RECORD RETENTION AND DISPOSITION POLICY

Category: Administration and Governance
Responsible Office: Policy and Operational Excellence
Responsible Executive: Vice President for Finance and Administration

Date Established: 5/16/11
Date Last Revised: 05/25/18

Summary

This policy defines the standards for retention, handling, and disposition of university records.

Policy

POLICY STATEMENT

The University at Buffalo (UB, university) requires retention of university records, regardless of format, for specific periods of time in accordance with federal, state, and other legal and institutional requirements. The university is committed to effective and consistent record management that:

- Maintains the privacy and security of institutional and constituent information
- Ensures records are retained for the required duration
- Preserves records of historical value
- Requires disposal of outdated and unnecessary records in a manner appropriate for the format
- Optimizes the use of space
- Minimizes the cost of record retention

Managing University Records

The designated Office of Record must maintain the official copy of a university record for the required duration outlined in the applicable record retention schedule and then disposed of in a manner appropriate for the record format.

Departments that are not designated as an Office of Record must dispose of duplicate copies of university records in an appropriate manner when there is no longer an administrative need for them. Retaining records when there is no legal requirement to do so may place additional burdens on the unit:

- Records containing personal identifying information must be protected against theft. If such records are accessed inappropriately or lost, the unit could be subject to fines, penalties, cost to notify individuals whose records were breached, and loss of reputation.
- In the event of a legal proceeding or audit, the unit must provide all documentation that has been maintained regardless of the retention requirements. This can be a very time consuming and costly process.

Offices who are not the Office of Record should refer to the Office of Record to provide them with the necessary copies.

Record Retention Schedules

The university is required to follow the record retention guidelines provided in the following schedules. These schedules indicate the minimum length of time that a record, regardless of format, must be retained. The applicable schedule is dependent on the type or source of the record.

- **State University of New York Records Retention and Disposition Schedule** – includes the record categories specific to the State University of New York (SUNY); other record categories of a more general nature are included in the New York State General Retention and Disposition Schedule. When records are included in both schedules, the SUNY requirements take precedence.
- **New York State General Retention and Disposition Schedule** – defines the record retention requirements for all New York State (NYS) agencies. Refer to this schedule for record categories not covered by the SUNY Retention and Disposition Schedule.
- **Research Foundation Records Management Policy** – provides legal and corporate retention and disposal requirements pertaining to Research Foundation (RF) business.

Confidentiality

Many records contain Category 1 – Restricted Data or Category 2 –Private Data. This data is protected by federal, state, or local regulations such as the *Family Educational Rights and Privacy Act* (FERPA), *Health Insurance Portability and Accountability Act* (HIPAA), and the *Fair Credit Reporting Act*. In addition to statutory requirements, Category 1 – Restricted Data and Category 2 – Private Data must be handled in accordance with the university's privacy and information security policies.

Preservation of Records Relevant to Legal Matters

Disposal of records, regardless of format, relevant to pending or anticipated litigation, claim, audit, agency charge, investigation, or enforcement action must be suspended until final resolution of the matter. Employees who become aware that an investigation or legal proceeding has commenced or is anticipated, must preserve all records with potential relevance.

Electronic Records

An Office of Record that chooses to maintain documents electronically must establish a procedure to implement the use of electronic records in substitution for original paper records. The procedure must ensure the:

- Process maintains the integrity of the original records, is reliable and secure, and that authenticity can be validated
- Image process preserves accurate images of original records, including signatures, worksheets, relevant notes, and other papers necessary to reconstruct and understand the original record
- System will not permit additions, deletions, or changes to the images without leaving a record of such additions, deletions, or changes
- Index system provides secure, on-time, and convenient access and retrieval of imaged records so that each document is sufficiently identified to permit retrieval
- Accessibility of electronic records is not lost because of changing technology, portability of the medium, or transfer to a different medium

- Metadata information that describes how, when, and by whom it was collected, as well as size and storage requirements, must be preserved with electronic records

An effective electronic record security procedure must:

- Allow only appropriate, authorized personnel access to electronic records and that such personnel are trained to protect sensitive, proprietary, or classified electronic records
- Provide for the backup and recovery of electronic records as protection against information loss
- Minimize the risk of unauthorized change or erasure of electronic records
- Retain the electronic record according to the retention schedule applicable to the original record.

Most records in the SUNY schedule have been pre-authorized for replacement so that paper records that have been scanned or otherwise converted may be destroyed prior to the end of their retention period. If not pre-authorized, replacement or destruction of the paper records can only occur upon approval by the State Archives.

Federal Acquisition Regulations (FAR) and RF policy require that original RF documents be retained for a minimum of one year after imaging to permit periodic validation of the imaging system.

Email

Generally, records transmitted through email systems have the same retention periods as records in other formats that are related to the same function or activity. It is recommended that users identify and purge all non-records in email, segregating official records from transitory information. There are two options for filing and managing email records: printing and filing in a manual filing system or transferring messages to an electronic filing system.

Records Retained by University Archives

Archival records are records that the university must keep permanently to meet fiscal, legal, or administrative needs or that contain historically significant information. Records do not have to be old to be archival. What makes a record worthy of permanent retention and special management is the continuing importance of the information it contains (e.g., President's annual reports, minutes of campus councils, governance organization minutes or handbooks, inaugural or commencement records, documents generated by or for the campuses such as strategic plans and accreditation reports)

The University Archives accepts records for permanent retention; it does not hold records temporarily or manage records until scheduled destruction.

Record Disposal

Perform record disposition regularly, at least once each year.

Disposal of University Records

When disposing of records, destroy them in an appropriate manner:

- recycle non-confidential paper records
- shred or render unreadable records with confidential information

- utilize a confidential disposal bin that will be emptied and disposed of by University Facilities utilizing black plastic trash bags; these papers are not recycled
- erase electronically stored non-confidential records
- overwrite or physically destroy the media on which confidential electronic records are stored.

