<table>
<thead>
<tr>
<th>Policy Number</th>
<th>TBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td>Applies To:</td>
<td>Faculty, Staff, Students and Contractors</td>
</tr>
<tr>
<td>Contact</td>
<td>TBD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved on Date:</th>
<th>xx/xx/xxxx</th>
<th>Effective Date:</th>
<th>xx/xx/xxxx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Review Date:</td>
<td>xx/xx/xxxx</td>
<td>Last Reviewed Date:</td>
<td>xx/xx/xxxx</td>
</tr>
</tbody>
</table>
Contents

A. INTRODUCTION ............................................................................................................. 3
B. PURPOSE ......................................................................................................................... 3
C. SCOPE ............................................................................................................................ 3
D. POLICY AUTHORITY ....................................................................................................... 4
E. DEFINITIONS ..................................................................................................................... 4
F. APPROVAL AND CHANGE PROCESSES ........................................................................ 4
G. ROLES & RESPONSIBILITIES ......................................................................................... 6
H. GENERAL SECURITY POLICY ....................................................................................... 7
   H.1 ASSET MANAGEMENT ................................................................................................. 7
   H.2 RISK MANAGEMENT ................................................................................................. 7
   H.3 ACCESS MANAGEMENT .......................................................................................... 8
   H.4 DATA SECURITY ....................................................................................................... 8
   H.5 PHYSICAL SECURITY ............................................................................................... 9
   H.6 HOST & OPERATING SYSTEM SECURITY ............................................................... 9
      H.6.1 Malicious Software Protection ...................................................................... 9
      H.6.2 Patch Management ........................................................................................... 10
   H.7 SOFTWARE SECURITY ............................................................................................. 11
   H.8 DATA & SYSTEM BACKUP ...................................................................................... 11
   H.9 IT INFRASTRUCTURE MANAGEMENT & MONITORING .................................... 12
   H.10 BUSINESS CONTINGENCY/SERVICE RECOVERY .............................................. 13
   H.11 COMMUNICATION AND OPERATIONS MANAGEMENT .................................... 13
   H.12 INCIDENT MANAGEMENT .................................................................................... 13
   H.13 SECURITY AWARENESS AND TRAINING .......................................................... 14
I. ASSURANCE ....................................................................................................................... 14
J. REPORTING ..................................................................................................................... 15
K. EXCEPTION PROCESS .................................................................................................... 15
L. NO EXPECTATION OF PRIVACY .................................................................................... 15
M. ENFORCEMENT ............................................................................................................. 16
N. REVIEW .......................................................................................................................... 16
A. Introduction

Information and information system resources are essential assets of all of the parts of the Connecticut State College and Universities (ConnSCU). Information is also an essential asset of students, staff, students’ parents, contractors, etc. and is required to be protected by various privacy policies, regulations, as well as other laws.

The entire community of the ConnSCU System (students, faculty, staff, contractors, etc.) is responsible for ensuring that computing and communication facilities are used in an effective, efficient, ethical and lawful manner. This Security Policy is provided to all members of the ConnSCU community to provide proper guidelines on each individual's responsibility to protect ConnSCU information. Every individual should understand his or her obligations relating to the policy statements described herein.

The ConnSCU staff responsible for planning, acquisition, configuration, deployment, management, and auditing of information systems should apply sound risk management practices when selecting security controls. This would include identifying what information is intended to be protected, what the threats are to that information or information system resources, and the proper cost-effective safeguards that need to be applied to adequately protect the information.

The ConnSCU Security Policy is a set of statements that articulates the overall intention and direction of the ConnSCU Information Security Program as determined by the Board of Regents. This policy is technology neutral and represents an ideal state. Some statements may apply primarily to users, some may apply mainly to staff members with responsibility for technology, and some may apply to both.

B. Purpose

The ConnSCU Security Policy defines the goals and components of ConnSCU Security Program and all supporting structures. It represents a commitment to implement secure practices and procedures. This document will be used as the basis for making other lower level information security decisions. High-level security policy should not need to be changed frequently.

