Acceptable Uses of Information Technology Resources

Southern University and A&M College
Baton Rouge, Louisiana

Effective:

The following employees are responsible for the accuracy of the information contained in this document

Responsible Officer: Director of Technology and Network Services

Responsible Office: Office of Technology and Network Services

Direct Comments to:

Office of Technology and Network Services
Suite 222, James B. Moore Hall
E. C. Harrison Boulevard
P. O. Box 12891
Baton Rouge, Louisiana 70813
Voice: (225) 771-3935
Fax: (225) 771-2883

<u>Acceptable Use of Information Technology Resources</u>
Policy Statement

Computers, networks and other electronic information systems are essential resources for accomplishing the Southern University and A&M College Baton Rouge's mission of instruction, research, and service outreach. The University grants members of the University community shared access to these resources in support of accomplishing the University's mission. These resources are a valuable community asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate educational and business activities. All authorized users of these resources are required to use them in an effective, efficient, and responsible manner.

Users must be aware and knowledgeable of the Users' Rights and Responsibilities, which outline their liability for personal communications, privacy rights and security issues, and consequences for violating this policy. Users should also be aware of the University's Rights and Responsibilities, as well as any additional requirements of the Southern University System. A list of relevant University information technology policies and guidelines is available in the Related Information section below.

This policy is intended to conform to the provisions of the Southern University System's Strategic Plan for Information and Technology Resource Management. All conflicts will be resolved and governed by the content of the System Strategic Plan.

Purpose for Policy

The purpose of this policy is:

- to safeguard the integrity of computers, networks, and data located at the Southern University and A&M College at Baton Rouge and at other locales that network with the university's computer and other related electronic systems;

- to ensure that the use of electronic communications complies with University policies, rules and regulations, federal and state laws and other applicable regulations;

- to protect the University against damages, liability and the legal consequences that may result from the misuse and/or abuse of its various electronic systems.

Contents

Who Should Know This Policy

All members of the Southern University community who assesses or receives information through electronic means provided by the University are charged with the responsibility of knowing the provisions of this policy. The following persons are particularly charged with the responsibility knowing and applying the provisions herein:

Chancellor	Vice Chancellors	Deans
Directors	Department Heads/Chairs	Principal Investigators
Faculty	Property Manager	All Employees
Undergraduate Students	Professional Program Students	Graduate Students
	Other Authorized Users	

Related Information

This following list of policy and informational sources is provided to assist users in locating guidelines and information related to fully utilizing and implementing this policy effectively and appropriately:

University:

- Southern University Code of Student Conduct

- Southern University Faculty and Staff Employment Manuals and/or Handbook

- Information Systems Division Policies and Procedures

- Campus Network Policies and Procedures

- Publishing Information on the World Wide Web

- Computer Laboratories Software Installation Policy

- Southern University Policy on Use of University Equipment and Property

Federal:
- Computer Fraud and Abuse Act, 1986

- Electronic Communications and Privacy Act

- Family Release and Privacy Information Act

Contacts

Subject	Contact	Telephone
Threatening Behavior	University Police	(225) 771-2770
Computer Misuse Emergency/In-Progress	Office of Technology and Network Services	(225) 771-3935
Network or System Attacks	Office of Technology and Network Services – CNM	(225) 771-2692
Administrative System Attacks	Information Systems Division	(225) 771-4410

History

This document appears in its original format and has not been amended since becoming effective.

Effective: _____

Definitions

Authorized User

Any individual or entity permitted to use University computers, networks or tele or video resources. Authorized users include students, staff, faculty, alumni, sponsored affiliates, and other individuals who have an association with the University that grants them access to University information technology resources. Some users may be granted additional authorization to access institutional data by the data owner or custodian.

Data Custodian

Data custodians are representatives of the University who are assigned the responsibility to serve as a steward of University data in a particular area. They are responsible for developing procedures for creating, maintaining, and using University data, based on University policy <u>and applicable state and federal laws</u>.

Information Technology Resources

Facilities, technologies, and information resources used for University information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, paging systems, video, multimedia, and instructional materials. This definition is not all-inclusive but rather reflects examples of University equipment, supplies and services.

Security Measures

Processes, software, and hardware used by system and network administrators to ensure the confidentiality, integrity, and availability of the information technology resources and data owned by the University and its authorized users. Security measures may include reviewing files for potential or actual policy violations and for investigating security-related issues.

Responsibilities

Users' Rights and Responsibilities

Members of the University community are granted access to information technology resources in order to facilitate their University-related academic, research, and job activities. The University policy on Academic Freedom extends to information resources that are available electronically. However, by using these resources, users agree to abide by all relevant Southern University and A&M College at Baton Rouge policies and procedures, as well as all current federal, state, and local laws. These include, but are not limited to University policies and procedures related to harassment, plagiarism, commercial use, security, and unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws.

Users are responsible for:

- reviewing, understanding, and complying with all policies, procedures and laws related to access, acceptable use, and security of University information technology resources;

- asking systems administrators or data custodians for clarification on access and acceptable use issues not specifically addressed in University policies, rules, guidelines, and procedures; and

- reporting possible policy violations to the appropriate entities listed in this document (See: Contacts and Procedures sections).