University Facilities provides confidential shredding for records that are not suitable for recycling.

Disposal of Category 1 – Restricted Data and Category 2 – Private Data

For disposal of Category 1 – Restricted Data and Category 2 – Private Data, departments should contract directly with a reputable vendor to ensure compliance with the appropriate regulations.

BACKGROUND

University records must be maintained to support operational needs and internal controls, protect privacy, and meet federal, state, and regulatory requirements. Document retention standards and systems must ensure that transactions and related authorizations are fully supported in the event of an audit, litigation, or other external action.

APPLICABILITY

This policy pertains to all university documents and records, regardless of format.

DEFINITIONS

Archival Record – records that the university must keep permanently to meet fiscal, legal, or administrative needs, or because they contain historically significant information. What makes a record worthy of permanent retention and special management is the continuing importance of the information it contains.

Category 1 – Restricted Data - Protection of the data is required by law or regulation. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Restricted data includes the definition of private information in the New York State (NYS) *Security and Breach Notification Act* as a foundation: bank account, credit card, debit card numbers; social security numbers; state-issued driver license numbers; and state-issued non-driver identification numbers. To this list, university policy adds protected health information (PHI), computer passwords, other computer access protection data, and passport numbers.

Category 1 – Restricted Data are exempt from disclosure or release under the NYS *Freedom of Information Law* (FOIL). The NYS *Information Security Breach and Notification Act* requires the university to disclose any breach of the data to New York residents. (State entities must also notify non-residents; see the NYS *Information Security Policy*.)

Individuals who access, process, store, or in any other way handle Category 1 – Restricted Data must implement controls and security measures as required by relevant laws, regulations, and

university policy. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation governs.

Category 2 – Private Data - Includes university data not identified as Category 1 – Restricted Data, and data protected by state and federal regulations. This includes Family Educational Rights and Privacy Act (FERPA)-protected student records and electronic records that are specifically exempt from disclosure by the NYS FOIL.

Category 2 – Private Data must be protected to ensure that they are not disclosed in a FOIL request. Private data must be protected in order to ensure that they are only disclosed as required by law, including FOIL. Decisions about disclosure must be made by the Records Management Officer.

The NIST *Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* maps to the Category 2 – Private Data risk classification.

Electronic record – information recorded in a format that requires a computer or other electronic device to access it and that otherwise satisfies the definition of a record.

Office of Record – the unit or individual designated as having responsibility for retention and timely destruction of official university records. If you are designated to maintain the original document, you are considered the Office of Record and must maintain the document for the period outlined in the applicable record retention schedule.

Record – the original copy of any record, document, or information that supports the transaction of university business. Paper or text documents, computer data, electronic records, microfilm, computer tapes, and video or audio recordings are considered records.

Record Coordinator – the primary resource in a business office who interprets policies and retention requirements related to the specific record type for which they have been assigned responsibility; also responsible for providing guidance to departmental record custodians pertaining to the retention and destruction of these records.

Record Custodian – the individual responsible for oversight of departmental records.

Retention Period – the length of time for which the Office of Record is responsible for the maintenance of specific university records.

RESPONSIBILITY

Department Chair or Unit Head

- Assign a departmental Record Custodian.
- Implement record management practices consistent with this policy.
- Restrict access to Category 1 – Restricted Data and Category 2 – Private Data.

Office of Record

- Maintain official records in accordance with the appropriate Record Retention Schedule and the requirements of this policy.
- Provide records when requested by internal or external entities when such requests are deemed appropriate and necessary.
- Destroy records in an appropriate manner.

Record Coordinators

- The subject matter expert for a specific record category (e.g., personnel, financial, student) who will provide guidance to departmental Record Custodians pertaining to the retention and destruction of the specific record categories for which they are responsible.

Record Custodian

- Determine if the department is the Office of Record for any records; consult with the Record Coordinator, as appropriate.
- Preserve appropriate records with historical value by transferring them to the University Archives.
- Appropriately dispose of all records for which the department is not the Office of Record.
- Consult the appropriate Record Retention Schedule and dispose of the records when the Schedule indicates they are no longer required when the department maintains the official university copy.
- Maintain a record of the identity, inclusive dates, and approximate quantity of disposed records.

Contact Information

Contact	Phone	Email
Records Management Officer	716-645-5464	hines@buffalo.edu
HIPAA Compliance	716-829-3866	hipaa-compliance@buffalo.edu
University Archives	716-645-2916, ext. 256	lib-archives@buffalo.edu
University Facilities	716-645-2025	custserv@facilities.buffalo.edu

Related Information

University Links

Confidential Shredding and Bulk Recycling
Offices of Record and Record Coordinators
Protection of University Data Policy
Records Management
Records Retention Schedules
UB HIPAA
UB HIPAA Business Associates

Related Links

Fair Credit Reporting Act
Family Educational Rights and Privacy Act (FERPA)
New York State Archives Managing Records
National Institute of Standards and Technology (NIST) 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
Personal Privacy Protection Law
Research Foundation Records Management Policy
State University of New York Email Retention Guidance
State University of New York Legal Proceeding Preparation (E-Discovery) Procedure, Document 6610
State University of New York Records Retention and Disposition Policy, Document 6609

History

May 2018	Updated the policy to: • Change the title of the policy from *Record Retention and Disposal* to *Record Retention and Disposition* • Revise terminology related to Category 1 – Restricted Data and Category 2 – Private Data to be consistent with the *Protection of University Data Policy*

Presidential Approval

Satish K. Tripathi *5/16/11*

Satish K. Tripathi, President Date