FITCHBURG STATE UNIVERSITY

60 - Configuration Management

Issued 8/29/2022
Version 1.0

Purpose

The purpose of this policy is to define the mechanisms for creating and maintaining a secure information technology environment for Fitchburg State University (FSU) information resources.

Scope

This policy applies to all FSU systems, specifically servers, network devices, workstations and mobile devices (where applicable).

Policy

All FSU systems shall be configured and managed using secure and industry vetted best practices. FSU System configuration standards shall be designed in accordance with industry best practices. Management of FSU systems includes the following activities:

- Event and system log monitoring
- Malware prevention and response
- Installation of system updates and patches.
- Device maintenance and repair

Role

IT Security Team: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented. Review and approve all system configuration standards and associated procedures.

IT Staff: Implement system configurations in accordance with FSU configuration standards and procedures. Review and respond to system and event log alerts. Distribute and manage malware prevention mechanisms. Respond to and remove malware infections. Distribute and manage system updates and patches.

References CIS

4.1 – 4.12 Secure Configuration of Enterprise Assets and Software
8.1 – 8.12 Audit Log Management

References PCI

PCI
Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Requirement 5: Use and regularly update anti-virus software or programs.
Requirement 6: Develop and maintain secure systems and applications.
Requirement 10: Track and Monitor all access to network resources and cardholder data.

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