Connecticut State
Colleges & Universities
Board of Regents for Higher Education

Information Technology

Policy

Information Security

Identifier: IT-003	
Revision Date: October 16, 2014	**Effective Date: March 1, 2015**
Approved by: BOR	**Approved on date: October 16, 2014**

Table of Contents

1. Introduction

This Policy governs Information Security requirements to protect Connecticut State Colleges and Universities (CSCU) information assets and meet our federal and state requirements, e.g. Gramm-Leach-Bliley Act (GLBA). CSCU is required to have an Information Security Program that addresses the Availability, Integrity and Confidentiality of CSCU information assets. These policies apply to all faculty, staff and students and are primarily administered by the campus leadership and local Data Stewards. This policy outlines 17 information security standards, from the National Institute of Standards and Technology (NIST), which form the foundational architecture of the security policy. Each security standard will have a more detailed standards developed to explain the specific implementation and policy requirements that each institution must meet to be in compliance.

Although no set of policies can address all scenarios of IT security, these policies and their subsequent detailed standards will outline procedures to secure CSCU data and assets. Their primary goal is to guide users and administrators towards reasonable decisions and actions, within the framework of the standard. The Chief Information Officer, working with the Chief Information Security Officer oversees information security activities and the development of these 17 detailed security standards. Through the 17 standards, CSCU will protect resources from threats and ensure compliance with applicable laws and industry requirements. CSCU IT resources, whether owned or contracted, will be configured to meet the requirements set forth in the 17 security standards. Agreements that involve a third party assessing or managing CSCU IT resources shall require the third party to be responsible for complying with the requirements within the various standards. The BOR, University and College are responsible for keeping computer systems protected from activities that could compromise the confidentiality, integrity and availability of the resource.

2. Purpose

The CSCU Information Security Policy is the cornerstone for the CSCU Information Security Program. The purpose of this Information Security Policy is to define what must be done to protect CSCU information assets for availability, integrity and confidentiality.

Secondly, the Information Security Policy assigns ownership and accountability for meeting these Information Security requirements by delineating key roles and responsibilities in meeting CSCU Information Security objectives. Fulfilling both of these objectives will enable CSCU to implement a comprehensive system-wide Information Security Program.

3. Implementation Methodology

CSCU needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill our academic mission. The information security program will be risk based. Implementation decisions will be made based on addressing the highest risk first. Using a layered ring approach, this policy will secure the inner ring, high risk data and systems, with the tightest controls and the outer ring, public data, with lower controls. This strategy allows the CSCU system to protect the availability, integrity and confidentiality of our system while using the least restrictive controls on academic systems and public networks.

CSCU recognizes that at times implementing the NIST standards will not be possible because of technical or administrative limitations. CSCU will, whenever possible, implement the NIST standards and if unable to meet the NIST standards, document the exception. Exceptions because of technical limitations, e.g. legacy system cannot meet password requirements, will only need to be documented and submitted to the ISPO.

4. Policy Authority

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

5. Scope

- This policy classifies networks, access, and security standards based on the data classification that resides on that network. This policy requires a level security protection on all internal networks, but places the greatest security requirements on networks which contain and process confidential data.
- For contracted and third party services, it is recognized that the CSCU will protect data transported via a secure internet connection. The third party is responsible by BOR contract for the protection and management of confidential data per federal and state statute, this policy and mandatory terms and conditions.
- This policy applies to all information assets and IT resources operated by the CSCU;
- This policy applies to all information assets and IT resources provided by CSCU through contracts, subject to the provisions and restrictions of the contracts ; and
- This policy applies to all authenticated users of CSCU information assets and IT resources.

The CSCU Security Program is framed on National Institute of Standards and Technology (NIST) and technical controls implemented based on SANS Critical Security Controls priorities. CSCU must develop appropriate standards and procedures required to support the Board of Regents (BOR) Information Security Policy**.** This policy will be further defined by standards, procedures, control metrics and control tests to assure functional verification.

