FITCHBURG STATE UNIVERSITY

Information Retention and Destruction Policy

Version 1.2	**Last Updated:** 4/17/2026
Security Level: Public	**Issued:** 9/7/2022

Purpose

Fitchburg State University's records are important assets. University records include all data you produce as an employee, whether paper or electronic. Media must be handled, stored, and disposed of properly to protect the critical data they contain. This policy outlines the university's requirements and guidelines for data and records management, as well as retention schedules.

Scope

All University records, in any media, must be retained and handled in accordance with applicable laws and regulations.

In addition, filing systems, storage arrangements, access procedures, retention schedules, and destruction procedures must conform to sound business practices, provide safe and secure methods of handling records, and prevent the inadvertent or malicious disclosure of confidential information. This policy includes non-computerized records.

Unauthorized disclosure of sensitive information may subject the university to legal liability, negative publicity, and monetary penalties. Data must be securely removed from storage media before transfer or disposal of the associated equipment. These same guidelines may also be applied to clearing media for reuse within the company.

Policy

Fitchburg State University, as a Massachusetts public higher-education institution, is subject to the Massachusetts Public Records Law (M.G.L. c. 66 §8 and c. 4 §7 clause 26) and must comply with all records-retention schedules issued by the Office of the Secretary of the Commonwealth. The University's retention and destruction practices follow the *Massachusetts Statewide Records Retention Schedule (06-18)* and any subsequent updates published by the Records Conservation Board (RCB).
https://www.sec.state.ma.us/divisions/archives/records-management/agency-records.htm

Fitchburg State University requires that its records be maintained in a consistent and logical manner and be managed so that the University:

- Meets legal standards for protection, storage, and retrieval (see the link to state retention policy);
- Protects the privacy of faculty, staff, and students as required by law;
- Optimizes the use of space; and
- Minimizes the cost of record retention

Statewide Records Schedule

Records retention schedules are established timetables for maintaining records and provide an established retention period for the length of time a record must be maintained to satisfy the purposes for which it was created and to fulfill the legal, fiscal, historical, and administrative requirements of the university.

Fitchburg State has determined the following records retention schedules apply to the University data based on the Massachusetts Statewide Agency Records Retention Schedule Quick Guide, as of March 23rd, 2026. This schedule is updated frequently and should be reviewed periodically for information on the Secretary of the Commonwealth of Massachusetts's Division of Public Records.

Section	**Schedule Section Numbers**	**Pages**
Administration	A01 - A12	1-12
Facilities, Transportation, and Construction	C01 - C08	14 - 26
Fiscal	D01 - D04	27 - 33
Information and Records Management	F01 - F07	34 -42
Legal and Regulatory	B01 - B05	44 - 50
Personnel	E01 - E06	52 58
Executive Office of Education	H01 - H10	59 - 67

Exemptions

The University expects all employees to fully comply with any published records retention or destruction policies and schedules, provided that all employees note the following general exception to any stated destruction schedule: If you believe, or the University informs you, that University records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until the university's legal determination that the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that the exception may apply,

or have any questions regarding the possible applicability of that exception, please seek legal advice from the university's Legal Counsel / General Counsel.

Media Types

The following items might require secure retention and/or disposal:

- Hard disks, SSDs
- Paper documents
- Reports
- Removable disks
- Optical storage media
- Program listings
- Test data
- System documentation
- Copiers
- Fax machines
- Printer disks

Destruction

The Technology Department shall ensure that University equipment deemed obsolete and tagged for disposal has any sensitive information properly deleted. Once verification is received that all data has been erased, the equipment shall be properly discarded or reused in accordance with applicable laws.

Data shall be reviewed to verify that the retention period for the data in question has been properly reached. All known audits and audit discrepancies regarding data scheduled for destruction must be settled before the records can be destroyed; all known investigations or court cases involving said data must be resolved before the records can be destroyed.

Last Copy of a Record

Records shall not be destroyed or otherwise disposed of without documented authorization consistent with the procedures established by the Massachusetts Records Conservation Board (RCB). Once records have reached their full retention period, you can apply for permission to destroy these records. To request destruction permission, complete Form RCB-2U – Universal Application for Destruction Permission (Paper and Electronic) and submit it to the Records Conservation Board at rcb@sec.state.ma.us. Where the statewide schedule indicates "permission from RCB not required," destruction may proceed once the retention period has expired.

