State of Michigan

Records Management Services

Tip Sheet: Employee Off-Boarding and Record Retention

Employee separation can have a significant impact upon an office's operations, because records could be lost, forgotten, or destroyed when an employee leaves. This can affect customer service, quality of work product, and employee morale. It also creates legal liabilities, if the records are requested for Freedom of Information Act (FOIA) requests or litigation, and they cannot be produced.

Records can be stored in a lot of places. Some of those places are centralized and shared by everyone in the office (such as file cabinets, shared network drives, SharePoint team rooms, etc.). Some storage spaces are assigned to specific individuals (such as cubicles, email accounts, individual network drives, OneDrive accounts, etc.).

Regardless of where the records are stored, the retention of these records is governed by Retention and Disposal Schedules. Schedules provide the only legal authorization to destroy records. However, implementation of schedules must be temporarily suspended when legal actions (like FOIA or litigation) take place.

Good Recordkeeping Systems Prevent Chaos

Work records are the property of the office, not the employee. Don't wait for an employee to leave to address how records are maintained by the office. A good recordkeeping system can help the office operate more effectively, regardless of who is working.

TIPS

- Employees should not keep work records in places that only they have access to. This includes email accounts, individual network drives, computer hard drives, peripheral devices (like CDs, DVDS, thumb drives, or external hard drives), cubicles, or personal devices or property (like personal cell phones or their home).
- Supervisors should designate the filing system for each business activity that they manage. This filing system can be paper-based or electronic.
- Establish recordkeeping rules for the filing systems, so search and retrieval of records is easy. Files need to be organized and named or labeled using conventions that make sense to everyone in the office.
- Ensure that the filing system is accessible to all employees who use the records to do their job. Otherwise, employees will hoard their own copies of records, or avoid using the designated filing system.
- Establish check-out and check-in procedures, so the location of files that are in use is known at all times.
- Employees should file email that needs to be kept to comply with retention schedules in the designated filing system as soon as a conversation ends.
- Employees should not keep duplicates in unofficial locations. Duplicates create the risk that different versions of a record will have different information (which creates confusion about

the accuracy of versions), that records will not be appropriately released for FOIA requests or litigation, that duplicates will be kept longer than the official copy, and that confidential information won’t have appropriate security.

- Work groups should designate who is responsible for keeping the group’s records, so they avoid duplicate storage.
- Supervisors should ensure consistent employee compliance with the filing system. If an employee has a mountain of records piled on their desk, or if the shared drive is a mess, it affects everyone in the office. It wastes resources, it increases search and retrieval time, and it causes frustration among employees.
- Ensure that all of the office’s records are covered by an approved record retention schedule.
- Ensure the office complies with retention schedules by regularly destroying records that have met their retention period. This should be done at least annually.

Employee Off-boarding

Supervisors become responsible for the accounts of their separated employees, including email, individual network drives, and M365 storage. Verify that the employee did not keep official records in any location that will be closed upon departure. Be aware that approximately 60-70% of records that are maintained by offices are redundant, obsolete, or trivial (ROT), and they need to be destroyed. Supervisors should focus on finding the records that are essential for current and future activities.

TIPS

- Identify if any records need to be kept, because their retention periods are not met (note: the records in these accounts may have multiple different retention periods).
- Determine if any of the records need to be re-filed into shared recordkeeping systems, so the employees who still work in the office can access them.
- Identify projects that the employee worked on. Then, do a keyword search for records that relate to those projects.
- Identify the major job duties of the employee, and search for folders, messages and documents that relate to those job duties.
- Identify the longest retention period for records the employee was responsible for, based upon their job duties. Delete anything older than that timeframe, and identify when the youngest records will be eligible for disposition.
- Designate other employees in the office with similar job duties and expertise as the former employee to review the records, and set a reasonable deadline for completing the review.
- Identify if the employee was involved in any active litigation or investigation that would require a record disposition hold after the employee departs.
- Manager or supervisor should submit a request to delete accounts of former employees after verifying all records are in a secure location. Employee accounts (email, individual network drives, M365 storage) will be deleted 30 days after request is submitted.