Security polices require the development, promulgation, implementation of standards, procedures, guidelines and on-going operational assurance or the policy to be considered complete. A security policy is not considered effective until all of the components of the policy have been completed.

Once this policy has been established it should be clearly communicated to users, staff, and management. A ConnSCU Information Security Manual must be developed, with separate sections providing security standards, procedures and guidelines for users and for staff.
responsible for information technology. All personnel must sign a statement indicating that they have read, understood, and agreed to abide by the policy, standards procedures, and guidelines.

C. Scope
The ConnSCU Information Security Policy outlined in this document applies to:

**Users:** All employees, faculty, staff, students, visitors and all others who utilize the electronic and non-electronic information resources of the ConnSCU

**Third Party Contractors:** will be provided a copy / link of this policy and all contractors should be compliant with the terms of this policy.

**Information Resources:** All data created stored, maintained, processed or transmitted by the ConnSCU as well as all internal and external networks, computing platforms, systems, software, hardware, equipment and facilities either owned or leased by the ConnSCU.

D. Policy Authority
This policy is issued by the Board of Regents for Higher Education for the ConnSCU.

E. Definitions
TBD after completion of initial review and identification of terms requiring definition by ITPC

F. Approval and Change Processes
It is vital that ConnSCU maintain an environment which provides its constituents a secure and protected technology environment, wherein policies, standards, procedures and guidelines are updated regularly. Changes to the ConnSCU environment would potentially introduce new security risks. It is important; therefore, that any changes in the technology environment be reviewed for information security impact before significant effort is undertaken in the acquisition or implementation of that change and part of the change control process.

In this context, a "change" can be one of the following:

- Any change in ConnSCU polices that require modification of security policies.
- Any change in the overall security environment that requires new measures to be deployed to keep the ConnSCU environment secure.
- The acquisition of a new software utility or application providing access to a data repository where protected data is maintained.
- Any modification to existing IT infrastructure including transmission, encryption, management or monitoring of the network.
The ConnSCU Board of Board of Regents must approve changes to the ConnSCU Information Security Policy. The changes shall be reviewed by the BOR President or his/her designee(s) and presented to the Board of Regents for its action.

The BOR Chief Information Officer or his/her designee must approve specific security standards, procedures and guidelines. Such approval will be provided in writing and reflected in ConnSCU Security Manuel. The BOR CIO will establish a mechanism for developing or modifying security policies, standards, procedures and guideline.
### G. Roles & Responsibilities

The tables below outline the roles and associated responsibilities in support of information security within ConnSCU:

- ConnSCU Board of Regents
- College & University Presidents
- BOR Chief Information Officer
- College & University Senior IT Leaders
- College & University Senior Administrators/Data Stewards
- Data Managers
- General Users of ConnSCU Information Resources

