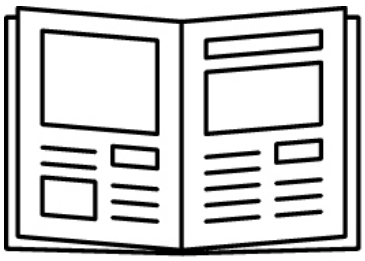
Records Management Guidelines



The University of Vermont

Table of Contents

Records Management Overview

Records management is the process of managing the University's information that is created and necessary for ongoing operations throughout the information life cycle, from the time of creation to its eventual disposition. This process includes identifying, classifying, storing, securing, retrieving, tracking and destroying or permanently preserving records.

These guidelines are intended to assist departments in fulfilling their record management responsibilities including complying with the Records Management and Retention policy and schedule by setting out responsibilities and recommended practices and standards for the record management life cycle.

Records Life Cycle

The Records Retention Schedule

The University's **Records Retention Schedule** identifies the *Responsible Departments* and *Retention Periods* for those records that the University has determined should be retained for a specified period. These records include those that:

- serve to document the University's actions, decisions, or statements;
- have an enduring operational value (e.g. specific student or business transaction records); or
- must be kept to satisfy legal or regulatory requirements.

Roles and Responsibilities

Individuals

The Chief Privacy Officer is responsible for the University's Records Management and Retention Policy including providing guidance for records management to University departments and overseeing the regular review of the records schedule.

The University Archivist is responsible for managing the University Archives and identifying records to be preserved.

VPs, Deans, Directors and Department Heads (depending on the unit, refer to Record Retention Schedule)– are responsible for the records management for their distinctive units, including identification of pertinent unit records, ensuring the Records Schedule accurately reflects their unit's records, ensuring that management of records is appropriately resourced and that the unit has assigned a **Records Coordinator** for day-to-day records oversight and management.

Records Coordinators are responsible for:

- Identification and awareness of the records maintained by their unit, both those on the records schedule and those maintained for internal operations
- Managing the record life cycle (creation, maintenance, disposition) for the department's records
- Knowledge of the retention requirements for records on the records schedule
- Creation of a schedule and program for internal departmental records as needed
- Familiarity with record keeping practices and standards in these guidelines

Departments

Records Identification and Creation

All departments create university records that document their core activities. To identify records that need to be managed,

All departments should:

- Review the University record schedule for records that they are responsible for. In addition to identifying departments responsible for specific University records, the schedule identifies records maintained by "All Departments" and "Dean's" Offices," that is, universal departmental records and those that pertain to individual schools or colleges. In addition to these records that are common throughout the University, departments should identify records they are uniquely responsible for.
- If your department creates unique records that are essential to your ongoing operations, but do not meet the criteria for records listed on the University's Record Schedule, your department should identify those records and create its own schedule for managing your unique operational records. Departments should incorporate their records management activities into their ongoing departmental practices.
- When keeping duplicate records of records that are maintained centrally by administrative offices as listed in the Records Schedule, duplicates should only be retained for the department's convenience and should never be retained longer than the official retention period listed on the schedule.
- Administrative Business Service Center (ABSC) Considerations. Departments that are served by the Administrative Business Service Center are still responsible for their administrative records on the records schedule for "All Departments" that may be processed the ABSC. While the ABSC assists in completing, processing and storing these documents in a shared folder on the University's server, departments are still responsible for purging these records when their retention period expires and are the responsible office for these records.

Custodial Administrative Offices identified on the Records Retention schedule additional responsibilities:

- In addition to the above, Custodial Administrative Offices identified on the Records Schedule are responsible for ensuring the schedule is accurate, current, complete and compliant with legal requirements or professional guidance. New records identified that should be added to schedule should be communicated to compliance@uvm.edu.

Developing your Records Program

Risk Assessment – Know your records

Prior to developing a records management program, departments should classify their records to determine the risk of accidental loss or exposure. This risk assessment will inform the levels of security and access controls needed, as well as backup requirements.
Below are examples of records from those with the greatest risk to the lowest.

