Access Control

Version: 1.0
Issued: 4/12/2017

PURPOSE

The purpose of this policy is to control and manage logical access to ***Fitchburg State University (FSU)*** information technology resources. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

This policy applies to any user who accesses ***FSU*** information technology resources.

POLICY

All access to ***FSU*** applications, systems, and hardware shall be authorized and approved. Any access not explicitly authorized and approved is prohibited. Access to specific applications, systems, components and technology infrastructure shall only be granted to employees with a legitimate, business-related need for such access. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

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 College.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Officer	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.
IT Staff	Ensure that individuals assigned to access their applications are authorized and assigned duties require access capabilities. Ensure that the IT infrastructure is protected against unauthorized access. Administer the setup of new network, system, and application accounts, changes to existing accounts, and disabling of accounts for no longer employed personnel in a timely manner. Distribute access control lists for annual reviews.
Management Team	Notify IT of new employees, terminated employees and changes in job responsibilities that would affect access rights. Determine who should have access to their resources. Periodically review access rights and notify IT when access privileges require adjustment.
All Users	Understand and adhere to this policy. Safeguard their user IDs and passwords. Access only those resources for which they are authorized. Immediately report unauthorized or suspected violations of this policy to their manager or the Information Security Officer.

Access Control

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
DS5.3 Identity Management DS5.4 User Account Management		

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