<table>
<thead>
<tr>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **Board of Regents** | a. Review & approve the ConnSCU Information Security Policy and all subsequent changes.  
b. Endorse the development and implementation of the ConnSCU Information Security Program across all colleges and universities.  
c. Oversee the security of all ConnSCU information resources. |
| **College & University Presidents** | a. Implement and maintain the ConnSCU Information Security Program at their respective institutions and ensure compliance with appropriate federal and state regulations.  
b. Ensure appropriate budgetary, staffing and training resources are established for the program.  
c. Designate data stewards responsible for ConnSCU information resources.  
d. Ensure Business Continuity. |
| **BOR Chief Information Officer** | a. Establish a mechanism for developing and modifying ConnSCU security policies, standards, procedures, and guidelines.  
b. Review & approve the ConnSCU security standards, procedures, guidelines, and all subsequent changes.  
c. Oversee all investigations and responses related to unauthorized access and/or disclosure of sensitive information as well as all computer security incidents.  
d. Establish a process to continuously assess and improve the quality and effectiveness of the ConnSCU Information Security Program  
e. Apprise the BOR President and Regents of unmitigated
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **College & University Senior IT Leaders**| a. Lead the implementation of ConnSCU Information Security Program at their respective institutions.  
b. Apprise of potential security breaches  
c. Apprise the Presidents of all unmitigated risks in privacy and security at their respective institutions.  
d. Assist in the development of ConnSCU security policies, standards, procedures, and guidelines. |
| **ITPC**                                 | a. Creates, maintains, and modifies IT Policy and recommends changes to the Board of Regents. |
| **College & University Senior Administrators/Data Stewards** | a. Serve as Data Stewards for their respective units.  
b. Understand their role and responsibilities in the preparation and execution of their unit's Business Continuity Plan.  
c. Determine who should have access to information resources within their jurisdiction, and what those access privileges should be (e.g., to read, to update, to print). Such access will be consistent with the Access Control and Data Security sections.  
d. Ensure a risk assessment is performed annually on assigned information assets.  
e. Implement the appropriate internal procedures for their units based on the risk assessment.  
f. Ensure that staff members within their units are trained and understand their security responsibilities.  
g. Ensure that staff members within their unit are in compliance with data management policies, standards and procedures |
| **Data Managers**                         | a. Process, store, and protect the institution data as specified by the Data Stewards of their respective units.  
b. Inform Data Stewards, college/university IT department, and/or BOR Information Security Office of any known security issues or incidents as soon as they become aware.  
c. Classify information assets with respect to confidentiality, integrity and availability  
d. Ensure that a backup and recovery process is in place for the information asset. |
| **General Users**                         | a. Adhere to all ConnSCU information technology policies.  
b. Inform college/university IT department and/or BOR Information Security Office of any known security issues or incidents as soon as they become aware. |
c. Cooperate with any security related investigations, processes, or procedures necessary to keep the ConnSCU information systems secured.

H. General Security Policy

The ConnSCU shall implement a comprehensive security program that applies to all colleges and universities. The BOR Chief Information Officer will establish a mechanism to develop or modify security standards, procedures, and guidelines in support of the implementation of the ConnSCU Security Program. The BOR Chief Information Officer will also establish a mechanism to continuously assess and improve the quality and effectiveness of the ConnSCU Security Program. The following represents a minimum set of logical and technology security controls shall be implemented at all ConnSCU locations. Each college or university may further enhance its protection with additional security controls.

H.1 Asset Management

The purpose of asset management is to ensure that ConnSCU information resources are identified, assigned a steward, and classified. Assets are resources that have value to an institution and must be protected. Assets include data (i.e., information) and the resources used to manage it during the data life cycle, i.e. usage, transmission, storage and disposal.

- Colleges and Universities shall maintain up to date records of mission critical information assets and their supporting resources.
- Senior administrators at colleges and universities shall serve as data stewards for their respective units.
- Data Stewards will ensure that ConnSCU information resources are classified according to the classification guidelines as follows:
  - Data Classification Level 3 (DCL3) – Data protected by legal requirements such as Gramm-Leach-Bliley Act (GLBA) and require a notification be issued if data is potentially compromised
  - Data Classification Level 2 (DCL2) – Data protected by legal requirements such as FERPA.
  - Data Classification Level 1 (DCL1) – Data protected by contractual obligation, such as details of research, information covered by non-disclosure agreements, or financial transactions not considered restricted data
  - Data Classification Level 0 (DCL0) – Data protected at the discretion of the owner, such as general university information, campus maps, or directory data
H.2 Risk Management

The purpose of Risk Management is to ensure that appropriate controls and countermeasures have been implemented to reduce risk to ConnSCU information resources to a level acceptable to the management.

- Colleges and universities shall conduct risk assessment exercise annually or whenever there is a significant change of operation environment.
- The data stewards shall define acceptable risk for a given asset and work with college/university IT department or BOR Information Security Program Office to implement procedures to eliminate or mitigate the risk.

