FITCHBURG STATE UNIVERSITY

Physical Security Policy

Version 1.2	**Last Updated:** 5/9/2024
Security Level: Public	**Issued:** 8/29/2022

Purpose

This policy controls physical access to Fitchburg State University data centers, information resources, and systems.

Scope

This policy applies to all Fitchburg State employees, contractors, and third parties who have physical access to Fitchburg State University data centers, information resources, and systems.

Policy

University equipment shall be installed in suitably protected areas. The following controls shall be implemented:

General Physical Security

- All doors and entrance locations of organizational facilities shall be locked when unattended and protected by electronic access controls.
- A record of the users of physical access controls such as facility keys and electronic cards shall be kept.
- Back-up media shall be located at a safe distance to avoid damage from a disaster at the main campus.
- Protection or mitigation must be implemented against fire, flood, and other environmental factors that could damage the resources. This includes:
    - Locations should utilize fire suppression equipment.
    - Locations should provide emergency power controls nearby.
    - Equipment is to be located on racks raised above floor level.
- Annual testing will be performed on all fire and protective systems.
- A video camera will record entry/egress at the door, with recordings retained for at least 90 days.
- Environmental controls will be implemented to ensure that temperature and humidity are maintained within limits for the equipment contained therein.

- Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptible power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities.
- Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or loaned to others by authorized users.

Visitor Security

- Third-party support services personnel are granted access to secure areas only when required, authorized, and supervised.
- Visitors to the data center must be escorted at all times and sign in and out on the Technology area log book, and indicate they have data center access.

Roles

Technology Security Team: Ensure awareness and compliance with this policy and the implementation of all component policies and procedures.

Technology Staff: Ensuring policy is followed, and information systems are installed in suitable protected areas.

Users: Responsible for complying with this policy, protecting information resources in their possession, and reporting incidents to the Security team.

References

CISv8 1.1 Establish and Maintain Detailed Enterprise Asset Inventory

PCIv4 Requirement 9 Restrict Physical Access to Cardholder Data

MA 201 CMR 17:00

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
8/29/2022	1	Steve Swartz, CIO Sherry Horeanopoulos, CISO	Creation of Policy, Start of Revision Tracking, Formatting of Document
2/24/2023	1.1	Steve Swartz, CIO	From Mike Ferreira: change power shutdown controls to "power controls nearby" From Eric Boughton: Update our IT log to indicate if data center access is required.
5/9/2024	1.2	Eric Boughton, CISO	Formatting, References, Added Technology Staff Role