



Origination:	03/2001
Last Approved:	07/2020
Last Revised:	07/2020
Next Review:	07/2021
Owner:	<i>Erika Linden</i>
Area:	<i>Administration</i>
References:	
Applicability:	<i>Des Moines University</i>

## Records Retention and Disposal Policy

### I. PURPOSE

Des Moines University is committed to effective records retention to preserve its history, ensure that critical records are available to meet business needs, comply with legal and accrediting requirements, optimize the use of space, minimize the cost of records retention and ensure that outdated and useless records are destroyed. To accomplish this goal, DMU requires that University records be retained for specific periods of time, that the records be maintained in designated official repositories and that records be retained, archived or destroyed according to the procedures outlined in this document.

### II. SCOPE

This policy applies to all University employees who create, store or use University Records in any format.

### III. DEFINITION

#### A. Record

The term "Record" under this policy means all forms of recorded information, regardless of physical characteristics or format, that are created, received, or filed in the course of University business. Records serve as evidence of the University's organization, functions, policies, decisions, procedures, operations and other activities. Records also document University programs, serving as resources for future historical research. While Records are easily recognizable in paper format, most Records are now created electronically, including e-mail, word processing files, spreadsheets, databases, web pages, videos and a variety of other digital formats.

The term "Record" does not apply to non-University information created, received or filed by a University employee while at work, or to transitory information with no business or historical value. Transitory information may include, but is not limited to, telephone and voicemail messages with no business or historical value.

"Business or historical value" means the usefulness of information for carrying out the day-to-day activities of the University, including documentation of the University's organization, functions, policies, decisions, procedures, operations and other activities.

For purposes of this policy, Records should be considered as one of four types:

1. Active Record

A record with current use for the department that generated it and that is easily accessible. Records

remain active for varying periods of time, depending on the purpose for which they were created.

2. Inactive Record

A record with no current use for the department that created it but that has not yet reached the end of its retention period. Inactive Records should be stored according to the procedures defined in this policy.

3. Archival Record

A record that is no longer currently used by the department in which it originated or was received, but has permanent legal, institutional or historical value. Archival Records are stored in the University Archives located in the library, or in a location approved by the University Library Director.

4. Expired Record

A Record that has been retained for the full period prescribed in the [Records Retention Schedule](#).

## B. Definition of Confidential Records

Confidential Records are those containing confidential information as defined in the [Data Classification](#) policy which include, but are not limited to, personally identifiable information, material subject to specific protections under federal or state law or regulations or under applicable contracts or non-disclosure agreements, or information whose loss or unauthorized disclosure could impair the functions of the University, cause significant financial or reputational loss or lead to possible legal liability.

## IV. POLICY

### A. Records Management and Ownership

DMU Records are retained in accordance with all applicable laws and regulations. All University employees are responsible for ensuring that University Records are maintained, preserved and destroyed in accordance with this policy. The University provides additional guidance on information and document management in policies related to information classification, information security, HIPAA, FERPA, and research.

1. All Records subject to this policy are the property of Des Moines University and not the property of a specific person, program or department.
2. The unauthorized destruction, removal, alteration or use of University Records is prohibited.
3. The management and storage of Records rests with the department creating the Record or to which the information in the Records pertains. Every office, department, program or college in control of University Records is responsible for the following:
  - a. Implementing Records management practices consistent with this policy, including the identification of Records for active, inactive or archival storage and proposing to the Chief Compliance Officer changes in the [Records Retention Schedule](#).
  - b. Identifying an individual within the office, department, program or college to serve as the Departmental Records Officer. The identity of this individual should be reported to the Chief Compliance Officer who will maintain a list of Departmental Records Officers. The Departmental Records Officers will assist departmental leadership with the following:
    - Participating in periodic training and educating department staff on Record management practices and procedures.
    - Preserving Records as required under this policy.
    - Properly disposing of Inactive Records at the end of the applicable retention period.

