SOUTHERN ILLINOIS UNIVERSITY
EDWARDSVILLE

Policies & Procedures

Table of Contents

Information Technology

Responsible Use Policy - 2D4 & 3C10

Introduction

Southern Illinois University Edwardsville (SIUE) provides extensive computing and network communication services for students, faculty, staff and individuals affiliated with the University. As a provider of these services, the University acknowledges that there is a shared responsibility between the users of these services and the network provider. The goal of this policy is to establish a framework of accepted conventions regarding the use, management and governance of computing and network resources, while remaining cognizant of the principles of academic excellence to which the University continually strives. While the responsible use of computer resources is ultimately the responsibility of each user, the oversight of this policy lies with the office of the Associate Vice Chancellor for Information Technology and Chief Information Officer.

Responsible Use
Institutional Purposes

University computing and network communication services resources are to be used to advance the University's mission of education, research, and public service. Faculty, staff, and students may use them only for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the University, and other University sanctioned or authorized activities. The use of University computing resources and network communication services for commercial purposes including any sort of solicitation is prohibited, absent prior written permission of the appropriate University official(s). Employee use of University computing resources for partisan political purposes, as prohibited by the State Officials and Employees Ethics Act (5 ILCS 430/ et seq.) is also prohibited.

The University acknowledges that occasionally faculty, staff, and students use University computing and network resources assigned to them or to which they are granted access for non-commercial, personal use. Such occasional non-commercial uses are permitted by faculty, staff, and students, if they are not excessive, do not interfere with the efficient operation of the University or its computing and network resources, or are not otherwise prohibited by this policy or any other University policy or directive.

Classification of Use

Decisions as to whether a particular use of computing and network resources conforms with this policy shall be made by the Provost's Office if the use involves faculty or student academic matters, by the Office of Student Affairs if the use involves non-academic student use, and by the Office of Human Resources if the use involves administrators or staff.

Computing use shall include, but is not limited to, using University provided computers, computing resources and networks or computer equipment to create, modify, manipulate or store files, information, or electronic media. This shall also include any creation, storage, manipulation or otherwise using electronic communications messages or email.

Cooperative Use

Computing resource users can facilitate computing at the University in many ways. Collegiality demands the practice of cooperative computing. It requires:

- Regular deletion of unneeded files from one's accounts on shared computing resources;
- Refraining from overuse of information storage space, printing facilities, processing capacity, or network services;
- Refraining from use of sounds and visuals which might be disruptive to others;
- Refraining from use of any computing resource in an irresponsible manner; and
- Refraining from unauthorized use of departmental or individual computing resources.

Impermissible Use

Computing resources may only be used for legal purposes and may not be used for any of the following purposes or any other purpose which is illegal, unethical, dishonest, or likely to subject the University to liability. Impermissible uses (some of which may also constitute illegal uses) include, but are not limited to, the following:

- Harassment;
- Libel or slander;
- Fraud or misrepresentation;
- Destruction of or damage to equipment, software, or data belonging to the University or others;
- Disruption or unauthorized monitoring of electronic communications;
- Violation of copyrights and software licensing agreements, or unauthorized copying or transmission of copyright-protected material;
- Unauthorized installation or use of software, and in particular, software which may create a security risk on University computer facilities;
- Unauthorized use of tools that inspect SIUE network traffic;
- Use of the University's trademarks, trade names, logos, insignia, or copyrights without prior approval by an appropriate University official;
- Violation, or attempted violation, of computer system security;
- Unauthorized use of computing accounts, access codes (including passwords), or network identification numbers (including e-mail addresses) assigned to others;
- Use of computer communication facilities in ways that impede the computing activities of others (such as randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities, and so forth);
- Inspecting, modifying, distributing or copying data, or software without proper authorization, or attempting to do so;

- Inspecting, modifying, distributing or copying electronic mail messages without proper authorization or in a manner other than in the ordinary course of University business;
- Development or use of unapproved listservs;
- Use of computing facilities for personal or private business purposes absent prior written permission of the appropriate University official(s);
- Academic dishonesty, including, but not limited to, plagiarism and cheating;
- Violations under the Student Conduct Code, Faculty Code of Ethics and Conduct, or other University policies;
- Violation of network usage policies (Here) and regulations, or violation of usage policies and regulations of networks of which the University is a member or which the University has authority to use;
- Unauthorized extension (wired or wireless) of the University network, including, but not limited to, routers and wireless access points;
- Any attempt to bypass network authentication or security mechanisms;
- Violation of any individual's privacy;
- 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;
- Posting or sending obscene material, as well as pornographic, or sexually explicit material without a legitimate educational purpose;
- Intentional or negligent distribution of computer viruses; and
- Concealing or misrepresenting user's name, affiliation or other identifier to mask irresponsible or offensive behavior or unauthorized use of identifier of other individuals or entities.

