Southern Illinois University School of Medicine
Responsible Use Guidelines

Introduction

Southern Illinois University School of Medicine (SIUSOM) provides extensive computing resources for students, faculty, staff and individuals affiliated with the School. As a provider of these services, SIUSOM acknowledges that there is a shared responsibility between the users of these services and the resource provider. The goal of this guideline 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 School continually strives.

This document constitutes the SIUSOM guidelines for the management of computer networks, personal computers and the resources made available thereby. This guideline is intended to reflect the academic and ethical principles of the School community and indicates, in general, the privileges and responsibilities of those using SIUSOM computing and network resources. A current copy of this document is available at: http://www.siumed.edu/ir/policy/.

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and facilities provided by SIUSOM are a privilege and NOT a right; access to such resources and facilities may be withdrawn, limited, modified or curtailed if there is reason to believe that the user has or may have violated this guideline, School or University policies, or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

All users, as a condition of their access to or utilization of SIUSOM computing or network services, agree to cooperate with and abide by SIUSOM and 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 SIUSOM computing services and waives any right of confidentiality. Any failure to cooperate fully with SIUSOM shall be considered a violation of this guideline.

Institutional Purposes

SIUSOM computing resources are to be used to advance the School's mission of education, research, patient care, and service to the community. Faculty, staff, and students may use them only for purposes related to their studies, their responsibilities for providing instruction, the discharge for their duties as employees, their official business with the School, and other School sanctioned or authorized activities. The use of SIUSOM computing resources and network services for commercial purposes including any sort of solicitation is prohibited, absent prior written permission of the

appropriate University official(s). Use of SIUSOM computing resources for political purposes is also prohibited.

Classification of Use

Decisions as to whether a particular use of computing and network resources conforms with this guideline shall be made by the Office of Dean and Provost if the use involves academic matters, by the Office of Student Affairs if the use involves non-academic student use, by the Office of Residency Affairs if the use involves residents or fellows, and by the Office of Human Resources if the use involves employees.

Computing use shall include, but is not limited to,

- Using SIUSOM provided computers and networks or computer equipment to create, modify, manipulate or store files, information, or electronic media.
- The creation, storage, manipulation or otherwise using electronic communications messages or email.
- Using SIUSOM communications networks for the purpose of accessing external resources (e.g. Internet, Partner Institutions, and Affiliates).

Cooperative Use

Computing resource users can facilitate computing at the School 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 as allowed by the State Records Act and if not subject to a litigation hold;
- Refraining from overuse of connect time, information storage space, printing facilities, processing capacity, or network services;
- Refraining from use of sounds and visuals which might be disruptive or offensive to others;
- Refraining from use of any computing resource in an irresponsible manner;
- Refraining from unauthorized use of computing resources.

Responsibilities of Users

The user is responsible for correct and sufficient use of the tools available for maintaining the security of SIUSOM computing resources and information assets. The following precautions are recommended:

- Users must not share computer accounts, passwords, and other types of authorization that are assigned to individual users with others;
- Users must assign an obscure account password and change it frequently;

- 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 malware (e.g. viruses, spyware, trojans, etc.) and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these programs;
- Users must take steps to ensure that personally owned or managed computers used to access SIUSOM resources and information assets are kept up to date with all critical patches and anti-malware software;
- 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 of certain materials to the Southern Illinois University users. Information regarding copyright may be obtained from the General Counsel's Office.
- Users must take all appropriate measures to ensure that protected information[1] is not inappropriately disclosed or otherwise compromised. If a user becomes aware of an actual or potential data compromise or misuse or improper disclosure of protected information, the user must immediately report the incident to the SIUSOM Information Security Officer (abuse@siumed.edu).
- Users may only access protected information in order to fulfill their individual job duties or professional responsibilities. Users may not access protected information of others (e.g., friends, relatives, co-workers, acquaintances, public figures) unless the user is conducting official School business.

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, damaging to the reputation of SIUSOM, inconsistent with the mission of SIUSOM, 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;

[1] Information that is protected from release by state and/or federal law/regulation or would require SIUSOM to provide notice to individuals and/or government agencies if information is lost, stolen or compromised; examples include protected health information (PHI/HIPAA), credit card numbers (PCI), banking information (GLBA), and protected student information (FERPA).

- Violation of copyrights and software licensing agreements, or unauthorized copying or transmission of copyright-protected material;
- Unauthorized installation or use of hardware or software, and in particular, software which may create a security risk to SIUSOM or its information assets;
- Use of the University's trademarks, trade names, logos, insignia, or copyrights without prior approval;
- Violation or attempted violation of computer system security;
- Unauthorized use of computer 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, etc.);
- 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 SIUSOM business;
- Development or use of unapproved mailing lists;
- 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, or other School or University policies;
- Violation of network usage policies 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;
- Violation of 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, viewing, or sending obscene, pornographic, sexually explicit, or offensive material;
- Posting or sending material that is contrary to the mission or values of the University;
- Intentional or negligent distribution of malware (e.g. viruses, spyware, trojans, etc.);

- 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.

