FITCHBURG STATE UNIVERSITY

Access Control Policy

Version 1.2	**Last Updated:** 8/8/2025
Security Level: Public	**Issued:** 8/29/2022

Purpose

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

Scope

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

Policy

All access to Fitchburg State University 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 limited to the minimum required to perform assigned duties.

Access Recertification & Authorization Oversight

System administrators shall perform a formal access-recertification of all user, service, and privileged accounts regularly, and immediately upon any role or employment change. Each review must confirm that every account's permissions align with current job duties and least- privilege principles; results are to be recorded in the system and co-signed by the relevant data owner or business manager. Any required access removals or modifications must be completed in a timely fashion, and all review evidence shall be retained for audit.

It is strongly recommended to conduct an annual or more frequent review of privileged users.

Roles

- <u>All Users</u>: 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 the Technology Department.
- <u>Technology Security Team</u>: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.

- System Administrators or Technology Staff: Ensure that individuals assigned to access their applications are authorized. Review assignments to ensure compliance with policy. Administer accounts as necessary, ensuring the disabling of accounts for terminated personnel in a timely manner. Maintain access control lists for review.
- HR, Management, or Provisioning Automation: Notify the Technology Staff 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 Technology Staff when access privileges require adjustment.

References

CISv8 Control 6: Access Control Management CISv8
Configure Data Access Control Lists

PCIv4 Requirement 7 Restrict Access to System Components and Cardholder Data PCIv4
Requirement 8 Identify Users and Authentication Access to System Components PCIv4
Requirement 9 Restrict Physical Access to Cardholder Data

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 in 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.

Revision History

Date of Change	Revision	Responsible	Summary of Change
8/15/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
5/5/2024	1.1	Eric Boughton, CISO	Formatting, IT to Technology Department, Adjusting References
8/08/2025	1.2	Eric Boughton, CISO Stefan Dodd, CIO	Added Access Recertification & Authorization. Added system administrator role. Added Oversight section. Minor Grammar changes. Annual Review