FITCHBURG STATE UNIVERSITY

58 - Change Management

Issued 8/29/2022

Version 1.0

Purpose

The purpose of this policy is to control all changes to Fitchburg State University (FSU) information resources. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

Scope

This policy applies to all changes to FSU information resources, including applications, hardware, and systems.

Policy

•All server or application changes shall be planned, approved, tested and documented.

•Critical or security patches for workstations may be applied to end-user systems through policy or automated methods without prior testing as the risk of data loss may outweigh usability testing.

•Only authorized staff shall perform changes.

•Assessment of the potential impact of such changes shall be conducted beforehand.

•Audit trail of all changes, configuration changes made, person who performed the change, date of the change, purpose of the change, whether the change was a success or failure and other relevant information shall be retained within the TOC database. https://toc.fitchburgstate.edu

•Procedures for recovering from unsuccessful changes shall be documented.

•Information Technology employees shall be notified regarding how these changes shall impact them. If system availability will be affected while the change is being made, affected individuals will be notified letting them know what to expect and when to expect it. They should also know whom to contact in case they experience difficulty as a result of the change.

•Current, complete backups shall be available before changes are made.

•An IT manager (approver), other than the implementer of the change, shall review and approve changes prior to installation into a production environment to ensure all necessary documentation is in place and procedures were followed.

•A change may be denied for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

•In certain circumstances emergency changes can be made without approvals beforehand. System failures, emergencies or the discovery of a critical vulnerability affecting security may necessitate emergency changes. These changes must include notification to users affected.

•From time to time information technology infrastructure components may require an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning. Whenever possible and where applicable maintenance windows will be defined to limit the impact to productivity.

•All changes shall be reviewed to ensure that organizational documentation (user documentation, network diagrams, procedures, knowledge bases etc) impacted by the change is updated accordingly.

•Significant changes to the environment must adhere to the FSU Risk Management Policy, Standards, and Procedures.

Role

IT Managers: Ensures change control policies and procedures are followed according to this policy and approves changes.

IT Staff: Follows this policy and maintains change documentation. Ensures that all changes to systems have been approved, tested and implemented in compliance with this policy. All documentation is updated to reflect changes.

References CIS

4.1 Establish and Maintain a Secure Configuration Process
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure

References PCI

PCI
Requirement 6: Develop and maintain secure systems and applications.

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