H.3 Access Management

Access management is intended to ensure the confidentiality, integrity and availability of ConnSCU information resources through the development and implementation of well-defined access control processes and procedures.

- The BOR Information Security Program Office shall establish standard rules and procedures for granting, managing and removing user rights to access ConnSCU information resources.
- Each user shall have a user identifier (ID) that is unique within the ConnSCU environment. Whenever possible, physical verification of the user should be made before assigning a user identifier (ID).
- BOR resources should employ a strong authentication process as best practice and employ a means to verify a user’s identity.
- The access control process shall be based on the premise that access to ConnSCU Information Resources is prohibited unless expressly granted.
- Access control rules and rights for various types of users shall be reviewed at least annually by data stewards in conjunction with the college/university IT department.
- Privileged access to systems includes access beyond the normal scope shall be granted to individuals based on the minimum required to fulfill their job responsibilities and only for the period of time they are needed.

H.4 Data Security

The policy in this section is intended to ensure that ConnSCU data is secured with respect to confidentiality, integrity and availability during all phases of the data life cycle, i.e. usage, transmission, storage, and disposal. Data security practices are designed to protect information regardless of its form (e.g., electronic, viewable on monitors, print).

- Access to the ConnSCU data shall be granted as specified by the data stewards.
• Encryption and message authentication will be applied to protected and sensitive information transmitted and stored on the ConnSCU network.
• Encryption will be used on DCL3 data stored in devices that are removable from a ConnSCU location.
• Only encryption methodologies approved by BOR Information Security Program Office will be used.
• Sensitive or proprietary ConnSCU encrypted files will have the encryption keys or tokens held in escrow by BOR Information Security Program Office or its designated representatives.
• ConnSCU data will be accessed, stored and transmitted only using secured approved methods. BOR Information Security Program Office, in conjunction with college/university IT department, shall develop and implement a process for data access, storage and transmission.
• Data stored electronically on surplus computer equipment will be destroyed in accordance with ConnSCU Procedure Disposal of Surplus Property.”

H.5 Physical Security

Physical security is essential for the protection of ConnSCU data. If protected data is stored in systems in unsecured locations all electronic security measures can be rendered ineffective through physical access to the system.

• Visitors or employees in operational areas such as the Data Center should be challenged to prove identity.
• Locking and checking procedures will be established, as provided in the ConnSCU Security Program Manual.
• Access to critical system components should be restricted to a small number of individuals (usually the administrator and backup personnel).
• A backup power source and other line conditioning equipment should be installed to protect network components against power failures, power surges, brownouts, line noise, etc.
• Critical IT infrastructure components will be located in a locked room to which access is restricted and monitored.

H.6 Host & Operating System Security

Policies in this section are intended to prevent unauthorized access to and maintain maximum availability of host and/or operating systems.

• A designated individual or group will be clearly identified to administer and maintain the host and operating system throughout its lifecycle.
• The BOR Information Security Program Office, in conjunction with college/university IT department, shall develop and implement a process to identify, assess, approve and install software on ConnSCU owned equipment.
• All software installed and used must be in accordance with license agreements.
• Prior to adding a new host to the production network, the IT department should conduct vulnerability assessment and security testing.

H.6.1 Malicious Software Protection

Securing systems against the introduction of malicious software will require proper system controls, security awareness training, and change management procedures. Malicious software includes but is not limited to computer viruses, computer spyware, network worms, trojan horses, and denial of service attacks.

• Use of unauthorized software will be prohibited.
• The software and data content of mission-critical systems shall be reviewed periodically to detect the presence of unauthorized files, either executable or data.
• When possible files from unknown sources shall be reviewed before use.
• Whenever possible, application level firewalls will be installed on all hosts or operating systems.
• Whenever possible, intrusion detection/prevention software will be installed on all hosts or operating systems.
• Whenever possible, anti-virus software will be installed and updated on all hosts or operating systems as necessary.
• Whenever possible, anti-spy ware software should be installed and updated on all hosts or operating systems as necessary.
• The BOR Information Security Program Office will establish a mechanism to warn ConnSCU community of malicious software.
• Hosts and operating systems will be monitored and security events will be recorded/logged.
• Log files shall be reviewed regularly as recommended by BOR Information Security Program Office. Log files will be maintained for a period of specified time or as required by law. Log files will be secured to prevent unauthorized alterations.

