System and Information Integrity (SI)

Purpose:

The following standards are established to support the policy 10.17 that "CSCU will identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within CSCU information systems; and monitor information system security alerts and advisories and take appropriate actions in response."

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. Flaw Remediation [NIST 800-53r4 SI2]

1.1 For all information systems:

a.) The Information System Owner must identify, report, and correct information system flaws;

b.) The Information System Owner must test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c.) The Information System Owner must install security-relevant software and firmware updates in a timely manner in accordance with assessment of risk; (See 10.100 ISST-Risk Assessment (RA)):

- For information systems categorized as low (L)

    a. Flaws/Vulnerabilities identified with an overall risk score of high (H) must be remediated within thirty (30) days.

    b. Flaws/Vulnerabilities identified with an overall risk score of moderate (M) or low (L) must be remediated within ninety (90) days.

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.1700	Approved	2/6/2020	2/6/2020	June 6, 2019	2/7/2020	

- For information system categorized as moderate (M)
    a. Flaws/Vulnerabilities identified with an overall risk score of high (H) must be remediated within fourteen (14) days.
    b. Flaws/Vulnerabilities identified with and overall risk score of moderate (M) must be remediated within thirty (30) days.
    c. Flaws/Vulnerabilities identified with an overall risk score of low (L) must be remediated within sixty (60) days.
- For information systems categorized as high (H)
    a. Flaws/Vulnerabilities identified with an overall risk score of high (H) must be remediated within seven (7) days.
    b. Flaws/Vulnerabilities identified with an overall risk score of moderate (M) must be remediated within fourteen (14) days.
    c. Flaws/Vulnerabilities identified with an overall risk score of low (L) must be remediated within thirty (30) days.

d.) The Information System Owner incorporates flaw remediation into the organizational configuration management process.

1.2 For moderate and high risk information systems, the Information System Owner employs automated mechanisms to determine the state of information system components with regard to flaw remediation. [NIST 800-53r4 SI-2 (2)]

a.) For information systems categorized as moderate (M);

- Every 14 days.

b.) For information systems categorized as high (H);

- Every 7 days.

2. Malicious Code Protection [NIST 800-53r4 SI3]

2.1 For all information systems, the Information System Owner:

a.) Employs malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network;

b.) Updates malicious code protection mechanisms whenever new releases are available;

c.) Standard malicious code protection software deployed on all workstations and servers must be configured to adhere to the following:

- Servers must be scanned for malicious code on a continuous basis.
- Workstations must be automatically scanned for malicious code on a daily basis.
- Malicious code protection software must allow users to manually perform scans on their workstation and removable media.
- Malicious code protection software must be updated concurrently with releases of updates provided by the vendor of the software. Updates should be tested and/or approved according to CSCU requirements.

d.) Malicious code protection mechanisms must be used to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) that is:

- Transported by electronic mail, electronic mail attachments, web accesses, removable media (e.g., Universal Serial Bus [USB] devices, diskettes or compact disks), or other common means.
- Inserted through the exploitation of information system vulnerabilities.
- Encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file.

e.) Malicious code protection mechanisms (including signature definitions) must be updated whenever new releases are available.

- As applicable, the malicious code protection software must be supported under a vendor Service Level Agreement (SLA) or maintenance contract that provides frequent updates of malicious code signatures and profiles.

f.) Malicious code protection mechanisms must be configured to:

- Perform periodic scans of the information system daily and real-time scans of files from external sources as the files are downloaded, opened, or executed.
- Block and quarantine malicious code and send alert to an administrator in response to malicious code detection.

g.) The following elements must be addressed during vendor and product selection and when tuning the malicious code protection software:

- The receipt of false positives during malicious code detection and eradication.
- The resulting potential impact on the availability of the information.

h.) In situations where traditional malicious code protection mechanisms are not capable of detecting malicious code in software (e.g., logic bombs, back doors), the organization must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, vulnerability scanning, and monitoring practices to help ensure that software does not perform functions other than those intended.

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

a.) Ensures malicious code protection mechanisms are centrally managed.

- Central management must include server-based solutions, not client-based. [NIST 800-53r4 SI3 (1)]
    a. The server-based solution must automatically check for and push out updates.

b.) Ensures the information system automatically updates malicious code protection mechanisms (including signature definitions). [NIST 800-53r4 SI3 (2)]

c.) Ensures the information system is configured to prevent non-privileged users from circumventing malicious code protection capabilities.

3. Information System Monitoring [NIST 800-53r4 SI4]

3.1 For all information systems, the Information System Owner:

a.) Monitors the information system to detect:

- Attacks and indicators of potential attacks; and
- Unauthorized local, network, and remote connections;

b.) Identifies unauthorized use of the information system;

c.) Deploys monitoring devices:

- Strategically within the information system to collect organization-determined essential information; and
- At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d.) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e.) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, based on law enforcement information, threat intelligence information, or other credible sources of information;

f.) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g.) Provides information system monitoring information to ISPO/Campus ISSO as needed.

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

a.) Employs automated tools to support near real-time analysis of events. [NIST 800-53r4 SI4(2)]

b.) Ensures the information system monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions. [NIST 800-53r4 SI4(4)]

c.) Ensures the information system alerts incident response officials in accordance with incident response standards when indications of compromise or potential compromise occur. [NIST 800-53r4 SI4(5)]

4. Security Alerts, Advisories and Directives [NIST 800-53r4 SI5]

4.1 For all information systems, the Information System Owner:

a.) Receives information system security alerts, advisories, and directives from relevant information system vendors, software, hardware, and other CSCU approved sites on an ongoing basis;

b.) Generates internal security alerts, advisories, and directives as deemed necessary;

c.) The ISPO will disseminate security alerts, advisories, and directives to Campus ISSOs;

- Campus ISSOs will disseminate security alerts, advisories, and directives to Campus Information System Owners;
- Information System Owners will disseminate security alerts, advisories, and directives to Data Owners and Users of the Information System;

d.) The Information System Owners implements security directives in accordance with established time frames, or notifies the Campus ISSO of the degree of noncompliance.

- Campus ISSOs must report noncompliance to the ISPO.

4.2 For high risk information systems, the Information System Owner employs automated mechanisms to make security alert and advisory information available throughout the organization. [NIST 800-53r4 SI5 (1)]

5. Memory Protection [NIST 800-53r4 SI16]

5.1 For moderate and high risk information systems, the Information System Owner ensures the information system implements safeguards to protect its memory from unauthorized code execution.

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.