CONNECTICUT STATE COLLEGES & UNIVERSITIES
BOARD OF REGENTS FOR HIGHER EDUCATION

BOR INFORMATION TECHNOLOGY COMMITTEE

Friday, April 5, 2013, ***11:30am - 1:30 p.m.***
61 Woodland Street, Hartford, CT 06105
2nd Floor, Room 238

AGENDA

1. *Approval of February 25, 2013 Minutes
2. BOR CIO General Status Report
3. *IT Policy Revision of BOR IT 001 (Acceptable Use Policy) and 002 (Electronic Communication)
4. **Move to Executive Session** - Evaluation of CCC Information Security Program
5. Return to Open Session
6. Adjourn

*=attachment

CONNECTICUT STATE COLLEGES & UNIVERSITIES
BOARD OF REGENTS FOR HIGHER EDUCATION

BOR INFORMATION TECHNOLOGY SPECIAL COMMITTEE

Special Meeting Minutes - Monday, February 25, 2013, 2:00 p.m. to 4:00 p.m.
61 Woodland Street, Hartford, CT 06105, 2nd Floor, Room 238

REVISED

REGENTS PRESENT
Nickolas Donofrio, Chair
Michael Pollard

REGENTS ABSENT
Matthew Fleury

BOR STAFF
Wendy Chang, Chief Information Officer
Braden Hosch, Director of Institutional Research/Academic Affairs
Terry O'Brien, Contact Compliance Officer
Karen Stone, Internal Auditor
Mary Lenehan, Assistant Attorney General
Victoria Lee Thomas, ITS Support Staff

ConnSCU Representatives
James Estrada, CCSU
George Claffey, COSC
Joe Tolisano, ECSU
Ken Spelke, SCSU
Tom DeChiaro, WCSU

CALL TO ORDER

Chairman Donofrio called the meeting to order at 2:10 p.m.

Chairman Donofrio and Regent Pollard introduced themselves and gave an overview of their IT experience.

Chairman Donofrio provided an overview of the committee's charge. Chairman Donofrio emphasized the importance of security and informed the group that IBM has agreed to do a security assessment of the system to provide useful feedback free of charge.

1. Approval of January 17, 2013 Minutes

Minutes were approved unanimously with a motion by Regent Pollard, seconded by Chairman Donofrio.

2. Data Collection, Data Sharing, and Report Preparation

Dr. Braden Hosch provided an overview of the draft Staff Report regarding Data Collection, Data Sharing, and Report Preparation stating the Board of Regents authorizes the Board of Regents President or his designee to collect records, maintain databases and conduct studies and research to serve the interests of the state, including execution of MOUs to engage in data sharing with state, federal and other agencies. Dr. Hosch also recommended one revision in the third paragraph of the resolution to read:

That the Board of Regents for Higher Education authorize the President of the Board to execute the Memoranda of Understanding to share data in a manner consistent with state and federal laws with state and federal and other agencies in the execution of such studies and reports. (Underlined words added)

Chairman Donofrio moved to approve the draft Staff Report with the mentioned revision. Seconded by Regent Pollard. Unanimously approved.

3. Discussion of CSU IT Operation

Members participated in a discussion following remarks by CSU and Charter Oak CIOs. During the course of their deliberations, the CIOs identified several items that require follow-up action, including, but not limited to: IT security, IT governance, architecture and project management and investment. After much discussion Chairman Donofrio acknowledged that there is much work to be done in these areas and assured the CIOs that he and Regents Pollard and Fleury are dedicated to addressing and rectifying these concerns. Chairman Donofrio went on to say he intends to provide transparent clarification as far as the role of the BOR Information Technology Committee and the role of Dr. Wendy Chang as the System CIO. Dr. Chang is the person that will be held accountable, therefore she has the authority, support and confidence of this Board when it comes to making cognizant decisions pertaining to the best interests for the entire system. Chairman Donofrio concluded by stated the CIOs must work together to advance system's interests. Dr. Chang stated that today's meeting was productive and an excellent starting point.

With no further business to consider, the meeting adjourned at 3:43 p.m.

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:	03/22/2013	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

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 Communications Assistance for Law Enforcement Act (CALEA), Public Act 98-142, and the State of Connecticut's "Electronic Monitoring Notice", the Board of Regents reserves the right to monitor and/or log all activities of all users using ConnSCU IT systems in a manner consistent with relevant collective bargaining agreements which may be amended from time to time. This includes, but is not limited to, files, data, programs and electronic communications records without the consent of the holder of such records.

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:	03/22/2013	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

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 Communications Assistance for Law Enforcement Act (CALEA), Public Act 98-142, and the State of Connecticut's "Electronic Monitoring Notice", the Board of Regents reserves the right to monitor and/or log all activities of all users using ConnSCU IT systems in a manner consistent with relevant collective bargaining agreements which may be amended from time to time. This includes, but is not limited to, files, data, programs and electronic communications records without the consent of the holder of such records.

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.