General Policies

Access to and utilization of the computing resources and facilities provided by the University are a privilege and NOT a right; access to such resources and facilities may be withdrawn, limited, modified or curtailed if there is reason to believe that the user has or may have violated this policy or applicable local, state or federal law. Additionally, violation of this policy can result in further discipline under the appropriate processes and procedures set forth by the University or civil or criminal prosecution.

All users, as a condition of their access to or utilization of University computing or network services, agree to cooperate with and abide by University policies, regulations and guidelines, and applicable local, state and federal law. The user agrees to cooperate in an investigation of alleged improprieties or abuse of the privilege of using University computing services and waives any right of confidentiality. Any failure to cooperate fully with the University shall be considered a violation of this policy.

Responsibilities of Users

The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- Users should not share computer accounts, passwords, and other types of authorization that are assigned to individual users with others;
- Users should assign an obscure account password and change it frequently, adhering to the University's Minimum Information Technology Security Guidelines;
- Users should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive or confidential information;
- Users should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these programs; and

- Users should consider whether information distributed using University resources should be protected from unauthorized use by the use of copyright notices or by the restriction of distributing certain materials to Southern Illinois University users. Information regarding copyrights may be obtained from the General Counsel's Office.

Security

SIUE will assume that users understand and are aware that electronic files, data, and communications are not necessarily secure.

Privacy and Confidentiality

The University reserves the right to inspect and examine any University-owned or operated communication system, computing resource, and/or files or information contained therein at any time, subject to the terms and conditions contained herein (viewing information in the course of normal system maintenance does not constitute disclosure). There shall be no expectation of privacy in the use of University computer resources.

Outside Sources

When sources outside the University request an inspection and/or examination of any SIUE-owned or operated communication system, computing resource, and/or files or information contained therein, the University will treat information as confidential unless any one or more of the following conditions exist when:

- Approved by the appropriate University official(s) of the head of the Department to which the request is directed;
- Authorized by the owner(s) of the information;
- Required by federal, state, or local law; and
- Required by a valid subpoena or court order.

Internal Sources

The Provost, or designee, may direct an inspection and/or examination of any University-owned or operated communication system, computing resource and/or files or information contained therein when:

- The inspection and/or examination serves a legitimate University purpose; and/or
- There is a reasonable suspicion that the inspection and/or examination will reveal a violation of local, state, or federal law, or University policy.

The applicable University grievance policy is available to anyone who has been aggrieved by the decision of the Provost or their designee.

Computers and Network Systems: SIUE Network Defined

The term SIUE Network is used here to denote the campus computer and data communications infrastructure at SIUE. It includes the campus backbone and local area networks, all equipment connected to those networks (independent of ownership), and all equipment registered to any domain name owned by the University and hosted systems. When connecting to the SIUE network, all devices become part of the SIUE Network and are subject to the policies set forth herein regardless of connection type (e.g. wired, wireless, or virtual private network).

External Networks

It is expected that all members of the University community will abide by the guidelines and policies set forth herein while pursuing University business, wherever located. Members of the University community who use networks, facilities, or computers not owned by the University shall adhere to this Responsible Use Policy and all policies and procedures established by the administrators of non-University networks, facilities, or computers they use. Whether or not an external policy exists, this Responsible Use Policy shall remain in effect and shall be adhered to by members of the University community at all times, when using University resources or data.

Electronic Mail/Communications

Electronic mail and communications have become an integral part of society and have become indispensable to the members of the University community. Users should be aware of the weak privacy afforded by electronic communications and electronic data storage. Users should not commit confidential information to either, and understand that there is no expectation of privacy in such communications.

Electronic mail and other forms of communication should be used in a responsible and courteous manner. Use of electronic mail, other communications services, or other network communications facilities to harass other users of the network is forbidden. All users need to be aware that material, which is obscene, defamatory, or violates the University's Non-Discrimination and Non-Harassment Policy will not be tolerated. The University reserves all rights to take appropriate measures to prevent, correct, or discipline behavior that violates this policy.

