BR 20-011

CT BOARD OF REGENTS FOR HIGHER EDUCATION

RESOLUTION

concerning

INFORMATION TECHNOLOGY SECURITY STANDARDS TO PROTECT CONNECTICUT STATE COLLEGES & UNIVERSITIES (CSCU) INFORMATION ASSETS TO MEET FEDERAL AND STATE REQUIREMENTS E.G. GRAMM – LEACH – BLILEY ACT (GLBA) AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

February 6, 2020

WHEREAS, The Board of Regents for Higher Education (BOR), via adoption of BR #14-110, Adoption of Information Security Policy, directed the development of National Institute of Technology and Standards (NIST) as the foundational requirement for data security, amongst all 17 constituent units, and.

WHEREAS, With the development of these standards having been completed, it is now necessary to update the existing Information Security Policy (ITS 003) to more clearly define, at a programmatic level, the Board's expectations; and

WHEREAS, The approval of these standards will require resources, both internal and external to the CSCU to implement the procedures necessary to meet the standards; and

WHEREAS, The governance that has brought this resolution to the Board has been through the Information Technology Steering Committee twice, the IT Investment Review Board and the Council of Presidents over a period of 18 months after an extensive development period; and

WHEREAS, Once the campus procedures are developed, every student, employee, third party and faculty member will have a defined role and responsibility in the security of information assets of CSCU; and

WHEREAS, The BOR recognizes that a CSCU Information Security Program must be consistent across all constituent units, utilize a risk-based approach to the selection and application of technical, managerial, and administrative controls, and be based on National Institute of Standards and Technology (NIST) Standards and Risk Management framework.

NOW THEREFORE BE IT RESOLVED, Upon the recommendation of the Information Technology Steering Committee, the Board of Regents for Higher Education hereby adopts ITS 004 CSCU Information Security **Policy** and the CSCU Information Security Program of NIST **Standards** and be it further.

RESOLVED, CSCU will develop and fund the CSCU Information Security Program using a regional shared services model, to ensure a cost-effective and practical approach to security management; and be it further

RESOLVED This action rescinds Board Resolutions #13-080 and-#14-110.

A True Copy,

Erin A. Fitzgerald, Secretary
Board of Regents for Higher Education

ITEM

Information Security Policy
Completing the requirements outlined in the CT Board of Regents for Higher Education BR #14-110, Adoption of Information Security Policy, the CSCU Chief Information Officer (CIO) and Information Security Program Office have developed a CSCU Information Security Policy, a risk management framework, information security governance structure, roles and responsibilities, standards, processes, and procedures aligned with the National Institute of Standards and Technology (NIST) standards and frameworks. These items are collectively identified as the "CSCU Information Security Program." The CSCU Information Security Program is a comprehensive, system-wide program designed to meet the control requirements associated with state and federal laws such as GLBA, FERPA, and PCI as well as regulatory requirements such as Federal Acquisition Regulation that mandate how data can be collected, processed, stored, and transmitted and what capabilities CSCU must have in place.

The policy (inclusive of risk management framework and governance) and initial standards were reviewed and approved through the Information Technology Steering Committee over a course of 18 months and several reviews. Additionally, CSCU engaged a security expert to act as the Investment Review Board to provide additional feedback of the entire Security Program to the steering committee, which resulted in a second review process. Essentially, the Security Program passed through the IT Steering Committee twice and through the Council of Presidents, with the latter acting as an additional review board.

BACKGROUND

As noted above, the BOR directed the development of a comprehensive, system wide information security program. Since that directive, the CSCU's Information Security Program Office has worked within the IT Governance Structure to obtain a final draft version of this policy and standards. This process was a resources intense endeavor and took several years to complete the final draft documents. During the same time period, the CSCU security and infrastructure teams completed the design, procurement and deployment of the Protective Enclave to act as an interim strategy until the security standards are developed, funded and implemented. The Protective Enclave provides many of the control requirements outlined in the standards. In that process, the various teams determined that previously developed policies and resolutions will need to be rescinded and replaced by these comprehensive standards. To that effect, the IT Steering Committee noted that Resolution 13-080 was no longer applicable, since the standards addressed specific roles, responsibilities and requirements of all CSCU staff with regards to security. Additionally, the IT Steering Committee recommends the adoption of ITS 004 to replace ITS 003 (BR 14-110).

The ITS 004 will be the governing policy defining the CSCU Information Security Program, roles, and responsibilities in a risk based framework. The policy clearly defines the Board's expectations so the standards can be applied consistently, defines the compliance requirements and communicates the consequences for non-compliance. Finally, the proposed policy defines the strategic value of information security, not only to the CSCU, but also to third parties with a relationship with CSCU. Most importantly these recommended changes provide the CSCU President with a defined role in the security program execution.

To comply with the comprehensive CSCU Information Security Program, campuses will require additional funding and staffing to develop campus specific procedures. These procedures define how each campus will conduct business to meet the CSCU program standards and processes. To control costs, the leadership teams are looking to a hybrid model to fund and operate this critical program. This model includes partnerships with vendors and the development and regionalization of a shared services structure to implement and manage the security program. Security staff will work under a shared services model regionally, reporting to the CSCU CIO to meet program requirements. CSCU institutions must develop campus information security programs and procedures consistent with the CSCU Information security programs that will ensure the availability, integrity and confidentiality of CSCU information systems assets.

Links to the proposed policy and program standards are below:

- DRAFT CSCU Information Security **Policy** (ITS 004)
- DRAFT CSCU Information Security **Program Standards**

RECOMMENDATION

That the Board of Regents for Higher Education, on the recommendation of the IT Steering Committee, adopts the proposed resolution concerning the CSCU Information Security Program (ITS 004) and adoption of Policy the Information Security Program Standards.

01/16/2020 – JRT/CSCU CIO
02/06/2020 – Board of Regents

w:\presidents office\board meetings\2020\2020-02-06\it\br sr it security policy and program standards.docx

CSCU Information Security Policy

Introduction

The use of technology is an integral part of the core mission objective of the Connecticut State Colleges and Universities (CSCU), to provide quality, affordable education in transformative learning environments for students and facilitate an ever increasing number of individuals to achieve their personal and career goals. Technology is ubiquitous within CSCU mission supporting business processes including interaction with students, faculty, staff, businesses, and state and federal agencies.

Technology also presents risks to CSCU's mission, from state and federal laws and regulatory compliance, data privacy and protection, availability of critical systems and infrastructure, to health and human safety.

To identify and manage these risks, a comprehensive, system-wide information security program must be developed, implemented, maintained, and continuously monitored and improved.

1.0 Purpose

1.1 This Security Policy consists of a set of decisions endorsed by the Board of Regents (BOR) about how CSCU will address protection of digital information and electronic information systems, required under state and federal law. These decisions are documented and communicated by the BOR to the constituent units. They detail the intentions and commitments of the BOR and the obligations for all individuals regarding compliance with this Security Policy.

This Security Policy serves several purposes, it:

a) Clearly defines management's expectations, so that requirements can be applied consistently.

b) Represents a risk framework that provides direction to CSCU, so that resources are allocated efficiently.

c) Acts as a measure against which compliance requirements can be validated.

d) Communicates the consequences for non-compliance.

e) Assigns responsibilities and highlights the strategic value of information security throughout the organization, and to relevant third parties.

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	BOR Resolution
IT-004	Approved by BOR	2/6/2020	2/6/2020	2/6/2020	2/6/2020	BR #20-011

2.0 Policy Authority

2.1 This policy is issued by the Board of Regents for Higher Education for the Connecticut State Colleges & Universities.

