FITCHBURG STATE UNIVERSITY

Remote Access Policy

Version 1.2	**Last Updated:** 2/6/2026
Security Level: Public	**Issued:** 9/14/2022

Purpose

This policy establishes the necessary procedures and requirements for any remote client or user connecting to the Fitchburg State University network. These requirements are implemented to mitigate the risk of damage resulting from the unauthorized use of university resources. Such potential damages include, but are not limited to, the compromise of sensitive or organizational information, intellectual property breaches, reputational harm, damage to essential internal systems, loss of system availability, or corruption of data integrity.

Scope

Anyone who accesses Fitchburg State's network, applications, systems, or hardware remotely.

Policy

All remote access to Fitchburg State University network, applications, systems, and hardware shall be authorized and approved; any access not explicitly authorized and approved is forbidden. Only faculty, staff, contractors, and approved third-party vendors with a demonstrated, legitimate business necessity will be granted remote access to designated networks, applications, systems, components, and technology infrastructure. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

Users authorized to use remote connections shall ensure that unauthorized users are not granted access to the Fitchburg State internal network via these connections. All individuals and machines accessing the network, including company-owned and personal equipment, are a de facto extension of Fitchburg State University's network and, therefore, are subject to the same rules and regulations stated in the Information Security Policies. Users of non-University-managed computers shall configure the equipment to comply with the Fitchburg State Acceptable Use Policy and related security compliance processes, including the Personal Device Policy.

All devices connected to the network via remote access technologies must:

- Use the most up-to-date antivirus software.
- Have the most recent security and operating system (OS) patches installed.
- Have security updates configured to auto-update.
- Web browsers and common applications shall be applied in a timely manner.

Remote access will be provided through Fitchburg State University's VPN or Virtual Desktop environment (depending on needs and circumstances). Department Heads or Management will approve access. For contractors, the requesting Manager or Department Head must provide approval and oversight.

Multi-factor authentication is required for remote access.

Users agree to apply safeguards to protect Fitchburg State information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include exercising discretion in deciding when and where to access data or services remotely, and preventing inadvertent or intentional viewing of displayed information.

Remote access to data or services may not be used to copy private or personal information, such as that residing on a privately owned computer, to company file shares, or other company-owned information systems.

Remote access services may be used only for the conduct of business related a work. Personal, family, private, or commercial use of any service available remotely is not permitted.

Roles

- Technology Managers: Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.

- Technology Staff: Ensure that individuals assigned to remotely access their applications are authorized and assigned duties require access capabilities. Ensure that the Technology infrastructure is protected against unauthorized remote access. Administer the setup of newly added devices to be used for remote access.

- Management Team: Determine which employees need remote access to their resources.

- All Users: Understand and adhere to this policy. Safeguard their user IDs and passwords. Immediately report suspected violations of this policy to their manager or the Technology Manager.

References

CISv8 6.3 Require MFA for Externally-Exposed Applications
CISv8 6.4 Require MFA for Remote Network Access

CISv8 12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
CISv8 13 .5 Manage Access Control for Remote Assets
PCIv4 Requirement 3 Protect Stored Account Data

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.

Revision History

Date of Change	Revision	Responsible	Summary of Change
9/14/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
4/10/2023	1	Steve Swartz, CIO	Reviewed No changes
5/9/2024	1.1	Eric Boughton, CISO	Formatting, References
2/6/2026	1.2	Eric Boughton, CISO Stefan Dodd, CIO	ADA Formating, Wording