Document History
Responsible Administrator: CIO
Responsible Office: Office of Technology
Effective Date: 1/26/2021
Approved by: President
Date of Revision: 11/19/2020

Responsible Computing Policy

Policy Statement

This policy describes the University's expectations for responsible and productive computing. This policy applies to all computer users accessing Southeastern's computing resources, whether affiliated with the university or not, and to all uses of those resources, whether from on campus or from remote locations. The guidelines and procedures listed herein are subject to change and become void upon the approval and printing of subsequent versions.

Purpose of Policy

Southeastern Louisiana University's computing systems and networks provide powerful and flexible facilities and services for teaching, learning, research, and administration. The use of those systems imposes certain responsibilities and obligations on the users-the faculty, staff and students of Southeastern. Acceptable use is courteous, ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It also demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. The University grants access to its computing systems based on policies, codes of conduct, and local, state, and federal laws. Computer users must use computing resources for authorized purposes only.

Applicability

The Responsible Computing Policy applies to all computer users (or simply users), defined as employees, students, official contractors of Southeastern Louisiana University who are authorized to use Southeastern's computing resources, or any other individual who accesses computers, terminals, or networks belonging to Southeastern Louisiana University.

Policy Procedure

Section I. Appropriate Use of Computing Resources

Computing resources:

1. Computing hardware: including, but not limited to, desktop and laptop computers and their installed or to-be installed integrated circuit cards, keyboards, mice, printers (including paper and ink or toner cartridges designated for use therein), scanners, speakers, cameras, microphones, modems, and other ancillary equipment, network hubs, routers, and all the cabling to connect them together or to connect them to power sources;
2. Computing software: including, but not limited to, operating systems, application programs, and the data, configuration and other files used by the operating systems and application program.

Authorized use:

Computing resources are authorized for use in direct support of administrative and academic duties (including coursework), and for other purposes typically allowed by academic freedom, as long as users do not, intentionally or through neglect:

1. Circumvent the security of Southeastern's computing resources or use Southeastern's computing resources to circumvent security elsewhere, without express consent.
2. Harm or modify, without permission, Southeastern's computing resources.
3. Use Southeastern's computing resources for business purposes unrelated to the mission of Southeastern.
4. Illegally reproduce, use, or distribute copyrighted, licensed or trademarked materials, including computing software.
5. Harass or intimidate others.
6. Prevent others from performing authorized duties and assignments.
7. Monopolize systems, overload networks, degrade services, or waste computer time, connect time, disk space, printer paper, manuals, or other resources.
8. Violate Southeastern, University of Louisiana System, or Board of Regents policies, or local, state, or federal laws.

Enforcement:

Southeastern considers any violation of acceptable-use principles or guidelines to be a serious offense. The University reserves the right to copy and examine any files or information resident on University systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violators are subject to suspension of computer access and/or other disciplinary actions as prescribed in the Student Code of Conduct and employee handbooks. In addition, offenders may be prosecuted under state and federal laws including (but not limited to):

1. Family Educational Rights and Privacy Act of 1974
2. Computer Fraud and Abuse Act of 1986
3. Computer Virus Eradication Act of 1989
4. Telecommunications Act of 1996
5. Communication Decency Act of 1996 (Exon amendment)
6. Federal Copyright Law (Title 17)
7. Louisiana Revised Statute 14:73 (state law addressing computer crime including offenses against intellectual property, destruction of computer equipment, and committing computer fraud)
8. Digital Millennium Copyright Act of 1998

Access to the text of these laws is available through the Sims Memorial Library Reference Department. It should be noted that in instances where Southeastern Louisiana University policies and guidelines are in conflict with federal or state law, federal and state laws assume precedence.

Section II. Guidelines for Appropriate Use of Computing Resources

Introduction

Southeastern Louisiana University treats the abuse or misuse of computing resources seriously. Abusers of computing resources and privileges may be subject to suspension of computer access and/or other serious penalties imposed by the University's judicial processes. In addition, some abuses of computing resources may be illegal by the laws of Louisiana or the United States of America. Such abuses will be reported to the appropriate authorities and may result in

eventual civil or criminal prosecution. In some cases, Southeastern may have the right to seek reparations where applicable.

Physical damage and theft

Computing tools like library resources are shared, public facilities, essential to the scholarship of everyone at the University. The intentional and unauthorized alteration, damage, destruction or theft of computer hardware, software, data, or related equipment clearly is a violation of University standards and is a felony as well. In addition to refraining from such abuse, users have an obligation to report physical damage or theft that they see committed by others.

Personal use for monetary gain

In general, Southeastern's computing resources may not be used for personal financial gain. The distribution or posting of advertisements or notices for profit is prohibited. In addition, networking links or connections to external entities that would promote the personal gain of users is not permitted. The University recognizes that employees involved in the University's mission of teaching, research, and service have expertise that sometimes results in compensation from an external source, e.g., royalties on a book, consulting, etc. The University does not prohibit the use of computer equipment for fulfillment of an employee's primary obligations.

Copyrights, trademarks and licensing agreements

It is against the law and a violation of the University’s policies to reproduce, store, or distribute copyrighted material, including text, images, trademarks, sound, logos, or software without the express permission of the copyright owner, except as allowed under copyright law. It is a breach of contract to use or distribute software that violates applicable software licensing agreements.

Software or hardware tampering

Users should realize that self-initiated changes in computing resources for the purposes of causing harm or mischief may affect the entire University community adversely and are expressly prohibited. This includes unauthorized alteration, substitution or deletion of hardware, programs, command files, data files, or documentation and also includes the introduction of Trojan horses and viruses.

