CONNECTICUT STATE COLLEGES & UNIVERSITIES
BOARD OF REGENTS FOR HIGHER EDUCATION

BOR INFORMATION TECHNOLOGY COMMITTEE

Friday, June 7, 2013, 1:00 p.m. to 3:00 p.m.
61 Woodland Street, Hartford, CT 06105
2nd Floor, Room 238

AGENDA

1. ***Approval of Minutes from April 5, 2013**
2. **BOR CIO Report**
3. ***Approval of IT-001 and IT-002 Revisions**
4. ***Approval of Expedited Approval Process for Interim Security Policies**
5. **Move to Executive Session**
   Review of Information Security Program Implementation
6. **Adjournment**

*=attachment

BOARD OF REGENTS FOR HIGHER EDUCATION
INFORMATION TECHNOLOGY COMMITTEE
Meeting Minutes – 11:30 a.m., Friday, April 5, 2013
Board of Regents, 61 Woodland Street, Hartford, CT

REGENTS PRESENT
Nicholas M. Donofrio, Chair
Matt Fleury
Michael Pollard

BOR STAFF
Wendy Chang, Chief Information Officer
Jeff Clark, Security Program Manager
Susan Grant, Senior Finance Officer – Accounting System Support
Terry O'Brien, Contract Compliance Officer
Karen E. Stone, Internal IT Auditor
Anna Prusak, ITS support staff

ConnSCU REPRESENTATIVES
James Estrada, CCSU
George Claffey, COSC
Roger Ferraro, Capital CC
Lynn Gregor, Asnuntuck CC
Joe Tolisano, ECSU
Ken Spelke, SCSU
Tom DeChiaro, WCSU

CALL TO ORDER

Chair Donofrio called the meeting to order at 11:30 a.m.

1. **APPROVAL OF FEBRUARY 25, 2013 MINUTES**
   Dr. Tolisano requested that the minutes be amended to better reflect Regents' emphasis on collaboration. After much discussion, Chairman Donofrio reiterated his statement with the following sentence:

   There is only one head of IT for the ConnSCU System and that is Wendy Chang. I as the Chair of the IT Committee of the Board of Regents for Higher Education support an open and collaborative approach to IT governance for the ConnSCU System where all constituents' ideas, thoughts, issues and impact are considered and factored into every decision.

   Representatives from all factions associated with IT in the ConnSCU system are always welcome at our meetings. It is my expectation that the six CIOs as well as the IT Directors will all work together in a collaborative and open manner. While there are management structures in place to resolve issues, we are fully prepared to engage as, where and when needed.

2. BOR CIO GENERAL STATUS REPORT

Each CIO and college representative provided an update on selected projects:

BOR:

Dr. Chang reported that System Office has approximately 60 collaborative projects under way. 1/3 of those are in construction; 1/3 in infrastructure (Telecom, network); and 1/3 in other initiatives. Every quarter, BOR IT produces a dashboard report providing a high level status summary of those projects. Regent Pollard requested that when the dashboard is forwarded to the BOR IT Committee, it includes 'Dashboard' in the e-mail subject line. Of current projects, Dr. Chang highlighted:

eTranscript – collaboration effort with State Dept. of Education (SDE) to replace paper/PDF process with electronic format which can be imported directly to Banner (ConnSCU's ERP). SDE and selected vendor, Pearson, created a transcript interface in the cloud. Approximately 60% of CT K12 districts already utilize Pearson technology for their Student Information Systems (SIS). SDE is tackling those districts first. The other 40% of K12 districts use other systems. There is no K12 technology standard. Dr. Chang explained that ConnSCU testing is expected to wrap up by the end of April. The next step will be for SDE to bring the 60% of K12 Pearson users on board with eTranscript. The anticipated timeline is 18 months. Current eTranscript deployment phase does not include support for Naviance.

The product will speed up the transcript process and enable ConnSCU IR to analyze the data. Chair Donofrio asked Dr. Chang to ensure that Maguire Associates, a consulting firm hired to study declining enrollment at ConnSCU, understands benefits of the effort.

Mr. DeChiaro observed that a more broad approach to recruitment is needed. For example, currently, WCSU receives SATs and transcripts from students who never submit applications. No one follows up to determine why. WCSU plans on working with Maguire Associates to review its recruitment processes.