3.0 Scope

3.1 This Policy shall apply to the following:

a) All digital and electronic information assets owned by, or operated on behalf of, any CSCU campus or constituent unit.

b) All users employed by CSCU, its constituent units, contractors, vendors or any other person with access to CSCU's digital and electronic information assets.

c) All categories of information in which the information asset is electronically stored, processed, or transmitted.

d) Information technology facilities, applications, hardware systems, and network resources owned, or operated on behalf of, any CSCU campus or institutional unit. This includes third party service providers' systems that access, process or store CSCU's protected information.

3.2 Auxiliary organizations, external businesses and organizations that use CSCU information assets must operate those assets in conformity with this Policy and the CSCU Information Security Program.

3.3 CSCU retains ownership or stewardship of information assets owned (or managed) by CSCU. CSCU reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity and ensure continued delivery of services to users. This can include, but is not limited to:

a) monitoring communications across network services;

b) monitoring actions on information systems;

c) checking information systems attached to the CSCU network for security vulnerabilities;

d) disconnecting information systems that have become a security hazard; or

e) Restricting data to/from information systems and across network resources.

3.4 These activities are intended to protect the confidentiality, integrity and availability of information and are not intended to restrict, monitor or utilize the content of legitimate academic and organizational communications.

4.0 CSCU Information Security Organization and Governance

4.1 **Board of Regents (BOR)**, is responsible for oversight of all information security across CSCU. The BOR enacts system-wide information security policy and sets organizational risk tolerance by review and approval of annual information security reports and recommendations.

4.2 The **CSCU President** is responsible to enforce BOR policy across CSCU and to hold system office and campus senior leadership accountable for compliance with the CSCU Information Security Program requirements; authorizes and assumes responsibility for operating an information system at an acceptable level of risk to the system and enterprise operations (including mission, functions, image, or reputation).

4.3 The **CSCU Chief Information Officer (CIO)** must appoint a Chief Information Security Officer (CISO) and establish the CSCU Information Security Program Office to develop and manage a system wide information security program. The CSCU CIO must oversee the CSCU Information Security Program and report and provide recommendations to the BOR and CSCU President annually; acts on behalf of the CSCU President to authorize and assume responsibility for operating an information system at an acceptable level of risk to system office and enterprise operations (including mission, functions, image, or reputation), system office and enterprise assets, or individuals; and reviews and approves CSCU information security program standards.

4.4 The **Chief Information Security Officer (CISO)** is responsible for recommending information security governance and policy implementation by the BOR; develops, manages, publishes, implements, and maintains system-wide information security standards, processes, and procedures; assess information security controls and program implementation across the system; monitors and reports on system-wide security program compliance and performance metrics; and provide guidance and recommendations to IT and other functional areas of the organization.

4.5 The **Information Security Program Office (ISPO)**, under the direction of the CISO, supports the functions of the CISO in the development, management, and operation of the CSCU Information Security Program.

4.6 The **Security Program Advisory Committee (SPAC)** provides recommendations, guidance, and advice to the CISO for consideration and

inclusion into information security policy, standards, process, and procedures that reflect regulatory and legal requirements concerning organizational data and its use. The members of this committee will be system wide stakeholders that include, but not limited to, representatives from the various business units such as Human Resources, Facilities, Finance, Legal, and Academic Affairs. This committee is chaired by the CISO.

4.7 Each **Campus President/CEO** is responsible for oversight of all information and information system security for their campus; ensures and enforces campus compliance with the BOR policies and CSCU Information Security Program requirements; authorizes and assumes responsibility for operating an information system at an acceptable level of risk to campus operations (including mission, functions, image, or reputation), campus assets, or individuals. Reviews and approves campus information security policy.

4.8 The **CCC/CSU CIOs** must oversee the campus Information Security Program and report and provide recommendations to the campus President/CEO, CSCU CIO, and the CISO annually; reviews and approves campus information security program standards, processes, and procedures.

4.9 The **Campus Information System Security Officer (ISSO)** is a member of the Information Security Program Office and is responsible for coordinating the development of, and maintaining, campus specific information security standards, processes, and procedures; assists in assessing campus information security controls and program implementation compliance; monitors and reports security program performance metrics to the CISO and campus CIO; and provide security guidance and recommendations to campus leadership.

4.10 The **Data Owner** is a CSCU senior leader with statutory, management, or operational authority for a specified business area and has the responsibility for establishing the policies and procedures governing data access, generation, collection, processing, dissemination, and disposal within their respective business areas.

4.11 The **Information System Owner (ISO)** is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The Information System Owner is responsible for ensuring compliance with information security requirements.

5.0 Information Security Program Principles

5.1 All CSCU faculty, staff, students, guests, and contracted third party vendors have an obligation to protect CSCU information assets in accordance with this policy and its supplemental Standards, Processes, and Procedures, which take into consideration the organizations mission, as well as the level of sensitivity and criticality of the information. CSCU promotes, supports and adopts an organizational culture that elevates the importance of its overall information security posture by implementation of the following principles:

a) Shared Responsibilities: All members of the CSCU community have individual and shared responsibilities to protect the organizations information assets and comply with CSCU policies and applicable federal and state laws and regulations.

b) Information Centric: Required security controls are identified by the data classification impact level of the data stored, processed or transmitted by an information system. Systems with information classified as "High" will have much more restrictive controls, while the organization will tolerate more risk with information classified as "Moderate" or "Low."

c) Location Independence: Regardless of where CSCU information resides, the same standards will apply.

d) Appropriate Use: Faculty, staff, students, guests, and contracted third party vendors will act in accordance with the principles included in the Acceptable Use Policy.

e) Risk Management and Acceptance: The CISO, through the Information Security Program Office, will establish, implement, and maintain an enterprise wide information security risk management framework based upon a NIST defined System Security Plan development, review and approval cycle.

f) Standards-based: CSCU will leverage nationally recognized security standards, including, but not limited to NIST guidelines in compliance with applicable state and federal laws and regulations.

g) Continuous Monitoring: CSCU will monitor, on an ongoing basis, the security technologies and controls that support this policy, compliance with applicable state and federal requirements, and changes to the CSCU information systems and technology environment.

6.0 Campus Information Security Programs

6.1 Each campus must develop, implement, document, and report on a campus' information security program in accordance with this policy and in compliance with CSCU Information Security Program requirements.

6.2 Each campus is responsible for the development, implementation, and maintenance of campus specific procedures, in compliance with CSCU Information security program requirements.

6.3 Campus programs are required to implement a governance and risk management program incorporating the fundamental principles embodied in the System Security Plan approval cycle notably; 1) Data Classification 2) Control Selection 3) Control Analysis and Metrics 4) Risk Assessment, and 5) Operational Approval.

7.0 Risk Management Framework

7.1 CSCU adopts a risk-based approach to the management of information and information system security through the implementation of the CSCU System Security Plan approval cycle in accordance with the NIST Risk Management Framework methodology. This framework implementation is paramount to effective information security programs.

8.0 Information and Information System Categorization

8.1 CSCU must establish and assign security categories for both information and information systems. The security categories will be based on the potential impact on CSCU should certain events occur which jeopardize the information and information systems required by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

9.0 Information Security Document Types and Order of Precedence

9.1 CSCU Information Security Policy consists of high-level, mandatory statements that provide direction as to what must be done across the CSCU system. These policies are enacted by the BOR and may not be superseded by CSCU Information Security Standards.

9.2 CSCU Information Security Standards contain lower-level mandatory statements that also address what must be done. Standards at this level are technology-independent and provide the minimum requirements that directly support, and are an extension of, CSCU Information Security Policy statements. These standards are developed by the CISO and approved by the CSCU CIO and may not be superseded by CSCU Information Security Processes.

9.3 CSCU Information Security Processes contain high-level, mandatory steps and actions that provide direction as to how a function must be done across the CSCU system; these processes are developed by the ISPO and approved by the CISO in accordance with CSCU information security standards and may not be superseded by CSCU Information Security Procedures.