Unauthorized access to computer resources

Circumventing logon or security measures to gain access into the computing system either directly or indirectly or in any other manner accessing or using computer facilities or data by stealth or any other surreptitious manner is not permitted. Unauthorized access also includes using Southeastern's computer resources to gain entry to external systems and to intercept or divert network transmissions without express consent.

Negligence

In order to maintain the levels of security and privacy expected by the Southeastern computer user community, users are reminded that computer user IDs, logons, passwords, encryption keys, and related access information must be safeguarded from use by unauthorized entities. Negligence includes failure to protect computer resources from physical or other abuse. Users should notify University management or security personnel of either threatened or actual abuse. Safeguarding Southeastern’s computer resources is the entire community's responsibility.

Unauthorized access and use of data

Southeastern's computer systems daily access data and records that can be considered sensitive or confidential. Access and uses of such data except by authorized persons is not permitted.

Harassment

The University community encourages free speech and intellectual debate. However, free speech does not include hostile, intimidating, or threatening language or behavior. Southeastern Louisiana University has a tradition of providing a caring, nurturing environment for students and employees. Any use of computer resources for the creation or promulgation of harassing language or behavior will be investigated and may lead to disciplinary and/or legal action. The Student Code of Conduct and the University's Harassment and Discrimination Policy further outline prohibitive behaviors.

Equitable use of shared resources

Southeastern's computer facilities, systems, networks and servers are shared and finite. Users should be sensitive to the needs of others by not monopolizing or wasting computer resources. Examples of activities that may impede others use of computing resources include sending chain letters, junk mail or broadcast messages to many users ("spamming"), installing or running a program that places undue burden on computer systems, excessive non-academic or personal game playing, online chatting or printing, and storing excessive data. Users should regularly review and delete unnecessary email and data files that are stored on shared resources.

Federal and State Laws Governing Computers and Computer Use

Several state and federal statutes govern the use of computers and computing resources, and these laws have implications for users at Southeastern. Users must abide within lawfully prescribed parameters. These include:

- The Computer Fraud and Abuse Act of 1986, which presents information on unauthorized access to a federal-interest computer or to an interstate network such as the Internet. Such access is strictly prohibited and is subject to federal prosecution.
- Louisiana Revised Statute 14:73, which sets state law for computer crime including offenses against intellectual property, destruction of computer equipment, and committing computer fraud.
- The Telecommunications Act of 1996 and the Communication Decency Act of 1996, which prohibit Internet users from making indecent or offensive materials accessible to minors. Under this legislation, the courts are scrutinizing some student WWW pages at American universities. While the constitutionality of this legislation has not been fully determined, it is best for users to be cautious.

Website Policy

Policies and guidelines for the administration and content of web pages on Southeastern's web site, and for references to pages outside of Southeastern's website, are addressed in the University's Website Policy. This policy includes notification procedures for non-compliance with Website Policy.

Section III. Ensuring the Privacy and Security of Electronic Correspondence and Data

The University recognizes and respects individual privacy and makes every effort to provide a secure environment. It must be emphasized, however, that the current state of technology does not guarantee that e-mail and data security

cannot be breached. Therefore, it is essential that the University users do their part to protect security by selecting and protecting passwords and not allowing others to use their accounts.

The University does not routinely monitor e-mail communication or examine University-owned computer hardware or software. However, the University reserves the right to monitor the volume of communications sent through the network, to implement procedures to ensure integrity and security of computing resources (e.g. virus scans), and to examine computer hardware and software when evidence is presented to University officials that a user or users may be using the University's communications and computing facilities in violation of policy, state, local or federal laws.

When accessing a computer account, users are required to enter a user ID and a password. The ID identifies the person who is accessing the computer, and the password verifies that the user is authorized to use the account.

Computer and/or network access accounts are assigned to users for their exclusive use. It is a violation of policy to exchange, reveal, steal or misappropriate passwords without the express consent of the authorized user. Protecting account passwords is critical. Active computer sessions should never be left unattended. This includes, but is not limited to, administrative, student admissions and registration, financials, human resources, document imaging, and email. If unauthorized users gain access to an account, they can cause considerable damage to the account and/or to other parts of the system. For example, unauthorized users could read personal e-mail or other files, delete important files, gain access to sensitive or confidential information, or send email from the account. The recipient of such email has no way of knowing that the sender was not the account's owner.

Suspected or attempted uses of account(s) by unauthorized persons should immediately be reported to the Office of Technology.

Choosing and maintaining a secure password

An effective password must be easy to remember but should also be difficult to guess. The guidelines below are in line with best practices individuals should consider when choosing and maintaining passwords for both work and personal use. Here are some good guidelines for creating an effective password:

1. Use mnemonics to create your password. A mnemonic is a formula, sentence or rhyme that helps you remember something. An example of a mnemonic password would be: "Even my 2 cats can't guess my password," the password becomes: em2ccgmp.
2. Mix letters and numbers.
3. Do not use words that can be found in the dictionary. Many password-cracking programs try all the words in a dictionary.
4. Do not use the names of friends, spouses, children, or pets. These are easy to guess.
5. Do not use dates, phone numbers or your social security number. These are also easy to guess.
6. Do not use something that is so hard to remember so that you have to write it down.
7. Do not use repeated characters or keyboard patterns such 000000 or asdfjkl.
8. Change your password frequently, at least every three months.
9. Consider using a password manager program. Free password management software is widely available.
10. Use 2-factor authentication to further secure your account.

[end of policy]