

Q: What makes the disposition process defensible?

A: Procedures that ensure:

- Correct records were accurately identified as being eligible for disposal
- Disposal activities were authorized, documented, and implemented according to reasonable, transparent, predictable, and consistent procedures and quality controls



Notes:

What makes the disposition process defensible? Procedures that ensure: the correct records were accurately identified as being eligible for disposal, and disposal activities were authorized, documented, and implemented according to reasonable, transparent, predictable, and consistent procedures and quality controls.

Disposition Methods

- Retention and Disposal Schedules identify which disposition method is approved at the end of a record's retention period:
 - Destruction
 - Complete obliteration of records so they cannot be retrieved or accessed
 - Preservation
 - Transfer of records with historical value to the Archives of Michigan for permanent preservation
- State Archivist chooses the disposition method, not the agency

Notes:

Retention and Disposal Schedules identify which disposition method is approved at the end of a record's retention period: Destruction or Preservation.

Destruction is the complete obliteration of records so they cannot be retrieved or accessed.

Preservation is the transfer of records with historical value to the Archives of Michigan for permanent preservation. Michigan law authorizes the State Archivist to choose the disposition method, not the agency.

Suspending Destruction

FOIA, Litigation, Audit, Investigation

- *Remember!* Immediately cease the destruction of relevant records
- Legal holds suspend retention schedules
- Holds apply to records in all formats
- Failure to cease the destruction could result in penalties
- Confirm holds before destroying records
 - Check with your supervisor, FOIA and litigation coordinators



Notes:

Agencies must suspend destruction of records that are requested for FOIA, litigation and audit, even if destruction is authorized by a retention schedule. If relevant records exist in electronic formats, agencies should notify information technology staff. Failure to cease the destruction of relevant records could result in penalties from state or federal courts. It is important to confirm whether the records in your office are covered by an active legal hold. Ask your supervisor, and if they are unsure, contact FOIA and litigation coordinators.

Physical Destruction Options



HELP. CONNECT. SOLVE.

Notes:

It is important that records be destroyed using appropriate methods. There are three primary methods for destroying physical records. They include the trash, recycling and confidential destruction.

Trash

- Trash bins and dumpsters are not secured
- Exposed to the environment
- Handlers may not have security screenings
- Trash is taken to an open landfill
- Landfill could be in another state or country
- DO NOT PUT RECORDS IN THE TRASH!



Notes:

Trash bins and dumpsters are not secured, and they are not locked to prevent access by “dumpster divers.” They are often exposed to the environment, and the contents could be scattered when transferred to a truck and while travelling. Trash handlers generally do not have to go through security screenings. Trash is taken to an open landfill that could be located in another state or country. The information could be accessed by anyone. Do not put records in the trash; it is for banana peels and coffee cups.

Recycling

- Collection containers are not locked
- Trucks and warehouses may not be secured
- Handlers may not go through security screenings
- Raw paper is sold on the open market
- Information remains accessible until records are processed at paper mill
- **DO NOT RECYCLE CONFIDENTIAL RECORDS!**



Notes:

Recycling bins and containers are not locked, and the material is taken to an open warehouse for processing and baling. During transit the material is often not secured, and the truck drivers and handlers may not go through security screenings or background checks. Raw paper is sold on the open market, and then hand sorted according to paper grades. Information in the records is not destroyed and remains intact throughout the process. It could be accessed by anyone until it is actually utilized at a paper mill. Do not recycle confidential records.

Shredding May Not Be Good Enough

- Strip cut shreds can still reveal full lines of text
- Shredded records can be reconstructed
- Be aware of how the shreds will be disposed of to prevent reconstruction



Notes:

Be aware that shredding may not be good enough. Strip cut shreds can still reveal full lines of text, and there is software on the market that can be used to reconstruct shredded records. This software works with strip shreds, cross cut shreds and hand ripped shreds. Be aware of how the shreds will be disposed of to prevent reconstruction. A bag of shredded records is like a red flag to dumpster divers. The flag says that the bag contains “good stuff.”

