



## **POLICIES AND PROCEDURES**

**Subject: Information Security, Computer & Communication Use**

**Policy No. 10**

**Pages: 9**

**Date: November 12, 2008**

**Approved by: Maria M. Houser, Associate Vice President for H R and Labor Relations**

**Signature:**

---

### **Policy**

The purpose of this policy is to provide guidance and establishes minimum standards when using the Internet and Southern Connecticut State University's electronic communication systems and personal phones.

Access to and use of computing and networking resources at SCSU are privileges extended to members of the Southern community. Access to the University's computing and networking resources is limited to authorized users for approved purposes only. Such resources include computer hardware and software, computer-based files and data, and all networks including the Internet. Approved purposes are those consistent with both the broad instructional, health care and research goals of SCSU and with the employee's occupational goals with the institution. All users must follow this policy and any additional policy that may be adopted by the University where the user is working.

SCSU may supplement this policy as it needs or requires, as long as such supplement is consistent with this policy.

### **Policy Details**

The University's electronic communication systems such as voice mail, e-mail, Web site, computers, network and Internet access systems, both internal and external, are to be used primarily to advance the University mission of education, research, and public service.

The University recognizes that academic freedom is an essential aspect of the University mission and will interpret and carry out this policy so as to respect that principle. The University will also endeavor to interpret and carry this policy in a

manner consistent with its various obligations to employees under existing collective bargaining agreements.

Communications transmitted through these systems should have a legitimate University-related business purpose. These electronic communications resources may only be used for legal purposes and may not be used in any manner or for any purpose which is illegal, dishonest, disruptive, threatening, damaging to the reputation of the University, inconsistent with the mission of the University, or likely to subject the University to liability. The use of University electronic communications systems or facilities for private or personal commercial purposes is strictly prohibited, including any sort of non-University related solicitation.

The University acknowledges that occasionally employees, faculty, student-employees, and other end-users use University electronic communications systems assigned to them for non-commercial, personal use. Such occasional non-commercial uses are permitted if they are not excessive, do not interfere with the performance of the employee or faculty member's duties, do not interfere with the efficient operation of the University or its electronic communications resources, and are not otherwise prohibited by this policy or any other University policy or directive.

### **Scope**

All employees of SCSU and those areas of the University where supervisors are authorized to give consultants, contract personnel or other non-employees, postdoctoral scholars and fellows, volunteers or interns, including part-time and visiting faculty, access to the University's Internet or electronic communication systems who will then require such individuals to abide by this policy.

### **Access and Use**

At certain times, SCSU may find it necessary to access and disclose information from computer and network users' accounts (to the extent required by law) in order to uphold contractual obligations or other applicable institutional policies or to diagnose and correct technical problems. For this reason, the ultimate privacy of messages and files cannot be ensured. In addition, system failures may lead to a loss of data; therefore users should not assume that their messages and files are secure.

Neither SCSU nor its agents restrict the content of material transported across its networks. While SCSU does not position itself as a censor, it reserves the right to limit access to its networks or to remove material stored or posted on computers when applicable SCSU policies, contractual obligations, or state or federal laws are violated.

### **Definitions**

Business Use—University-provided computer systems that allow access to the Internet and electronic communication systems are the property of the University

and are provided to facilitate the effective and efficient conduct of State business. Users are permitted access to the Internet and electronic communication systems to assist in the performance of their jobs.

Computer Network—Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Confidential Information— Information maintained and classified by the University that requires special precautions because its unauthorized disclosure, alteration, loss, or destruction will likely cause perceivable damage to someone or something.

Electronic Communication Systems— System used as a means of sending and receiving messages electronically through connected computer systems or the Internet, such as e-mail or voice mail.

Electronic Communications—Electronic communications include, but are not limited to, the World Wide Web, Internet based discussion groups, electronic bulletin board systems, electronic mail (including bulk), telephone, voice mail, fax, or any type of wireless transmission. Employees must adhere to this policy when using (1) the University's Internet connection, (2) the University's internal networks [intranet system], (3) the University's connection to the public telephone system, and (4) University owned equipment. Electronic communications are any information, graphics, or data sent or retrieved by electronic systems.

Internet—is an international network of independent computer systems. The World Wide Web is one of the most recognized means of using the Internet.

Personal Use—Personal use means use that is not job-related.

Users— are all the employees of the University who use an agency's Internet and/or electronic communication systems.

### **No Expectation of Privacy**

To the fullest extent permitted by state and federal law, the University reserves the rights to intercept, disclose, and use the wire and electronic communications transmitted by University users. No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the University's equipment and/or access. The University has a right to monitor any and all aspects of their computer systems including, but not limited to, sites, instant messaging systems, chat groups, or news groups visited by users, material downloaded or uploaded and e-mail sent or received by users. Such monitoring may occur at any time, without notice, and without the user's permission.

