State of Michigan
Records Management Services

Tips: Record Clean-up

Central Office Files vs Individual Files

- Individual employees should only have files at their desk for active projects or assignments.
- The central filing system should be the master record.
- Employees should check out files when they take them to their desk. Use a log or an out card to document who took the file and when they took it.
- Employees should return closed or inactive files to the central filing system promptly. Make this a step in the standard operating procedures for closing a project or case.
- Reference and duplicate documents maintained by individual employees should be reviewed regularly to identify and toss obsolete materials.

Implementing Retention (paper and electronic)

- Store the records for each business process in a separate filing system.
- Know the approved retention period for the records in the filing system.
- It may help to organize some files chronologically, if they are eligible for Records Center storage or destruction when they reach a specified age.
- Establish a system for flagging closed files when they close. Make this a step in the standard operating procedures for closing a project or case. Create a separate location for storing closed files so they are not mixed with active files. For example, if closed files are stored at the Records Center, box them when they close and ship the box when it is full.
- Destroy physical records in a confidential destruction bin, if they contain confidential or sensitive information.
- Retention and Disposal Schedules identify which records have historical value and should be transferred to the Archives of Michigan for permanent preservation.
- Verify that records are not needed for FOIA, litigation or audit before purging.
- If a record exists in both paper and electronic formats, decide which is the duplicate, and avoid storing both.
- Electronic records are hardware and software dependent. Establish a plan for keeping them accessible when the original technology becomes obsolete.

Shared Network Drives

- Used to store records that are shared by office employees, including drafts and templates.
- Establish office rules for appropriate use to avoid uncontrolled growth and disorganization.
- A file plan will help organize the drive. It will have separate sections for each program in the office, and separate sections for each business process. *(See Guide to Organizing and Naming Files.)*
- Establish naming conventions for files and documents to promote consistency and easy retrieval. *(See Guide to Organizing and Naming Files.)*

- Supervisors should designate which employees are responsible for periodic cleaning of specific files.

Individual Network Drives

- Used to store personal records needed at work (work-related travel, professional development and training, personnel documents, etc.)
- Do not store music, videos, photos and documents that are not needed for work duties.

E-Mail Accounts

- There is no single retention period for all e-mail. Retention is based upon the content of the message.
- Keep e-mail that is related to tasks or activities that are active or incomplete in the e-mail account.
- File e-mail that is about completed issues/activities in the designated filing system for the business process.
- Delete duplicates, drafts, informational notices, mass mails, junk mail, etc.
- Only keep the last message in a conversation string, if it contains all previous communications and attachments.
- Communicate with co-workers who receive the same message, to determine who is responsible for keeping the records.
- Ask your supervisor for direction, if you do not know which e-mail you are responsible for filing, or where it should be filed.

Computer Hard Drives and Desktops (C:\ drive)

- Are not backed up to protect against loss of vital information.
- Are not accessible to co-workers.

External Storage Devices (disks and drives)

- Intended for temporary storage and transport of records.
- Are not personal property
- May not have sufficient security to protect sensitive or confidential information.
- Are not backed up to protect against loss of vital information.
- May not be accessible to co-workers.
- Are unstable and have a short shelf life.

Agency Owned Data (databases, spreadsheets, document management systems, cloud and vendor storage, etc.)

- Data that has met its retention period should be purged regularly, in compliance with an approved schedule. Agency may need to establish procedures with IT or vendor to support this activity.
- Some databases need a field (like an open/closed toggle, or a date field) that can be used to identify data that is eligible for purging.
- Confirm data backup processes with IT or vendor.