Planning (PL)

Purpose:

The following standards are established to support the policy statement 10.13 that "CSCU will develop, document, periodically update, and implement security plans for CSCU information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the 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. System Security Plan [NIST 800-53r4 PL2]

1.1 For all information systems:

a.) The Information System Owner, in consultation with the Campus ISSO is responsible to develop and maintain a System Security Plan (SSP) for each information system. A system security plan (SSP) must describe the processes, procedures, and security controls currently being used or planned to be implemented to manage and secure the information system to meet security requirements, including rationale for the tailoring and supplemental decisions that must be developed, documented, updated, and implemented for the information system.

b.) The SSP must:

- Be consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the information system and its operational environment both generally and in technical terms.

a. Information processing flow, including key inputs and outputs, must be described.

b. All IT assets, including hardware, software, and (if appropriate) networking/telecommunications equipment, must be listed and described.

c. The information system and subsystem authorization boundaries must be explicitly defined.

d. The description must include applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high level design).

e. The description must reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, wireless technology, public access, hosting or operation at a facility outside of the organization's control), as applicable.

- Describe all relationships with or connections to information systems outside CSCU, or between internal systems but across system boundaries.

a. The information for each connection must include:

i. The name of the connected information system.

ii. The information system's organization and point of contact.

iii. The type of system.

iv. The authorization for the connection be it a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Interconnection Security Agreement (ISA) as appropriate for the organization and purpose.

v. The date of the signed connection agreement.

vi. The CSCU information security categorization.

vii. The name and title of the interconnected information system's authorizing official.

- Provides an overview of the security requirements for the system;
- Identifies any relevant overlays, if applicable;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

c.) The Campus ISSO must review and produce a security control assessment report, based on the authorized security control assessment plan, of the SSP and provide the security control assessment report, as part of the authorizing package, to the BOR CIO/Campus President/CIO;

d.) The BOR President/Campus President or BOR CIO/Campus CIO must review the SSP, security control assessment report, and any plan of action and milestones report prior to plan implementation;

- The only sections of an SSP permitted to be made available to users of the information system are the rules of behavior and remote access requirements, otherwise, the SSP is considered sensitive and is prohibited from being released to unauthorized personnel.

e.) The Information System Owner distributes copies of the system security plan and communicates and documents subsequent changes to the plan with the Campus ISSO;

f.) The Information System Owner and Campus Information System Security Officer reviews the security plan for the information system;

- At least annually or when a significant change occurs to the information system's operating environment or security requirements;
    a. A significant change includes a change in the points of contact, system architecture, system status, system interconnections, system scope, or C&A status.
- The document review history must be updated to reflect the date the review was performed.

g.) The Information System Owner updates and maintains the system security plan to address changes to the information system/environment of operation.

- Planned significant changes must be defined in advance and identified in the SSP as well as in the configuration management process. The SSP must be updated to factor in planned information system enhancements, to ensure that required security-related activities are planned for in advance.

- The SSP must be updated based on the results of the continuous monitoring process. The Campus ISSO must review and provide a new security control assessment report to the BOR CIO/Campus President/CIO to include updates or changes to the SSP.
- Updates or changes to the SSP must be reviewed and re-authorized by the CSCU CIO/Campus before implementation.

h.) The Information System Owner and Campus ISSO must create a plan of action and milestones (POAM) document to address:

- weaknesses identified during system implementation, control assessments, investigations, or when impacted by unforeseen significant events, such as a breach, a new threat, or previously unknown vulnerability;

i.) The Campus ISSO protects the security plan from unauthorized disclosure and modification.

2. Rules of Behavior [NIST 800-53r4 PL4]

2.1 For all information systems, the Information System Owner:

a.) Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

b.) Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

c.) Reviews and updates the rules of behavior annually or as needed; and

d.) Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

2.2 For all moderate and high risk information systems, the Information System Owner includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. [NIST 800-53r4 PL4 (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.