The CSCU Security Program will be based on NIST Special Publication 800-53; this publication is structured into 17 control groupings, herein referred to as Information Security Standards.

6. Roles and Responsibilities

a. **Board of Regents (BOR):** (i) Issues Information Security Policy; (ii) Sponsors the Development and Implementation of a Comprehensive Information Security Program; (iii) Oversees the security of all CSCU Information Resources.

b. **BOR Chief Information Officer (CIO):** The BOR Chief Information Officer is responsible for the design, implementation, operations and compliance functions of the BOR Information Security Program for all CSCU constituent units. Their responsibilities include:

1. Establish the Information Security Program Office to assist in all the responsibilities and functions related to the BOR Information Security Program.
2. Designate a Chief Information Security Officer (CISO) or appropriate third party to manage the Information Security Program Office.
3. Annually provide the Board of Regents a report detailing the security program effectiveness and the risk.

c. **College and University Presidents:** The College and University Presidents are responsible for assuring that their respective institutions are complying with the BOR Information Security Program inclusive of all policies, standards, and procedures including managerial, administrative and technical controls for their institutions.

d. **Chief Information Security Officer (CISO):** The Chief Information Security Officer is appointed by the BOR CIO and manages information security throughout CSCU. The CISO, under the direction of the BOR CIO, is responsible for the development, implementation and maintenance of a comprehensive Information Security Program for the CSCU. This includes security policies, standards and procedures which reflect best practices in information security. The program with be based on standards developed by the National Institute of Standards and Technology.

e. **Security Compliance Working Group (SCWG):** The Security Compliance Working Group will be advisory to the CISO, BOR CIO, local IT Leadership and the College and University Presidents. Their primary function is to develop and draft policy requirements working closely with the CISO and campuses based on the security standards. The SCWG will be available to perform security assessments of the standards at their respective campuses.

f. **Contact Information:** To report security incidents, abuse or questions. Please ensure you include your local University or College reporting structure.

CIO, Joseph Tolisano: tolisanoj@ct.edu
General Email: SecProg@ct.edu

7. Information and Information System Classifications

CSCU will establish 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 need by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories will be used in conjunction with vulnerability and threat information in assessing risk and controls.

8. Provisions for Information Security Standards

Access Control

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.

Awareness and Training

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.

Audit and Accountability

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.

Assessment and Authorization

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.

Configuration Management

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.

Contingency Planning

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.

Identification and Authentication

CSCU will 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.

Incident Response

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.

Maintenance

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.

Media Protection

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.

Physical and Environmental Protection

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.

Planning

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.

Personnel Security

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 and procedures.

Risk Assessment

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.

System and Services Acquisition

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.

System and Communications Protection

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.

System and Information Integrity

CSCU will: (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.

9. Enforcement

Enforcement is the responsibility of the local University or College president or designee. For purposes of protecting the CSCU network and information technology resources, the BOR Chief Information Officer will work in conjunction with College/University President and the respective campus IT department, as requested remove or block any system, device, or person from the CSCU network that is reasonably suspected of harming or causing potential risk to CSCU information technology systems or network. These non-punitive measures will be taken to maintain business continuity and information security; users of the College/University information technology resources will be contacted for coordination and assistance.

10. No Expectation of Privacy

There is no expectation of privacy in the use of CSCU IT resources. CSCU reserves the right to inspect, monitor and disclose all IT resources including files, data, programs and electronic communications records without the consent of the holder of such records. Please see the State of CT Electronic Monitoring Notice.

11. Exceptions

Compliance with this Information Security Policy is mandatory. All CSCU entities must comply with the roles, responsibilities, and security policies statements set forth in this document to ensure the confidentiality, integrity, and availability of institutional information. Further, CSCU entities must ensure that contractors engaged by them are aware of the security controls required by federal and Connecticut state laws and regulations and these controls are agreed to within the contract. CSCU recognizes that some portions of the Information Security Policy may have to be bypassed from time-to-time because of technical or business reasons.