- Conferring with Library Director regarding which Records should be considered for storage in the University Archives.
  - Transferring historically significant Inactive Records to the University Archives.
  - Protecting Records from misuse, damage, alteration, destruction, or theft, or from access by unauthorized parties.
  - Reviewing Records annually to determine the completeness and accuracy of the records retention system and to adjust Record status based on the retention schedule.
  - Monitoring compliance with this policy.
  - Conferring with the Chief Compliance Officer regarding questions.
4. Every committee, whether at the University or department level, is responsible for maintaining Records that describe the decisions, discussions, recommendations and other information pertaining to the charge of the committee. Committee Records hold significant value as historical records because they document decision-making, governance and changes over time and, accordingly, are archival material.
  5. When an employee leaves a position, all Records under the control of that employee should be reviewed and managed according to this policy. To ensure smooth transitions, the Records may need to be transferred to another employee, into the department's filing system or to an off-site location. University departments should establish procedures to ensure that Records in the possession of employees at the time of separation are managed properly and that important University information is not inadvertently destroyed or mishandled.

## **B. Management of Confidential Records**

University Records containing confidential information, particularly those protected by FERPA and HIPAA, will be maintained, controlled and protected to prevent unauthorized access. Confidential Records will be destroyed, retained or archived as defined by the [Records Retention Schedule](#) and based on procedures outlined in this policy.

## **C. Oversight and Review**

The Chief Compliance Officer will provide ongoing Record retention and disposal review and oversight. The Chief Compliance Officer will guide the University in the implementation, monitoring and periodic review of this policy and compliance with this policy.

# **V. PROCEDURES FOR RECORDS RETENTION AND DESTRUCTION**

## **A. Records Retention Schedule**

1. The [Records Retention Schedule](#) defines the length of time each type of Record shall be retained. A University Record should not be retained beyond the period specified in the schedule unless a reasonable probability exists that the Record may be needed in the future.
2. The [Records Retention Schedule](#) should be reviewed at least annually by each department. Proposed changes, additions or revisions to the schedule should be reviewed with the appropriate department or division leadership and submitted to the Chief Compliance Officer for evaluation of the legal, fiscal, administrative and historical value of the Record to determine the appropriate length of time to maintain

such records. The Chief Compliance Officer will amend the Records Retention Schedule as necessary.

3. The [Records Retention Schedule](#) lists types of Records and the length of time those Records must be retained. Questions regarding the retention period for a specific Record or class of Records not included in the retention and disposal schedule should be directed to the Chief Compliance Officer.
4. Exceptions to the Records Retention Schedule
  - a. Litigation and Potential Litigation: Regardless of the [Records Retention Schedule](#), any Record or other document (hard copy or electronic) that is relevant or potentially relevant to pending litigation or to any matter reasonably likely to result in litigation must be retained until such litigation is completely resolved and closed.
  - b. Government Investigations: Regardless of the [Records Retention Schedule](#), any University Record or other document (hard copy or electronic) that is relevant or potentially relevant to any pending government investigation or inquiry must be retained until such investigation or inquiry is finally resolved and closed.
  - c. To ensure compliance with these restrictions, the senior official responsible for overseeing the litigation or investigation will communicate to all appropriate personnel regarding the designation of University Records to be maintained outside of the specified retention period. Records subject to such designation are to be retained until notice has been sent authorizing their release. Once released, the Records will be maintained or destroyed according to the retention schedule.

## B. Retention Practices

1. University Records must be maintained in the following manner:
  - a. Confidential Records

Departments must implement practices that protect confidential information contained in University records in accordance with relevant laws and University policies. Such protections must be applied in maintaining Active Records, the storage of Inactive and Archival Records and the destruction of Expired Records. In other words, the level of security that applies to a confidential Active Record must be maintained when such a Record becomes inactive, archival or expired.
  - b. Transition from Active to Inactive or Archival Status

Each department will review Records for which they are responsible at least annually to determine if they are Active, Inactive, Archival or Expired.