9.4 CSCU Information Security Procedures contain lower-level mandatory steps and actions that provide direction as to how a function must be done across the CSCU system; these procedures are developed by the ISPO and approved by the CISO in accordance with CSCU information security standards and processes.

10.0 CSCU Information Security Program Provisions

10.1 Risk Assessments: CSCU must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

10.2 Awareness and Training: CSCU must (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of CSCU information systems; and (ii) ensure that CSCU personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

10.3 Incident Response: CSCU must (i) establish an operational incident handling capability for CSCU information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate CSCU officials and/or authorities.

10.4 Access Control: CSCU must 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.

10.5 Audit and Accountability: CSCU must (i) create, protect, and retain system audit records to the extent needed to enable the effective monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

10.6 Security Assessment: CSCU must (i) periodically assess the security controls in information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in information systems; (iii) authorize the operation of information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

10.7 Configuration Management: CSCU must (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.

10.8 Contingency Planning: CSCU must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for CSCU information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

10.9 Identification and Authentication: CSCU must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to CSCU information systems.

10.10 Maintenance: CSCU must (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.

10.11 Media Protection: CSCU must (i) protect digital information system media, both physical and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

10.12 Physical Protection: CSCU must (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

10.13 Security Planning: CSCU must develop, document, periodically update, and implement security plans for CSCU information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

10.14 Personnel Security: CSCU must (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that CSCU information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with CSCU security policies and procedures.

10.15 System and Services Acquisition: CSCU must (i) allocate sufficient resources to adequately protect CSCU information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third party providers employ adequate security measures, through federal and Connecticut state law and contract, to protect information, applications, and/or services outsourced from the organization.

10.16 System and Communications Protection: CSCU must (i) monitor, control, and protect CSCU communications (i.e., information transmitted or received by CSCU information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within CSCU information systems.

10.17 System and Information Integrity: CSCU must (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within CSCU information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Policy Violations

Any CSCU campus or constituent unit found to operate in violation of this Policy and supplemental CSCU Information Security Standards, Processes, and Procedures may be held accountable for remediation costs associated with a resulting information security incident or other regulatory non-compliance penalties, including but not limited to financial penalties, legal fees, and other costs.

Faculty, staff, or students who violate this policy and supplemental CSCU Information Security Standards, Processes, and Procedures may be subject to disciplinary action commensurate with HR or other appropriate administrative policies.

Definitions

CSCU	Connecticut's system of Connecticut State Colleges and Universities (CSCU) comprises four public universities, twelve community colleges, and one online state college. The system is governed by the Board of Regents for Higher Education.
Campus	For the purposes of information security governance, a campus is an individual institution, location, or regional group within the CSCU system that is administered by a President as chief executive.
Information System Asset	Any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.
Information System	A discrete set of electronic and digital information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

References

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.

FIPS-199 (Standards for Security Categorization of Federal Information and Information Systems, Feb, 2004.)

The Gramm - Leach Bliley Act (GLBA)

Policies superseded by this policy

- IT-003, Information Security Policy, March 2015.
- CT Board of Regents for Higher Education Resolution; Concerning the Design, Implementation Operational Management and Assurance/Compliance of the Information Security Program for the Board of Regents of Higher Education, October 17, 2013.
- For CSU this policy supersedes the CSU Information Security Standards.
- For CCC this policy supersedes 1.1 IT Policy Common Provisions.

CSCU INFORMATION SECURITY PROGRAM STANDARDS

APPROVED BY BOR ON FEBRUARY 6, 2020
BOARD RESOLUTION BR #20-011
EFFECTIVE FEBRUARY 6, 2020

CSCU

Connecticut State Colleges & Universities

February 6th, 2020

CSCU INFORMATION SECURITY PROGRAM OFFICE

CSCU

Risk Assessment (RA)

Purpose:

The following standards are established to support policy statement 10.1 that "CSCU will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information."

Scope:

1. All 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. Security Categorization [NIST 800-53r4 RA2]

For All Information Systems

1.1 The Data Owner in coordination with the Information System Owner, categorizes information and the information system in accordance with the "***Information System and Data Categorization Process***";

1.2 The Information System Owner documents the security categorization results (including supporting rationale) in the system security plan for the information system; and

1.3 The ISSO reviews and approves the security categorization decision.

2. Risk Assessment [NIST 800-53r4 RA3]

For All Information Systems

2.1 The ISSO conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

a.) Prior to information system implementation and with completed system security plan;

b.) Prior to significant changes to authorized information systems;

c.) Upon discovery of new vulnerabilities through incident response, or otherwise;

d.) At the request of Authorizing Officials, or Authorizing Official Designees, for system security plan authorization purposes;

e.) ISPO security control assessments;

f.) As needed based on CSCU CIO or CISO request.

2.2 The ISSO documents risk assessment results in the information system security plan, risk assessment report;

2.3 Authorizing Official, or Designee, review risk assessment report results;

a.) Prior to authorizing use of information system; and

b.) Prior to authorizing significant changes to already authorized information systems;

2.4 The ISSO disseminates risk assessment results to the Information System Owner, Data Owner(s), and Authorizing Officials, or their Designees, for the Information System; and

2.5 The ISSO updates the risk assessment reports biennially or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

3. Vulnerability Scanning [NIST 800-53r4 RA5]

For All Information Systems

3.1 The Information System Owner ensures scans for vulnerabilities in the information system and hosted applications are performed;

a.) When new vulnerabilities potentially affecting the system/applications are identified and reported; and

b.) For information systems categorized as low (L);

- Every 30 days;

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

- Every 14 days;

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

- Every 7 days;

3.2 The Information System Owner employs vulnerability scanning tools and techniques that must;

a.) Support SCAP version 1.2 or greater compliancy;

b.) Facilitate interoperability among tools, including;

- Asset\Inventory Management Systems;
- Security Event Management Systems;
- Incident Response Procedures;
- Patch and Configuration Management Systems; and
- Electronic Messaging and Notification systems;

c.) Automate components of vulnerability management, including;

- Updating the scanning tools vulnerability repository;
- Identify and document all platforms, and software on the information system;
- Create a vulnerability remediation schedule by prioritizing vulnerabilities based on assessed overall risk;
- Track and document remediation plans and status;
- Report results of the vulnerability management process to the Information System Owner and ISPO.

d.) Analyze identified vulnerabilities based on;

- The impact of the vulnerability on the information system;
    a. CVSS Base score: 0.0-3.9 – L
    b. CVSS Base score: 4.0-6.9 – M
    c. CVSS Base score: 7.0-10.0 - H
- Threat intelligence;
    a. Reliable, widely available exploit code is available and actively in use or no exploit code is required to exploit the vulnerability - H
    b. Functional exploit code exists, but is not always reliable and is not widely available - H
    c. Limited function proof of concept code is available but would require substantial modification for use by an attacker - H

d. A theoretical exploit exists, but exploit code is not available - M

e. Attempts to exploit the vulnerability are seen in continuous monitoring – H

f. Attempts to exploit the vulnerability are not seen in continuous monitoring – M

g. Attacks are currently reported by other organizations – H

h. Attacks are not currently reported by other organizations - M

- Exposure;

a. No compensating controls are available to reduce the likelihood of the successful exploit of a vulnerability - H

b. Compensating controls partially reduce the likelihood of the successful exploit of a vulnerability (e.g. by increasing the difficulty of successfully exploiting the vulnerability) - M

c. Comprehensive compensating controls provide close to the same effect as remediating the vulnerability - L

e.) Assign overall risk score for each identified vulnerability using;

- Impact x (Threat Intelligence x Exposure) = Overall Risk Score.

f.) Enumerate the information system platforms, software flaws, and improper configurations;

- Enumerate information system platforms using the Common Platform Enumeration (CPE);
- Enumerate information system software flaws using the Common Vulnerabilities and Exposures (CVE);
- Enumerate improper configurations based on the Common Configuration Enumeration (CCE)

g.) Formatting checklists and test procedures;

h.) Capability to readily, and automatically, update the information system vulnerabilities to be scanned: [NIST 800-53r4 RA5 (1)]

- Daily;
- Prior to a new scan;

- When new vulnerabilities are identified and reported.

i.) Capable of privileged access authorization vulnerability scanning activities.

