Acceptable Use

Identifier: IT-001	
Revision Date: 1/1/2017	**Effective Date: 10/18/2012**
Approved by: BOR	**Approved on date: 10/18/2012**

Table of Contents

1. Introduction

This Policy governs the Acceptable and Responsible Use of Information Technology and related Resources of Connecticut State Colleges and Universities (CSCU). 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 CSCU IT resources is a privilege dependent upon appropriate use. Users of CSCU IT resources are responsible for using IT resources in accordance with CSCU policies and the law. Individuals who violate CSCU policy or the law regarding the use of IT resources are subject to loss of access to IT resources as well as additional CSCU disciplinary and/or legal action.

2. Purpose

The purpose of this policy is to provide the CSCU 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 CSCU IT systems to:

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

3. Scope

This Policy applies to:

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

4. Policy Authority

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

5. 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.

6. Provisions

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

- Use resources solely for legitimate and authorized administrative and academic purposes.
- Ensure that any personal use of CSCU IT resources be limited and have no detrimental impact on institution operations, job performance or CSCU 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 CSCU IT resources must **NOT**:

- Use CSCU IT resources to violate any CSCU policy or state or federal law.
- Use another person's credentials, User ID, or password to access resources.
- Use another person’s files or data without permission.
- Gain 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 CSCU IT resources, or transmit them over CSCU networks.
- Harass or intimidate others or interfere with the ability of others to conduct CSCU business.
- Directly or indirectly cause strain on IT resources such as downloading large files, unless prior authorization from the appropriate CSCU authority as determined by the institution is given.

- Use CSCU IT resources for unauthorized purposes which 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.

7. No Expectation of Privacy

All activities involving the use of CSCU IT systems are neither personal nor private. Therefore users should have no expectation of privacy in the use of these resources. Information stored, created, sent, or received via CSCU 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 CSCU 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.

8. Assurance

Each CSCU institution shall incorporate the Acceptable and Responsible Use Policy as part of the terms and conditions for issuing institution computer network accounts. Each CSCU 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 CSCU institution shall make the Acceptable Use Policy accessible to all employees and students.

9. Enforcement

Violations of CSCU Acceptable and Responsible Use policy may result in appropriate disciplinary measures in accordance with local, state, and federal laws, as well as CSCU Policies, general rules of conduct for all college and university employees, applicable collective bargaining agreements, and CSCU student conduct codes.

For purposes of protecting the CSCU 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 CSCU network that is reasonably suspected of violating CSCU 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.

10. Exception Process

CSCU 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 CSCU 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.)

11. 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.

12. Disclaimer

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

13. Related Publications

Related Policies

- [Link to BOR Information Security Policy when approved]

Related Standards and Procedures

- [Link to Support Services Procedure Page]

Web Sites

- [General Link to Support Services Website]

14. Revision History

Previous versions of this standard

- 10.18.2012

History of Changes

1. Page 2, Introduction, added the word related to first sentence
2. Page 3, Provisions, modified bullets under acceptable use to add; credentials, or, to access resources, Use another persons files or data without permission, gain.
3. Page 4, added which to top bullet.
4. Page 4, added neither personal, nor private to Nor private.
5. Page 4, Enforcement, deleted the
6. Throughout document changed CSCU to CSCU.

Standards superseded by this standard

- None