Monitoring can occur when SCSU reasonably believes it necessary to do so to protect the integrity, security, or functionality of University or other computing

resources or to protect the University from liability; When there is reasonable cause to believe SCSU's policies have been, or are being, violated; When a user appears to be engaged in unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; Or the law otherwise permits it.

The University may delete files, data or information stored on SCSU computing systems after notice to the staff members. The appropriate supervisor or designee must authorize any such activities under this policy.

In addition, electronic records may be subject to the Freedom of Information Act and therefore, available for public distribution.

### **Prohibited Activities**

Connecticut and federal laws provide for civil and criminal penalties for violations of the law. Certain activities are prohibited when using the Internet or electronic communications. These include, but are not limited to:

- Accessing, downloading, printing or storing information with sexually explicit content as prohibited by law (see Conn. General Statutes Sec. 53a-251 "Computer Crime");
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or other-wise unlawful messages or images;
- The electronic transportation of obscene materials across state lines;
- Installing or downloading computer software, programs, or executable files contrary to policy;
- Unauthorized copying, uploading or downloading of copyrighted materials or proprietary University information contrary to policy;
- Uploading or downloading access-restricted information contrary to policy or in violation of policy;
- Sending e-mail using another's identity, an assumed name, or anonymously;
- Permitting a non-user to use for purposes of communicating the message of some third party individual or organization;
- E-mail stalking, threats, or harassment;
- Destruction of University data or equipment;
- Any usage that interferes with or disrupts network users, services, or computers. Disruptions include, but are not limited to, distribution of unsolicited advertising, and deliberate propagation of computer viruses;
- Use of e-mail for creating or forwarding any jokes especially those which contain sexual or ethnic topics or slurs, chain messages, or any other non-work related messages; checking and/or responding to personal e-mail via another (second party) e-mail system such as Yahoo! or Hotmail; sending or forwarding messages referring to political causes or activities; messages concerning participation in sports pools, baby pools or other sorts of gambling activities; religious activities; distribution groups or

- “listservs” for non-work related purposes; solicitations or advertisements for non-work related purposes;
- Use of the Internet for pirating software; stealing passwords; hacking other machines on the Internet; participating in the viewing or exchange of pornography or obscene materials; personal job searches; shopping on-line for non-work related items; checking/viewing stocks or conducting any personal financial planning activities;
  - Connecting personally owned hardware or installing and/or using non-State licensed software;
  - Any activities where users engage in acts that are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, broadcasting unsolicited mailings or other messages, creating unnecessary output or printing, or creating unnecessary network traffic;
  - Or any other activities designated as prohibited by this policy.

Use of SCSU computers or communication systems for any of the above actions may result in progressive discipline up to and including termination.

### **Personal Use**

In general, incidental and occasional personal use of the University’s Internet access or electronic communication systems is permitted when supervisor approval has been obtained or in accordance with policy guidelines; however, personal use is prohibited if it:

- Interferes with the user’s productivity or work performance, or with any other employee’s productivity or work performance;
- Adversely affects the efficient operation of the computer system;
- Used to engage in political activity such as supporting a candidate for public office.
- Results in copyright infringement or abuse, or excessive use of bandwidth;
- Violates any provision of this policy or any supplemental policy adopted by the University supplying the Internet or electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law. (See Authority section below.)

NOTE: Users employing the University’s Internet or electronic communication systems for personal use must present their communications in such a way as to be clear that the communication is personal and is not a communication of Southern Connecticut State University.

### **Security**

The distribution of electronic communications is difficult to control and routing mistakes can easily occur. Copies of electronic communications can be forwarded without the sender’s knowledge or permission to unintended recipients. Therefore, electronic communications should be drafted and sent with

at least the same level of care, professional judgment and discretion as paper memoranda or documents.

## **GUIDELINES**

### **User Responsibilities**

The conduct of computer users who access the Internet or send e-mail containing the University's domain address (i.e., \_\_\_@southernct.edu) may be perceived as reflecting on the character and professionalism of the University. When engaging in such conduct, whether for personal or official purposes, employees are expected to do so in a responsible and professional manner. All users are responsible for exercising appropriate care to protect the University's computer systems against the introduction of viruses. When using the University's Internet access or electronic communications, equipment and capability, individuals must:

- Use the Internet or electronic communication systems only in accordance with State and University policy or for which access is authorized.
- Maintain the conditions of security and confidentiality (including safeguarding of passwords) under which they are granted access to such systems and not inappropriately shared with others.
- Check with the appropriate University staff prior to downloading or accessing a file or document if the source of the file or other circumstances raises doubts about its safety.
- Be aware of computer viruses and other destructive programs, and take steps to prevent damage to SCSU equipment and systems.

