Contents

Policy Name

4.1070 Records Management and Retention

Purpose and Scope

This policy defines the Records Management and Retention practices for Alvernia University ("AU")

Alvernia University requires that University records be retained for specific periods of time and has designated official repositories for their maintenance. These records must be managed according to the procedures outlined in this document.

The University is committed to effective records retention to preserve its history, meet business and legal needs and standards, optimize the use of space, minimize the cost of record retention, and ensure that outdated and useless records are destroyed. All records created, received, or maintained by University departments during their operations belong to the University and are retained and disposed of according to this policy. University records must be kept until the stated minimum retention period has elapsed.

Responsibilities

Title or Role	Definition and What They are Responsible For
Director, Environmental Health, Safety and Risk Management	Maintains and enforces this policy. Receives exceptions to the policy.
Senior Vice President of Academic Affairs and Provost	Maintains and enforces this procedure. Receives exceptions to the policy.
Senior Leadership Team	Serves as final approval for policy and assists with reviewing exceptions to the policy.

Policy

The University is committed to effective records retention to preserve its history, meet business and legal needs and standards, optimize the use of space, minimize the cost of record retention, and ensure that outdated and useless records are destroyed. All records created, received, or maintained by University departments during their operations belong to the University and are retained and disposed of according to this policy. University records must be kept until the stated minimum retention period has elapsed.

Those responsible for adhering to this policy should consult the University's Records Retention Schedule

For policy questions, clarification, and interpretation, contact the Director of Environmental Health, Safety and Risk Management.

Definitions:

Active Records: Documents including both written and printed matter, books, drawings, maps, plans, photographs; microfiche; films, sound and video recordings; computerized data on disk, tape, or any other electronic media record

in a format not mentioned; or copies thereof made or received by any academic or administrative office of the University in connection with the transaction of University business, and retained by such office as evidence of the activities of the University or because of the information contained therein.

Administrative Value: The usefulness of records in current or future University operations.

Archival Records: University records which are inactive and are not required to be retained in the office in which they originate or are received. These records have permanent or enduring legal, fiscal, administrative, research or historical value and therefore should be retained and preserved indefinitely.

Correspondence: Any form of written communication sent or received during a department's business. The term includes letters, memos, notes, e-mail, faxes, etc.

Creator: The person, department, or office that creates, receives, or assembles records.

Data Steward: The division head, department head or designee charged with implementation of this policy regarding records of his or her unit, department, program, and/or committee.

Disposable Records: University records which have temporary value, and in consequence thereof, may be destroyed after the lapse of a specified period of time, or after the occurrence of some act which renders them valueless.

Disposition: The action to be taken at the end of the active life of a record. Dispositions may include 1) retain permanently in the office of creation; 2) transfer to inactive storage; 3) transfer to remote storage; 4) transfer to the University Archives; 5) destroy after the legal retention period.

Fiscal Value: Required for budget development, financial reporting, or audit purposes.

Inactive Records: Records which are no longer used on a regular basis.

Information Technology: The Information Technology Department of the University.

Legal Value: Contain or constitute evidence of the University's legally enforceable rights and obligations.

Metadata: the data providing information about one or more aspects of the data, i.e. data on the data.

Memorabilia: Items of historical value such as programs, posters, brochures, clippings, buttons, flags, stickers, etc.

Official Repository: The department or office designated as having responsibility for retention and timely destruction of particular types of official University records. Such responsibility is assigned to the data steward.

Research or Historical Value: Document the purpose, growth, history, services, programs, and character of the campus.

Retention Period: The minimum time a record must be kept by law, custom, or the custodians of the record.

Schedule: The Records Retention Schedule maintained by the Director of Environmental Health, Safety & Risk Management.

University Archivist: Senior Leadership or their designee is responsible for 1) identifying which official University records are archival; and 2) effecting the transfer of archival records from the office in which they originated or were received to the University Archives, subject to the appropriate retention schedule referenced in this document.