Chair Donofrio inquired if all sites utilize Common Application: ECSU does; SCSU is considering it. Community Colleges have open enrollment; consequently Common Application is not applicable to them. Mr. Tolisano stated that ECSU's applicant pool went up 50% with the Common App. Chair Donofrio noted that increase of applicant pool is good; understanding whether the yield increased is very important. Mr. Tolisano offered to share ECSU's interface to Banner for interested parties. Participation in Common App requires membership in Common Application Association. There is a considerable wait period.

P20-WIN – collaboration between BOR and SDE. The project is led by Department of Labor in collaboration with the State IT. BOR IT is working with IR to collect Preschool through 20 data for an education-workforce central repository. The system is expected to become available this summer. Next step will involve entering data and determining the owner and responsibility for maintaining the data.

Chair Donofrio stated that for CT to be special, it needs to track its students from enrollment to employment. Very few CT students come to ConnSCU for self-actualization. ConnSCU also needs to do a better job keeping track of alumni. Currently, contact is maintained with only approximately 20% of alumni.

The National Clearinghouse can tell where ConnSCU's dropouts re-enrolled. For alumni tracking - strategic planning has been suggested. Mr. DeChiaro noted that WCSU is in the process of migrating data to Raiser's Edge, donor relationship management software.

Chair Donofrio suggested engaging Maguire Associates in the conversation by adding them to the BOR IT agenda.

WCSU:

Network Infrastructure Upgrade – 18-24 months project; part of Security Initiative. Requires DCS involvement. Funding to be provided by BOR.

DR/Business Continuity – identification and full replication of key services campus-to-campus, use of Exagrid and load balancing.

Backup tapes continue to be used to some degree at ConnSCU. Ms. Stone confirmed that, currently, they are being encrypted.

ECSU and WCSU each have SANS on their sites and they are looking into replicating to each other.

Cyber Security – WCSU does not have a CISO.

Recruitment to Graduation – mapping & reengineering of the process.

Mr. DeChiaro proceeded to a shared governance model proposed by University and Charter Oak CIOs. Chair Donofrio emphasized that a new President will be named soon and that he will have final say on the governance. The good of the system must be the #1 goal. Regent Fleury asked if colleges were involved in the discussion. Mr. DeChiaro replied that there have been some discussions with colleges.

ECSU:

Luminis – working on an online presence for alumni. This is a 3 year project. When logged on, students will see classes and schedule. Alumni will see lectures, athletic events, etc. Lifetime e-mail facilitates the project.

SCSU:

Student Success – a new initiative for use of predictive analytical tools to help advisors work closer with undergraduate students. Scheduled for production this summer. It is a perpetual system. Chair Donofrio asked that Mr. Spelke reaches out to President Nuñez, a co-chair of EPAC – a state mandated group of people looking for this kind of initiatives.

Asnuntuck

Manufacturing Technical Program – Considered a model in CT. Students have 96% rate of getting a job. Currently managing technical expansion – relocating WACC TV station to enlarge manufacturing. Moving main equipment room for growth. Rely on BOR IT resources and sister institutions.

FootPrints Help Desk – just went into production this past week.

Capital

Phone & Network Upgrade – heavy reliance on BOR IT. Currently, waiting for a phone & network upgrade. This is an 18 month project. Network and Phone are not in a totally bad shape.

Backups & Virtualization. Working on backups with Three Rivers on backups. Cont. Ed programs' computer labs need to be as flexible as possible. Desktop storage will be removed; monitors will be attached to the network. VDI can't be rolled out further until network is upgraded

Charter Oak

6-month Security Initiative – Re-architecture of core network and phone systems. This weekend will mark final milestone.

For CCC, network and phones tie together. At CSUS, universities manage local network; SO connects everyone together. The phone system will be VoIP. CCC and Charter Oak utilize Cisco. CSUS has not yet picked a phone vendor; currently, it uses Avaya. Converting from Avaya to Cisco presents a complication.

CT Ed Academy – Charter Oak submitted a proposal to establish CT Ed Academy to digitize state's current training assets.

3. IT POLICY REVISION OF BOR IT 001 (ACCEPTABLE USE POLICY) AND 002 (ELECTRONIC COMMUNICATION)

Requested changes need to be reviewed by Internal Counsel. Item has been tabled. It will be reviewed at the next meeting.

