Access Control (AC)

Purpose:

The following standards are established to support the policy statement 10.4 that "CSCU will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise."

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. Account Management [NIST 800-53r4 AC2]

1.1 For all information systems, Information System Owners in consultation with Data Owners:

a.) Identifies and documents the types of information system accounts needed to support business functions;

b.) Assigns account managers for information system accounts;

c.) Establishes conditions for group and role membership;

- Accounts to be added to a privileged group or role must be approved by the CSCU CIO/Campus CIO.

d.) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

- Accounts to be added to a privileged group or role must be approved by the CSCU CIO/Campus CIO.

e.) Requires approvals by Data Owner for requests to create information system accounts;

f.) Establish a process for the creation, enabling, modification, disabling, and removal of information system accounts in accordance with:

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.400	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

- Signed approval from Information System Owners and Data Owners;
- Request must include the user name, job title, assigned role or group membership, user contact information, and intended use or business function.

g.) Monitors the use of information system accounts;

h.) Notifies account managers:

- When accounts are no longer required;
- When users are terminated or transferred; and
- When individual information system usage or need-to-know changes;

i.) Authorizes access to the information system based on:

- A valid access authorization;
- Intended system usage; and
- Other attributes as required by the organization or associated mission/business functions;

j.) Reviews accounts for compliance with account management requirements yearly; and

k.) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

2. Access Enforcement [NIST 800-53r4 AC3]

2.1 The Information System Owner ensures that:

a.) The information system enforces approved authorizations for logical access to information and system resources in accordance with the following:

- Access controls must be enabled between users (or process acting on behalf of user) and objects in the information systems. The following is the minimum standard for access controls:
- Access to the system must be provided using Role-Based Access Control (RBAC) policies.
- Access enforcement mechanisms must use access control lists including permissions and, in the case of network access, TCP/IPv4 addresses and ports.

3. Information Flow Enforcement [NIST 800-53r4 AC4]

3.1 The Information System Owner ensures that:

a.) The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems.

4. Separation of Duties [NIST 800-53r4 AC5]

4.1 ISPO guides the oversite of Separation of Duties by:

a.) Separating Data Owners, Information System Owners and Information System Administrators roles;

b.) Documenting separation of duties of individuals; and

c.) Defining information system access authorizations to support separation of duties.

5. Least Privilege [NIST 800-53r4 AC6]

5.1 For all information systems, the Information System Owner will ensure access adheres to the principle of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which provide the minimum necessary privileges to accomplish explicitly authorized tasks in accordance with assigned and authorized roles.

5.2 For Moderate and high risk information systems,

a.) CSCU CIO/Campus CIO explicitly authorizes privileged access to information systems through the documented and defined roles in the system security plan. [NIST 800-53r4 AC6(1)]

b.) The Information System Owner restricts privileged accounts on the information system to defined and documented roles approved through the system security plan. [NIST 800-53r4 AC6(5)]

6. Unsuccessful Logon Attempts [NIST 800-53r4 AC7]

6.1 For all information systems, the Information System Owner ensures that the information system:

a.) Enforces a limit of five consecutive invalid login attempts by a user during a fifteen-minute time period;

b.) Automatically locks the account until released by an administrator when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

7. System Use Notification [NIST 800-53r4 AC8]

7.1 For all information systems, the Information System Owner ensures that the information system:

a.) Displays to users a system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal and state laws, policies, regulations, standards, and guidance and states that:

- Users are accessing a CSCU information system;
- Information system usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
- Use of the information system indicates consent to monitoring and recording;

b.) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

c.) For publicly accessible systems:

- Displays system use information, Acceptable Use Policy statement, before granting further access;
- Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- Includes a description of the authorized uses of the system.

8. Session Lock [NIST 800-53r4 AC11]

8.1 For all information systems, the Information System Owner ensures that the information systems:

a.) Prevent further access to the system by initiating a session lock after thirty minutes of inactivity or upon receiving a request from a user; and

b.) Retain the session lock until the user reestablishes access using established identification and authentication procedures.

8.2 For moderate and high risk information systems, the information system must conceal, via the session lock, information previously visible on the display with a publicly viewable image. [NIST 800-53r4 AC11(1)]

9. Session Termination [NIST 800-53r4 AC12]

9.1 The Information System Owner ensures that the information system automatically terminates a user session after:

a.) An idle timeout; and

b.) User logout;

10. Remote Access [NIST 800-53r4 AC17]

10.1 For all information systems, the CSCU President/Campus President or CSCU CIO/Campus CIO in consultation with the ISPO:

a.) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b.) Authorize remote access to the information system prior to allowing such connections.

10.2 For all information systems, the Information System Owner:

a.) Ensures that the information system monitors and controls authorized remote access methods [NIST 800-53r4 AC17(1)];

b.) Ensures that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions [NIST 800-53r4 AC17(2)];and

c.) Ensures that the information system routes all remote accesses through authorized and managed network access control points [NIST 800-53r4 AC17(3)].

10.3 For all information systems, the Information System Owners in consultation with the Data Owners:

a.) Authorize the execution of privileged commands and access to security-relevant information via remote access only for documented and defined business needs; and

b.) Document the rationale for such access in the security plan for the information system. [NIST 800-53r4 AC-17(4)]

11. Wireless Access [NIST 800-53r4 AC18] [NIST 800-171r1 3.1.16]

11.1 For all information systems, the CSCU President/Campus President or CSCU CIO/Campus CIO in consultation with ISPO:

a.) Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

b.) Authorize wireless access to the information system prior to allowing such connections.

11.2 For all information systems, the Information System Owner ensures that the information system protects wireless access to the system using secure authentication and encryption of traffic. [NIST 800-53r4 AC18(1)]

12. Access Control for Mobile Devices [NIST 800-53r4 AC19]

12.1 For all information systems, the CSCU President/Campus President or CSCU CIO/Campus CIO in consultation with ISPO:

a.) Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

b.) Authorize the connection of mobile devices to organizational information systems.

12.2 For moderate and high risk information systems,

a.) The information system owner employs full-device encryption to protect the confidentiality and integrity of information on CSCU mobile devices used for business functions within the organization. [NIST 800-53r4 AC19(5)]

13. Use of External Information Systems [NIST 800-53r4 AC20]

13.1 For all information systems, CSCU CIO in collaboration with ISPO and SPAC, establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a.) Access the information system from external information systems; and

b.) Process, store, or transmit organization-controlled information using external information systems.

13.2 For moderate and high risk information systems;

a.) Information System Owners permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

- Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
- Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. This agreement must be kept with the system security plan. [NIST 800-53r4 AC20(1)]

b.) The Information System Owner ensures any information system portable storage devices must is prohibited for use by authorized individuals on external information systems. [NIST 800-53r4 AC20(2)]

14. Publically Accessible Content [NIST 800-53r4 AC22]

14.1 For all information systems, the CSCU Chancellor/Campus President or CSCU CIO/Campus CIO with guidance from ISPO/Campus ISSO:

a.) Designates individuals authorized to post information onto a publicly accessible information system;

b.) Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c.) Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

d.) Reviews the content on the publicly accessible information system for nonpublic information quarterly or upon request from ISPO/Campus ISSO and removes such information, if discovered.

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.