FITCHBURG STATE UNIVERSITY

66 - Security Training and Awareness

Issued 9/13/2022

Version 1.0

Purpose

The Purpose of this policy is to define the program to be implemented to maintain an effective knowledge transfer of company information security policies at Fitchburg State University (FSU) and provide security awareness training. Employees, temporaries and contractors who have access to the 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 organizational employees and contractors who have access to FSU 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 and training with respect to FSU 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. Employees shall abide by University's information security policies. After the training has been conducted, FSU will maintain such records, as it deems appropriate that confirm that an employee, temporary worker or contractor received training.

The primary purpose of an effective information security awareness and 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 that users clearly understand their responsibilities for protecting information resources
- Ensuring that users are knowledgeable about the company's information security policies and practices, and develop skills and knowledge so they can perform their jobs securely

Training may be delivered in person or online.

The CISO is responsible for managing the IT security training and awareness program. The IT Security Team and staff will inform users of their requirements, monitor compliance with the training requirement and update management regarding compliance of their employees.

Role

Chief Information Security Officer: Develops and/or facilitates 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 Security Team: Ensure that all employees are appropriately trained and understand their roles in implementing the company's Information Security Policies.

All Users: Complete annual security training. Review, understand and agree to comply with all company Information Security Policies and Guidelines

References CIS

14.1 – 14.9 Security Awareness and Skills Training

References PCI

PCI
Requirement 6: Build and Maintain Secure Applications and Systems
Requirement 12: Maintain a policy that addresses information security for all personnel.

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.

Security Level

Public