4. MOVE TO EXECUTIVE SESSION – EVALUATION OF CCC INFORMATION SECURITY PROGRAM

5. RETURN TO OPEN SESSION

ADJOURN

With no further business to consider, the meeting adjourned at 2:30PM.

Submitted,

Anna Prusak

ITEM

Approval of the revisions concerning IT-001 Acceptable and Responsible Use of Information Technology and Resources Policy and IT-002 Electronic Communication Policy for the Board of Regents for Higher Education and its Institutions.

RECOMMENDED MOTION FOR FULL BOARD

RESOLVED, that the Board of Regents hereby approves the revised versions of IT-001 Acceptable and Responsible Use of Information Technology and Resources Policy and the IT-002 Electronic Communication Policy for the Board of Regents for Higher Education and its Institutions.

BACKGROUND

The two policies were approved by the full Board on October 18, 2012. In response to the concerns brought forward by AAUP, the IT Policy Committee added statements in the Privacy section that reference to the collective bargaining agreements. The Committee also added new definitions to further clarify the roles and responsibilities.

CONNECTICUT STATE COLLEGES & UNIVERSITIES
BOARD OF REGENTS FOR HIGHER EDUCATION

Policy, Standard, Procedure, Guideline

Policy Number	IT-001
Description:	Acceptable and Responsible Use of Information Technology and Resources
Applies To:	Faculty, Staff, Students, and Contractors
Contact Information:	Information Security & Policy Program Office, Office of Information Technology

Approved on Date:	10/18/2012	Effective Date:	10/18/2012
Last Modified Date:	05/28/2013	Next Review Date:	10/01/2015

Introduction

This Policy governs the Acceptable and Responsible Use of Information Technology and Resources of Connecticut State Colleges and Universities (ConnSCU). Information Technology (IT) resources are a valuable asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate academic and administrative use.

The usage of ConnSCU IT resources is a privilege dependent upon appropriate use. Users of ConnSCU IT resources are responsible for using IT resources in accordance with ConnSCU policies and the law. Individuals who violate ConnSCU policy or the law regarding the use of IT resources are subject to loss of access to IT resources as well as additional ConnSCU disciplinary and/or legal action.

This policy represents a minimum set of requirements that shall be implemented at all ConnSCU locations. Any ConnSCU institution that is responsible for the operation controls of the IT resources may further enhance the policy with additional restrictions that apply to its own local institution environment.

Purpose

The purpose of this policy is to provide the ConnSCU community with common rules for the usage of IT resources.

The intent of this policy is to provide information concerning the appropriate and inappropriate use of ConnSCU IT systems to:

- Ensure ConnSCU IT resources are used for purposes consistent with ConnSCU mission and goals;
- Prevent disruptions to and misuse of ConnSCU IT resources;
- Ensure ConnSCU community is informed of state and federal laws and ConnSCU IT policies governing the use of ConnSCU IT resources and;
- Ensure IT resources are used in a manner, which comply with such laws and policies.

Scope

This Policy applies to:

- All IT resources owned or managed by the ConnSCU;
- All IT resources provided by the ConnSCU through contracts and other agreements with the ConnSCU; and
- All users and uses of ConnSCU IT resources.

Policy Authority

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

Definitions

Knowledge of the following definition is important to understanding this Policy:

- IT Resources: This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and electronic communication.
- ConnSCU authority: The President or his/her designees of the institution that operationally manages the IT resources or data.

Provisions

To adhere to the Acceptable and Responsible Use policy, users of ConnSCU IT resources must:

- Use resources solely for legitimate and authorized administrative and academic purposes.
- Ensure that any personal use of ConnSCU IT resources be limited and have no detrimental impact on institution operations, job performance or ConnSCU IT resources.
- Protect their User ID and IT resources from unauthorized use. Users are responsible for all activities on their User ID or that originate from IT resources under their control.
- Access only information that is their own or is publicly available or to which authorized access has been given by the appropriate ConnSCU authority.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Use shared resources appropriately. (e.g. refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources).

