FITCHBURG STATE UNIVERSITY

102 - Incident Response

Issued 9/7/2022

Version 1.1

Purpose

The purpose of this policy is to define the response of Fitchburg State University (FSU) to security incidents involving FSU people, information, systems, applications, and hardware.

Scope

This policy applies to all FSU security incidents. A security incident is defined as any attempt, successful or unsuccessful, to disable, compromise, bypass, alter, or by any other means maliciously misuse FSU people, information, systems, applications, and hardware.

Policy

- All reported security incidents shall be responded to in a timely manner.
- An incident report form must be completed and retained for each incident.
- In response to a security incident, the FSU IT team in conjunction with additional Incident Response Team members shall address the following:

Detection – Corroborate and define the incident.
Assessment – The incident should be classified based on available information to determine whether Network communications require closure or Disaster Recovery plans require implementation
Forensics - Data related to the incident shall be gathered and analyzed
Containment – Measures shall be taken to separate impacted systems from the rest of the company environment
Recovery – Systems shall be restored to normal operation as soon as possible and follow policy and procedures for applicable Backup and Recovery.
Post-Mortem – an analysis of the incident, FSU response to the incident, and lessons learned.

- Employees are required to report information security incidents and suspicious incidents to either their manager or the IT Security Team.
- Awareness of this requirement, identification and reporting of Information Security Incidents, is a component of the required Information Security Awareness Training Program. Such training shall be administered as part of the new hire on-boarding process as well as on an annual basis.
- Additional, role-specific training is administered to IT and other staff as merited by job responsibilities and access level: systems, network infrastructure, physical security and/or datacenter.
- Report incidents as required by the Massachusetts Breach Laws, General Laws, Chapter 93H

Role

IT Security Team: Leads information security incident response and coordinates reporting to external entities; determines if incident follow-up is needed; ensures all incidents and resolution activities are fully documented and tracked; ensures compliance with regulatory requirements.

IT Staff: Respond to information security incidents according to policy and procedures.

Management Team: Engage legal council, authorities, and external reporting entities as appropriate.

All Users: Report incidents to manager or IT Security Team promptly.

References CIS

17.1 - 17.9 Incident Response Management

References PCI

PCI

Requirement 11: Regularly test security systems and processes.
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 Restricted