Configuration Management Policy

Version: 1.0
Issued: 4/28/2017

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. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

This policy applies to all ***FSU*** systems, specifically servers, network devices, and workstations.

POLICY

All ***FSU*** systems shall be configured and managed using secure and industry recognized 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;
- Changes to default system and application passwords;
- Makes use of change management when applicable (see ***Change Management Policy***).

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Manager	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

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
DS9 Ensure System Security AI6 Manage Changes ME1 Evaluate IT Performance ME2 Internal Control Monitoring	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	

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
	network resources and cardholder data. MA 201 CMR 17:00 Section 17.04	

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	7/28/2015	Compass ITC	Initial Draft