To adhere to Acceptable and Responsible Use policy, users of ConnSCU IT resources must **NOT**:

- Use ConnSCU IT resources to violate any ConnSCU policy or state or federal law.
- Use another person's ConnSCU User ID or password without prior authorization from the appropriate ConnSCU authority.
- Use another person's ConnSCU IT resource, files, or data without prior authorization from the owner or appropriate ConnSCU authority.
- Have unauthorized access or breach any security measure including decoding passwords or accessing control information, or attempt to do any of the above.
- Engage in any activity that might be harmful to IT resources or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to computer data.
- Make or use illegal copies of copyrighted materials or software, store such copies on ConnSCU IT resources, or transmit them over ConnSCU networks.

- Harass or intimidate others or interfere with the ability of others to conduct ConnSCU business.
- Directly or indirectly cause strain on IT resources such as downloading large files, unless prior authorization from the appropriate ConnSCU authority as determined by the institution is given.
- Use ConnSCU IT resources for unauthorized purposes may include but are not limited to, the conduct of a private business enterprise, monetary gain, commercial, religious or political purposes.
- Engage in any other activity that does not comply with the general principles presented above.

No Expectation of Privacy

ConnSCU IT systems and resources are the property of the State of Connecticut and use thereof by the user is restricted to the performance of official State business or activities approved through the collective bargaining process.

Pursuant to Communications Assistance for Law Enforcement Act (CALEA), Public Act 98-142, and the State of Connecticut's "Electronic Monitoring Notice", information related to usage and utilization of ConnSCU IT systems and resources is constantly being collected and logged. While IT personnel do not review the contents of this information except when necessary in the course of the discharge of official duties and as permitted by law, all users should know that such information is subject to subpoena, discovery, the Connecticut Freedom of Information Act and such other disclosure processes as may be authorized by law.

Assurance

Each ConnSCU institution shall incorporate the Acceptable and Responsible Use 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 the Acceptable Use Policy. Each ConnSCU institution shall make the Acceptable Use Policy accessible to all employees and students.

Enforcement

Violations of ConnSCU Acceptable and Responsible Use 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 all colleges 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 BOR Information Security Program Office, in conjunction with college/university IT department, may

temporarily remove or block any system, device, or person from the ConnSCU network that is reasonably suspected of violating ConnSCU information technology policy. 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 resolution.

Exception Process

ConnSCU recognizes that some portions of the Acceptable and Responsible Use of Information Technology Resources 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 appropriate ConnSCU authority as specified in the provisions above. All other exceptions shall be approved by the BOR CIO or designee.
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. The 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.)

Exception Request

To request an exception, please submit the Information Security Exception request to SecProg@ct.edu

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.

Review

This policy will be reviewed every three years by the Board of Regents.

CONNECTICUT STATE COLLEGES & UNIVERSITIES
BOARD OF REGENTS FOR HIGHER EDUCATION

Policy, Standard, Procedure, Guideline

Policy Number	IT-002
Description:	Electronic Communication
Applies To:	Faculty, Staff, Students and Contractors
Contact Information:	Information Security & Policy Program Office, Office of Information Technology, Board of Regents

Approved on Date:	10/18/2012	Effective Date:	10/18/2012
Last Modified Date:	05/28/2013	Next Review Date:	10/01/2015

Introduction

The Connecticut State Colleges and Universities (ConnSCU) encourages the use of electronic communications to share information and knowledge in support of ConnSCU mission and goals. To this end, ConnSCU provides and supports interactive, electronic communications resources and services.

The usage of ConnSCU IT resources is a privilege dependent upon appropriate use. Users of ConnSCU IT resources are responsible for using IT resources in accordance with ConnSCU policies and the law. Individuals who violate ConnSCU policy or the law regarding the use of IT resources are subject to loss of access to IT resources as well as additional ConnSCU disciplinary and/or legal action.

This policy represents a minimum set of requirements that shall be implemented at all ConnSCU locations. Any ConnSCU institution that is responsible for the operation controls of the IT resources may further enhance the policy with additional restrictions that apply to its own local institution environment.

Purpose

The purpose of this Policy is to:

- Promote the use of electronic communication as an official means of communication within ConnSCU
- Ensure that ConnSCU electronic communications resources are used for purposes appropriate to the ConnSCU mission and goals;
- Prevent disruptions to and misuse of ConnSCU electronic communications resources and services;
- Ensure that the ConnSCU community is aware that use of ConnSCU electronic communications resources is subject to state and federal laws and the ConnSCU policies; and
- Ensure that electronic communications resources are used in compliance with those laws and the ConnSCU policies.