    - If a department determines that Active Records are no longer needed for business or academic reasons, but the applicable retention period has not yet expired, the records are categorized as "Inactive" and transferred to the University's off-site storage facility with destruction date noted for automatic disposal.
    - If a department determines that Active Records that are no longer needed for business/ academic reasons are Archival, it should confer with the University Archivist to coordinate transfer of the records to the University Archives. In all cases the department must contact the Library staff prior to sending any files or artifacts to confirm acceptance and ensure a timely and orderly ascension into the archives inventory.
2. Record Formats
  - a. Hard Copies. Hardcopies must be retained in a hardcopy form unless it is converted to electronic format in a University centrally managed system.

- b. Electronic Records, including e-mails. Electronic Records, such as e-mails and other electronic documents that are not retained in a University centrally managed system, should be saved in a format that the University can reproduce for later access if necessary.

E-mail Records that have been printed should be saved as paper documents. Regardless of the format in which the e-mails are saved, employees should retain or destroy them in accordance with the [Records Retention Schedule](#).

University Records maintained in electronic form must be stored on network servers, not on an individual computer or other devices where controls may not be in place for sufficient retention. Electronic Records stored within the University's centrally-managed system must follow the [Information and System Use policy](#). Each Record should be stored in a manner that is accessible by more than one authorized user so that the Record remains accessible in the absence or departure of a single individual.

## C. Destruction Protocols

1. When the retention period for Active or Inactive Records has expired (and the records are non-archival), the Records should be destroyed.
2. Records that are not confidential may be over written, degaussed, discarded or recycled.
3. Destruction of records containing confidential information must be completed in a manner that permanently and irretrievably destroys the material as follows:
  - a. Paper Records:
    - May be destroyed on-site by shredding; or
    - May be placed in locked storage bins for pick-up and destruction by the provider contracted by the University for this service. Confidential Records being held for destruction must be stored in locked containers. Employees must transfer confidential material to locked containers daily before leaving their workspace.
  - b. Electronic Records and other non-paper media:
    - Must be destroyed or erased so that confidential information cannot be read or reconstructed. Simply deleting the Record is not sufficient to ensure destruction; the data sanitation process required will depend on the type of media.
    - Contact Information Technology Services for assistance in destruction of electronic media.

## D. Archival Records Retention

1. Archival records shall be retained permanently within the collection unless they fit one or more of the criteria for deaccessioning.
  - a. Criteria for Deaccessioning and Disposal
    - The record is of poor quality and lacks value for exhibition or research purposes.
    - The record is a duplicate that has no value as part of a series.
    - The archive's possession of the record may not be consistent with applicable law, (e.g., the work may have been stolen or illegally imported in violation of applicable laws).
    - The authenticity or attribution of the record is determined to be false or fraudulent.
    - The physical condition of the record is so poor that restoration is not practical or would

compromise the material's integrity. Records damaged beyond reasonable repair that are not of use for study or teaching purposes may be destroyed.

- The record is no longer consistent with the mission or collecting goals of the Archive.
- The Archive is unable to care adequately for the record because of the record's requirements for storage or display or its continuing need for special treatment.

2. Items meeting these criteria will be submitted, along with a proposal for deaccessioning, by the Archivist to the Library Director for approval.

- a. After approval by the Library Director, the Archivist will thoroughly document the deaccessioned item, and then appropriately remove from the collection.