Not All Shreds are Equal



strip cut shred compared
to grinder shred



comparing different
particle sizes

Notes:

Not all shreds are equal. The image on the left shows the difference between strip cut shreds and grinder shreds that comply with the State of Michigan's confidential records destruction contract. The image on the right shows examples of different destruction particle sizes.

Confidential Destruction

- Prevents reconstruction of materials
- Prevents inappropriate release of information
- State of Michigan contract requirements
 - Paper: 1mm x 5mm particle size
 - Material is recycled ♻️
 - Film, computer hard drives and disks: 1/35 inch particle size
- **SECURELY DESTROY ALL CONFIDENTIAL RECORDS**



Notes:

Confidential destruction methods prevent reconstruction of materials, and the inappropriate release of information. The State of Michigan contract requires that paper be destroyed to 1 mm x 5mm particle size. This can be accomplished with pulverization or grinding, and then the material is recycled. Film, computer hard drives and disks must be destroyed to 1/35 inch particle size, which is essentially dust. It is accomplished with grinding. It is vitally important that all agencies securely destroy all confidential records.

Vital Records Control (VRC)

- Statewide Confidential Destruction Service
 - Bins are locked
 - Company is bonded
 - Destroyed within 24 hours of pickup
 - Secure vehicles and facility
 - Flexible scheduling for pickup
- Contact VRC:
 - 616-735-2900
 - <https://vitalrecordscontrol.com/>



Notes:

VRC is the current vendor for statewide confidential destruction. They provide locked bins in state office buildings for storing records until they are picked up for destruction. The employees are bonded and have background checks, and they must destroy records within 24 hours of pickup. All vehicles and the facility are secured, and they offer flexible scheduling for pickup of materials. Each location that hosts a bin is linked to an agency's index code for billing. Please make sure that your bins are full each time they are picked up to keep the costs down. VRC can be contacted by calling 616-735-2900.

Confidential Destruction Process



RTMB

70/95

HELP. CONNECT. SOLVE.

Notes:

These are images of the confidential destruction process. First is an image of the locked bins. Next, is a scale for weighing the bins. Then the grinding machine. Finally, the ground paper.

Pulverized Paper



Notes:

This is an image of what pulverized paper looks like compared to the size of a penny.

Confidential Destruction of Records

- [Confidential Destruction of Records tutorial is available online](#)
- Tutorial takes about 10 minutes



Notes:

If you have co-workers who handle confidential records, there is a 10-minute online tutorial about confidential destruction.

Electronic Records Destruction

- Delete Does Not Mean Delete!
- Deleted files might be stored elsewhere
 - Recycle bins
 - Backup tapes
 - Duplicate copies (printouts, disks, external drives, cloud, Internet)
- Comply with SOM IT Standard 1340.00.110.04 (*Secure Disposal of Installed and Removable Digital Media*)



Notes:

Agencies need to dispose electronic documents and data in compliance with schedules too. Keep in mind that delete does not necessarily mean delete. Deleted files might be stored elsewhere including electronic trash bins, backup tapes, computer memory until it is overwritten, and there could be duplicates in a lot of places. It is also important to know that computer forensic tools can sometimes recover records from overwritten memory. Be aware that DTMB has a procedure for securely destroying digital storage media.

Data Disposition

- Databases and IT Applications
 - Can data be deleted?
 - Select data fields to query to find data eligible for destruction
 - Identify who has the capability to run the query and delete the data
 - Internal employees, DTMB IT, vendor, etc.
 - Confirm that data deletion won't corrupt the data that remains
 - Determine the frequency of data disposition
 - Does any data need to be transferred to the Archives of Michigan?

Notes:

Technology raises unique questions and issues about the disposition of data and documents in databases and IT applications. For example, can data be deleted? Some databases and applications are designed in a way that prevents data deletion. If data can be deleted, select data fields to query to find data eligible for destruction. Then, identify who has the capability to run the query and delete the data – for example, internal employees, DTMB IT, or a vendor. Next, confirm that data deletion won't corrupt the data that remains. If there is a risk of data corruption, you should work with IT to identify a solution, or request a schedule revision of the retention period. It is important to establish defensible procedures that describe how the disposition will be conducted, including the frequency. Finally, determine if any data needs to be transferred to the Archives of Michigan, and contact the Archives to make transfer arrangements, if necessary.