Scope

This Policy applies to:

- All electronic communications resources owned or managed by ConnSCU including the content of electronic communications, electronic attachments and transactional information associated with such communications;
- All electronic communications resources provided by ConnSCU through contracts and other agreements with ConnSCU;

- All users and uses of ConnSCU electronic communications resources; and
- All ConnSCU electronic communications records in the possession of ConnSCU employees or other users of electronic communications resources provided by ConnSCU.

Policy Authority

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

Definitions

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

Electronic Communication: Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications services, including but not limited to email and telephone.

Electronic Communications Records: Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications services. This definition of electronic communications records applies equally to the contents of such records, attachments to such records, and transactional information associated with such records.

Electronic Communications Resources: Any combination of telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

Electronic Communications Services: Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

ConnSCU Authority: The President or his/her designees of the institution that operationally manages the IT resources or data.

Provisions

ConnSCU encourages the use of electronic communications resources for legitimate and authorized academic and administrative purposes and makes them widely available to the ConnSCU community. To insure the reliable operation of these resources, their use is subject to the following:

- Email is an official means for communication within ConnSCU unless otherwise prohibited by law. The colleges and universities reserve the right to send official communications to employees and students via email. In the event of an emergency, the colleges and universities shall utilize all available communication mechanisms including email to reach employees and students.
- All employees and students will be given official college/university email accounts. Official university communications shall be sent to official college/university email addresses. Employees and students are expected to check their official email accounts on a frequent and consistent basis in order to stay current with campus related communications. Failure to receive or read official communications does not absolve the employee or student from knowing and complying with the content of such official communications.
- Employees are not allowed to conduct official ConnSCU business via private (unofficial) email accounts unless specifically authorized by the appropriate ConnSCU authority.
- Individuals, who choose to have their emails auto-forwarded to private (unofficial) email addresses, do so at their own risk. The college/university is not responsible for any difficulties that may occur in the transmission of the emails.
- Contents of all electronic communications shall conform to state and federal laws and ConnSCU policies regarding protection of privacy, intellectual property, copyright, patents and trademarks
- Using electronic communications resources for any purpose restricted or prohibited by state and federal laws, regulations or ConnSCU policies is prohibited.
- Using electronic communications resources for monetary gain or for commercial, religious, or political purposes that are not directly related to ConnSCU institutional missions or otherwise authorized by appropriate ConnSCU authority is prohibited.
- Usage that directly or indirectly causes strain on the electronic communications resources is prohibited.
- Capturing, opening, intercepting or obtaining access to another person's ConnSCU electronic communications, except as otherwise permitted by the owner or appropriate ConnSCU authority is prohibited.
- Using electronic communications to harass or intimidate others or to interfere with the ability of others to conduct ConnSCU business is prohibited.
- Users of electronic communications resources shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of ConnSCU unless authorized to do so by the appropriate ConnSCU authority.

- Directly or by implication, employing a false identity (the name or electronic identification of another), except under the following circumstances, is prohibited:

  A supervisor may direct an employee to use the supervisor's identity to transact ConnSCU business for which the supervisor is responsible. In such cases, an employee's use of the supervisor's electronic identity does not constitute a false identity.

  A user of the ConnSCU electronic communications services may not use a pseudonym (an alternative name or electronic identification for oneself) for privacy or other reasons, unless authorized by an appropriate ConnSCU authority for business reasons.

- Forging email headers or content (i.e., constructing an email so it appears to be from someone else) is prohibited.
- Unauthorized access to electronic communications or breach any security measure is prohibited.
- Interfering with the availability of electronic communications resources is prohibited, including but not limited to the following: (i) sending or forwarding email chain letters or their equivalents in other electronic communications services; (ii) "spamming," i.e., sending electronic junk mail or junk newsgroup postings; (iii) "letter-bombing," i.e., sending an extremely large message or sending multiple messages to one or more recipients to interfere with the recipient's use of electronic communications resources; or (iv) intentionally engaging in other practices such as "denial of service attacks," i.e., flooding the network with traffic.
- Distribution of an electronic mail to the entire or a substantial portion of a campus community must obtain prior approval as specified by the receiving institution.