3.3 The Information System Owner reviews vulnerability scan reports and approves and documents remediation plans;

3.4 The Information System Owner approves and documents roles, and individuals assigned to those roles, allowed to run privileged access authorization scanning activities;

3.5 The Information System Owner ensures legitimate vulnerabilities are prioritized and remediated in a timely manner in accordance with assessment of risk;

a.) For information systems categorized as low (L)

- Vulnerabilities identified with an overall risk score of high (H) must be remediated within thirty (30) days.
- Vulnerabilities identified with an overall risk score of moderate (M) or low (L) must be remediated within ninety (90) days.

b.) For information system categorized as moderate (M)

- Vulnerabilities identified with an overall risk score of high (H) must be remediated within fourteen (14) days.
- Vulnerabilities identified with and overall risk score of moderate (M) must be remediated within thirty (30) days.
- Vulnerabilities identified with an overall risk score of low (L) must be remediated within sixty (60) days.

c.) For information systems categorized as high (H)

- Vulnerabilities identified with an overall risk score of high (H) must be remediated within seven (7) days.
- Vulnerabilities identified with an overall risk score of moderate (M) must be remediated within fourteen (14) days.
- Vulnerabilities identified with an overall risk score of low (L) must be remediated within thirty (30) days.

3.6 The Information System Owner must share information obtained from the vulnerability scanning process and security control assessments with the ISPO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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.

CSCU

Awareness and Training (AT)

Purpose:

The following standards are established to support the policy statement 10.2 that "CSCU will: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of CSCU information systems; and (ii) ensure that CSCU personnel are adequately trained to carry out their assigned information security-related duties and responsibilities."

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. Security Awareness [NIST 800-53R4 AT2]

1.1 ISPO provides basic security awareness training to all information system users (including managers, senior executives, and contractors):

a.) As part of initial training for new users;

b.) When required by information system changes; and

c.) Annually

1.2 For moderate and high risk information systems, ISPO must include security awareness on recognizing and reporting potential indicators of insider threat. [NIST 800-53R4 AT-2(2)]

2. Role-Based Security Training [NIST 800-53R4 AT3]

2.1 For all information systems, the Information System Owner and Data Owner must provide role-based security training to personnel with assigned roles and responsibilities:

a.) As part of initial training for new users within three months of hire or access change;

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.200	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

b.) When required by information system changes; and

c.) Biennial thereafter.

2.2 Additionally, for moderate and high risk information systems, the Information System Owner and Data Owners must provide role based security training to personnel with assigned roles and responsibilities:

a.) As part of initial training for new users within 2 weeks of hire or access change;

b.) Before authorizing access to the information system or performing assigned duties;

c.) When required by information system changes; and

d.) Biennial thereafter.

2.3 For all information systems, the Information System Owner and Data Owners must include, as part of all role-based training:

a.) Reporting incidents;

b.) Information system specific security procedures and responsibilities; and

c.) Information system rules of behavior and usage.

3. Security Training Records [NIST 800-53 AT-4]

3.1 ISPO will document and monitor basic security awareness training activities. And retain those records for three years as defined in the CT Records retention statute (S2-340 Training Records, Employee).

3.2 Information System Owners will document and monitor role-based information system security training. And retain those records for three years as defined in the CT Records retention statute (S2-340 Training Records, Employee).

3.3 Data Owners will documents and retains security training records for the users of its data for three years as defined in the CT Records retention statute (S2-340 Training Records, Employee).

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.

General Records Retention Schedules for State Agencies, S2: Personnel Records, Connecticut State Library, Office of the Public Records Administrator, Item S2-340, January 2010.

CSCU

Incident Response (IR)

Purpose:

The following standards are established to support the policy statement 10.3 that "CSCU will: (i) establish an operational incident handling capability for CSCU information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate CSCU officials and/or authorities."

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. Incident Response Training [NIST 800-53r4 IR2]

1.1 For all CSCU information systems, ISPO provides incident response training to CSCU employees, business partners and vendors consistent with their incident response roles and responsibilities.

a.) In coordination with Data Owners, training of individuals assuming an incident response role or responsibility, will occur within 4 weeks of that responsibility being assigned;

b.) When required by information system changes; and

c.) Annually thereafter.

1.2 For moderate and high risk information systems, ISPO:

a.) Incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. [NIST 800-53r4 IR2 (1)]

b.) Employ automated mechanisms to provide a more thorough and realistic incident response training environment. [NIST 800-53r4 IR2 (2)]

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.300	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

2. Incident Response Testing [NIST 800-53r4 IR3]

2.1 For all CSCU information systems, ISPO tests the incident response capability for the information system annually using checklists, simulations and tabletop exercises to determine the incident response effectiveness and documents the results.

2.2 For moderate and high risk information systems, ISPO coordinates incident response testing with organizational elements responsible for related plans. [NIST 800-53r4 IR3 (2)]

3. Incident Handling [NIST 800-53r4 IR4]

3.1 For all information systems the CSCU CIO along with ISPO, Campus Information System Security Officers, Data Owners, and Information System Owners:

a.) Implements an incident handling capability for security incidents that includes identification, containment and assessment, eradication and recovery, notification and follow-up and conclusion;

b.) Coordinates incident handling activities with contingency planning activities; and

c.) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

3.2 For moderate and high risk information systems the CSCU CIO along with ISPO, Campus Information System Security Officers, Data Owners, and Information System Owners:

a.) Employs automated mechanisms to support the incident handling process. [NIST 800-53r4 IR4 (1)]

b.) Correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. [NIST 800-53r4 IR4 (4)]

4. Incident Monitoring [NIST 800-53r4 IR5]

4.1 For all information systems ISPO tracks and documents information system security incidents.

4.2 For moderate and high risk information systems, ISPO employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. [NIST 800-53r4 IR5 (1)]

5. Incident Reporting [NIST 800-53r4 IR6]

5.1 For all information systems, CSCU:

a.) Requires CSCU personnel, including but not limited to, Data Owners, Information System Owners, Information System Administrators and Information Users, to report suspected security incidents to the organizational incident response, CSCU CERT, immediately; and

b.) Requires security incident information to be reported to ServiceDesk@ct.edu

5.2 For moderate and high risk information systems, ISPO employs automated mechanisms to assist in the reporting of security incidents. [NIST 800-53r4 IR6 (1)]

6. Incident Response Assistance [NIST 800-53r4 IR7]

6.1 For all information systems, ISPO coordinates an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

6.2 For moderate and high risk information systems, the organization employs automated mechanisms to increase the availability of incident response-related information and support. [NIST 800-53r4 IR7 (1)]

7. Incident Response Plan [NIST 800-53r4 IR8]

7.1 For all information systems ISPO:

a.) Develops an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;

- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization;
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by CSCU CIO.

b.) Distributes copies of the incident response plan to CSCU President/Chancellor, CSCU CIO, Campus Presidents, Campus Information System Security Officers, Data Owners, and Information System Owners.

c.) Reviews the incident response plan annually.

d.) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e.) Communicates incident response plan changes to CSCU President, CSCU CIO, Campus Presidents, Campus Information System Security Officers, Data Owners, and Information System Owners, and

f.) Protects the incident response plan from unauthorized disclosure and modification.