Archives of Michigan



Michigan's first
constitution, 1835



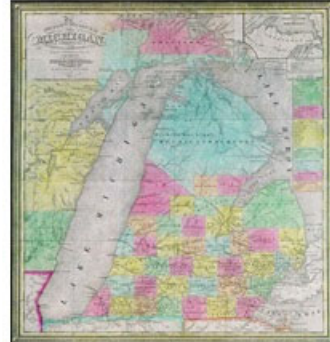
HELP. CONNECT. SOLVE.

Notes:

Government records are approved for transfer to the Archives of Michigan on Retention and Disposal Schedules. Every government agency has the potential to create records that will be transferred to the Archives.

Archives of Michigan

- Provides for the permanent preservation of records with legal and historical value
- Schedules identify which records are transferred to the Archives
- Storage areas have environmental and security controls
- Transferred records are held by the Archives for the people of Michigan
- Records can be accessed by the public, unless confidential



Notes:

The Archives of Michigan provides for the permanent preservation of records with legal and historical value. Retention and Disposal Schedules identify which records are transferred to the Archives, and agencies cannot destroy those records. The Archives' storage areas have environmental and security controls to protect records. All transferred records are held by the Archives for the people of Michigan. Records in the Archives can be accessed by the public, unless they are confidential or there are other privacy or security concerns. (Agencies can work with the Archives to identify any access restrictions or concerns.)

Transferring Records to the Archives

- Records Center Transfer
 - Annual transfer of designated state records to the Archives
 - Agency receives a notice from the Records Center before the records are transferred
- Direct Transfer
 - Contact the Archives at govarchives@michigan.gov to receive instructions



Notes:

Records are transferred to the Archives of Michigan in two ways.

The records can either be sent to the Records Center first for off-site storage, and then be transferred to the Archives in compliance with the Retention and Disposal Schedule. If this happens, the agency will receive a notice annually that identifies the records that are authorized for transfer to the Archives. The agency must approve the transfer before it is implemented.

The other method is to send the records directly to the Archives. Please contact the Archives at govarchives@michigan.gov to receive instructions for transferring records.

Archives of Michigan

702 West Kalamazoo Street

Lansing, Michigan 48913

517-335-2576

govarchives@michigan.gov

<https://www.michigan.gov/archivesofmi/>



RTMB

77/95

HELP. CONNECT. SOLVE.

Notes:

The Archives is located in the Michigan Library and History Center building at 702 W. Kalamazoo St in Lansing. Agencies can call the Archives at 517-335-2576 or email them at govarchives@michigan.gov. Their website is www.Michigan.gov/archivesofmi.

It's Time to Get Organized!

Plan a Clean-up Day



RTMB

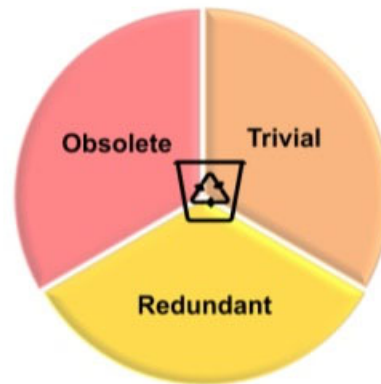
HELP. CONNECT. SOLVE.

Notes:

It's time for your office to get organized. Remember, your recordkeeping problems are only going to get worse if they are ignored. So you should plan a clean-up day for your office.

Redundant, Obsolete, Trivial (ROT) Records

- **Redundant:** Records that exist and are duplicated in multiple places, whether in the same filing system or across multiple locations
- **Obsolete:** Records that already met their retention period and are not subject to additional legal requirements
- **Trivial:** Records that have little to no business value



Notes:

Redundant, Obsolete, and Trivial records are known as ROT.

