Change Management Policy

Version: 1.0
Issued: 4/28/2017

PURPOSE

The purpose of this policy is to control all changes to ***Fitchburg State University (FSU)*** information technology resources. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and ensure enhancements work as designed. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

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

POLICY

All changes shall be planned, approved, tested and documented.

- Only authorized staff shall perform changes;
- Assessment of the potential impact of such changes shall be conducted;
- Audit trail of all changes, configuration changes made, person who performed the change, date of the change, purpose of the change, and other relevant information shall be retained;
- Procedures for testing and approving changes shall be implemented prior to promotion to production;
- Procedures identifying responsibilities for aborting and recovering from unsuccessful changes are document and can be implemented;
- Information users 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 of 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 backups shall be available when changes are made;
- An IT manager, other than the implementer of the change, shall review changes prior to installation into a production environment except in emergency situations to ensure all 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;
- System failures or the discovery of a critical vulnerability affecting security may necessitate emergency changes without prior approval;
- 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.

ENFORCEMENT

Any employee found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including termination of employment.′

Change Management Policy

Version: 1.0
Issued: 4/28/2017

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
IT Manager	Monitors that change control policies and procedures are followed according with this policy and approves all proposed changes unless performed in an emergency situation.
IT Staff	Follows this policy and shall maintain a log with the change documentation. Ensure that changes to systems have been approved, documented, tested and implemented in compliance with the policy.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
AI.6 Manage Changes AI.7 Install and accredit solutions and changes	PCI Requirement 6: Develop and maintain secure systems and applications. 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