## VI. PROCEDURES FOR MANAGING OFF-SITE STORAGE AND DESTRUCTION

1. The University currently contracts with MDS Records Management for the off-site storage of University Records. Each department will be responsible for the expense of off-campus storage that will be reflected in account 110-XXXX-53299 in its individual budget. University funds may not be used to store Records that exceed the time period specified in the [Records Retention Schedule](#). Departments are cautioned to avoid the storage of duplicative Records that are the primary responsibility of other departments. Documents that do not meet the definition of a University Record and duplicate materials are to be destroyed rather than sent to offsite storage
2. The Administrative Assistant in Accounting and the Accounts Payable Associate will assist in the off-campus storage procedure and will be the key University contacts for company-level administration, including department-level authorizations in the absence of a Level 1 authority for the department.
3. The Chief Compliance Officer will provide any needed assistance in the interpretation of or compliance with the [Records Retention Schedule](#).
4. Records which are to be stored must be placed in a banker's box with one or two cubic foot capacity and with handles or hand-openings. New boxes may be purchased through the University's contracted office supplies vendor.
  - a. All records stored at MDS must comply with the following guidelines:
    - All boxes must be labeled with a destruction date or marked for permanent retention.
    - Boxes should include similar documents or documents with the same destruction date.
    - Review each file prior to storage to remove and destroy duplicative materials or those that do not need to be retained.
    - Face all file folders in the same direction.
    - Leave approximately 1 – 1.5 inches of space in the box to facilitate servicing.
    - Do not mix record media (i.e. microfiche) with paper Records.
    - Do not use hanging folders, 3-ring binders, or binder clips.
  - b. Each box stored at MDS requires a "container bar code" and a transmittal form. The bar codes and transmittal forms may be obtained from MDS by calling (515) 266-6301.
    - The container bar code includes a large bar code and a small numbered tab.
      - Place the large bar code on the lower left corner of the handle-end of the box.

- Place the small numbered tab on the transmittal form with the corresponding box description.
  - Complete the transmittal form (obtained from MDS) and make a copy for your Records.
    - For a more detailed report of the items contained within a box, create your own document on Word or Excel that will contain the specifics.
  - c. Call MDS for pickup of boxes (515) 266-6301.
5. MDS manages the destruction of boxes in accordance with the destruction date provided for each container sent to the MDS storage facility.
- a. Prior to destruction, a form is sent to DMU for destruction approval and signature from the requesting department's Level 1 MDS authorized individual and one additional MDS authorized individual from the department.
  - b. MDS maintains the signed form for 10 years after the documents have been destroyed. The MDS system permanently maintains the information of the documents destroyed and the DMU personnel approving the destruction. DMU personnel may request this information as needed.
6. Each department will designate one person as the Departmental Records Officer. The Departmental Records Officer will:
- a. Become knowledgeable about the [Records Retention Schedule](#).
  - b. Determine the disposition of departmental records per the [Records Retention Schedule](#).
  - c. Facilitate the review and approval of Destruction Reports sent by Accounting listing boxes scheduled for destruction. Obtain two authorized signatures on each page of the Destruction Report; one signature must be from a Level 1 authorized individual as recorded on MDS authorization lists.
  - d. Maintain a master list of all departmental Records in storage.
  - e. Maintain the MDS authorization signature sheet for boxes stored off-site.
  - f. Maintain the MDS transmittal forms for boxes stored off-site including:
    - The bar code number of each box sent for storage.
    - The box number as assigned by the department.
    - The date range for the Records contained in each box
    - An index or listing of the files/Records contained in each box.
    - The name of the department to which the Records belong.
    - The account number that is applicable to the box.
    - The date the box was sent to storage.
    - The date the box is to be destroyed or reviewed for destruction.
  - g. Maintain the MDS pickup and delivery work orders and receipt as well as the containers by account report as provided by MDS.
7. The department budget officer will receive monthly invoices for the storage costs of department Records along with other billable activity such as adding, retrieving, and destroying records. Invoices must be reviewed for accuracy by the budget officer or designee. This individual must communicate with the Accounts Payable Associate on a timely basis about any issues or discrepancies on invoices.
8. Records that are not sent to MDS for storage must be reviewed for destruction on at least an annual basis

by the Departmental Records Officer.

## Approved By:

Angela Franklin, Ph.D., President

### General Disclaimer

The information available in PolicyStat is not to be treated or implied as a contract but rather as a unilateral statement of University policies. The University reserves the right to revoke, modify or suspend any of its policies or procedures at any time without notice.

## Attachments

[Records Retention Schedule for 2020](#)

## Approval Signatures

Approver	Date
Angela Franklin	07/2020
Erika Linden	07/2020

## Applicability

Des Moines University

COPY