H.6.2 Patch Management

Patch management includes procedures for identifying, evaluating, approving, testing, installing, and documenting patches.
The BOR Information Security Program Office, in conjunction with college and university IT departments shall develop and implement patch management procedures.

Each IT department shall designate administrator(s) to evaluate, assess and implement patch management for the hosts and operating systems in their control.

System monitoring should be used to check the effectiveness of patches adopted and to verify conformity to security standards.

H.7 Software Security

Security penetrations most often capitalize on weaknesses in software and the use of information generated by the software.

- The BOR Information Security Program Office shall provide guidelines to ensure that, prior to introducing any software application into the operational ConnSCU environment, the software conforms to the ConnSCU information security standards.
- All information systems media, such as disks and CD-ROMs introduced to the ConnSCU environment, will be scanned for malicious code. Code that has been vetted and approved for use in the production environment must be archived on appropriate media, and archived for reference and backup and/or restoration purposes.
- All software used on the ConnSCU must be used in concert with its license. Software covered by the GNU Public License must be treated as licensed software.
- All open source/freeware must be assessed and approved by BOR Information Security Program Office, or in conjunction with college/university IT department, prior to installation on the ConnSCU systems.
- Data input to applications should be validated to ensure that the data is correct and appropriate.
- Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
- Regular system scanning and verification of application vulnerabilities should be performed.

H.8 Data & System Backup

The policy in this section is intended to ensure the integrity and availability of ConnSCU electronic data by protecting it from loss or corruption due to events such as natural or man-made disasters, system or hardware failures and human errors.

- All ConnSCU production systems and information will be backed up on a regular basis.
- A system backup shall be performed before and after major changes to any operating system, system software or applications.
• A record of all backup processes performed, including verification of their success, shall be maintained.
• IT departments shall define and document backup procedures for various ConnSCU production systems.
• Backup media shall be tested regularly to ensure that it is reliable, complete and efficient. Restoration procedures shall be documented and tested regularly to verify effectiveness and to ensure their completion within the time allotted.
• All network backup procedures shall only be performed on ConnSCU owned or the trusted network.
• A copy of the backup media shall be available on-site to ensure current data is readily available. At least one copy of the backup media shall be stored at an off-site location. The offsite storage location will be at a distance sufficient to avoid damage from a disaster at the main site.
• The security controls (i.e. logical and physical security) applied to the onsite and offsite backup information and resources shall be at least as strong as the primary resource.
• Service level agreements shall be required for any contract with an external vendor that provides off-site storage of data (e.g., response time). Backup media will be retrievable within a procedurally defined period of time. All recovery requests should be documented.
• The retention period for backups shall meet the legal or statutory requirements.

H.9 IT Infrastructure Management & Monitoring

The policy in this section are intended to ensure that appropriate controls are being followed and are effective in ensuring the integrity and availability of ConnSCU IT Infrastructure. This is accomplished through monitoring and intrusion detection processes that are used to identify and document unauthorized activity as well as information faults and exceptions.

• IT infrastructure standards and configurations shall be documented in the ConnSCU Security Program Manual. The standards will be based on best practices and reviewed regularly to ensure compliance with current standards.
• All changes to the ConnSCU IT Infrastructure shall be authorized only through the BOR change control management process.
• The BOR IT management team, in conjunction with college and university IT departments, will maintain a formal inventory of IT components and will check the configuration(s) regularly to ensure that all components/devices attached to the network are authorized.
• The BOR IT management team, in conjunction with college and university IT departments, shall conduct risk analysis or security assessment whenever significant changes to the IT infrastructure occur.
• Physical access to the network hosts need to be limited to authorized IT management personnel and secured. The servers, backup facilities, UPS, network switches, etc.
should be installed in locked areas that are only normally accessible to the Operations organization.

