FITCHBURG STATE UNIVERSITY

Security Training and Awareness Policy

Version 1.3	**Last Updated:** 2/13/2026
Security Level: Public	**Issued:** 9/13/2022

Purpose

This policy establishes a program to ensure effective knowledge transfer of the University's information security policies at Fitchburg State University and to provide security awareness training. Employees, temporary employees, and contractors with access to the University's information systems must adhere to data protection policies that govern the confidentiality, integrity, availability, and security of the University's information.

Scope

This policy applies to all employees, temporary workers, and contractors who have access to Fitchburg State information resources, whether individually controlled or shared, stand-alone or networked. This includes networking devices, personal computers, mobile devices, workstations, associated peripherals and software, and any hard-copy information.

Policy

All employees shall complete security awareness training on Fitchburg State's information security policies and procedures upon hire and at least annually thereafter. The Human Resources Department is responsible for notifying a new hire immediately of the requirement to complete online security awareness training. After training is conducted, Fitchburg State University will maintain records, as it deems appropriate, to confirm that an employee, temporary worker, or contractor received training.

The purpose of the information security awareness training program is to establish and sustain an appropriate level of protection for data and information resources by increasing users' awareness of their information security responsibilities. Specific objectives include:

- Improving awareness of the need to protect information resources
- Ensuring users understand their responsibilities for protecting information resources
- Mandatory training requires users to be fully aware of the company's information security policies and practices, including acknowledgment of the Written Information Security Program (WISP) and the acceptable use policy.
- Ensure employees develop the necessary skills and knowledge to perform their jobs securely. This includes providing specialized training tailored for roles with privileged access.

Security awareness training may be delivered in person or online.

Security awareness is reinforced through ongoing activities designed to measure and improve user behavior. The University conducts recurring simulated phishing exercises, periodic awareness reinforcement, and targeted micro-training. Results are monitored to identify risk trends, and individuals with repeated phishing test failures may be assigned remedial training. Program effectiveness is evaluated through participation metrics, assessment outcomes, and periodic reporting to institutional leadership in alignment with NIST and CIS security awareness practices.

Role-Based Training

To address risks associated with elevated access and specialized function, individuals with privileged access or sensitive responsibilities must complete supplemental role-based training aligned to their roles, including:

- PCI-DSS
- Privileged-access System Administrators
- CJIS Security and Privacy privileged-role training

Roles

- Chief Information Security Officer: Develops and manages the Information Security Training and Awareness program, ensuring all personnel receive the appropriate security training associated with their jobs, and maintains records of training received.
- HR and Technology Security Team: Ensure that all employees are appropriately trained and understand their roles in implementing the University's Information Security Policies.
- Management Team: Inform users of their training requirements, monitor compliance with those requirements, and update the CISO on employee compliance.
- All Users: Complete annual security training. Review, understand, and agree to comply with all University's Information Security Policies and Guidelines.

References

- CISv8 14 Establish and Maintain a Security Awareness Program
- PCIv4 Requirement 12 Support Information Security with Organizational Policies and Programs
- MA 201 CMR 17:00 Section 17.04

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
8/15/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
4/3/2023	1.1	Steve Swartz, CIO Eric Boughton, CISO	Minor grammatical fixes.
5/9/2024	1.2	Eric Boughton, CISO	Formatting, Updating References, adjusting role definitions, Removed duplications
2/13/2023	1.3	Stefan Dodd, CIO Eric Boughton, CISO	Minor working edits, added Role-based Training, and self-phishing section