FITCHBURG STATE UNIVERSITY

59 - Access Control

Issued 8/29/2022

Version 1.0

Purpose

The purpose of this policy is to control logical access to Fitchburg State University (FSU) applications, systems, and hardware and the execution of automated functions.

Scope

This policy applies to all FSU employees, contractors, and third parties who access FSU applications, systems, or hardware.

Policy

All access to FSU applications, systems and hardware shall be authorized and approved. Any access not explicitly authorized and approved is forbidden. Access to specific applications, systems, components and technology infrastructure shall only be granted to employees or contractors with a legitimate need.

The level of access granted and privileges assigned shall be shall be limited to the minimum required to perform assigned duties.

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.

IT Staff: Ensure that individuals assigned to access their applications are authorized. 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 terminated personnel in a timely manner. Maintain access control lists for review.

HR, Management or Provisioning Automation: 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 roles 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 suspected violations of this policy to their manager or to the IT Department.

References CIS

3.3 Configure Data Access Control Lists
6 Access Control Management

References PCI

PCI
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 8: Identify and authenticate access to system components.
Requirement 12: Maintain a policy that addresses information security for all personnel.

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