FITCHBURG STATE UNIVERSITY

Security Training and Awareness

Version 1.2	**Last Updated:** 5/9/2024
Security Level: Public	**Issued:** 9/13/2022

Purpose

This policy defines a program to maintain an effective knowledge transfer of company information security policies at Fitchburg State University and provide security awareness training. Employees, temporary employees, and contractors who have access to company information systems must adhere to the data protection policies that outline the protection, confidentiality, integrity, and availability of information systems.

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, and any associated peripherals and software, as well as any hardcopy information.

Policy

All employees shall complete security awareness training with respect to Fitchburg State information security policies and procedures upon hire and, subsequently, at least annually. The Human Resources Department is responsible for notifying a new hire immediately of the requirement to complete online Security Training. After the training has been conducted, Fitchburg State University will maintain such records, as it deems appropriate to confirm 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
- Ensuring users are knowledgeable about the company's information security policies and practices, and develop skills and knowledge so they can perform their jobs securely

Security awareness training may be delivered in person or online.

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 maintaining records of training received.

HR and Technology Security Team: Ensure that all employees are appropriately trained and understand their roles in implementing the company's Information Security Policies.

Management Team: Inform users of their requirements, monitor compliance with the training requirement, and update the CISO regarding compliance of their employees.

All Users: Complete annual security training. Review, understand, and agree to comply with all company 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, Adjusted Role definitions, Removed duplications