Electronic mail communications on University networks or equipment, including, but not limited to, electronic mail and personal information, is subject to examination by the University when:

- It is necessary to maintain or improve the functioning of University computing resources;
- There is a suspicion of misconduct under University policies, or suspicion of violation of local, state, or federal laws; or
- It is necessary to comply with, or verify compliance with, local, state, or federal law.

If the University inadvertently discovers messages or data files within its network that lead it to suspect the presence of illegal activities or activities which violate University policies, then the University will be free to use that discovered information to pursue investigations or inform the appropriate authorities.

Examination of Contents of Electronic Messages and Files

System Files and Logs: In the course of resolving system performance or security problems, system administrators may examine the contents of files that control the flow of tasks through the system or that grant unauthenticated access to other systems. This includes system logs that document some activities of users.

Process for Requesting Disclosure of Contents of Messages and Files

A. Requesting Disclosure: Requests for disclosure must be made in writing through regular reporting channels, consistent with the guidelines below. Requests for disclosure are made to the Chief Information Officer (CIO), who is assigned the responsibility for implementing this policy and ensuring that the scope of the disclosure is limited to a legitimate University purpose. The CIO carries out these responsibilities in consultation with Legal Counsel and other appropriate offices. The CIO may designate an individual to act on their behalf in fulfilling these responsibilities. All authorizations by the

CIO or designee will include specifications for the form and timing of notification to the person whose information is accessed or disclosed.

B. Action While a Request is Pending: While a request consistent with this process is pending or under consideration, the requesting unit executive officer may ask computer system administrators to take reasonable, necessary steps to maintain, store, or otherwise prevent the deletion or modification of the information being sought. This must be done in such a way as to maintain the privacy of said information until the requested disclosure is reviewed. The Office of the CIO may be able to advise units on appropriate procedures.
C. Notification of Affected Individual(s): When the CIO or a designated authorized administrator provides access to, and disclosure of, email messages and/or file content under provisions of external laws, regulations or applications of this University policy, the requesting administrator will normally notify in *advance* the individual(s) whose information is to be released, indicating the information to be released and the law, regulation or policy that governs the release. If individuals are not notified in advance, the CIO will be responsible for determining when notification is appropriate and for ensuring that such notification is carried out. Circumstances in which notification may be delayed include, but are not limited to, (1) the presentation by legal bodies of subpoenas or other instruments prohibiting advance notification, (2) situations where the safety of individuals is involved, or (3) investigations or inquiries conducted under published University policies.
D. Conditions for Disclosure: In the absence of legally compelled access or disclosure, the CIO is authorized to grant access to a user's file contents or electronic mail messages, or to give copies of them to any third party *within* the University only if *all* the guidelines below are met:
    1. The access or disclosure is requested in writing through regular University reporting channels, including the unit executive officer of the individual whose information is being disclosed and the next administrator in that reporting chain.
    2. The reason for the requested disclosure serves a legitimate University purpose.
    3. The disclosure is not invasive of legitimate privacy interests or unreasonable under the circumstances, e.g., in light of alternative means of acquiring the information or achieving the requester's purpose.
    4. The nature and scope of the disclosure is submitted in writing to and approved by the CIO. This request is normally submitted by the approving executive officer indicated above.
    5. The affected individuals are notified in a timely manner in writing of any access or disclosure.
E. Review of Disclosure: The SIUE Network users whose information is accessed or disclosed under the above provisions should use existing University complaint and/or grievance procedures when concerned about the application of this policy.

Sanctions

Violations of this policy shall subject users to the regular disciplinary processes and procedures of the University for students, staff, administrators, and faculty and may result in loss of their computing privileges. Illegal acts involving University computing resources may also subject violators to prosecution by local, state and/or federal authorities.

Disclaimer

As part of the services available through the SIUE campus network, the University provides access to a large number of conferences, lists, bulletin boards, and Internet information sources. These materials are not affiliated with, endorsed by, edited by, or reviewed by the University, and the University takes no responsibility for the truth or accuracy of the content found within these information sources.

Existing University Rules and Regulations

This policy is intended to be an addition to existing University rules and regulations, and does not alter or modify any existing University rule or regulation.

Approved by Chancellor effective 3/28/24
This policy was issued on April 1, 2024, replacing the September 9, 2019 version.
Document Reference: 2D4 & 3C10
Origin: OC 1/11/13; OC 9/5/19; OC 3/28/24