Internet Use

Internet access is provided to assist users in furthering the mission of SIUSOM. Using the Internet for personal or entertainment purposes is a violation of Board of Trustee's Policy 5.J.3.g.

Impermissible uses of network access (some of which may also constitute illegal uses) include, but are not limited to, the following:

- Unauthorized extension of the SIUSOM network using equipment including: wireless access points, routers, hubs, switches, network connection sharing devices, etc.
- Use of peer-to-peer software and/or file sharing software, such as KaZaA, Bearshare, Gnutella, BitTorrent,iMesh, etc., that can be used to share files such as movies, music, or software in violation of copyright laws
- Non SIUSOM related audio/video streaming including but not limited to: Internet radio, NetFlix, iTunes, news, movie or television broadcasts, etc.
- Obscenity, pornography, threats, harassment, defamation, theft, copyright infringement, unauthorized access to computer resources, fraud, distribution of malware/malicious software, sending unsolicited bulk messages etc.
- Online gaming.

SIUSOM may inspect, monitor, record and/or block some protocols, traffic or programs to ensure the stability, security and/or performance of its computing resources.

Data Security

SIUSOM pursues a risk-based and cost-effectiveness-based security management strategy to most efficiently use its limited resources to best minimize the School's exposure to threats, hazards, and improper use or disclosure of protected information. It is assumed that users are aware that electronic files, data, and communications are not necessarily secure. Users of email systems should be aware that electronic mail in its present form is generally not secure and is vulnerable to unauthorized access and modification. Protected information shall not be sent by email unless secured by an authorized mechanism, e.g. secure messaging, encryption, etc.

SIUSOM is required by local, state and federal law and University policy to ensure the security of protected information it creates, receives, maintains, or transmits. SIUSOM and authorized users of its computing resources are required to take reasonable precautions to ensure the confidentiality, integrity and availability of these information assets.

SIUSOM will make available to interested persons information concerning reasonable methods for attempting to protect information assets and computing resources from

loss, tampering, and/or unauthorized access. The Information disclosed will vary according to the sensitivity of the data/system involved and the requestor's affiliation with SIUSOM.

Privacy and Confidentiality

SIUSOM reserves the right to inspect and examine any SIUSOM 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 is no reasonable expectation of privacy as it relates to information stored on SIUSOM computers or computing resources except to the extent provided by law. A former employee has no right to obtain information stored on SIUSOM computers or computing resources.

External Requestors

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

- When approved by the appropriate University official(s);
- When authorized by the owner(s) of the information;
- When required by federal, state, or local law;
- When required by a valid subpoena, search warrant, or court order;

When notice is required by law, search warrant, court order, or subpoena, users will receive notice of such disclosures.

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 States 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.

Internal Requestors

The Office of Human Resources, Legal Counsel or other appropriate SIUSOM official or their designees, may direct that an inspection and/or examination of any SIUSOM 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 a violation of impermissible use of computing resources.

If SIUSOM inadvertently discovers information that leads it to suspect the presence of illegal activities or activities which violate School or University policies, SIUSOM will be

free to use that discovered information to pursue investigations or inform the appropriate authorities.

The applicable University grievance policy is available to anyone who has been aggrieved by the inspection, examination or disclosure of SIUSOM computing resources or information assets by authorized SIUSOM personnel.

External Networks

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

Software Piracy

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 media, including labor and creativity resulting in computer software. It encompasses respect for the right to acknowledgement and the right to determine the form, manner, and terms of publication and distribution.

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.

Electronic Mail/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, offend, or annoy other users is forbidden. All users need to be aware that material which is obscene, defamatory, or violates University guidelines on non-discrimination will not be tolerated. SIUSOM reserves all rights to take appropriate measures to prevent, correct, or discipline behavior that violates this guideline.

Sanctions

Violations of this Guideline shall subject users to the regular disciplinary processes and procedures of SIUSOM and 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 campus computing resources, the University provides access to a vast amount of information. These materials are not affiliated with, endorsed by, edited by, or reviewed by SIUSOM or the University, and SIUSOM and the University takes no responsibility for the truth or accuracy of the content found within these information sources. Moreover, some of these sources may contain material that is offensive or objectionable to some users.

Existing University Rules and Regulations

This guideline is intended to be an addition to existing SIUSOM and University policies and guidelines and does not alter or modify any existing SIUSOM or University rule or regulation.

Related References

- Policies of the SIU Board of Trustees
- 5 ILCS 430 State Officials and Employees Ethics Act
- 815 ILCS 530/ Personal Information Protection Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Security Standards Council (PCI)

Revision History

Date	Type	Author	Description
15 Oct 2004			Approved by IMPC
16 Jun 2005	Technical	REF	Added *Revision History*
21 July 2005	Technical	REF	Clarified streaming definition
3 Jan 2014	Substantive	PMF	Additions to address protected information Added *Data Security* Added *Internet Use* Added *Related References* Minor content reordering
13 Feb 2014			Approved by IMPC
7 April 2014			Approved by SIUSOM Executive Committee