FITCHBURG STATE UNIVERSITY

64 - Information Retention and Destruction

Issued 9/7/2022

Version 1.0

Purpose

The records of Fitchburg State University are important assets. University records include all data you produce as an employee, whether paper or electronic. The purpose of this policy is to define the university's requirements and guidelines for data and records management as well as retention schedules.

Media must be handled, stored, and disposed of properly in order to protect critical data stored upon it. Fitchburg State University requires that university records, as defined herein, regardless of format, be retained for periods of time or disposed of in accordance with Massachusetts State Retention Laws.
https://www.sec.state.ma.us/arc/arcpdf/MA_Statewide_Records_Schedule.pdf

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. The secure removal of data from data storage media must be completed before transfer or disposal of the associated equipment. These same guidelines may also be applied to clearing media for reuse within the company.

Media containing confidential information shall be disposed of securely (e.g. by incineration, cross-cut shredding or sanitation) and safely when no longer required.

Policy

Records retention schedules are an established timetable for maintaining records and provide an established retention period as to 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 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 for 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

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 exception may apply, or have any question regarding the possible applicability of that exception, please seek legal advice from the university's communications department.

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

- •Paper documents
- •Reports
- •Removable disks
- •Optical storage media
- •Program listings
- •Test data

- •System documentation
- •Copiers
- •Fax machines
- •Hard disks, SSDs
- •Printer disks

All devices holding University data that is intended for reuse within the University must be first sanitized. Data sanitization is the process of deliberately, permanently, irreversibly removing or destroying the data stored on a memory device. A device that has been sanitized has no usable residual data.

Sanitization processes include using a software utility that completely erases the data, a separate hardware device that connects to the device being sanitized and erases the data, and/or a mechanism that physically destroys the device so its data cannot be recovered. The use of standard disk formatting programs, simple file overwriting or deletion does not meet this requirement.

Hardcopy media containing internal or confidential information must be cross-cut shredded prior to disposal.

IT shall ensure that University equipment that is deemed obsolete and tagged for disposal will have 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.

Certification of all destroyed media (non-hardcopy) containing company data shall be maintained, identifying that data was destroyed or wiped.

Role

Chief Information Security Officer/Materials Management: Follows management standards and performs auditing to ensure that media is being handled and disposed of in accordance with this policy.

Department Management: Ensure that any media they own, and media that contains data or applications that they own, are handled and disposed of in accordance with this policy. Responsible for updating retention schedules as necessary.

IT 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 company data. Responsible for handling and disposing of departmental files, documents and other records within the guidelines set forth by this policy

---

References CIS

3.1 Establish and Maintain a Data Management Process
3.4 Enforce Data Retention
3.5 Securely Dispose of Data

References PCI

Requirement 3: Protect stored cardholder data
Requirement 9: Restrict physical access to cardholder data

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.

Security Level

Public