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	Next Review:
IT-004	BOR Approved	2/6/2020	2/6/2020	2/6/2020	2/6/2020	2/6/2021

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.