Policy Procedure

A. Managing Official University Records

Departments and offices that maintain University records are called "official repositories." These administrative units are responsible for establishing appropriate record retention management practices. Each department head or designee (data steward) must:

- implement the unit's and/or office's record management practices;
- ensure that these management practices are consistent with this policy;
- educate staff within the administrative unit in understanding sound record management practices, including protection of official records against misuse, misplacement, damage, destruction, or theft;
- implement safeguards against accidental or deliberate deletion or alteration of electronic records;
- preserve inactive records (see: Definitions above) of historic value, and transfer those records to the University Archives;
- ensure that access to confidential files is restricted, whether in the original department or after transfer to the University Archives;
- implement appropriate access and audit controls on electronic record data; and
- destroy inactive records that have no archival value upon passage of the applicable retention period

B. Preserving or Disposing of Official University Records

When the prescribed retention period (see the Schedule) for official University records has passed, a determination of whether to preserve or dispose of the documents must be made. The University Archivist, who has the authority to designate which records are archival, should be consulted when deciding if a record is of historical value to the University.

1. Archival Records: If it is determined that the records are archival, contact the University Archivist for a consultation. No materials should be sent to the Archives without the prior approval of the University Archivist. The University Archives are located in the University Library.
2. Non-archival Records: If it is determined that it is appropriate to dispose of the records, destroy them in one of the following ways:
    a. Recycle non-confidential paper records.
    b. Shred or otherwise render unreadable confidential records.
    c. Erase or destroy electronically stored data.
3. Electronic Records: Electronic records generated and maintained in University information systems or equipment (including mainframe, mini, micro computing/storage systems, and any other electronic device not mentioned) should be periodically reviewed to ensure that these requirements are met. Examples of common electronic records include word processing documents, electronic mail, databases, and web sites.
    a. Electronic records must be captured within a reliable record management application whenever possible. If possible, records should include essential data and metadata describing the content and structure of the record and the context of creation. Accurate links should be maintained between all related paper and electronic and record elements.
    b. Electronic records must be evaluated by Information Technology staff to determine retention requirements. Electronic record management applications must provide for automated retention and destruction of electronic records in accordance with disposition schedules. Data Stewards, in consultation

with appropriate Information Technology staff, must develop strategies for long-term preservation of electronic records. These strategies must:

- include provisions for guaranteeing availability and integrity of electronic records through system migration.
- mitigate the risk of data inaccessibility due to hardware obsolescence, storage medium deterioration, or software dependence.
- include appropriate policies and procedures for data backup.

c. Electronic records in jeopardy of permanent, unavoidable access loss should be converted to paper or other human readable format and preserved accordingly.

C. Value of Records.

University records (regardless of the storage medium) can be disposed of upon reaching the minimum retention period stated in this policy, provided the records have no future administrative, legal, research, historical or fiscal value, as defined in the Definition section herein.

The Data Steward is responsible for performing, at least annually, a review to determine the value or usefulness of departmental records. During this review, the Data Steward should identify and designate for disposal destruction or transfer to an archive) the records with elapsed retention periods (time maintained in office plus time in inactive records area) that are no longer useful. By August 31 of each year the Data Steward will have completed the yearly records review.

D. Confidential Records

The purpose of the guidelines set forth in this Section to define confidential records, strengthen safeguards against the unauthorized or accidental disclosure of confidential records and information, and to define appropriate measures for reasonable care in the disposal of confidential information, including its protection during storage, transportation, handling and destruction.

1. The following types of records are absolutely confidential:
   a. individual education records of living students or living former students, as defined by the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, unless the student or former student grants access in writing or unless one of the exceptions contained within FERPA applies;
   b. individual employment records of living current or former faculty members, administrators or other staff members, including records which concern hiring, appointment, promotion, tenure, salary, performance, termination or other circumstances of employment, unless the faculty member, administrator, or staff member grants access in writing;
   c. records that include "protected health information" as the same is defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. 1171 et seq. and regulations promulgated thereunder;
   d. records that include "nonpublic personal information" protected under the safeguarding rules of the Gramm-Leach-Bliley Act of 2000 (GLBA);
   e. other records where usage might constitute an invasion of privacy;

f. records the use of which has been restricted by contract; and
g. any other records with specific regulatory confidentiality requirements.

2. The following types of records generally will be treated as confidential:
   a. administrative records of the University for twenty-five years from date of their creation, with certain exceptions, such as those which must be open in conformance with law;
   b. records of a sitting administration; and
   c. records the disclosure of which might expose the University to legal liability.