### **Supervisor Responsibility**

- Supervisors are responsible for insuring that individuals are assigned the appropriate level of security access to systems;
- Upon transfer or termination of employment, supervisors should immediately initiate request and follow-up to insure security access has been deleted;
- Supervisors must define and communicate departmental expectations on personal use of equipment and systems;

### **University Responsibilities**

SCSU may develop a written policy, consistent with this policy which supplements or clarifies specific issues for the University. With regard to use of the Internet and electronic communications, the University is responsible for:

- Communicating this policy, if appropriate, to current users and to new users before granting them access to the University 's Internet or electronic communication systems;
- Retaining electronic records in accordance with the retention requirements;
- Requiring and retaining acknowledgement statements, signed by each user, acknowledging receipt of a copy of this policy.

### **Mass Communications**

Distribution of bulk/broadcast/mass email, voice mail or fax messages beyond an individual's area of responsibility are allowed with appropriate approvals. Prior to distribution, the proposed communication must be approved. For approval, the communication is sent to the appropriate party below along with a description of the purpose and target audience.

University wide communications require the approval of the Department's supervisor or designee. Safety/Security communications require Chief of Police or designee approval.

### **Telephone & Cellular Calls**

Telephones are the property of the University and are intended for business purposes. Excessive or unauthorized use of telephones for personal calls is not permitted. Individuals are responsible for understanding departmental expectations.

- Long Distance Calls—may only be charged to SCSU when related to University business purposes.
- Local Calls—occasional use of SCSU business telephones for personal local calls can generally be accommodated within reason.
- Personal Cellular Phones— While at work employees are expected to exercise the same discretion in using personal cellular phones as is expected for the use of University telephones. Excessive personal calls including text messaging during the workday can interfere with employee productivity and be distracting to others. Employees should restrict their personal calls and texting during work time and only use their personal cell phones during scheduled breaks or scheduled lunch periods in non-working areas. Employees are therefore asked to make any other personal calls on non-work time where possible and to ensure that friends and family members are aware of the University's policy. Flexibility will be provided in circumstances demanding immediate attention. The University will not be liable for the loss of personal cellular phones brought into the workplace.

## **Violations**

The appropriate level of disciplinary action will be determined on a case-by-case basis, with sanctions up to or including termination depending on the severity of the offense such as in cases involving willful, flagrant, or repeated violation of this policy.

## **Authority**

- 18 USC §1030—Fraud and related activity in connection with computers.
- 18 USC § 875— Extortions and threats: Interstate communications.
- 18 USC § 1028—Fraud and related activity in connection with identification documents, authentication features and information.
- 18 USC § 1343—Fraud by wire, radio, or television.
- 15 USC § 7704—other protections for users of commercial electronic mail.
- 17 USC § 506; §1201—Criminal Offenses: Copyright.
- Connecticut General Statutes Sec. 36a-701b; Secs. 1-266 to 1-286; Secs. 53-451 to 53-454; 53a-90a; 52-570b; 53a-301; 53a-250; 53a-251 to 53a-261.
- State Computer Harassment or "Cyber Stalking" Laws—C.G.S. §53a-182b; 531-183.
- CSU System Board of Trustees policy #11 *"Copyright Policy and Educational Program at CSU"* (BR #04-64)
- CSU System Board of Trustees Policy Book 1.9 *"Policy on Computer Use for Employees of the Connecticut State University"* (BR #86-48)
- CSU System Board of Trustees policy #12.1 *"Use of Electronic Signatures"* (BR #01-51)
- CSU System Board of Trustees resolution concerning *"Review, Use, and Dissemination of Sensitive and/or Confidential Information"* (01/26/07)
- C.G.S. §4d-2 (c) (1), the Chief Information Officer of DOIT is responsible for developing and implementing policies pertaining to information and telecommunication systems for state agencies.
- CSU System policy as approved by the Board of Trustees *"General Guidelines to Improving Information Security Practices within the Connecticut State University System"*
- Department of Information Technology policy *"Freedom of Information Access to Computerized Public Records"*
- Public Act 98-142, "An Act Requiring Notice to Employees of Electronic Monitoring by Employers",
- Dept. of Information Technology *"Acceptable Use of State Systems Policy"* May 2006 (Addendum added November 2006)
- Connecticut State Library General Letter 98-1 *"Electronic and Voice Mail Management and Retention Guide for State and Municipal Government Agencies"*
- State of Connecticut Comptroller's Office *"Software Inventory Control Policy and Procedures"*;

- Family Education Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley (Financial Modernization) Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Electronic Communications Privacy Act (ECPA)
- SCSU Employee Handbook
- Connecticut Personal Data Act

### **Exceptions**

Any exception to the procedures in this Policy shall require prior written approval from the Associate Vice President of Human Resources and Labor Relations or designee of this University.