Configuration Management (CM)

Purpose:

The following standards are established to support the policy statement 10.7 that "CSCU will: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational 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. Baseline Configuration [NIST 800-53r4 CM2]

1.1 For all information systems, the Information System Owner develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

a.) The baseline configuration must include documented, up-to-date specifications to which the information system is built and configured;

b.) The baseline configuration must document and provide information about the components of an information system including:

- Standard operating system/installed applications with current version numbers.
- Standard software load for workstations, servers, network components, and mobile devices and laptops.
- Up-to-date patch level information.
- Network topology.
- Logical placement of the component within the system and enterprise architecture.

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.700	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

- Technology platform.

c.) New baselines must be created as the information system changes over time as this includes maintaining the baseline configuration;

d.) The baseline configuration of the information system must be consistent with CSCU's enterprise architecture.

1.2 For moderate risk information systems, the Information System Owner must;

a.) Review and update the baseline configuration of the information system:

- Annually;
- When required due to changes in installed software and/or hardware;
- As an integral part of information system component installations and upgrades;
- When an increase in interconnection with other systems outside the authorization boundary or significant changes in the security requirements for the system. [NIST 800-53r4 CM2 (1)]

b.) Retain, as deemed necessary, older versions of baseline configurations to support rollback. [NIST 800-53r4 CM2 (3)]

1.3 For high risk information systems, the Information System Owner must:

a.) Employ automated mechanisms in order to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

b.) Enforce a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

c.) Manage a separate baseline configuration from the operational baseline configuration for development and test environments.

2. Configuration Change Control [NIST 800-53r4 CM3]

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

a.) Determines, in consultation with Data Owners, the types of changes to the information system that are configuration-controlled;

b.) Reviews proposed configuration-controlled changes to the information system and, in consultation with the Data Owners, approves or disapproves such changes with explicit consideration for security impact analyses;

c.) Documents configuration change decisions associated with the information system;

d.) Implements approved configuration-controlled changes to the information system;

e.) Retains records of configuration-controlled changes to the information system for two years;

f.) Audits and reviews activities associated with configuration-controlled changes to the information system; and

g.) Coordinates and provides oversight for configuration change control activities through the Change Action Board (CAB) that convenes weekly.

2.2 For moderate risk information systems, the Information System Owner tests, validates, and documents changes to the information system before implementing the changes on the operational system. [NIST 800-53r4 CM3 (2)]

2.3 For high risk information systems, the Information System Owner employs automated mechanisms to:

a.) Document proposed changes to the information system;

b.) Notify Data Owners and the CAB of proposed changes to the information system and request change approval;

c.) Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period];

d.) Prohibit changes to the information system until designated approvals are received;

e.) Document all changes to the information system; and

f.) Notify Data Owners and the CAB when approved changes to the information system are completed. [NIST 800-53r4 CM3 (1)]

3. Security Impact Analysis [NIST 800-53r4 CM4]

3.1 For all information systems, the Information System Owner analyzes changes to the information system to determine potential security impacts prior to change implementation.

3.2 For high risk information systems, the Information System Owner analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. [NIST 800-53r4 CM4 (1)]

4. Access Restrictions for Change [NIST 800-53r4 CM5]

4.1 For moderate risk information systems, the Information System Owner must:

a.) Define, document, approve, and enforce physical and logical access restrictions associated with changes (e.g., upgrades, modifications) to the information system.

- Individuals authorized to perform configuration changes must be documented in the CMP.
- Logical and physical access control lists that authorize qualified individuals to make changes to an information system or component must be created and maintained.
- Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

b.) Maintain access records to ensure that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system.

- All information system changes associated with access privileges for such changes must be reviewed.
- The ISPO/Campus Information System Security Officer shall review and verify access lists quarterly and shall document any variances that are found.

4.2 For high risk information systems, the Information System Owner must:

a.) Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. [NIST 800-53r4 CM5 (1)]

b.) Conduct reviews of information system changes semi-annually and when indications so warrant to determine whether unauthorized changes have occurred.