Lowest Risk ←----------→Highest Risk

• Legally protected Records include those containing Personally Protected Data as defined by UVM's Privacy and Information Security policies. This information includes student records that are covered under FERPA, HIPAA protected health information, and personal information protected under VT law that includes an individual name with social security number, motor vehicle license number, or financial account number. Exposure of these types of records could result in notification requirements as well as fines and penalties. • Archival Records – records that have enduring or historical value. Archival designation is subject to UVM Archivist approval.
Confidential or proprietary information – examples of these records include personnel files, litigation or legally privileged records, contractual information, procurement bids prior to contracting, and other records that may be protected under Vermont public records laws.
Operating or General business records – records pertaining to ongoing University operations, excluding those above, that are not protected by law, contract, or policy and do not contain sensitive information. Examples include invoices, travel reimbursements, purchasing card documentation, non-sensitive emails or correspondence. These records would reflect records that are not made public by the University as a normal course of business, but could likely be obtained via a formal public records request.
Public Records – these are records that the University normally makes publically available, examples include directory information of students and employees, information on courses and academic program, University policies and procedures, financial statements, public reports and board meeting minutes.

Records Maintenance and Storage

Once records that need to be maintained have identified, departments should develop plans for storing and securing the records.

Maintaining/Storing

Availability Principle
Records should be stored and organized in a manner that permits them to be readily retrievable for operational use. This may require an organizational system or indexing that simplifies identification and retrieval of records. For example, all records of the same type may be stored in a single physical or electronic location and organized by common groupings or traditional sorting (e.g. dates, names, alphabetical, or other categories that are normally used to sort similar data). For physical records, prioritizing availability and proximity may be driven by frequency of use. Electronic Records may necessitate an indexing that archives the system of organization through the use of *metadata*. Descriptive metadata includes information about the data that can aid in identification and accessibility. When developing an electronic record keeping system, documenting the meta data elements assist how the data is organized and can make retrieval more efficient. Conforming the metadata among different records with similar data elements may also make storage and accessibility of related records more effective.

A well-designed records storage system enhances a department's productivity for daily operations and in circumstances where legal mandates require timely access to records. Considerations when planning a records storage system include location, costs, ease of access, frequency of use and protection of information.

Record Integrity

All records should be protected from unauthorized alteration. Integrity of records is expected by those that rely on this information including government agencies, donors, creditors as well as the public. Sensitive records requiring the highest security should include audit trails identifying who accessed records, when accessed occurred, and what changes if any were made to the record.

Security

All non-public records should be protected from unauthorized access. Sensitive or protected records require greater security with controls to limit access to those authorized to access them and should only be accessed for legitimate business purposes. Both physical and technical security standards should be applied to records based on their risk level and storage format.

Examples of ***physical*** safeguards include:

- Locked doors and storage cabinets

- Restricted building access
- Surveillance cameras
- Logging off or set to sleep mode workstations
- Safeguards against fire or flood for physical records
- Backup sites

Examples of **technical** standards include:
Following password standards

- Data encryption
- Biometric access
- Dual Authentication

Record Security and Protection – Legally Protected Records

Managing records containing legally protected information involves restricting the methods of access, storage and transfer. Departments should consult the Information Security and Privacy policies and related procedures when managing these records or contact iso@uvm.edu for guidance.

Some examples of legally protected records include:

- student records,
- records containing HIPAA protected health information,
- social security numbers,
- financial accounts,
- credit card information,
- driver's license information, and
- records that UVM is contractually bound to safeguard as prescribed by contract.

In general, the most secure methods for storing or transferring records include:

- UVM Managed shared drives,
- UVM Secure file transfer,
- Encrypted hardware (e.g. encrypted laptops, encrypted thumb drives)
- Locked cabinets and locations that are physically restricted from unauthorized access

Personal email accounts and unencrypted devices should not be used to store or transfer sensitive records. Any use of third party vendors or software for storing or transmitting these records should be approved by the ISO Office- see below Third-party Agreements.