- The BOR network management team, in conjunction with college and university IT departments, shall implement procedures to monitor IT infrastructure and detect and alert unauthorized activities.
- The BOR IT management team, in conjunction with college and university IT departments, shall implement audit logs recording user activities, exceptions, and information security events. The logs shall be reviewed regularly and kept for a designated period or as required by law.
- Request to attach a new network to ConnSCU network shall be reviewed by the BOR Information Security Program Office, in conjunction with college/university IT department. An inspection of the new network should be conducted in order to determine whether the connection would introduce any security weaknesses to the ConnSCU network.
- Secure remote connections such as Virtual Private Networks (VPN) and Secure Sockets Layer (SSL) shall be implemented for access to all ConnSCU information deemed confidential and sensitive. Guidelines and restrictions on the effective use of such connections should be included in college and university remote access policies and procedures.
- User access to IT infrastructure services shall be based on level of authorized use.
- A bandwidth management system shall be used to monitor and control bandwidth usage. Quality of Service (QoS) should be implemented for mission critical applications.

**H.10 Business Contingency/Service Recovery**

The Business Contingency/Service Recovery (BC/SR) Planning counter-acts interruptions to business activities, to protect mission critical processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. The IT Business Contingency/Service Recovery Plan is an integral part of, and should be incorporated in, any overall Crisis Management Plan of colleges and universities.

- Each college/university IT department shall develop an IT Business Contingency/Service Recovery plan that will enable institution to provide IT services to its students and enable employees to continue performing critical business functions for different levels of severity of service disruption.
- The IT BC/SR Plan will be reviewed annually. Within reasonable limits of funding, time, and resources, the IT BC/SR Plan will be exercised on an annual basis. Results of such testing will be reported to BOR Information Security Program Office.
H.11 Communication and Operations Management

Communication and Operational Management is a process that ensures that any change made to an Information Resource is documented, reviewed and approved. It encompasses both larger planned changes such as projects and smaller reactive changes such as software patches and unscheduled server boots. Operational Management also encompasses environmental changes (e.g., HVAC, power and building access that might affect resource availability). Change management minimizes the adverse consequences caused by changes to ConnSCU information resources.

- Operating procedures should be documented, maintained and made available to all users who need them.
- Formal change control procedures are required for all ConnSCU production systems house at BOR and/or colleges and universities.
- An approved Emergency Configuration Change Process can be used when changes are required on the fly due to outages, or to restore or ensure operations.
- Configuration management shall be implemented to control and maintain the documentation of the baseline of data, hardware, software, networks, and procedures, records of property control and audits of inventory items for all ConnSCU production systems.
- Duties and areas of responsibility should be segregated to reduce the opportunities for unauthorized or unintentional or misuse of the organization’s assets.
- Services delivered by third parties need to have appropriate security controls, service definitions and agreements need to be operational reviewed for compliance on a regular basis.
- Resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

H.12 Incident Management

Incident management is to ensure that the identification, management and reporting of information security incidents occur in a consistent and timely manner. Incident management includes the effective and timely reporting of and response to security incidents and vulnerabilities as well as the evaluation of event data to reduce and/or mitigate future occurrences.

- The BOR Information Security Program Office shall define and implement incident management procedures for a set of critical security incidents.
- Colleges and universities shall implement local incident management procedures that complement BOR’s procedures.
• The BOR Chief Information Officer shall oversee all investigations and responses related to unauthorized access and/or disclosure of sensitive information as well as all computer security incidents to minimize risk to BOR and its institutions.
• Each institution shall name a point of contact for the reporting of information security incidents and coordinating incident responses with BOR Information Security Office. This point of contact, along with their designated backup, shall be clearly communicated to the campus community.
• All ConnSCU employees and students are expected to cooperate with any security incident investigation.

