EDINBORO UNIVERSITY OF PENNSYLVANIA

SECURITY TO TECHNOLOGY FACILITIES POLICY
Policy No. D054

Recommended for Approval by _____
Mr. Guilbert Brown, Vice President Finance and Administration

Approved by _____ on 2/2/15
Dr. Julie Wollman, President

Review Data: As Required

INTRODUCTION

Pennsylvania State System of Higher Education (PASSHE) Universities and divisions have physical access to Information Technology (IT) facilities and resources such as servers, backup media, and communication closets, which enables these organizations to bypass any application or operating system security. Organizations are to take great care in physically securing IT facilities and resources to ensure the integrity of their systems and networks.

PURPOSE

The purpose of this document is to establish information security guidelines to help ensure that PASSHE IT facilities and resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

POLICY

IT facilities and resources include data centers, computer rooms, telephone closets, network operation centers, network communication closets, voicemail system rooms, and similar areas containing IT facilities and resources. All IT facilities and resources should be physically protected in proportion to the criticality, functional importance and data classification.

Protection measures include:

1. Separated, locked and designated limited access areas.

2. Environmentally controlled to ensure operating conditions are within specifications for equipment located within the confines of the area.

3. Equipped with environmental and safety monitoring devices to ensure compliance with regulated or statutory requirements.

4. Inspected on a regular basis to ensure compliance with health, safety, fire, security, and maintenance requirements.

5. Taking pictures and / or video, including by cell phones equipped with cameras, should be prohibited without authorization from the facility director or designee.

Access to restricted IT facilities and resources is limited to authorized persons:

1. The process for granting door keys or access cards for these facilities and resources is to include the approval of the person responsible for the facility or room.

2. The facility manager or designee should have a master record of all personnel who have access to all Information Technology facilities including but not limited to the data center, networking closets, telecomm closets, and the network operations center.

3. Access requests should be renewed annually to maintain approved access. Managers should notify appropriate personnel immediately when access is no longer required due to an employee's termination or a change in job responsibilities.

4. Access cards and/or keys issued for access to restricted IT facilities and resources may not be shared or loaned to others.

5. Entry into the IT restricted spaces by tailgating other staff should not be permitted.

6. Employees, business partners and citizen visitors without the proper access credentials may be granted temporary access via verbal or signed orders when conditions require their immediate access, or visitor access is approved. These individuals:
    a. Should be recorded in the facility sign-in/sign-out log. This log should have appropriate language on each page, or otherwise prominently displayed, indicating the minimal visitor responsibilities associated with accessing the facility.
    b. Should be issued a temporary identification badge and required to wear it openly.
    c. Should be supervised at all times while in restricted areas by a party with authorized access to the IT facilities and resources.

7. Access records and sign-in logs should be maintained and archived for routine review for a period of not less than one year.

8. No one should be permitted to enter a controlled-access facility, area, or room without being authenticated and having his/her privileges verified.

9. University personnel must supervise all non-University personnel entering the data centers.

10. Maintenance of data center equipment and the facility by PASSHE staff and third parties is required. Maintenance may include but in not limited to general cleaning and maintenance on electrical and mechanical systems. Maintenance visits by non-University staff should be scheduled in advance and known by the facility manager of the data center and related information technology spaces. Maintenance staff should be supervised at all times and / or under surveillance. All maintenance personnel should carry an approved identification credential and adhere to University policies and procedures.

11. As a condition of obtaining access to the facility, all University faculty, staff, students and third party visitors should agree not to disclose information they may obtain about the facility except to those who are required to have the information to conduct legitimate university business.

Organizations should ensure procedures are in place to provide immediate access to IT facilities and resources to fire, safety, and other emergency personnel in the case of an emergency. To the extent possible, data center personnel should have had response discussions in advance of an emergency with first responders responsible for the center.

GUIDELINES FOR FUTURE PLANNING

As renovations and construction of facilities occur, they should include restricted rooms dedicated to information technology and infrastructure (i.e. HVAC controls, surveillance systems, security systems) systems.

CONTACT INFORMATION:

Vice President Finance and Administration
219 Meadville Street
Edinboro, PA 16444
814-732-2585