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.

CSCU

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.

CSCU

Audit and Accountability (AU)

Purpose:

The following standards are established to support the policy statement 10.5 that "CSCU will: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted 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. Auditable Events [NIST 800-53 AU2]

1.1 All Information Systems must produce audit records for the following events:

a.) System startup and shutdown

b.) User logon and logoff

c.) Modifications of privileges and access controls

d.) Account creation, modification, or deletion

e.) Password changes

1.2 Moderate and High Risk Information Systems must additionally produce audit records for the following events:

a.) System alerts and error messages

b.) System administration activities including configuration changes

c.) Starting and stopping of processes and services

d.) Installation, modification, and removal of software

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.500	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

e.) Access to and modification of high risk (DCL2, DCL3) information and data.

1.3 Information systems that primarily provide information security control functions and capabilities must additionally produce the audit records associated with those functions (e.g. firewall policy logs, intrusion detection logs, access control logs, anti-virus logs, etc.)

1.4 The Information Security Program Office (ISPO) must review and update the selected audited events biannually, or as required. [NIST 800-53 AU-2(3)]

2. Content of Audit Records [NIST 800-53 AU3]

2.1 Audit log records must include at least the following elements:

a.) Identifier of the system that generated the event

b.) Date and time when the event occurred

c.) The action or type of event and any relevant data

d.) Success or failure of the action

e.) Subject identity (e.g., user, device, process context)

f.) Remote address, if the event occurs over a network connection

3. Audit Storage Capacity [NIST 800-53 AU-4]

3.1 The audit storage capacity must be configured to allow for sufficient space to record all necessary auditable actions identified in section 1, Auditable Events, and section 9, Audit Record Retention, to prevent the capacity from being exceeded.

4. Response to Audit Processing Failures [NIST 800-53 AU-5]

4.1 All Information Systems must be configured to:

a.) Alert designated officials in the event of an audit failure or when audit storage capacity is 80%, and again at 90% utilization automatically. [NIST 800-53 AU-5(1)]

b.) Distribute alerts by a mechanism that allows system administrators to receive it at any time including after normal working hours (e.g., email, text message).

c.) Once the maximum storage capacity for audit logs is reached, the information system must overwrite the oldest audit records.

4.2 Moderate and High Risk Information Systems must additionally:

a.) When devices cannot generate logs or the maximum storage capacity has been reached, the information system must be configured to send an alert to system administrators within two minutes. Procedures must reflect escalation of priority resolution actions after twenty-four hours. [NIST 800-53 AU-5(2)]

5. Audit Review, Analysis, and Reporting [NIST 800-53 AU-6]

5.1 For all information systems the Information System Owner must:

a.) Review and analyze audit logs and records weekly for indications of inappropriate or unusual activity; and report findings in accordance with CSCU Incident Handling Procedures.

5.2 Moderate and High Risk Information Systems must additionally:

a.) Review and analyze audit logs and records daily for indications of inappropriate or unusual activity; and reports findings in accordance with CSCU Incident Handling Procedures.

b.) Employ automated tools that can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation, analysis, reporting, and alerting to support organizational processes for investigation and response to suspicious activities. [NIST 800-53 AU-6(1)]

c.) Analyze and correlate audit records across different repositories to gain CSCU-wide situational awareness. [NIST 800-53 AU-6(3)]

5.3 The level of audit review, analysis, and reporting may be adjusted if there is a change in risk to CSCU operations, assets, or personnel. Adjustments must be based upon advisories, warnings, legal, or regulatory notification such as, but not restricted to: [NIST 800-53 AU-6(10)]

a.) United States Computer Emergency Readiness Team (US-CERT) alerts

b.) CSCU Information Security Program Office (ISPO) advisories

c.) Law Enforcement Requests

d.) Freedom of Information Requests

e.) eDiscovery \ Legal Requirements

f.) Security Investigations

5.4 All staff involved with audit log review and analysis responsibilities must:

a.) Be trained on how to review and analyze audit logs

b.) Report incidents in according with the CSCU Incident Handling Procedures.

6. Audit Reduction and Report Generation [NIST 800-53 AU-7]

6.1 Moderate and High Risk Information Systems must:

a.) Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and does not alter original audit records.

b.) Provide the capability to process audit records for events of interest based on the following audit fields within audit records: [NIST 800-53 AU-7(1)]

- Individual identities
- Event types
- Event locations
- Event times and time frames
- Event dates
- System resources involved, IP addresses involved
- Information object accessed

7. Time Stamps [NIST 800-53 AU-8]

7.1 The information system must be configured to use the internal system clock to generate time stamps for audit records; audit record timestamps must include:

a.) Date and time to millisecond precision; and

b.) Time zone in use by the device.

7.2 The information system must synchronize system clocks daily with a CSCU defined authoritative time source when the time difference is greater than thirty seconds. [NIST 800-53 AU-8(1)]

8. Protection of Audit Information [NIST 800-53 AU-9]

8.1 All Information Systems must:

a.) Protect audit information and audit tools from unauthorized access, modification, and deletion. Audit information includes all information (e.g. Audit records, audit settings, and audit reports) needed to successfully audit information system activity

b.) Audit logs that contain high risk (DCL2, DCL3) records must be encrypted using a FIPS-140-2 compliant cryptography. [NIST 800-53 AU-9(3)]

8.2 Moderate and High Risk Information Systems must also:

a.) Authorize access and modification to management of audit functionality to only a defined subset of privileged users. [NIST 800-53 AU-9(4)]

8.3 High Risk Information Systems must additionally:

a.) Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

b.) Back up audit records onto a physically different system or system components than the system or component being audited. [NIST 800-53 AU-9(2)]

c.) Use file integrity monitoring or change detection software on audit logs to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts.

9. Audit Record Retention [NIST 800-53 AU-11]

9.1 All information systems must:

a.) Retain audit logs for at least one (1) year with a minimum of ninety (90) days immediately available for analysis to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

b.) Comply with the Connecticut General Records Retention Schedule for State Agencies, Specifically, S6-100: Information Systems Usage Records, and implement whichever retention period is most rigorous, binding or exacting.

c.) Audit Log records that are relevant to litigation hold notifications or active investigations must be preserved until notice that these logs may be destroyed.

10. Audit Generation [NIST 800-53 AU-12]

10.1 All information systems must:

a.) Provide audit generation capabilities for security related events defined in section 1.1, Audit Records.

b.) Generate audit records for the events, defined in section 1.1, Audit Events, with the content defined in Section 2, Content of Audit Records.

10.2 Moderate and High Risk Information Systems must additionally:

a.) Provide audit generation capabilities for security related events defined in section 1.2, Audit Records.

b.) Generate audit records for the events, defined in section 1.2, Audit Events, with the content defined in Section 2, Content of Audit Records.

11. Session Audit [NIST 800-53 AU-14]

11.1 Moderate and High Risk Information Systems must:

a.) Provide capabilities to record application layer details and packet data for all network sessions across boundaries.

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.

General Records Retention Schedules for State Agencies, S6: Information Systems Records, Connecticut State Library, Office of the Public Records Administrator, Item S6-100, December 2010.

Security Assessment and Authorization (CA)

Purpose:

The following standards are established to support the policy statement 10.6 that "CSCU will: (i) periodically assess the security controls in CSCU information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in CSCU information systems; (iii) authorize the operation of CSCU information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls."

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. Security Assessments [NIST 800-53r4 CA2]

1.1 For all information systems the ISPO:

a.) Develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

b.) Assesses the security controls in the information system and its environment of operation at least once of three (3) years, when significant changes after initial authorization, and until the system is decommissioned to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c.) Produces a security assessment report that documents the results of the assessment; and

d.) Provides the results of the security control assessment to the CSCU CIO, Campus ISSO, CSCU President/Campus President, and Information System Owner.