H.13 Security Awareness and Training

Each ConnSCU institution shall incorporate the Information Security Policy as part of the terms and conditions for issuing institution computer network accounts. Each ConnSCU institution shall have all full-time and part-time employees, including student employees, acknowledge that they have read and understand their roles and responsibilities with respect to information security. Each ConnSCU institution shall make the Information Security Policy accessible to all employees and students.

The BOR Information Security Program Office shall coordinate security awareness training for all colleges and universities. All ConnSCU employees, including student employees, students and contractors should receive appropriate security awareness training. Some Employees shall receive additional training as appropriate to their job functions. Security awareness training must comply with meeting Federal and State Requirements.

I. Assurance

The BOR Chief Information Officer is responsible for developing a mechanism to continuously assess and improve the quality and effectiveness of the ConnSCU Information Security Program.

• The BOR Information Security Program Office is responsible for reviewing relevant statutory, regulatory, and contractual requirements and developing the organization’s approach for documenting and verifying the requirements are meet.
• ConnSCU records need to be protected from loss, destruction, and falsification, in accordance with State of Connecticut and federal record retention requirements.
• The BOR Information Security Program Office is responsible for the security testing of the ConnSCU infrastructure. This is done at regular intervals of functional testing and penetration testing.
• The IT departments at BOR, colleges, and universities are responsible for on-going systems monitoring to ensure that any attempts, whether successful or unsuccessful, to gain unauthorized access or to make unauthorized changes to a computer system, are identified and investigated in a timely manner.
• The BOR Information Security Program Office along with the BOR IT staff shall conduct security self-assessment or Risk Analysis at regular intervals to identify any weaknesses in IT security scheme.
• The BOR Information Security Office shall cooperate with internal and external audit in areas of security reviews, inspections, and assessments.
• Responsibilities for notifying IT of employment termination or change of employment should be clearly defined and assigned.
• The access rights of all employees, contractors and third party users to ConnSCU systems and facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

J. Reporting

Each ConnSCU institution shall annually provide the Board of Regents a report detailing the security controls implemented at their locations. The BOR Information Security Program Office will develop and maintain a reporting structure covering the controls outlined in this Policy.

K. Exception Process

ConnSCU recognizes that some portions of the Security Policy may have to be adjusted 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.
2. The exception does not disrupt or compromise other portions of the ConnSCU service delivery capability.
3. The implementation of the exception is vetted through the Change Management Process.
4. BOR Information Security Program Office, in conjunction with college/university IT department, is able to establish a monitoring function to assess the operations of the implementation exception.
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.)
6. The BOR Information Security Program Office shall define an exception request process and communicate to all ConnSCU users.

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.

L. No Expectation of Privacy

All activities involving the use of ConnSCU IT systems are not personal or private. Therefore users should have no expectation of privacy in the use of these resources. Information stored,
created, sent or received via ConnSCU IT systems is potentially accessible under the Freedom of Information Act. Pursuant to Public Act 98-142.

In addition, the State of Connecticut’s “Electronic Monitoring Notice” reserves the right of the Board of Regents to monitor and/or log all activities of all users using ConnSCU IT systems without notice. This includes, but is not limited to, files, data, programs and electronic communications records without the consent of the holder of such records.

M. **Enforcement**

Violations of information security policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws, as well as ConnSCU Policies, General Rules of Conduct for College and University Employees, applicable collective bargaining agreements, and the ConnSCU Student Conduct Codes.

For purposes of protecting the ConnSCU network and information technology resources, the Information Security Office may temporarily remove or block any system, device, or person from the ConnSCU network that is reasonably suspected of violating ConnSCU information security policy. These non-punitive measures will be taken only to maintain business continuity and information security, and users of the college/university information technology resources will be contacted for resolution.

N. **Review**

This policy will be reviewed at least every three years by the ITPC. ITPC, if necessary, will make recommendation of changes to the ConnSCU Board of Regents,