Accordingly, exceptions may be made provided:

1. The need for the exception is legitimate and approved by the BOR CIO or designee and local University or College president, who ultimately holds the risk
2. The exception does not disrupt or compromise other portions of the CSCU service delivery capability.
3. The implementation of the exception is vetted through and approved by the IT Steering Committee.
4. The College/University IT department must be able to establish a monitoring function to assess the operations of the implementation exception. Monitoring will be approved by the BOR CIO.
5. The exception has a defined lifecycle, in that the "retirement" of the exception is scheduled (e.g., "when Release 4.9 is implemented," "at contract termination," etc.)

12. Exception Request

To request an exception, please submit the Information Security Exception request to, secprog@ct.edu that is responsible for briefing the BOR CIO and appropriate administrators.

The requestor and BOR Information Security Program Office will define the approved alternative configuration if different than the original proposal of the requestor.

The exception process is NOT an alternative to the Change Control Management process.

13. Disclaimer

CSCU disclaims any responsibility for and does not warrant information and materials residing on non-CSCU systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CSCU, its faculty, staff or students.

14. Related Publications and Guidance –

NIST 800-53, FIPS-199

This Information Security Policy defines mandatory requirements for protecting information. It is issued in accordance with:

- Board of Regent Policies and Resolutions Connecticut General Statutes Code of Federal Regulations United States Code
- State Data Retention Schedule S6

15. Revision History

Previous versions of this policy

- None

Policies superseded by this policy

- For CSU this policy supersedes BOT Resolution 06-9 and 06-10 for the policy only.
- For CSU this policy does not supersede the CSU Information Security Standard. As standards are developed in support of this policy they will supersede sections of the standard.
- For CCC this policy is supersedes 1.1 IT Policy Common Provisions. Remaining CCC policies will remain in effect until standards are developed to support this policy.

16. Definitions

Access Controls: The technology, processes, and procedures used to limit and control access to information technology (IT) resources; these controls are designed to protect against unauthorized entry or use.

Accounts: User accounts are the means of access for real people to a computer system, and provide separation of the users' activities with the system environment, preventing damage to the system or other users. User accounts are assigned a username

Active Directory: A software system that stores, organizes and provides access to information in a directory created by Microsoft. It is responsible for authenticating and authorizing all users and computers within a network.

Administrator: See System Administrator.

Authentication: The act of verifying the identity of a user and the user's eligibility to access computerized information.

Authorization: The function of specifying access rights to resources.

Availability: The state of a system in a functioning condition.

Business Continuity Plan (BCP): A document describing how an organization responds to an event to ensure critical business functions continue without unacceptable delay or change.

CAS: Known as Central Authentication Service, CAS permits a user to access multiple applications while providing their username and password only once.

Chief Information Security Officer (CISO): Head of the Information Security Office.

Computer Maintenance: Tasks that must be performed on computers in order to keep them running at optimal efficiency. These tasks include applying security patches, running and maintaining antivirus software, and keeping the computer and data secure.

Confidentiality: Secrecy

Credit Card Data: Data that identifies a credit card account. This data includes primary account numbers (PAN), service codes, expiration date, magnetic stripe or storage chip data, and card validation codes.

Critical Systems and Data: Systems and data that are essential to the operations of the University of to a specific department.

Data: Records and information in a form suitable for use with a computer.

Data Administrators: People who are responsible for applying appropriate controls to data based on its classification level and required protection level. These people are usually system administrators

Data Stewards: People with the responsibility of ensuring the proper handling of administrative, academic, public engagement, or research data.

Data Restoration Procedures: The process used to reinstate data that has been backed up.

Data Users: People that read, enter, or update data.

Desk Audits: The act of reviewing documentation to verify technical and procedural details.

Development Environment: Software staging system, where development takes place that is separate from the actual system

Disaster: A negative event that lasts longer than the maximum tolerable downtime

Recovery (DR) Plan: A document that outlines how the University will respond to a disaster and resume critical business functions within a predetermined period of time with minimum amount of loss.