1.2 For moderate and high risk information systems the ISPO:

a.) Employs assessors or assessment teams with independence from the information system owner to conduct security control assessments. [NIST 800-53r4 CA2 (1)]

b.) Includes as part of security control assessments:

- Occur once every two (2) years;
- Perform announced or unannounced assessments;
- Will include, but not limited to, one or more of the following methods of testing:

    a. In-depth Monitoring;

    b. Vulnerability Scanning;

    c. Malicious User Testing;

    d. Insider Threat Assessment;

    e. Performance/Load Testing. [NIST 800-53r4 CA2 (1)]

2. System Interconnections [NIST 800-53r4 CA3]

2.1 For all information systems the Campus President and Campus CIO in consultation with the Campus ISSO and the Information System Owner:

a.) Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

b.) The information system owner documents, for each authorized interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

c.) Reviews and updates Interconnection Security Agreements yearly.

2.2 For moderate and high risk information systems;

a.) The information system owner ensures that a deny-all, permit-by-exception policy is employed for the information system to connect to external information systems. [NIST 800-53r4 CA3 (5)]

3. Plan of Action and Milestones [NIST 800-53r4 CA5]

3.1 For all information systems the Information System Owner in consultation with the Campus ISSO:

a.) Develops a plan of action and milestones for the information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b.) Updates existing plan of action and milestones yearly or upon notification based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

4. Continuous Monitoring [NIST 800-53r4 CA7]

4.1 For all information systems, the ISPO must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

a.) Establishment of metrics to be monitored;

b.) Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;

c.) Ongoing security control assessments in accordance with the approved CSCU continuous monitoring strategy;

d.) Ongoing security status monitoring of CSCU-defined metrics in accordance with the approved CSCU continuous monitoring strategy;

e.) Correlation and analysis of security-related information generated by assessments and monitoring;

f.) Response actions to address results of the analysis of security-related information; and

g.) Reporting the security status of the organization and the information system to CSCU President, CSCU CIO, Campus President, Campus CIO, Campus ISSO, and Information System Owner.

4.2 For moderate and high risk information systems.

a.) The ISPO employs assessors or assessment teams with independence from the information system owner to monitor the security controls in the information system on an ongoing basis. [NIST 800-53r4 CA7 (1)]

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.

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.

- 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.

CSCU

Contingency Planning (CP)

Purpose:

The following standards are established to support the policy statement 10.8 that "CSCU will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for CSCU information systems to ensure the availability of critical information resources and continuity of operations in emergency situations."

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. Information System Backup [NIST 800-53r4 CP9]

1.1 For all information systems:

a.) The Information System Owner and Data Owners will identify and document both Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for the Information System.

b.) The Information System Owner must backup data residing on information systems including, but not limited to, the following:

- Backups of user-level information contained in the information system.
- Backups of system-level information contained in the information system. System-level information includes, for example, system state information, operating system and application software, and licenses.
- Backups of information system documentation including security-related documentation.
- The frequency of information system backups shall be consistent with the information systems' RTOs and RPOs.

c.) The Information System Owner must protect the confidentiality, integrity, and availability of the system backup information at the storage location.

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.800	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

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

a.) Tests backup information at least once per year to verify media reliability and information integrity. [NIST 800-53r4 CP9 (1)]

b.) Protect the confidentiality and integrity of the system backup information at the storage location using CSCU approved encryption and cryptographic hashing methods.

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

a.) Stores backup copies in a separate, CSCU approved facility or in a fire-rated container that is not collocated with the operational system. [NIST 800-53r4 CP9 (3)]

2. Information System Recovery and Reconstitution [NIST 800-53r4 CP10]

2.1 For all information systems, the Information System Owner

a.) Ensures the information system can be recovered and reconstituted to a known state after a disruption, compromise, or failure.

b.) Documents recovery and reconstitution mechanisms and procedures.

c.) Ensure the information system's recovery and reconstitution procedures:

- Are based on organizational priorities, established RPO, RTO, and reconstitution objectives, and appropriate metrics.
- Include the deactivation of any interim information system capability that may have been needed during recovery operations.
- Include an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure.

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

a.) Ensure the information system's recovery and reconstitution procedures also include the following during disruptions and during recovery and reconstitution:

- Essential operations shall be continued; and

- Confidentiality and integrity of the information will be protected.

b.) Ensures the information system implements transaction recovery for systems that are transaction-based. [NIST 800-53r4 CP10 (2)]

2.3 For high risk information systems, the Information System Owner provides the capability to reimage information system components immediately from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. The restoration time-period of the information system shall be consistent with the information systems' RTOs and RPOs. [NIST 800-53r4 CP10 (4)]

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.

CSCU

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.

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.

Media Protection (MP)

Purpose:

The following standards are established to support the policy statement 10.11 that "CSCU will: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse."

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. Media Access [NIST 800-53r4 MP2]

1.1 For all information systems, the Data Owner and Information System Owner ensure that access to digital media is restricted to authorized users.

2. Media Marking [NIST 800-53r4 MP3]

2.1 For all moderate and high risk information systems, the Data Owner and Information System Owner ensure that:

a.) Information system digital media is marked indicating the distribution limitations, handling caveats, and applicable data classification markings (if any) of the information.

3. Media Storage [NIST 800-53r4 MP4]

3.1 For all moderate and high risk information systems, the Data Owner and Information System Owner ensure that:

a.) All digital media is physically controlled and stored within environmentally appropriate, and access restricted environments.

b.) Data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices) must be encrypted.

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.1100	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

c.) Information system media is protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

4. Media Transport [NIST 800-53r4 MP5]

4.1 For all moderate and high risk information systems, the Data Owner and Information System Owner ensure that:

a.) Digital media is protected and controlled during transport outside of controlled areas using defined security measures that are CSCU approved;

b.) Accountability is maintained for information system media during transport outside of controlled areas;

c.) Activities associated with the transport of information system media are documented; and

d.) The activities associated with the transport of information system media is restricted to authorized personnel.

e.) The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. [NIST 800-53r4 MP-5(4)]

5. Media Sanitization [NIST 800-53r4 MP6]

5.1 For all information systems, the Data Owner and Information System Owner ensure that:

a.) Digital media is sanitized prior to disposal, release out of organizational control, or release for reuse using approved CSCU sanitization techniques and procedures in accordance with applicable federal and state standards and policies; and

b.) Sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information are employed.

5.2 For high risk information systems, the Data Owner and Information System Owner ensure that media sanitization and disposal actions are reviewed, approved, tracked, documented, and verified. [NIST 800-53r4 MP6 (1)]

5.3 For high risk information systems, the Data Owner and Information System Owner ensure that testing to sanitization equipment and procedures to verify that the intended sanitization is being achieved occurs annually. [NIST 800-53r4 MP6 (2)]

5.4 For moderate and high risk information systems, the Data Owner and Information System Owner ensure that nondestructive sanitization techniques are applied to portable storage devices prior to connecting such devices to the information system under the following circumstances:

a.) Such devices are first purchased from the manufacturer or vendor prior to initial use; or

b.) The organization loses a positive chain of custody for the device.

6. Media Use [NIST 800-53r4 MP7]

6.1 For all information systems, ISPO will approve removable media device types and requirements for use with information systems.

6.2 For all information systems, the Data Owner and Information System Owner ensure that:

a.) Non-CSCU approved removable media device use on information systems is prohibited.

6.3 For all moderate and high risk information systems, the Data Owner and Information System Owner prohibits the use of portable storage devices when such devices have no identifiable owner. [NIST 800-53r4 MP-7(1)]

Roles & Responsibilities

Refer to the Roles and Responsibilities located on the website.

