FITCHBURG STATE UNIVERSITY

87 - Third Party Access Policy

Issued 10/14/2022

Version 1.0

Purpose

This policy establishes the rules for third-party access to Fitchburg State University information systems, datacenters and IT secure areas.

Scope

This policy outlines responsibilities and expectations of anyone from an outside source (contracted or otherwise) who require access to Fitchburg State University‘s information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of Fitchburg State University personnel responsible for the contracting and/or supervising of the third party.

Policy

Computer Room and Third Policy Guidelines:

•All third-party access to the Data Center should be scheduled to occur during regular business hours, or on off hours if a service disruption is planned.

•When third parties are scheduled to have access to the Data Center, the IT staff must be notified in advance of the date, time, and type of work to be performed.

•When the third party arrives, he/she will report to a staff contact that scheduled the visit. The third party is required to sign in and wear an ID that identifies them as a visitor. The staff contact will escort the third party to the IT area. The third party is to be informed that he/she will take direction from the IT staff point person in relation to their activity in the Data Center.

•Prior to the onset of any work, the third party will describe the activities that are planned.

•The IT staff point person is responsible for explaining what measures need to be taken to protect the computer hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the IT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the IT staff to do what needs to be done to protect the computer systems before starting their work.

•The third party will report to and receive instructions from the IT staff point person regarding their work in the Data Center. The IT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed before leaving the area.

•This policy will be provided to each third party entity. They will also be required to sign a data protection agreement that they have read and understood this policy.

Information Systems Third Party Policy Guidelines:

1. Any third-party agreements and contracts must specify:

•The work that is to be accomplished and work hours.
•Fitchburg State University information that the third party should have access to.
•The minimum security requirements that the third party must meet (i.e., method for remote access).
•How Fitchburg State University information is to be guarded by the third party. Signing of an agreement is typically required.
•Strict use of Fitchburg State University’s information and information resources for the purpose of the business agreement by the third party. Any other information acquired by the third party in the course of the contract cannot be used for the third-party’s own purposes or divulged to others.
•Feasible methods for the destruction, disposal, or return of Fitchburg State University information at the end of the contract.

•The return of company property such as laptop, after the completion or termination of the agreement.

2. Third party must comply with all applicable Fitchburg State University standards, agreements, practices and policies.

3. Fitchburg State University will provide an IT point of contact for the third party. This point of contact will work with third party to ensure compliance.

4. Third party will provide Fitchburg State University with all additional third parties working on project.

5. Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with Fitchburg State University's password policy.

6. Any third-party device that is connected to Fitchburg State University systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage incurred to Fitchburg State University in the event of an incident.

7. Each third-party employee that has access to Fitchburg State University's sensitive information should be cleared by IT to handle that information.

8. Third-party employees must report all security incidences to the appropriate IT manager.

9. Third party must follow all applicable change control procedures and processes.

10. All third-party employees are required to comply with all applicable auditing regulations.

11. All third-party maintenance equipment on Fitchburg State University's network that connects to the internet will be assigned to a separated contractor network when use for authorized purposes.

12. Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to Fitchburg State University or destroyed immediately upon departure. The third party will also provide written certification of that destruction within 24 hrs. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by Fitchburg State University.

13. Fitchburg State University will eliminate third-party access to facilities after the contract has been completed or terminated. The following steps must be performed: Remove third party authentication and all means of access to systems; Make sure that incoming e-mail is re-routed to an appropriate person; Archive any third-party software configuration, and transfer ownership to designated internal staff.

Role

IT Staff and Management: Follows this policy for access to third parties. Appoints a point of contact for managing the relationship with the third party.

Information Security Officer: Oversee the Compliance of the Policy, review the policy periodically and update the policy as needed.

References CIS

15.4 Ensure Service Provider Contracts include Security Requirements

References PCI

PCI
Requirement 8
Requirement 9
Requirement 12

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.