5. Least Functionality [NIST 800-53r4 CM7]

5.1 For all information systems, the Information System Owner:

a.) Configures the information system to provide only essential capabilities;

b.) Disables unused and unnecessary physical and logical ports and protocols on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.

c.) Maintains a list of the ports that are required to be left open with a statement of business necessity provided for each required port.

d.) Ensures the use of the following functions, ports, protocols, and/or services, at a minimum, must be specifically prohibited or restricted:

- Domain Name System (DNS)
    a. Port 53 / Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- File Transfer Protocol (FTP)
    a. Ports 20, 21 / TCP
- Hypertext Transfer Protocol (HTTP)
    a. Port 80 / TCP
- Internet Message Access Protocol (IMAP)
    a. Port 143 / TCP, UDP
- Internet Relay Chat (IRC)
    a. Port 194 / UDP
- Network Basic Input Output System (NetBIOS)
    a. Port 137 / TCP, UDP
- Post Office Protocol 3 (POP3)
    a. Port 110 / TCP
- Session Initiation Protocol (SIP)
    a. Port 5060 / TCP, UDP
- Simple Mail Transfer Protocol (SMTP)
    a. Port 25 / TCP
- Simple Network Management Protocol (SNMP)

a. Port 161 / TCP, UDP

- Structured Query Language (SQL)
  a. Port 118 / TCP, UDP
  b. Port 156 / TCP, UDP
- Telnet
  a. Port 23 / TCP

5.2 For moderate risk information systems, the Information System Owner:

a.) Reviews the information system annually to identify unnecessary and/or non-secure functions, ports, protocols, and services; and

b.) Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure. [NIST 800-53r4 CM7(1)]

c.) Ensures the information system prevents program execution in accordance with defined policies regarding software program usage and restrictions or rules authorizing the terms and conditions of software program usage. [NIST 800-53r4 CM7(2)]

d.) Identifies software programs not authorized to execute on the information system;

e.) Employs an allow-all, deny-by-exception policy (blacklist) to prohibit the execution of unauthorized software programs on the information system; and

f.) Reviews and updates the list of unauthorized software programs annually. [NIST 800-53r4 CM7(4)]

5.3 For high risk information systems, the Information System Owner:

a.) Employs a deny-all, permit-by-exception policy (whitelist) to allow the execution of authorized software programs on the information system; and

b.) Reviews and updates the list of authorized software programs annually. [NIST 800-53r4 CM7(5)]

6. Information System Component Inventory [NIST 800-53r4 CM8]

6.1 For all information systems, the Information System Owner:

a.) Develops and documents an inventory of information system components that:

- Accurately reflects the current information system;
- Includes all components within the authorization boundary of the information system;
- Is at the level of granularity deemed necessary for tracking and reporting; and
- Must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:
    a. Manufacturer.
    b. Type.
    c. Model.
    d. Serial number.
    e. Physical location.
    f. Software license information.
    g. Information system/component owner.
    h. Associated information system name.
    i. Software/firmware version information.
    j. Networked component/device machine name or network address.

b.) Reviews and updates the information system component inventory:

- Annually;
- Updated as an integral part of the component installations, removals, and information system updates. [NIST 800-53r4 CM8(1)]

c.) The inventory of information system components must be available for review and audit by designated CSCU officials.

6.2 For moderate risk information systems, the Information System Owner:

a.) Employs automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system quarterly; and

b.) Disables network access by such components; isolates the components; and notifies ISPO/Campus ISSO. [NIST 800-53r4 CM8(3)]

6.3 For high risk information systems, the Information System Owner employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. [NIST 800-53r4 CM8(2)]

7. Configuration Management Plan [NIST 800-53r4 CM9]

7.1 For moderate and high risk information systems, the Information System Owner develops, documents, and implements a configuration management plan for the information system that:

a.) Addresses roles, responsibilities, and configuration management processes and procedures;

b.) The CMP must define detailed processes and procedures for how configuration management is used to support development life cycle activities at the information system level.

- The CMP must define the Configuration Items (Cis) for the information system and when the CIs are placed under configuration management in the system development life cycle.
    a. The CMP must establish the means for identifying CIs throughout the system development life cycle and a process for managing the configuration of the CIs.

c.) The CMP must describe:

- How to move a change through the change management process.
- How configuration settings and configuration baselines are updated.
- How the information system component inventory is maintained.
- How development, test, and operational environments are controlled.
- How documents are developed, released, and updated.

d.) The configuration management approval process must include:

- Designation of key management stakeholders who are responsible for reviewing and approving proposed changes to the information system.
- Designation of security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

e.) Protects the configuration management plan from unauthorized disclosure and modification.

8. User-Installed Software [NIST 800-53r4 CM11]

8.1 For all information systems:

a.) ISPO must develop and recommend CSCU-defined policies and standards governing the installation of software by users;

b.) The Information System Owner enforces software installation policies and standards through procedural, automated, or combination of both methods.

c.) The Information System Owner monitors and reviews user compliance yearly.

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.