System and Services Acquisition (SA)

Purpose:

The following standards are established to support the policy statement 10.15 that "CSCU will: (i) allocate sufficient resources to adequately protect CSCU information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third party providers employ adequate security measures, through federal and Connecticut state law and contract, to protect information, applications, and/or services outsourced from the organization."

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. Allocation of Resources [NIST 800-53r4 SA2]

1.1 For all information systems the CSCU CIO/Campus CIO, determines information security requirements for the information system or information system service in mission/business process planning;

a.) Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

b.) Establishes a discrete line item for information security in organizational programming and budgeting documentation.

2. System Development Life Cycle [NIST 800-53r4 SA3]

2.1 For all information systems, the Information System Owner:

a.) Manages the information system using defined system development life cycle that include planning, system analysis and requirements, system design, development, integration and testing, implementation, and operations and maintenance phases that incorporates information security considerations;

b.) Defines and documents information security roles and responsibilities throughout the system development life cycle;

c.) Identifies individuals having information security roles and responsibilities; and

d.) Integrates the organizational information security risk management process into system development life cycle activities.

3. Acquisition Process [NIST 800-53r4 SA4]

3.1 For all information systems the Information System Owner in collaboration with the ISPO, includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, CSCU policies, regulations, standards, and organizational mission/business needs:

a.) Security functional requirements;

b.) Security strength requirements;

c.) Security assurance requirements;

d.) Security-related documentation requirements;

e.) Requirements for protecting security-related documentation;

f.) Description of the information system development environment and environment in which the system is intended to operate; and

g.) Acceptance criteria.

3.2 For all moderate and high risk information systems the Information System Owner, in collaboration with the ISPO, requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. [NIST 800-53r4 SA4 (1)]

3.3 For all moderate and high risk information systems the Information System Owner requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed at a level of detail needed to complete a System Security Plan that includes:

a.) security-relevant external system interfaces; and

b.) high-level design. [NIST 800-53r4 SA4 (2)]

3.4 For all moderate and high risk information systems the Information System Owner requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. [NIST 800-53r4 SA4 (9)]

3.5 For all information systems the Information System Owner employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. [NIST 800-53r4 SA4 (10)]

4. Information System Documentation [NIST 800-53r4 SA5]

4.1 For all information systems, the Information System Owner:

a.) Obtains administrator documentation for the information system, system component, or information system service that describes:

- Secure configuration, installation, and operation of the system, component, or service;
- Effective use and maintenance of security functions/mechanisms; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b.) Obtains user documentation for the information system, system component, or information system service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
- User responsibilities in maintaining the security of the system, component, or service;

c.) Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and notifies ISPO/Campus ISSO in response;

d.) Protects documentation as required, in accordance with the risk management strategy; and

e.) Distributes documentation to CSCU CIO/Campus CIO, ISPO/Campus ISSO.

5. Security Engineering Principles [NIST 800-53r4 SA8]

5.1 For all information systems, the Information System Owner applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

6. External Information System Services [NIST 800-53r4 SA9]

6.1 For all information systems, the Information System Owner:

a.) Requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal and state laws, CSCU policies, regulations, and standards;

b.) Employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

6.2 For all moderate and high risk information systems, the Information System Owner, requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

7. Developer Configuration Management [NIST 800-53r4 SA10]

7.1 For all moderate and high risk information systems, the Information System Owner, requires the developer of the information system, system component, or information system service to:

a.) Perform configuration management during system, component, or service design, development, implementation, and operation;

b.) Document, manage, and control the integrity of changes to items under configuration management;

c.) Implement only organization-approved changes to the system, component, or service;

d.) Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e.) Track security flaws and flaw resolution within the system, component, or service and report findings to ISPO and campus ISSO.

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.