Datacenter Physical Security Policy

Version: 1.0
Issued: 4/28/2017

PURPOSE

The purpose of this policy is to control physical access and environmental controls for ***Fitchburg State University (FSU)*** information technology datacenter facilities. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

This policy applies to all ***FSU*** employees, contractors, and third parties who have physical access to ***FSU*** information technology datacenter facilities.

POLICY

College equipment shall be installed in suitably protected areas with minimum indication of their purpose. The following controls shall be implemented:

General Physical Security

- All doors and entrance locations of datacenter facilities shall be locked when unattended and protected during non-business hours by electronic alarms;
- A record of the users permitted physical access shall be maintained and audited on a regular basis;
- Back-up media shall be located at a safe distance to avoid damage from a disaster;
- Protection must be implemented against fire, flood, and other hazards and/or environmental factors;
- Datacenter access shall be restricted to only authorized personnel and authorized third parties when escorted;
- Provide emergency power shutdown controls;
- 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 be present with recordings retained for one month when possible;
- Provide an uninterruptible power supply and a generator when possible. Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable 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;
- The Visitor must sign in and out of the datacenter logbook, documenting their name, company if any, and purpose of visit.

ENFORCEMENT

Any employee found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including termination of employment.

Datacenter Physical Security Policy

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Officer	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.
All Users	Responsible for complying with this policy, protecting information resources in their possession, and to immediately report unauthorized or suspicious activities or violations of this policy to their manager and the Information Security Officer.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
DS12 Manage the Physical Environment	MA 201 CMR 17:00	

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	7/28/2015	Compass ITC	Initial Draft