No Expectation of Privacy

ConnSCU IT systems and resources are the property of the State of Connecticut and use thereof by the user is restricted to the performance of official State business or activities approved through the collective bargaining process.

Pursuant to Communications Assistance for Law Enforcement Act (CALEA), Public Act 98-142, and the State of Connecticut's "Electronic Monitoring Notice", information related to usage and utilization of ConnSCU IT systems and resources is constantly being collected and logged. While IT personnel do not review the contents of this information except when necessary in the course of the discharge of official duties and as permitted by law, all users should know that such information is subject to subpoena, discovery, the Connecticut Freedom of Information Act and such other disclosure processes as may be authorized by law.

Assurance

Each ConnSCU institution shall incorporate the Electronic Communication Policy as part of the terms and conditions for issuing institution email accounts. Each ConnSCU institution shall have all full-

time and part-time employees, including student employees, acknowledge that they have read and understand the Electronic Communication Policy. Each ConnSCU institution shall make the Electronic Communication Policy accessible to all employees and students.

Enforcement

Violations of ConnSCU information technology 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 all 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 BOR Information Security Program Office, in conjunction with college/university IT department, may temporarily remove or block any system, device, or person from the ConnSCU network that is reasonably suspected of violating ConnSCU electronic communications policy. 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 resolution.

Exception Process

ConnSCU recognizes that some portions of the Electronic Communication 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 appropriate ConnSCU authority as specified in the provisions above. All other exceptions shall be approved by the BOR CIO or designee.
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. The 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.)

Exception Request

To request an exception, please submit the Information Security Exception request to SecProg@ct.edu

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.

Review

This policy will be reviewed every three years by the Board of Regents.

ITEM

Establish an expedited approval process for Interim Information Security Policies.

BACKGROUND

Issues

- The security policies across the constituent units are inconsistent and at times contradictory.
- Without a set of security policies that is consistent across all BOR constituent units, the BOR is unable to implement a comprehensive assurance program.
- The formal IT policy development, review, and approval process takes 12-18 months per policy.
- There are 17 "must have" security policies. Since May 2011, only two policies have been developed, reviewed, and approved. Fifteen (15) more security policies have yet to be developed.

Interim Security Policy Development and Approval Process

- Establish an Information Security Interim Policy Committee that understands the risks and legal implications of policy. The Committee will develop interim high priority security policies. See Appendix for the list of high priority security policies. The membership are:

    - BOR Legal Counsel
    - University or College President representative (1)
    - VP or Dean of Finance & Administration representatives (2)
    - BOR Security Program Manager
    - BOR CIO

    Each member is expected to commit two hours per week for the next six months.

- Upon creation, each interim policy will be presented to the BOR IT committee for approval.
- Upon approval by the BOR IT committee, the interim policy will be communicated to colleges and universities for immediate implementation.
- Upon approvals of all interim policies, the entire policy set will go through the formal review process and be submitted to the full Board for approval.
- After approval by the full Board, implementations will be modified to reflect the changes of the policies, if any.

- Those policies that are not listed in the Appendix will go through the formal IT policy development, review, and approval process.

Appendix

Information Security Policies are clustered into several policy areas, for organizational purposes. These policies should be viewed as an integrated whole, rather than as individual unrelated policies. The following 17 security policies are considered high priority.

1. **General Information and Technology Policies**
   - 1.1. Overview and Common Provisions
   - 1.2. Employee Responsibilities for Information Security Practices
   - 1.3. Information Security Awareness and Training
   - 1.4. Security Assurance, Monitoring and Enforcement

2. **Infrastructure Management**
   - 2.1. Change Management
   - 2.2. Network Policy
   - *2.3. Mobile Computing and Storage Device*

3. **Account Management**
   - 3.1. Acceptable Use
   - 3.2. Electronic Communications Policy
   - 3.3. Password Policy

4. **Data Management**
   - 4.1. Confidential Data Management
   - 4.2. Data Classification
   - 4.3. Data Management Roles and Responsibilities
   - 4.4. Access Control, Authentication and Authorization Process

5. **Vulnerability and Incident Management**
   - 5.1. Vulnerability Management
   - 5.2. Incident Reporting and Response
   - 5.3. Investigation and Correction of Security Incidents