Maintenance (MA)

Purpose:

The following standards are established to support the policy statement 10.10 that "CSCU will: (i) perform periodic and timely maintenance on CSCU information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance."

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. Controlled Maintenance [NIST 800-53r4 MA2]

1.1 For all information systems, the Information System Owner:

a.) Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b.) Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c.) Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

d.) Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

1.2 For all information systems, the CSCU CIO/Campus CIO must explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.

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

a.) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

b.) Documents and retains maintenance records for the information system that includes the following information:

- Date and time of maintenance.
- Name of individual(s) performing the maintenance.
- Name of escort, if applicable.
- Description of maintenance performed.
- List of equipment removed or replaced (including identification numbers, if applicable).

c.) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed. [NIST 800-53r4 MA2 (2)]

2. Maintenance Tools [NIST 800-53r4 MA3]

2.1 For all information systems, the Information System Owner:

a.) Approves, controls, and monitors information system maintenance tools; and

b.) Checks media containing diagnostic and test programs for malicious code before the media are used in the information system. [NIST 800-53r4 MA3(2)]

2.2 For high risk information systems, the Information System Owner prevents the unauthorized removal of maintenance equipment containing organizational information by:

a.) Verifying that there is no organizational information contained on the equipment;

b.) Sanitizing or destroying the equipment;

c.) Retaining the equipment within the facility; or

d.) Obtaining an exemption from the CSCU CIO/Campus CIO explicitly authorizing removal of the equipment from the facility. [NIST 800-53r4 MA3(3)]

3. Non-Local Maintenance [NIST 800-53r4 MA4] [NIST 800-171r1 3.7.5]

3.1 For all information systems, the Information System Owner:

a.) Approves and monitors nonlocal maintenance and diagnostic activities;

b.) Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c.) Employs strong multifactor authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

d.) Maintains records for nonlocal maintenance and diagnostic activities; and

e.) Terminates session and network connections when nonlocal maintenance is completed.

3.2 For all moderate and high risk information systems, the Information System Owner documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections. [NIST 800-53r4 MA4 (2)]

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

a.) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or

b.) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system. [NIST 800-53r4 MA4 (3)]

4. Maintenance Personnel [NIST 800-53r4 MA5]

4.1 For all information systems:

a.) The CSCU CIO/Campus CIO establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b.) The Information System Owner ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and

c.) The Information System Owner designates organization personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

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.