Third Party Agreements

When records are maintained through an agreement with a third-part vendor, departments are responsible to ensure that agreements include provisions to meet availability, integrity, security, retention and disposition requirements. All agreements should provide for the transfer of active records to the University at the end of the agreement or contract term. Departments maintaining sensitive or protected information that are maintained by a "cloud" vendor should verify that vendor servers reside

in the United States. Any use of third party vendors or software for storing or transmitting legally protected records will be subject to ISO review and approval.

Records Disposition and Destruction

Risks of:

Not Keeping Records Long Enough:

- Regulatory fines or disallowances
- Poor institutional knowledge
- Lawsuits or contract disputes
- Audit findings

Keeping Records Longer than Needed:

- Expense of retention. Paper retention includes space considerations which are ever more critical under IBB. Electronic data storage costs while lower still carry a cost based on volume and type of storage.
- Costs of Discovery – in the event of a litigation, excess records that have been kept beyond their disposal date cannot be destroyed and will have to be identified and gathered through time and labor extensive processes.
- Litigation/Government Review– excess records could contain information that could be used against the University in the event of adverse litigation or government review.

Disposal Plans

Departments should create disposition plans for the records they maintain. This plan should identify what records are disposed of and when they have been disposed, including the method of disposal/destruction. The method of disposal should follow the risk assessment classification. Any record containing confidential or legally protected information must be securely and permanently destroyed, meaning that the content cannot be recreated. When uncertain, departments should err on the side of secure disposal.

Physical records containing confidential or legally protected information should be securely shredded. Use of an approved University vendor will meet this requirement; University Purchasing maintains a list of preferred vendors for records disposal.

Electronic Records should be securely deleted or purged. Secure disposal includes identifying whether backups or redundant systems exist, so that all records may be scheduled for timely and secure disposal. When adopting a new software system intended to maintain specific University records, forethought should be given to ensure that the system will allow for efficient identification and disposal of records at the end of their retention period. Coordinate with third party vendors that maintain records to ensure that records are disposed of securely and timely.
It is important to follow ETS guidance when disposing of hardware that may contain University records; see Disposal of Surplus Computers and Electronic Waste.

Archival Considerations

Archival Records are permanent records that have historical or enduring value to the University. The University keeps these records permanently. In general, records have enduring value if they document the University's *organizational structure and changes, history, strategic decisions, and social history, or are official publications.* Archival records may include correspondence, reports, memoranda and notes, announcements, accreditation files, photographs, and meeting minutes. The University Archivist should be consulted prior to disposing records that may meet these criteria; no *active* records should be considered for archiving.

Research Data Considerations

Research Data - Principal Investigators (PI) are responsible for data collection, maintenance, and retention of University-owned Research Data in accordance with any applicable award agreement provisions. These agreements may require security plans and/or identify retention requirements.

Exceptions to Disposal – Records Preservation Directives

In certain circumstances a record preservation directive or litigation hold notice may be issued in accordance with procedures established by the Office of General Counsel. The Office of General Counsel or other oversight office will inform departments when legal holds or preservation directives exist for certain records. Departments may normally follow their disposal schedule unless they have been notified of such a directive.
When a directive is received, no employee who has been formally notified of a record preservation directive may discard, destroy, alter, or delete a record that falls within the scope of that directive. Violation of the directive may subject the individual to disciplinary action, up to and including dismissal, as well as personal liability for civil or criminal sanctions by courts or law enforcement agencies. Contact the Office of General Counsel to determine when a hold or directive has been lifted and normal disposal may resume. See Records Preservation Directive UOP for more information.

Contacts and Support

The following offices are available to answer questions and provide consultation to departments developing their records management programs:

- Archival Records: Chris Burns, University Archivist, chris.burns@uvm.edu, 656-2631
- General questions, including retention periods: Compliance Services, Compliance@uvm.edu, ph: 656-3098
- Securing sensitive records: Information Security Office, ISO@uvm.edu
- Identifying records disposal vendors purchasing@uvm.edu
- Unsure? Contact: compliance@uvm.edu

Other Resources

Vermont State Archives –Records Management Best Practices

Association of Records Managers and Administrators (ARMA) – Generally Accepted Recordkeeping Practices