Electronic Protected Health Information (ePHI): Electronic confidential patient information that must be secured against unauthorized exposure as per HIPAA.

Encrypted Data: Data that has undergone the process of encryption

Encryption: A technique used to transform plain text so it is unintelligible but recoverable.

Encryption Key: The input into an encryption algorithm that allows the data to be encrypted.

File Auditing: The logging of opening, modifying, or deleting files on a computer.

File Sharing: Distributing or providing access to electronic data files, usually via a network connection.

Firewall: A network device used to block network access to Information Technology resources

HIPAA: The Health Insurance Portability and Accountability Act address the security and privacy of health data.

Incident: An attempted or successful event resulting in unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

Information Security: Administrative, physical and technical controls that seek to maintain confidentiality, integrity, and availability of information.

Information Security Awareness Training (ISAT) Program: Training of University faculty and staff regarding the protection of various information technology resources.

Information Security Office (ISO): The unit responsible for overall information security functions for the University.

Information Technology: The act of managing technology, including computer software, information systems, computer hardware, and programming languages.

Information Technology (IT) Resources: Tools that allow access to electronic technological devices, or are an electronic technological device themselves These resources include data; computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; and peripheral devices.

Insecure Communication Networks: Data networks that are designed without security requirements in mind.

Integrity: The trustworthiness of information technology resources.

Live simulations: Imitating certain events in order to help test processes and procedures

Log Harvesting: IT resources used to collect logs from various information technology (IT) resources.

Logging: The process of electronically recording activities of IT resources.

Malware: Malicious software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to information technology (IT) resources.

PCI-DSS: An IT standard for organizations that handle credit card data.

Personally Identifiable Information (PII): Data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Production Environment: Final working stage of software development or network planning when product is rolled out to users.

Protected Health Information (PHI): Confidential patient information that must be secured against unauthorized exposure as per HIPAA.

Public computers: Computers that may be used by anyone in the general public

Recovery Point Objective: The maximum tolerable period in which data might be lost from an IT Service due to a breach or malfunction.

Recovery Time Objective: The duration of time and a service level within which a resource must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in availability.

Regulated Data: Information whose dispersal is determined by permission constraints, some users have access, while others do not.

Remote Desktop: The ability to control the keyboard and mouse of a computer from a remote location.

Restricted Data and Protective Enclave Networks: Networks and Systems that process and access confidential data, on restricted and isolated networks, with unique logins, restricted systems and white listed to only site required for restricted processing.

Risk Assessment: An analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of IT resources.

Security Vulnerability: A security exposure in an operating system or other system software or application software component which an attacker can exploit to gain access to the systems programs or data.

Server: A computer program running to serve the requests of other programs, the “clients".

Screen Lock: An automatic lock of a computer such that it may not be accessed without a username and password.

Shibboleth: A method of allowing sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

Software Patches: A piece of software designed to fix problems with, or update a computer program or its supporting data.

Spam Messages: The use of electronic messaging systems (*e.g.*, email) to send unsolicited bulk messages indiscriminately.

Strong Password: A password that requires extensive resources to guess using either brute force algorithms or human common sense.

System Administrator: A person employed to maintain and operate a computer system or network.

Tabletop Testing: A gathering of relevant individuals to review a specific process in order to improve or update the process.

Test Environment: Staging software development or network construction where the product is stress tested and bug tracked before final deployment.

Third Party: not the original creator of a product.
Threat: An action or event that possess a possible danger to a computer system and the potential for exploitation of vulnerability.

Unencrypted Data: Plaintext data that has not undergone the encryption process.

Users: People authorized to use information technology (IT) resources.

Virus: Malware that uses it host to propagate itself to other hosts.

Walkthroughs: A simulation of a process via a gathering of individuals in order to test and improve the process.

Whole Disk Encryption: Process by which the entire hard drive of a computer is encrypted