Physical and Environmental Protection (PE)

Purpose:

The following standards are established to support the policy statement 10.12 that "CSCU will: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems."

Scope:

1. Institutional Units of the Connecticut State College and University System including the Connecticut Board of Regents System Office.

2. All Connecticut State College and University institutional units' information systems.

Standard:

1. Physical Access Authorizations [NIST 800-53r4 PE2]

1.1 For all information systems, the Information System Owner:

a.) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b.) Issues authorization credentials for facility access;

c.) Reviews the access list detailing authorized facility access by individuals yearly; and

d.) Removes individuals from the facility access list when access is no longer required.

2. Physical Access Control [NIST 800-53r4 PE3]

2.1 For all information systems, the Information System Owner:

a.) Enforces physical access authorizations at entry/exit points to the facility where the information system resides by;

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.1200	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

- Verifying individual access authorizations before granting access to the facility; and
- Controlling ingress/egress to the facility using one or more physical access control systems/devices;

b.) Maintains physical access audit logs for entry/exit points;

c.) Escorts visitors and monitors visitor activity;

d.) Secures keys, combinations, and other physical access devices;

e.) Inventories physical access devices every year; and

f.) Changes combinations and keys yearly and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

3. Access Control for Transmission Medium [NIST 800-53r4 PE4]

3.1 For all moderate and high risk information systems, the Information System Owner controls physical access to information system distribution and transmission lines within organizational facilities using electronic or physical locking mechanisms.

4. Access Control for Output Devices [NIST 800-53r4 PE5]

4.1 For all moderate and high risk information systems, the Information System Owner controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

5. Monitoring Physical Access [NIST 800-53r4 PE6]

5.1 For all information systems, the Information System Owner:

a.) Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b.) Reviews physical access logs yearly and upon occurrence of incidents or potential indications of incidents; and

c.) Coordinates results of reviews and investigations with the organizational incident response capability and ISPO.

5.2 For all moderate and high risk information systems, the Information System Owner monitors physical intrusion alarms and surveillance equipment. [NIST 800-53r4 PE6 (1)]

6. Visitor Access Records [NIST 800-53r4 PE8]

6.1 For all information systems, the Information System Owner:

a.) Maintains visitor access records to the facility where the information system resides for one year; and

b.) Reviews visitor access records yearly.

6.2 For high risk information systems, the Information System Owner employs automated mechanisms to facilitate the maintenance and review of visitor access records. [NIST 800-53r4 PE8 (1)]

7. Alternate Work Site [NIST 800-53r4 PE17]

7.1 For all information systems, the Information System Owner:

a.) Employs safeguarding mechanisms at alternate work sites;

b.) Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c.) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Roles & Responsibilities

Refer to the Roles and Responsibilities located on the website.

Definitions

Refer to the Glossary of Terms located on the website.

References

ITS-04 CSCU Information Security Policy

NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016.