3. The following are recommended procedures for destruction of confidential records:
   a. Retention Period: Only those records retained for a period of time equal to or greater than as set forth on the Schedule may be disposed of in accordance with these guidelines.
   b. In the event of a claim, lawsuit, government investigation, subpoena, summons or other ongoing matters, upon service of legal process (subpoena, summons or the like), or upon learning of an investigation or audit, or if a claim is made, whether formal or informal, or a dispute arises, the retention periods shall be suspended and records related to the legal process, claim, dispute, investigation or audit should not be destroyed.
   c. Record retention periods may be modified from time to time by government regulation, judicial or administrative consent order, private or governmental contract, pending litigation or audit requirements. Such modifications supersede the requirements listed in this policy. Suspension of record destruction required by any of these reasons will be accomplished by a notice sent out to affected units by the University Counselor or the a member of Senior Leadership.
      - Note: No document list can be exhaustive. Questions regarding the retention period for any specific document or class of documents not included in these tables should be addressed to the University Archivist or the Director of Environmental Health, Safety and Risk Management.
      - Caution: Departments and units that are not official repositories and that retain duplicate or multiple copies of these university records should dispose of records when they are no longer useful.

E. Destruction Authorization

Data Stewards are responsible for authorizing the disposal of records. When the records to be disposed of are confidential, the services of the document destruction service with which the University has contracted. As of the date of this policy, the University maintains a contract with a vendor for secure document destruction. No documents that contain sensitive or confidential information should be placed in the trash without being shredded.

F. G. Disposal of Electronic Records, Film and Tapes

Electronic or machine-readable records containing confidential information require a two-step process for assured, confidential destruction. Deletion of the contents of digital files and emptying of the desktop "trash" or "waste basket" is the first step. It must be kept in mind; however, that reconstruction and restoration of "deleted" files are quite possible in the hands of computer specialists. With regard to records stored on a hard drive, it is recommended that commercially available software applications be utilized to remove all data from the storage device. When

properly applied, these tools prevent the reconstruction of any data formerly stored on the hard drive. With regard to floppy disks, CDROMs and back-up tapes, these storage devices should be physically destroyed.

Film, audio and videotapes containing confidential information should also be physically destroyed, not simply thrown away. It is possible to overwrite audio and videotapes with other, non-confidential sound and images, but if this is done, it should be done by an authorized member of the staff in the office of origin.

G. Destruction Record

A destruction record is an inventory describing and documenting those records, in all formats, authorized for destruction, as well as the date, agent, and method of destruction. The destruction record itself should not contain confidential information. It is anticipated that in most cases only one copy of the destruction record will be retained, in the office of origin. The destruction record may be retained in paper, electronic, or other formats.

H. I. Policy Review

This policy and the record retention schedule will be reviewed every three (3) years for the purpose of making any necessary revisions considering technological developments, changes in legal requirements, or changes in administrative practice. The Director of Environmental Health, Safety and Risk Management, with the advice of University Counsel, will be responsible for the review and update of the policy. Each unit's Data Steward will be responsible for transmitting record retention updates pertaining to his or her own unit to the Director of Environmental Health, Safety and Risk Management for inclusion in the Schedule.

Approved versions of these policies will be posted on the AU Portal.

Exceptions to Policy

Exceptions to this policy must be requested in writing by filling out the Policy and Procedure Exception form and submitting to the individual named in the Responsibilities section who assists with reviewing exceptions to this policy.

Policy Review

The Operations policies should be reviewed on a 3-year cycle and updated when institutional needs or goals change. The Director of Environmental Health, Safety and Risk Management, with the advice of University Counsel, will be responsible for the initial review and update of the policy. Each unit's Data Steward will be responsible for transmitting record retention updates pertaining to his or her own unit to the Director of Environmental Health, Safety and Risk Management for inclusion in the Schedule.

References and Related Policies

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

Related Policies

N/A

Exhibits

See Records Retention Schedule posted on MyAlvernia (Alvernia login required.)

Document Review Log

Date Reviewed	Description of Changes
2015	Carried over from 2015 approved policy
3/14/2024	SLT Approved