
J. Electronic Information Systems Privacy Issues and Statement of Ethics

Southern Illinois University takes justifiable pride in the electronic information systems provided to its faculty, staff, and students. These resources include computer systems, University-owned computers and workstations, software, data sets, and communications networks. Members of the University community may use these resources only for purposes related to their studies, instruction, the discharge of duties as employees, official business with the University, or other University-sanctioned activities. Any other use, unless specifically authorized, is prohibited.

Access to the University's electronic information systems is a privilege to which all University faculty, staff, and students may be entitled to some degree. Certain responsibilities accompany that privilege; understanding them is important for all users. Those within the University community who make use of these resources are subject to high standards of ethics to insure the privacy, security, and property use of data. Recognized as primary educational, research, and administrative asset, the University's electronic information systems should be protected from unauthorized modification, destruction, disruption, or disclosure--whether accidental or intentional.

1. User Responsibility for Security of Stored Information

The user is responsible for correct and efficient use of the tools each electronic information system provides for maintaining the security of stored information.

- a. Individual users to whom computer accounts, passwords, and other types of security authorizations have been assigned must obey any express restrictions on disclosure of such authorizations to others. No otherwise authorized disclosure may be made until the proposed recipient of the disclosure has demonstrated familiarity with the security requirements for usage of the authorizations and agreed to comply with them.
- b. The user must strive to understand the level of protection each electronic information system automatically applies to files and supplement that protection, if necessary, for sensitive information.
- c. The microcomputer user must be aware of computer viruses and other destructive computer programs, and take steps to avoid being either their victim or propagator.

Chapter: 5. Financial /Administrative Affairs

Section: J. Electronic Information Systems
Privacy Issues and Statement of
Ethics

d. Use of computers by individuals implies that they accept responsibility for protecting any information (processed and/or stored under directories or accounts assigned to them) which is derived from restricted, licensed, or proprietary information.

2. Confidentiality of Stored Information

a. Information stored on electronic information systems is considered confidential, whether protected by the computer system or not, unless the owner intentionally makes that information available to other groups or individuals. The University assumes that computer users wish the information they store on central and campus shared computing resources to remain confidential.

b. Requests for the disclosure of confidential information outside the University will be governed by the provisions of law, including but not limited to the Family Educational Rights and Privacy Act of 1974, the State Records Act, and the Illinois Freedom of Information Act. All such requests will be honored only when approved by University officials who are the legal custodians of the information requested, or when required by state or federal law, or court order. A current statute which protects the electronic mail users is the federal Electronic Communications Privacy Act of 1986. This law basically protects messages while in transmission on a public mail service as well as after messages are received and stored on that service.

3. Inappropriate Usage

Computing and networking resources may be used only in accordance with accepted University practice. Examples of inappropriate and unacceptable use of computing and networking resources include:

- a. harassment of other users.
- b. destruction of or damage to equipment, software, or data belonging to the University or other computer and networking users.
- c. disruption or unauthorized monitoring of electronic communications.
- d. violations of computer system security.
- e. unauthorized use of computer accounts, access codes, or network identification numbers assigned to others.

Chapter: 5. Financial /Administrative Affairs

Section: **J.** Electronic Information Systems
Privacy Issues and Statement of
Ethics

- f. use of computer and/or network facilities in ways that impede the computing activities of others.
 - g. use of computing facilities for personal or business purposes unrelated to the mission of the University.
 - h. violation of copyrights and software license agreements.
 - i. violation of the usage policies and regulations of the networks of which the University is a member or which at least has authority to use.
 - j. violation of another user's privacy.
 - k. academic dishonesty such as plagiarism or cheating.
 - l. accessing, or attempting to access, another individual's or entity's data or information without proper authorization regardless of the means by which this access is attempted or accomplished.
 - m. giving another individual the means to access data or information they are not authorized to access.
 - n. obtaining, possessing, using, or attempting to use passwords or other information about someone else's account.
 - o. inspecting, modifying, distributing, or copying data, mail, messages or software without proper authorization, or attempting to do so.
 - p. tapping phone or data lines.
4. Electronic Mail

The University considers electronic mail to be a confidential, direct communication between sender and receiver(s). Accordingly, it should not be monitored, observed, viewed, displayed or reproduced in any form by anyone other than the sender or intended recipient(s). E-mail users should exercise the same restraint and caution in drafting messages that they would when writing a formal memorandum using University letterhead and assume that their messages will be saved and be seen by someone other than the original addressee.

Electronic mail may be disclosed to others with a need to know under law and University policy. Examples include:

Chapter: 5. Financial /Administrative Affairs

Section: **J.** Electronic Information Systems
Privacy Issues and Statement of
Ethics

- a. Incidental disclosure to technicians or supervisors during maintenance or repair procedures.
- b. Disclosure to internal or external auditors pursuant to their audit programs.
- c. Disclosure to adverse parties in civil lawsuits pursuant to mandated discovery procedures or to attorneys for the University for use in preparing a defense against such suits.
- d. Disclosure to administrative, regulatory or law enforcement authorities discharging their mandated functions, or to attorneys for the University for use in defending against charges or sanctions.
- e. Disclosure made for the purpose of resolving internal disputes including but not limited to those arising under grievance policies; parking and traffic regulations; student conduct codes; academic admissions, retention, grading and degree awards policies or practices; patent and copyright policies; indemnification policy liability and self-insurance programs; electronic information systems policies, and any external appeals of unresolved internal disputes.

5. Sanctions

Violations of the policies described herein for use of computing resources will be dealt with seriously. Violators are subject to disciplinary procedures of the University and, in addition, may lose computing privileges. Illegal acts involving the University computing and networking facilities may also be subject to prosecution by state and federal authorities.

I. Software Piracy Policy Statement

1. Southern Illinois University

Respect for the intellectual work and property of others is vital to the mission of higher education. This principle applies to works of all authors and publishers in all the media, including the labor and creativity resulting in computer software. It encompasses respect for the right to acknowledgment and the right to determine the form, manner, and terms of publication and distribution.

Unauthorized copying of software is illegal and may force the University as well as individuals to incur legal liability. The United States Copyright Law protects software authors and publishers in much the same manner as patent law protects inventors. Unauthorized copying of software, including programs, applications, data bases and code, deprives developers of a fair return for their work, may result in increased prices, may reduce the level of future support and enhancement available to the University, and may inhibit the development of new software products.

Unless software has been placed in the public domain, the owner of a copyright holds exclusive right to the reproduction and distribution of his or her work. The purchaser of software generally purchases only a license to use the software on one machine. Most licenses do not permit copying although a licensee may generally make a backup or archival copy. Some institutional licenses permit copying for use on local area networks or on multiple machines, but such uses must be authorized in a license agreement commonly called a site license, which might include a network license or a limited-use license.

It is the policy of Southern Illinois University that unauthorized copying of computer software will not be tolerated. Such copying is both unethical and illegal. University employees and students making, acquiring, or using unauthorized copies of computer software may be subject to University disciplinary sanctions as well as legal action by the copyright owner. Neither the University nor the State of Illinois will provide legal indemnification or defense for employees or students whose violation arises out of willful misconduct as defined in 2 Policies of the Board E.

The Chancellors of Southern Illinois University at Carbondale and Southern Illinois University at Edwardsville shall develop procedures for the implementation of this policy, pursuant to V Bylaws 8.