Incident Response Policy

Version: 1.0
Issued: 4/28/2017

PURPOSE

The purpose of this policy is to define the response of ***Fitchburg State University (FSU)*** to electronic information security incidents. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

This policy applies to all ***FSU*** electronic information security incidents, henceforth referred to as an "incident," which are defined as any attempt, successful or unsuccessful, to disable, interrupt, compromise, bypass, alter, or by any other means misuse ***FSU*** information technology resources.

POLICY

- All reported incidents shall be responded to in a timely manner.
- An Incident Report Form (IRF) must be completed for each incident.
- In response to an incident, the following shall be addressed, as applicable:
    - **Detection** – Corroborate and define the incident;
    - **Assessment** – The incident should be classified based on available information to determine whether network communications require closure or activation of the ***Business Continuity Plan***;
    - **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 ***FSU*** 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 and students are required to report incidents to either the Helpdesk or other appropriate personnel.
- Additional role-specific training may be administered to staff members as required by job responsibilities and access level to systems, network infrastructure, physical security, and/or datacenter.

ENFORCEMENT

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, termination of employment or expulsion from the University.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Officer	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	Report incidents and/or respond to information security incidents according to policy and procedures.

ROLE	RESPONSIBILITY
Management Team	Report incidents and/or engage legal counsel , authorities, and external reporting entities as appropriate.
All Users	Report incidents to manager, or Information Security Officer promptly.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
DS5 Ensure System Security DS8 Manage Service Desk Incidents		

Incident Response Policy

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	1/12/2016	Compass ITC	Initial Draft