- **Redundant:** Records that exist and are duplicated in multiple places, whether in the same filing system or across multiple locations
- **Obsolete:** Records that already met their retention period and are not subject to additional legal requirements
- **Trivial:** Records that have little to no business value – such as junk mail, reference information that is no longer useful, personal records, or system files that are automatically generated by an IT application

Why do employees hoard records?

- **Uncertainty:** never know when you might need it
- **Productivity:** more stuff demonstrates more effort
- **Fear:** don't want to be in trouble if it is gone
- **Technology:** enables creation and storage of more
- **Volume:** no time or motivation to sort through the stuff
- **Hidden:** out of sight, out of mind
- **Accountability:** no requirement to clean up

Notes:

Why do employees hoard records?

- **Uncertainty:** you never know when you might need it.
- **Productivity:** some employees think more stuff demonstrates more effort.
- **Fear:** employees don't want to be in trouble if it is gone.
- **Technology:** enables creation and storage of more stuff.
- **Volume:** employees don't have time or motivation to sort through the stuff.
- **Hidden:** electronic records in particular are out of sight, out of mind.
- **Accountability:** no requirement to clean up. If your supervisor does not tell you to clean up the mess, why would you spend the time to do it?

Sorry...
We can't clean your office for you.



RTMB

HELP. CONNECT. SOLVE.

Notes:

Sorry, Records Management Services cannot clean your office for you.

Clean up Time - First Steps

- Clean-up the low-hanging fruit first
 - Non-records
 - Delete non-records that are not needed
 - Don't keep duplicates longer than the retention period of the official record
 - Store reference documents separately from official records
 - Transitory Records
 - Delete when issue is addressed, and they are no longer needed
 - Personal Records
 - Delete personal records that are not needed
 - Do not store using government resources



Notes:

It's clean up time. Here are some steps you can take to make the process less stressful. Clean-up the low-hanging fruit first. It should be easier to find and delete the following types of documents:

1. Non-records - delete non-records that are not needed, don't keep duplicates longer than the retention period of the official record, and store reference documents separately from official records.
2. Transitory Records - delete when issue is addressed, and they are no longer needed.
3. Personal Records - Delete personal records that are not needed, and do not store personal records using government resources.

Clean up Time - Next Steps

- Official Records
 - Identify if the records are covered by a general schedule or an agency-specific schedule
 - Contact RMO for assistance if the record is not listed on an approved schedule
 - Destroy records that already met their retention period
 - Use shared filing systems
 - Most employees are only responsible for < 5 record series

Notes:

Next Steps

4. Official Records - identify if the records are covered by a general schedule or an agency-specific schedule. Contact RMO for assistance if the record is not listed on an approved schedule. Destroy records that already met their retention period. Use shared filing systems. Remember, most employees are only responsible for less than 5 record series, so it should not be difficult to remember how long to keep stuff.

Clean up Time - More Steps

- Manage email daily
 - Don't let the volume of email get out of control
 - Make retention decisions upon receiving or sending a message
- Regularly clean up all storage spaces: email, shared drive, file cabinets, cubicles, document management systems, databases, etc.
- Suspend the destruction of records, if necessary
 - FOIA, Litigation, Audit, Investigation

Notes:

More Steps:

5. Manage email daily - don't let the volume of email get out of control, make retention decisions upon receiving or sending a message.
6. Regularly clean up all storage spaces - email, shared drive, file cabinets, cubicles, document management systems, databases, etc.
7. Suspend the destruction of records, if necessary for FOIA, litigation, audit, or investigation.

Snack It & Pack It Day

- Purpose
 - Kick start record clean-up
 - Initiate a routine clean-up habit
- Select a date
 - Everyone is available, no meetings, no leave time
- Distribute information to staff
 - Orientation presentation
 - Tip Sheet: Records Clean-up
- Clean-up
 - Shared and individual locations
 - Physical and electronic locations



Notes:

Plan a Snack It & Pack It Day. The purpose of this day is kick start a record clean-up, and to initiate a routine clean-up habit. Select the date and clear everyone's calendars of meetings for the day. Make sure everyone is working on clean-up day and not on leave. Then distribute information to staff, including the orientation presentation and a tip sheet that are available online. These can be used at a staff meeting about a month prior to the clean-up day to help employees plan ahead. Make sure staff plan to clean-up both shared and individual storage locations, as well as physical and electronic storage locations.

