Identification and Authentication (IA)

Purpose:

The following standards are established to support the policy statement 10.9 that "CSCU will: (i) identify information system users, processes acting on behalf of users, or devices; and (ii) authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to 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. Identification and Authentication (Organizational Users) [NIST 800-53r4 IA2]

1.1 For all information systems:

a.) The Information System Owner ensures the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) before allowing access.

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

a.) Ensures the information system implements multifactor authentication for network access to privileged accounts. [NIST 800-53r4 IA2(1)]

b.) Ensures the information system implements multifactor authentication for network access to non-privileged accounts. [NIST 800-53r4 IA2(2)]

c.) Ensures the information system implements multifactor authentication for local access to privileged accounts. [NIST 800-53r4 IA2(3)] d.) Ensures the information system implements replay-resistant authentication mechanisms for network access to privileged accounts. [NIST 800-53r4 IA2(8)]

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

a.) Ensures the information system implements multifactor authentication for local access to non-privileged accounts. [NIST 800-53r4 IA2(4)]

b.) Ensures the information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts. [NIST 800-53r4 IA2(9)]

2. Device Identification and Authentication [NIST 800-53r4 IA3]

2.1 For moderate and high risk information systems, the information system owner ensures:

a.) Devices are uniquely identified and authenticated before establishing connections with the information system.

3. Identifier Management [NIST 800-53r4 IA4]

3.1 For all information systems the Information System Owner:

a.) Authorizes assignment of individual, group, role, or device identifiers;

b.) Selects and assigns information system identifiers that uniquely identifies an individual, group, role, or device;

- Assignment of individuals, group, role, or device identifiers shall ensure that no two users or devices have the same identifier.

c.) Ensure assigning the identifier to the intended individual, group, role, or device;

d.) Preventing reuse of identifiers for seven (7) years; and

e.) Disable the identifier with more than 365 days of non-use.

4. Authenticator Management [NIST 800-53r4 IA5]

4.1 For all information systems:

a.) The Information System Owner must verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

b.) Information System Owners ensure authenticators for individuals, groups, roles, or devices shall have sufficient strength of mechanism for their intended use.

c.) The Information System Owner must ensure the information system stores and transmits only cryptographically-protected passwords;

d.) The Information System Owner must establish and implement administrative procedures for initial authenticator distribution, lost/compromised, or damaged authenticators, and for revoking authenticators.

- If a user knows or suspects that their password has been compromised, they shall immediately:
    a. Notify their supervisor.
    b. Report a known or potential security breach to the ISPO.
    c. Request reset or change of their password, or if self-service password mechanisms are used, immediately change their own password.

e.) The Information System Owner ensures that default content of authenticators (i.e., passwords provided for initial entry to a system) must be changed before implementation of the information system or component.

- The information system owner shall confirm that software and/or hardware upgrades, updates, and patches do not reinstall default passwords.

f.) The Information System Owner must change or replace authenticators periodically.

- All newly assigned passwords shall be changed the first time a user logs into the information system.
- Passwords shall be set to automatically expire in 90 days or sooner.

g.) The Information System Owner must ensure the following minimum and maximum lifetime restrictions and re-use conditions are adhered to regarding authenticators:

- Passwords shall have a minimum lifetime of one (1) day and a maximum lifetime of 90 days.
- Password reuse for a specific account is prohibited for 10 generations.

a. Password history shall be set with a history of at least 10 passwords.

h.) The Information System Owner must protect authenticator content from unauthorized disclosure and modification;

i.) Information System Users shall take reasonable and specific measures to safeguard authenticators.

- Users shall maintain possession of their individual authenticators, not loan or share authenticators with others, and report lost or compromised authenticators immediately to their supervisor and the ISPO as a security event.

j.) The Information System Owner must ensure devices be configured to safeguard authenticators (e.g., certificates, passwords).; and

k.) The Information System Owner must ensure authenticators for shared group/role accounts be changed when membership to those accounts changes.

4.2 For all information systems the Information System Owner ensures the information system, for password-based authentication:

a.) Enforces minimum password complexity of:

- Passwords may not contain the user's account name, identifier value or display name;
- Must be a minimum of 8 characters in length
- Must be composed of at least one characters from each of the following four categories, as provided in the application or operating system schema:

  a. Uppercase letters (e.g., A, B, C, Y, Z, etc.)

  b. Lowercase letters (e.g., a, b, c, y, z, etc.)

  c. Special characters (e.g., ! @, #, $, %, ^, &, etc.)

  d. Numbers (e.g., 1, 2, 3, 4, 5, etc.)

b.) Enforces at least six (6) changed characters when new passwords are created.

c.) Allows the use of a temporary password for system logons with an immediate change to a permanent password. [NIST 800-53r4 IA5(1)]

5. Authenticator Feedback [NIST 800-53r4 IA6]

5.1 For all information systems the Information System Owner ensures the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

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.