Definitions

Security Marking	The term security marking refers to the application/use of human-readable security attributes.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Non-digital Media	Non-digital media includes, for example, paper and microfilm.

Controlled Areas	Controlled areas are areas or spaces for which CSCU provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.
Information System Media	Information system media includes both digital and non-digital media.
Removable Media	Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).
Portable Storage Devices	A Portable device that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data).
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

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.

Physical and Environmental Protection (PE)

Purpose:

The following standards are established to support the policy statement 10.12 that "CSCU will: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing 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. Physical Access Authorizations [NIST 800-53r4 PE2]

1.1 For all information systems, the Information System Owner:

a.) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b.) Issues authorization credentials for facility access;

c.) Reviews the access list detailing authorized facility access by individuals yearly; and

d.) Removes individuals from the facility access list when access is no longer required.

2. Physical Access Control [NIST 800-53r4 PE3]

2.1 For all information systems, the Information System Owner:

a.) Enforces physical access authorizations at entry/exit points to the facility where the information system resides by;

- Verifying individual access authorizations before granting access to the facility; and
- Controlling ingress/egress to the facility using one or more physical access control systems/devices;

b.) Maintains physical access audit logs for entry/exit points;

c.) Escorts visitors and monitors visitor activity;

d.) Secures keys, combinations, and other physical access devices;

e.) Inventories physical access devices every year; and

f.) Changes combinations and keys yearly and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

3. Access Control for Transmission Medium [NIST 800-53r4 PE4]

3.1 For all moderate and high risk information systems, the Information System Owner controls physical access to information system distribution and transmission lines within organizational facilities using electronic or physical locking mechanisms.

4. Access Control for Output Devices [NIST 800-53r4 PE5]

4.1 For all moderate and high risk information systems, the Information System Owner controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

5. Monitoring Physical Access [NIST 800-53r4 PE6]

5.1 For all information systems, the Information System Owner:

a.) Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

b.) Reviews physical access logs yearly and upon occurrence of incidents or potential indications of incidents; and

c.) Coordinates results of reviews and investigations with the organizational incident response capability and ISPO.

5.2 For all moderate and high risk information systems, the Information System Owner monitors physical intrusion alarms and surveillance equipment. [NIST 800-53r4 PE6 (1)]

6. Visitor Access Records [NIST 800-53r4 PE8]

6.1 For all information systems, the Information System Owner:

a.) Maintains visitor access records to the facility where the information system resides for one year; and

b.) Reviews visitor access records yearly.

6.2 For high risk information systems, the Information System Owner employs automated mechanisms to facilitate the maintenance and review of visitor access records. [NIST 800-53r4 PE8 (1)]

7. Alternate Work Site [NIST 800-53r4 PE17]

7.1 For all information systems, the Information System Owner:

a.) Employs safeguarding mechanisms at alternate work sites;

b.) Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c.) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

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.

Planning (PL)

Purpose:

The following standards are established to support the policy statement 10.13 that "CSCU will develop, document, periodically update, and implement security plans for CSCU information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the 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. System Security Plan [NIST 800-53r4 PL2]

1.1 For all information systems:

a.) The Information System Owner, in consultation with the Campus ISSO is responsible to develop and maintain a System Security Plan (SSP) for each information system. A system security plan (SSP) must describe the processes, procedures, and security controls currently being used or planned to be implemented to manage and secure the information system to meet security requirements, including rationale for the tailoring and supplemental decisions that must be developed, documented, updated, and implemented for the information system.

b.) The SSP must:

- Be consistent with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the information system and its operational environment both generally and in technical terms.

a. Information processing flow, including key inputs and outputs, must be described.

b. All IT assets, including hardware, software, and (if appropriate) networking/telecommunications equipment, must be listed and described.

c. The information system and subsystem authorization boundaries must be explicitly defined.

d. The description must include applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high level design).

e. The description must reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, wireless technology, public access, hosting or operation at a facility outside of the organization's control), as applicable.

- Describe all relationships with or connections to information systems outside CSCU, or between internal systems but across system boundaries.

    a. The information for each connection must include:

        i. The name of the connected information system.

        ii. The information system's organization and point of contact.

        iii. The type of system.

        iv. The authorization for the connection be it a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or Interconnection Security Agreement (ISA) as appropriate for the organization and purpose.

        v. The date of the signed connection agreement.

        vi. The CSCU information security categorization.

        vii. The name and title of the interconnected information system's authorizing official.

- Provides an overview of the security requirements for the system;
- Identifies any relevant overlays, if applicable;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

c.) The Campus ISSO must review and produce a security control assessment report, based on the authorized security control assessment plan, of the SSP and provide the security control assessment report, as part of the authorizing package, to the BOR CIO/Campus President/CIO;

d.) The BOR President/Campus President or BOR CIO/Campus CIO must review the SSP, security control assessment report, and any plan of action and milestones report prior to plan implementation;

- The only sections of an SSP permitted to be made available to users of the information system are the rules of behavior and remote access requirements, otherwise, the SSP is considered sensitive and is prohibited from being released to unauthorized personnel.

e.) The Information System Owner distributes copies of the system security plan and communicates and documents subsequent changes to the plan with the Campus ISSO;

f.) The Information System Owner and Campus Information System Security Officer reviews the security plan for the information system;

- At least annually or when a significant change occurs to the information system's operating environment or security requirements;
    a. A significant change includes a change in the points of contact, system architecture, system status, system interconnections, system scope, or C&A status.
- The document review history must be updated to reflect the date the review was performed.

g.) The Information System Owner updates and maintains the system security plan to address changes to the information system/environment of operation.

- Planned significant changes must be defined in advance and identified in the SSP as well as in the configuration management process. The SSP must be updated to factor in planned information system enhancements, to ensure that required security-related activities are planned for in advance.

- The SSP must be updated based on the results of the continuous monitoring process. The Campus ISSO must review and provide a new security control assessment report to the BOR CIO/Campus President/CIO to include updates or changes to the SSP.
- Updates or changes to the SSP must be reviewed and re-authorized by the CSCU CIO/Campus before implementation.

h.) The Information System Owner and Campus ISSO must create a plan of action and milestones (POAM) document to address:

- weaknesses identified during system implementation, control assessments, investigations, or when impacted by unforeseen significant events, such as a breach, a new threat, or previously unknown vulnerability;

i.) The Campus ISSO protects the security plan from unauthorized disclosure and modification.

2. Rules of Behavior [NIST 800-53r4 PL4]

2.1 For all information systems, the Information System Owner:

a.) Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

b.) Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

c.) Reviews and updates the rules of behavior annually or as needed; and

d.) Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

2.2 For all moderate and high risk information systems, the Information System Owner includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. [NIST 800-53r4 PL4 (1)]

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.

Personnel Security (PS)

Purpose:

The following standards are established to support the policy statement 10.14 that "CSCU will: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that CSCU information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with CSCU security policies, standards, and procedures."

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. Personnel Screening [NIST 800-53r4 PS3]

1.1 For all information systems, the Information System Owner and Data Owners must ensure:

a.) Individuals have been screened prior to authorizing access to the information system; and

b.) Personnel screening and rescreening must be consistent with applicable state and federal laws, CSCU policies, regulations, and standards.

2. Personnel Termination [NIST 800-53r4 PS4]

2.1 For all information systems, the Information System Owner in collaboration with the Data Owner, upon termination of individual employment:

a.) Disables information system access within the same day of notification;

b.) Terminates/revokes any authenticators/credentials associated with the individual;

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.1400	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

2.2 For all information systems, the Data Owner, upon termination of individual employment:

a.) Conducts exit interviews that include a discussion of:

- Continued obligations under information system non-disclosure, confidentiality, or user access agreements.
- Determine all information systems to which the individual had access and email distribution list memberships.

b.) Retrieves all security-related organizational information system-related property;

c.) Retains access to organizational information and information systems formerly controlled by terminated individual; and

d.) Notifies the Information System Owner within the same day of termination.

