FITCHBURG STATE UNIVERSITY

67 - Remote Access

Issued 9/14/2022

Version 1.0

Purpose

The purpose of this policy is to define the process and requirements for connecting to the Fitchburg State University (FSU) network from any remote host. These requirements are designed to minimize the potential exposure to damages, which may result from unauthorized use of company resources. Damages include the breach of sensitive or organizational information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system availability, or the corruption of information integrity.

Scope

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

Policy

All remote access to FSU applications, systems and hardware shall be authorized and approved, any access not explicitly authorized and approved is forbidden. Remote access to specific applications, systems, components and technology infrastructure shall only be granted to personnel 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.

Employees and third parties authorized to utilize remote connections shall ensure that unauthorized users are not allowed access to the FSU internal network utilizing these connections. All individuals and machines, while accessing the network, including company-owned and personal equipment, are a de facto extension of FSU 's network and therefore their machines are subject to the same rules and regulations stated in the Information Security Policies. Users of computers that are not company property shall configure the equipment to comply with the FSU Acceptable Use Policy and FSU Security compliance processes.

All devices that are connected to the network via remote access technologies must use the most up-to-date antivirus software, and be up-to-date on available patches. This includes personal computers. Security patches for installed operating systems (with auto-update enabled), web browsers, and common applications shall be applied in a timely manner.

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.

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 provide approval for access. In the case of contractors, the requesting Manager or Department Head must provide approval and oversight. Multi-factor authentication will be required for remote access.

Users agree to apply safeguards to protect FSU information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remotely access data or services, prevention of 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.

Role

IT Manager: 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 remotely access their applications are authorized and assigned duties require access capabilities. Ensure that the IT 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 IT Manager.

References CIS

6.3 Require MFA for Externally-exposed Applications
6.4 Require MFA for Remote Network Access
12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
13.5 Manage Access Control for Remote Assets

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