Security Assessment and Authorization (CA)

Purpose:

The following standards are established to support the policy statement 10.6 that "CSCU will: (i) periodically assess the security controls in CSCU information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in CSCU information systems; (iii) authorize the operation of CSCU information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls."

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. Security Assessments [NIST 800-53r4 CA2]

1.1 For all information systems the ISPO:

a.) Develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

b.) Assesses the security controls in the information system and its environment of operation at least once of three (3) years, when significant changes after initial authorization, and until the system is decommissioned to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c.) Produces a security assessment report that documents the results of the assessment; and

d.) Provides the results of the security control assessment to the CSCU CIO, Campus ISSO, CSCU President/Campus President, and Information System Owner.

1.2 For moderate and high risk information systems the ISPO:

a.) Employs assessors or assessment teams with independence from the information system owner to conduct security control assessments. [NIST 800-53r4 CA2 (1)]

b.) Includes as part of security control assessments:

- Occur once every two (2) years;
- Perform announced or unannounced assessments;
- Will include, but not limited to, one or more of the following methods of testing:
    a. In-depth Monitoring;
    b. Vulnerability Scanning;
    c. Malicious User Testing;
    d. Insider Threat Assessment;
    e. Performance/Load Testing. [NIST 800-53r4 CA2 (1)]

2. System Interconnections [NIST 800-53r4 CA3]

2.1 For all information systems the Campus President and Campus CIO in consultation with the Campus ISSO and the Information System Owner:

a.) Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b.) The information system owner documents, for each authorized interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c.) Reviews and updates Interconnection Security Agreements yearly.

2.2 For moderate and high risk information systems;

a.) The information system owner ensures that a deny-all, permit-by-exception policy is employed for the information system to connect to external information systems. [NIST 800-53r4 CA3 (5)]

3. Plan of Action and Milestones [NIST 800-53r4 CA5]

3.1 For all information systems the Information System Owner in consultation with the Campus ISSO:

a.) Develops a plan of action and milestones for the information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b.) Updates existing plan of action and milestones yearly or upon notification based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

4. Continuous Monitoring [NIST 800-53r4 CA7]

4.1 For all information systems, the ISPO must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

a.) Establishment of metrics to be monitored;

b.) Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;

c.) Ongoing security control assessments in accordance with the approved CSCU continuous monitoring strategy;

d.) Ongoing security status monitoring of CSCU-defined metrics in accordance with the approved CSCU continuous monitoring strategy;

e.) Correlation and analysis of security-related information generated by assessments and monitoring;

f.) Response actions to address results of the analysis of security-related information; and

g.) Reporting the security status of the organization and the information system to CSCU President, CSCU CIO, Campus President, Campus CIO, Campus ISSO, and Information System Owner.

4.2 For moderate and high risk information systems.

a.) The ISPO employs assessors or assessment teams with independence from the information system owner to monitor the security controls in the information system on an ongoing basis. [NIST 800-53r4 CA7 (1)]

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.