2.3 For high risk information systems, the Information System Owner employs automated mechanisms to notify upon termination of an individual. [NIST 800-53r4 PS4 (2)]

3. Personnel Transfer [NIST 800-53r4 PS5]

3.1 For all information systems, the Data Owner:

a.) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

b.) Initiates transfer or reassignment actions within the same day following the formal transfer action;

c.) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d.) Notifies the Information System Owner within the same day.

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.

System and Services Acquisition (SA)

Purpose:

The following standards are established to support the policy statement 10.15 that "CSCU will: (i) allocate sufficient resources to adequately protect CSCU information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third party providers employ adequate security measures, through federal and Connecticut state law and contract, to protect information, applications, and/or services outsourced from the organization."

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. Allocation of Resources [NIST 800-53r4 SA2]

1.1 For all information systems the CSCU CIO/Campus CIO, determines information security requirements for the information system or information system service in mission/business process planning;

a.) Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

b.) Establishes a discrete line item for information security in organizational programming and budgeting documentation.

2. System Development Life Cycle [NIST 800-53r4 SA3]

2.1 For all information systems, the Information System Owner:

a.) Manages the information system using defined system development life cycle that include planning, system analysis and requirements, system design, development, integration and testing, implementation, and operations and maintenance phases that incorporates information security considerations;

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.1500	Approved	2/6/2020	2/6/2020	June 10, 2019	2/6/2020	

b.) Defines and documents information security roles and responsibilities throughout the system development life cycle;

c.) Identifies individuals having information security roles and responsibilities; and

d.) Integrates the organizational information security risk management process into system development life cycle activities.

3. Acquisition Process [NIST 800-53r4 SA4]

3.1 For all information systems the Information System Owner in collaboration with the ISPO, includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, CSCU policies, regulations, standards, and organizational mission/business needs:

a.) Security functional requirements;

b.) Security strength requirements;

c.) Security assurance requirements;

d.) Security-related documentation requirements;

e.) Requirements for protecting security-related documentation;

f.) Description of the information system development environment and environment in which the system is intended to operate; and

g.) Acceptance criteria.

3.2 For all moderate and high risk information systems the Information System Owner, in collaboration with the ISPO, requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. [NIST 800-53r4 SA4 (1)]

3.3 For all moderate and high risk information systems the Information System Owner requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed at a level of detail needed to complete a System Security Plan that includes:

a.) security-relevant external system interfaces; and

b.) high-level design. [NIST 800-53r4 SA4 (2)]

3.4 For all moderate and high risk information systems the Information System Owner requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. [NIST 800-53r4 SA4 (9)]

3.5 For all information systems the Information System Owner employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. [NIST 800-53r4 SA4 (10)]

4. Information System Documentation [NIST 800-53r4 SA5]

4.1 For all information systems, the Information System Owner:

a.) Obtains administrator documentation for the information system, system component, or information system service that describes:

- Secure configuration, installation, and operation of the system, component, or service;
- Effective use and maintenance of security functions/mechanisms; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

b.) Obtains user documentation for the information system, system component, or information system service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
- User responsibilities in maintaining the security of the system, component, or service;

c.) Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and notifies ISPO/Campus ISSO in response;

d.) Protects documentation as required, in accordance with the risk management strategy; and

e.) Distributes documentation to CSCU CIO/Campus CIO, ISPO/Campus ISSO.

5. Security Engineering Principles [NIST 800-53r4 SA8]

5.1 For all information systems, the Information System Owner applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

6. External Information System Services [NIST 800-53r4 SA9]

6.1 For all information systems, the Information System Owner:

a.) Requires that providers of external information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal and state laws, CSCU policies, regulations, and standards;

b.) Employs processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

6.2 For all moderate and high risk information systems, the Information System Owner, requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

7. Developer Configuration Management [NIST 800-53r4 SA10]

7.1 For all moderate and high risk information systems, the Information System Owner, requires the developer of the information system, system component, or information system service to:

a.) Perform configuration management during system, component, or service design, development, implementation, and operation;

b.) Document, manage, and control the integrity of changes to items under configuration management;

c.) Implement only organization-approved changes to the system, component, or service;

d.) Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e.) Track security flaws and flaw resolution within the system, component, or service and report findings to ISPO and campus ISSO.

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.

System and Communication Protection (SC)

Purpose:

The following standards are established to support the policy statement that "CSCU will: (i) monitor, control, and protect CSCU communications (i.e., information transmitted or received by CSCU information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within 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. Application Partitioning [NIST 800-53r4 SC2] [NIST 800-171r1 3.13.3]

1.1 For all moderate and high risk information systems, the Information System Owner ensures the information system separates user functionality (including user interface services) from information system management functionality.

2. Information in Shared Resources [NIST 800-53r4 SC4]

2.1 For all moderate and high risk information systems, the Information System Owner ensures the information system prevents unauthorized and unintended information transfer via shared system resources.

3. Boundary Protection [NIST 800-53r4 SC7]

3.1 For all information systems, the Information System Owner:

a.) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

b.) Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and

c.) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

3.2 Ensures the information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). [NIST 800-53r4 SC7(5)]

3.3 Ensures the information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling). [NIST 800-53r4 SC7(7)]

4. Transmission Confidentiality and Integrity [NIST 800-53r4 SC8]

4.1 For all information systems, the Information System Owner ensures:

a.) The information system protects the confidentiality and integrity of transmitted information;

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

a.) The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information during transmission. [NIST 800-53r4 SC8(1)]

5. Network Disconnect [NIST 800-53r4 SC10]

5.1 For moderate and high risk information systems, the Information System Owner ensures the information system terminates the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity.

6. Cryptographic Key Establishment and Management [NIST 800-53r4 SC12]

6.1 For all information systems, the Information System Owner ensures cryptographic keys for required cryptography employed within the information system is in accordance with CSCU defined requirements for key generation, distribution, storage, access, and destruction.

7. Cryptographic Protection [NIST 800-53r4 SC13]

7.1 For moderate and high risk systems, the Information System Owner ensures the information system implements CSUS approved cryptography for the protection of data.

8. Collaborative Computing Devices [NIST 800-53r4 SC15]

8.1 For all information systems, the Information System Owner:

a.) Prohibits remote activation of collaborative computing devices; and

b.) Provides an explicit indication of use to users physically present at the devices.

9. Mobile Code [NIST 800-53r4 SC18]

9.1 For all information systems:

a.) The ISPO Defines acceptable and unacceptable mobile code and mobile code technologies;

b.) The ISPO Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c.) The Information System Owner Authorizes, monitors, and controls the use of acceptable mobile code within the information system.

10. Voice Over Internet Protocol [NIST 800-53r4 SC19]

10.1 For all information systems:

a.) the ISPO establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b.) The Information System Owner authorizes, monitors, and controls the use of VoIP within the information system.

11. Secure Name/Address Resolution Service (Authoritative Source) [NIST 800-53r4 SC20]

11.1 The information system:

a.) Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b.) Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

12. Secure Name/Address Resolution Service (Recursive or Caching Resolver) [NIST 800-53r4 SC21]

12.1 The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

13. Architecture and Provisioning for Name/Address Resolution Service [NIST 800-53r4 SC22]

13.1 The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

14. Session Authenticity [NIST 800-53r4 SC23]

14.1 For all information systems, the Information System owner ensures the information system protects the authenticity of communications sessions.

15. Protection of Information at Rest [NIST 800-53r4 SC28]

15.1 For moderate and high risk information systems, the Information System Owner ensures the information system protects the confidentiality and integrity of information at rest.

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.

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.
- For information system categorized as moderate (M)

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	

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.