University Administrative Policy

Policy Name: Information Technology Services Datacenter Physical Security Policy
Responsible Office: CIO
Originator of the Policy: CIO
Effective Date: July 11, 2016
Revision History:
Web Link: https://www.salemstate.edu/policies/

---

1. Rationale

The purpose of this policy is to control physical access to Salem State University (SSU) facilities, information resources, and systems.

2. Statement of Policy

University datacenter equipment shall be installed in suitably protected areas with minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities. 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 those who have physical access to the datacenter shall be maintained and audited on a regular basis.
- Back-up media shall be located at a safe distance to avoid damage from a datacenter disaster.
- Protection must be implemented against fire, flood, and other 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 pointed at the door with recordings retained for three months.
- Provide an uninterruptible power supply. 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 to the datacenter logbook, documenting their name and purpose of visit.

3. Scope

University datacenter equipment shall be installed in suitably protected areas with minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities. 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 those who have physical access to the datacenter shall be maintained and audited on a regular basis.
- Back-up media shall be located at a safe distance to avoid damage from a datacenter disaster.
- Protection must be implemented against fire, flood, and other 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 pointed at the door with recordings retained for three months.
- Provide an uninterruptible power supply. 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 to the datacenter logbook, documenting their name and purpose of visit.

4. Fiscal Considerations

	Direct Costs / Savings / Revenue Generation	**Indirect Costs / Savings / Revenue Generation**
Initial Implementation	Varies over time	Varies over time
Ongoing	Varies over time	Varies over time

5. Responsibilities

Responsible Party	**List of Responsibilities**
CISO	Ensure awareness and compliance with this policy.
CIO	Ensure that this policy and all component policies and procedures are maintained and implemented
Deputy CIO, Technology Services	Document access control procedures. Implement approved access procedures.
All IT Employees	Understand and adhere to this policy. Safeguard their access codes and key card. Access the data center only when necessary to complete job duties. Immediately report suspected violations of this policy to their manager, the CISO, the CIO.

6. Policy Enforcement

Violation(s)	It shall be a violation of this policy to promulgate any applicable policy in contravention of the requirements outlined herein.
Potential consequences	Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, termination of employment or expulsion from the University
How to report	Contact CISO or CO

7. Reference Documents

Policy or Document	**Web Address**
n/a	

8. **Contact(s)**

Subject	Office or Position	Telephone Number	Email
	CIO, CISO		

9. **Effective Date:** Upon approval by the president.

10. **Dissemination:** Posted on the university web site.

11. **Review Cycle:** Initial review after 12 months; subsequent review every 5 years.