Notice on form RCB-2U:

> *Your Agency must submit this form to request permission to destroy the last copy of a record as authorized by the current retention schedule. You do not need to submit a form to destroy administrative use records.*

Data Sanitization

All devices or media containing University data intended for reuse, transfer, recycling, or disposal must first be sanitized using an approved method appropriate to the media type and the sensitivity of the data. Data sanitization is the process of deliberately, permanently, and irreversibly removing or destroying data stored on a device or medium so that no usable residual data remains.

Approved sanitization methods may include software-based wiping tools, dedicated hardware-based sanitization devices, degaussing where appropriate, or physical destruction of the media. The selected method must be sufficient to prevent the recovery of University data. Standard disk formatting, routine file deletion, or similar basic overwriting methods **do not** satisfy this requirement.

Hardcopy records containing internal, confidential, or otherwise sensitive information must be securely destroyed prior to disposal, such as by cross-cut shredding, incineration, or other approved method appropriate to the information's sensitivity. Media containing confidential information must be disposed of securely and safely when no longer required.

Physical destruction methods used to sanitize media may include, but are not limited to, disintegration, incineration, melting, pulverizing, and shredding. Any such method must render the media and the data it contains unreadable, unrecoverable, and incapable of reconstruction.

Documentation of Destruction

All destruction of University records or media performed pursuant to this policy must be documented. At a minimum, the documentation must identify:

- The records or media destroyed
- State the date of destruction
- Describe the method of destruction or sanitization used
- Identify the applicable retention schedule or other authority permitting destruction
- Identify the individual, department, or vendor responsible for performing or overseeing the destruction.

When destruction is performed by a third party, a certificate of destruction must be obtained and retained. Documentation related to the sanitization or destruction of electronic media shall be maintained by the Technology Department or other authorized office. Departments are responsible for maintaining documentation related to the destruction of records or media under their authority, unless another office has been formally designated to do so.

Roles

- Chief Information Security Officer: Follows management standards and performs auditing to ensure that media is being handled and disposed of in accordance with this policy.
- Materials Management: Coordinates the collection, transfer, surplus, reuse, recycling, and disposal of University-owned equipment and media in accordance with applicable laws, regulations, and University policy. Maintains appropriate records of equipment disposition and works with the Technology Department and other responsible offices to ensure that equipment is not released, transferred, sold, recycled, or discarded until required data sanitization or destruction has been completed and documented.
- Legal / General Counsel: Provides legal guidance regarding records retention, preservation, disclosure, and destruction requirements. Advises the University on applicable laws, regulations, public records obligations, investigations, audits, subpoenas, and litigation holds. Determines when normal destruction schedules must be suspended due to actual or reasonably anticipated litigation, investigation, audit, or other legal requirement. Works with department leadership, the Technology Department, and other appropriate offices to ensure records are preserved when necessary and may authorize release from a legal hold when appropriate.
- Department Management: Ensure that any media they own, and media that contain data or applications that they own, are handled and disposed of in accordance with this policy. Responsible for updating retention schedules as necessary.
- Technology Staff: Responsible for monitoring/assisting with electronic records and destruction of electronic records once the retention period has expired.
- Staff: Store university data only on approved media and report the loss, damage, or theft of any media containing university data. Responsible for handling and disposing of departmental files, documents, and other records within the guidelines set forth by this policy.

References

- CISv8 3.1 Establish and Maintain a Data Management Process
- CISv8 3.4 Enforce Data Retention
- CISv8 3.5 Securely Dispose of Data
- NIST SP 800-88r2 Guidelines for Media Sanitization
- PCIv4 Requirement 3 Protect Store Account Data
- Secretary of the Commonwealth of Massachusetts website
- Massachusetts Statewide Records Retention Schedule, Schedule Number 06-18

- Form RCB-2U – Universal Application for Destruction Permission (Paper and Electronic)
- Massachusetts Electronic Records Management Guidelines

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Revision History

Date of Change	Revision	Responsible	Summary of Change
9/7/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
5/9/2024	1.1	Eric Boughton, CISO	Formatting, Review, Updating references
4/17/2026	1.2	Eric Boughton, CISO Stefan Dodd, CIO	Added Quick References to State Retention, a disposal section and changes for ADA Compliance