FITCHBURG STATE UNIVERSITY

Encryption Policy

Version 1.2	**Last Updated:** 5/9/2024
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 use approved encryption algorithms to protect restricted information. Fitchburg State University must use only approved cryptographic techniques and follow federal regulations and adhere to legal authority that is granted for the dissemination and use of encryption technologies.

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

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

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