System and Communication Protection (SC)

Purpose:

The following standards are established to support the policy statement that "CSCU will: (i) monitor, control, and protect CSCU communications (i.e., information transmitted or received by CSCU information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within CSCU 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. Application Partitioning [NIST 800-53r4 SC2] [NIST 800-171r1 3.13.3]

1.1 For all moderate and high risk information systems, the Information System Owner ensures the information system separates user functionality (including user interface services) from information system management functionality.

2. Information in Shared Resources [NIST 800-53r4 SC4]

2.1 For all moderate and high risk information systems, the Information System Owner ensures the information system prevents unauthorized and unintended information transfer via shared system resources.

3. Boundary Protection [NIST 800-53r4 SC7]

3.1 For all information systems, the Information System Owner:

a.) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b.) Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and c.) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

3.2 Ensures the information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). [NIST 800-53r4 SC7(5)]

3.3 Ensures the information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling). [NIST 800-53r4 SC7(7)]

4. Transmission Confidentiality and Integrity [NIST 800-53r4 SC8]

4.1 For all information systems, the Information System Owner ensures:

a.) The information system protects the confidentiality and integrity of transmitted information;

4.2 For moderate and high risk information systems, the Information System Owner ensures:

a.) The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information during transmission. [NIST 800-53r4 SC8(1)]

5. Network Disconnect [NIST 800-53r4 SC10]

5.1 For moderate and high risk information systems, the Information System Owner ensures the information system terminates the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

6. Cryptographic Key Establishment and Management [NIST 800-53r4 SC12]

6.1 For all information systems, the Information System Owner ensures cryptographic keys for required cryptography employed within the information system is in accordance with CSCU defined requirements for key generation, distribution, storage, access, and destruction.

7. Cryptographic Protection [NIST 800-53r4 SC13]

7.1 For moderate and high risk systems, the Information System Owner ensures the information system implements CSUS approved cryptography for the protection of data.

8. Collaborative Computing Devices [NIST 800-53r4 SC15]

8.1 For all information systems, the Information System Owner:

a.) Prohibits remote activation of collaborative computing devices; and

b.) Provides an explicit indication of use to users physically present at the devices.

9. Mobile Code [NIST 800-53r4 SC18]

9.1 For all information systems:

a.) The ISPO Defines acceptable and unacceptable mobile code and mobile code technologies;

b.) The ISPO Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c.) The Information System Owner Authorizes, monitors, and controls the use of acceptable mobile code within the information system.

10. Voice Over Internet Protocol [NIST 800-53r4 SC19]

10.1 For all information systems:

a.) the ISPO establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b.) The Information System Owner authorizes, monitors, and controls the use of VoIP within the information system.

11. Secure Name/Address Resolution Service (Authoritative Source) [NIST 800-53r4 SC20]

11.1 The information system:

a.) Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b.) Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

12. Secure Name/Address Resolution Service (Recursive or Caching Resolver) [NIST 800-53r4 SC21]

12.1 The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

13. Architecture and Provisioning for Name/Address Resolution Service [NIST 800-53r4 SC22]

13.1 The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

14. Session Authenticity [NIST 800-53r4 SC23]

14.1 For all information systems, the Information System owner ensures the information system protects the authenticity of communications sessions.

15. Protection of Information at Rest [NIST 800-53r4 SC28]

15.1 For moderate and high risk information systems, the Information System Owner ensures the information system protects the confidentiality and integrity of information at rest.

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.