Clean-up Should be Comprehensive

- Give assignments to employees
 - Everyone needs to review email, cubicles, desktops, individual network drives, etc.
 - Who is reviewing file cabinets?
 - Who is reviewing the shared drive? (assign folders to SMEs)
 - Who is reviewing databases, spreadsheets, document management systems, and IT applications?
 - Who is contacting the agency's vendors about records that they create and store for the agency?



Notes:

Clean-up should be comprehensive. Give assignments to employees for clean-up day. Everyone needs to review email, cubicles, desktops, individual network drives, etc. However, who is reviewing the file cabinets? Who is reviewing the shared drive? Do specific folders need to be assigned to subject matter experts? Who is reviewing databases, spreadsheets, document management systems, and IT applications? Who is contacting the agency's vendors about records that they create and store for the agency?



Notes:

This poster is a fun way to get motivated for Snack It & Pack It Day. It says, "Don't be an air head, milk dud, or goober. Get all your chicks and ducks in a row!"

You have mounds and mounds of whatchamacallit all over the milky way.

Take a few extra steps and detour from your daily responsibilities to clean.

Remember to take 5 and delete your spam. It will only take a minute.

Score big by cleaning and help save your office 100 grand.

Let's make sure there is good and plenty space in the office and network storage.

Don't be a ding dong. Mike and Ike and all your peeps are doing it. So should you!

Ps. Be sure to snicker and chuckle while you clean. It will make the time fly!"

Quiz Time!

Are the statements on the following slides True or False?



Notes:

Are the statements on the following slides true or false?

Our office should have check out/
check in procedures for our paper
and electronic files.

- True
- False

89/95

Notes:

Is this statement true or false? Our office should have check out/check in procedures for our paper and electronic files.

The correct answer is: True. Employees need to know where files are located when a shared filing system is used.

It's ok to keep personnel communications in my work email account for the entire retention period.

- True
- False

90/95

Notes:

Is this statement true or false? It's ok to keep personnel communications in my work email account for the entire retention period.

The correct answer is: False. Personnel records won't be accessible to the employees who need them if they are stored in an email account. They should be kept with the other personnel records.

On clean-up day I need to destroy the withdrawn applications that contain social security numbers according to the retention schedule. I can put them in the recycle bin.

- True
- False

91/95

Notes:

Is this statement true or false? On clean-up day I need to destroy the withdrawn applications that contain social security numbers according to the retention schedule. I can put them in the recycle bin.

The correct answer is: False. Records that contain confidential information, like social security numbers, need to be put in confidential records destruction bins, so they are disposed of properly.

When a case file closes our office should move it to an inactive file location for the remainder of the retention period.

- True
- False

92/95

Notes:

Is this statement true or false? When a case file closes our office should move it to an inactive file location for the remainder of the retention period.

The correct answer is: True. Keeping active and inactive files in separate locations makes it easier to find records, and to apply retention.

My Records Center box is only partially filled with records, so it's ok to put our office's holiday decorations in the box.

- True
- False

93/95

Notes:

Is this statement true or false? My Records Center box is only partially filled with records, so it's ok to put our office's holiday decorations in the box.

The correct answer is: False. Holiday decorations are not records and cannot be sent for storage. However, it is ok to send partially filled boxes to the Records Center.

We can help!

Records Management Services

3400 N. Grand River Ave.

Lansing, Michigan 48909

517-335-9132

recordscenter@michigan.gov

State Government:

<https://inside.michigan.gov/recordsmanagement>

Local Government:

<https://www.michigan.gov/recordsmanagement>

 The image can't be displayed.



HELP. CONNECT. SOLVE.

Notes:

Please contact Records Management Services if you need assistance with records retention, recordkeeping systems, and other records management issues. The phone number is 517-335-9132.

Thank you for taking this class. We hope you will visit our website and take more records management classes.