FITCHBURG STATE UNIVERSITY

Encryption Policy

Version 2.0	**Last Updated:** 10/31/2025
Security Level: Public	**Issued:** 9/7/2022

Purpose

The purpose of this policy is to provide the information security requirements at Fitchburg State University for the use of encryption algorithms to protect confidential or restricted information.

Scope

This policy applies to the encryption algorithms used to protect confidential and restricted information. A risk-based approach drives all Fitchburg State data encryption requirements. Considerations include legal or regulatory requirements, data inventory, classification, method(s) of access, storage or transmission mechanisms, and other contributing security controls in place.

Policy

Fitchburg State University shall utilize approved encryption algorithms to safeguard sensitive information. Fitchburg State University must use only approved cryptographic techniques, follow federal regulations, and adhere to the legal authority granted for the dissemination and use of encryption technologies. Data containing internal or restricted information shall be encrypted in accordance with the risk to the institution and applicable legal and federal standards.

All end-user laptops and desktops will be encrypted using appropriate encryption software for Windows, Apple, or other operating systems. Public-use lab and podium computers do not require encryption.

Mobile storage containing internal or restricted information shall be encrypted to the same standard as the operating system it is attached to.

Enterprise storage, such as server hard drives or SSDs, Cloud storage, and off-site storage, should ensure the use of best practice techniques, including encrypting at rest and encrypted backups.

Approved Cryptographic Standards

Fitchburg State University shall utilize only cryptographic modules and techniques that meet the following **minimum** standards to protect confidential and restricted information.

Data at Rest (DAR) Encryption

Data stored on end-user devices, enterprise storage, or mobile media must be protected using a Federal Information Processing Standard (FIPS) 140-2 validated module employing the following minimum requirements:

- Algorithm: Advanced Encryption Standard (AES-256)
- Mode: Galois/Counter Mode (GCM) or Cipher Block Chaining (CBC) with appropriate integrity checks.
- Mandatory Tools**:**
    - Full Disk Encryption (FDE): University-managed laptops and desktops must utilize vendor-provided FDE (e.g., BitLocker for Windows, FileVault 2 for macOS) or an approved enterprise FDE solution.
    - Removable Media: Must use AES-256 encryption or an approved encrypted container technology (e.g., password-protected zip archives utilizing AES-256).

Data in Transit (DIT) Encryption

All confidential or restricted information transmitted across any network (internal or external) must be protected using a secure, standard communication protocol with the following minimum requirements:

Protocol	**Minimum Acceptable Version**	**Deprecated/Forbidden**
Transport Layer Security (TLS)	TLS 1.2	SSL (all versions), TLS 1.0, TLS 1.1
Secure Shell (SSH)	SSHv2	SSHv1
Internet Protocol Security (IPsec)	Must use **AES-256** and **SHA-256** or stronger for integrity.	DES, 3DES, MD5

Hashing and Key Derivation

Cryptographic hashing algorithms must be used to protect passwords and verify data integrity.

- **Hashing Algorithms:** Secure Hash Algorithm **SHA-256** or higher (e.g., SHA-384, SHA-512).
- **Password Storage:** Passwords must be stored using **salted and iterated key derivation functions** (KDFs) such as **PBKDF2, bcrypt, or scrypt**, with an approved iteration count determined by the Technology Security Team.

Key Management Requirements

The security of the data is dependent on the security of the encryption keys.

- **Key Storage:** Keys used for encrypting enterprise-level restricted data must be stored in a FIPS 140-2 compliant hardware security module (HSM) or an approved secure key vaulting system. Keys must be stored separately from the data they encrypt.

- **Key Protection:** All keys must be protected by strong, complex passwords/passphrases or protected using multi-factor authentication where applicable.
- **Key Recovery and Escrow:** Full Disk Encryption recovery keys for all University-owned devices must be securely escrowed and managed by the Technology Team to ensure data accessibility for legitimate business purposes.
- **Key Rotation:** Master encryption keys for enterprise storage should be rotated or re-keyed at a minimum every two years.

Exemptions and Exceptions

Exemption Authority

Any request for an exception to the mandated encryption requirements outlined in this policy or its associated standards must be submitted by the Technology Staff (or data owner) and must receive formal, written approval from the Technology Security Team (or the designated Information Security Officer). Technology Staff may not unilaterally approve exceptions.

Criteria for Exemption

Exemptions will only be considered under the following conditions:

- **Risk Mitigation:** The data classification and accompanying risk assessment indicate that the confidential or restricted data is protected by documented compensating security controls that provide an equivalent level of security to the required encryption standard.
- **Business Use Case:** The required encryption mechanism demonstrably prevents a critical business function or is proven to be technically incompatible with a necessary system or application, and no reasonable alternative solution exists.
- **Data Characteristics:** The data in question is verifiably non-sensitive or de-identified such that its disclosure would not constitute a notifiable breach under MA 201 CMR 17:00 or other applicable regulations.

Exemption Documentation and Review

All approved exemptions must adhere to the following documentation and review standards:

- **Documentation Required:** Staff must submit a formal exemption request that details the following:
    - The specific policy requirement being exempted.
    - The **Data Classification** level of the information involved.
    - The precise **Business Use Case** necessitating the exemption.
    - A full description of the **compensating controls** in place.
    - The **potential risk** of a data breach under the exempted condition.
- **Validity Period:** All approved exemptions will be valid for a maximum period of one (1) year.
- **Mandatory Review:** The Technology Security Team must review and re-approve all existing exemptions annually or whenever there is a significant change to the system, data classification, or legal requirements.
- **Central Repository:** All exemption requests and final approvals must be **c**entrally documented and archived for audit purposes and future reference by the Technology Security Team.

Roles

Technology Security Team: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.

Technology Staff: Ensure that confidential and restricted data is appropriately protected. Implement encryption policies and procedures in accordance with FSU configuration standards.

Management Team: Provide information to aid in the risk analysis to determine the necessity and applicability of encryption mechanisms.

References

CIS Version 8 Controls
3.6 Encrypt Data on End-User Devices
3.9 Encrypt Data on Removable Media
3.10 Encrypt Sensitive Data in Transit
3.11 Encrypt Sensitive Data at Rest
4.1 Establish and Maintain a Secure Configuration Process
11.3 Protect Recovery Data

PCI Version 4 Requirements
Requirement 2 Apply Secure Configurations to All System Components
Requirement 3 Protect Stored Account Data
Requirement 4 Protect Cardholder Data with Strong Cryptography

MA 201 CMR 17:00 Section 17.15

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
9/15/2023	1.1	Steve Swartz, CIO Eric Boughton, CISO	Formatting, Review

5/9/2024	1.2	Eric Boughton, CISO	Formatting, References
10/31/2025	2.0	Eric Boughton, CISO	Added Enterprise Storage, Approved Cryptographic Standards, and Exemption sections