Personnel Security (PS)

Purpose:

The following standards are established to support the policy statement 10.14 that "CSCU will: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that CSCU information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with CSCU security policies, standards, and procedures."

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. Personnel Screening [NIST 800-53r4 PS3]

1.1 For all information systems, the Information System Owner and Data Owners must ensure:

a.) Individuals have been screened prior to authorizing access to the information system; and

b.) Personnel screening and rescreening must be consistent with applicable state and federal laws, CSCU policies, regulations, and standards.

2. Personnel Termination [NIST 800-53r4 PS4]

2.1 For all information systems, the Information System Owner in collaboration with the Data Owner, upon termination of individual employment:

a.) Disables information system access within the same day of notification;

b.) Terminates/revokes any authenticators/credentials associated with the individual;

2.2 For all information systems, the Data Owner, upon termination of individual employment:

a.) Conducts exit interviews that include a discussion of:

- Continued obligations under information system non-disclosure, confidentiality, or user access agreements.
- Determine all information systems to which the individual had access and email distribution list memberships.

b.) Retrieves all security-related organizational information system-related property;

c.) Retains access to organizational information and information systems formerly controlled by terminated individual; and

d.) Notifies the Information System Owner within the same day of termination.

2.3 For high risk information systems, the Information System Owner employs automated mechanisms to notify upon termination of an individual. [NIST 800-53r4 PS4 (2)]

3. Personnel Transfer [NIST 800-53r4 PS5]

3.1 For all information systems, the Data Owner:

a.) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

b.) Initiates transfer or reassignment actions within the same day following the formal transfer action;

c.) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d.) Notifies the Information System Owner within the same day.

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.