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/xx/2012
Next Review Date:	10/01/2015	Last Reviewed Date:	10/04/2012

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.

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.

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.
- 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 IT resource, User ID, password, files, or data.
- 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 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.

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 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.