Liability for Personal Communications

Users of University information technology resources are responsible for the content of their personal communications. The University does not and will not accept responsibility or liability for any personal or unauthorized use of its resources by users. The University will act to protect itself from claims of damages caused by the abuse or use of its information technology resources for personal reasons and/or in unauthorized ways. In using the University's information technology resources, all users agree to hold the University harmless and to protect the University from liability claims arising from their personal or unauthorized use of these resources.

Privacy and Security Awareness

Users should be aware that although the University takes reasonable security measures to protect and secure the integrity of its computing resources and accounts assigned to individuals, the University does not guarantee absolute security and privacy. Users should follow the appropriate security procedures listed in the Guidelines section of this policy to assist in keeping systems and accounts secure.

The University assigns responsibility for protecting its resources and data to system administrators and data custodians, who treat the contents of individually assigned

accounts and personal communications as private and do not examine or disclose the contents except:

1. as required for system maintenance, including security measures;

2. when there exists reason to believe that an individual is violating the law or University policy; and/or

3. as permitted by applicable policy or law.

Consequences for Policy Violations

Access privileges to the University's information technology resources will not be denied to any authorized user without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its computers and networks or to protect itself from liability, the University may temporarily deny a user access to those resources. Allegations of policy violation(s) will be referred to appropriate University investigative and disciplinary units. For example, alleged violations by students may be directed to the Office of Student Affairs. The University may also refer suspected violations of law to appropriate University and external law enforcement agencies. Depending on the nature and severity of the offense, policy violations may result in loss of access privileges, University disciplinary action, and/or criminal prosecution.

The University's Rights and Responsibilities

As the owner of the computers and networks that comprise the University's technical infrastructure, the University owns all official administrative data that resides on its systems and networks, and is responsible for taking the necessary measures to ensure the security of its systems, data, and users' accounts. The University does not seek out personal misuse. However, when the University becomes aware of violations, either through routine system administration activities or from a complaint, it is the University's responsibility to investigate reported or suspected violations, as needed or directed, and to take the action(s) necessary to protect its resources and/or to provide information relevant to an investigation.

The University shall ensure that all employees and other users are aware of policies and procedures governing technology deployment and that the University reserves its right periodically inspect and audit the uses of its technology resources.

Individual units within the University may define additional conditions of use and may provide additional details, guidelines, and/or restrictions for using resources or facilities under their control. However, all such additions must be approved and be consistent with this policy.

Roles and responsibilities for specific University entities and individuals are defined in greater detail below.

Director of Technology and Network Services and/or Director Information Systems Division will:

- Designate individuals who have the responsibility and authority for information technology resources at SUBR.

- Establish and disseminate enforceable rules regarding access to and acceptable use of information technology resources.

- Establish reasonable security policies and measures to protect data and systems.

- Monitor and manage system resource usage.

- Investigate problems and alleged violations of University information technology policies.

- Refer violations to appropriate University offices, such as the Office of the Chancellor and the University Police Department, for resolution or disciplinary action.

College or Department will:

- Create, disseminate and enforce conditions of use that are consistent with University-wide policies for using the University's facilities and/or resources under its control.

- Monitor the use of University resources under its control.

- Investigate problems and alleged violations of the University's information technology policies.

- Refer known violations of this policy to appropriate University offices, such as the Office of Technology and Network Services, the Office of the Chancellor, and the University Police Department, for resolution or disciplinary action. Suspected policy violations should be reported to the appropriate entity listed in the Contacts section of this document.

Data Custodians will:

- Grant authorized users appropriate access to the data and applications for which they are stewards; work with University data security and network personnel to limit access to authorized users with a legitimate role-based need.

- Review access rights of authorized users on a regular basis.

- Respond to questions from users relating to the appropriate use of system/network resources.

- Implement and oversee processes to retain or purge information according to University records retention schedules.

Acceptable Use of Technology Policy

- Determine the criticality and sensitivity of the data and/or applications for which they are stewards; determine which University data is public and private based on University definitions, in consultation with the University's Office of Records and Information Management.

- Ensure that appropriate security measures and standards are implemented and enforced for the data under their control, in a method consistent with University policies and sound business practices. The security measures implemented should be based on the criticality, sensitivity, and public or private nature of the data, and may include methodologies, change management, and operational recovery plans.

- Investigate problems and alleged violations of University information technology policies.

- Refer violations to appropriate University offices such as the Office of the Vice Chancellor, General Counsel and the University Police Department for resolution and/or disciplinary action.

System/Network Administrator will:

- Take reasonable action to ensure the authorized use and security of data, networks, and the communications transiting the system or network.

- Participate and advise as requested in developing conditions of use or authorized use procedures.

- Respond to questions from users relating to appropriate use of system/network resources.

- Cooperate with appropriate University departments and law enforcement officials in investigating alleged violations of policy or law.

Office of Records and Information Management will:

- Assist data custodians in classifying information as public or private. Secure official rulings from the Office of the General Counsel on public and private information.

University Police Department will:

- Respond to alleged violations of criminal law.

- Coordinate all activities between the University and outside law enforcement agencies.

General Counsel will:

- Provide legal advice relative to official rulings on public, private and confidential information.

- Provide representation and guidance, as appropriate when requested, during investigations, reviews, etc.

Procedures

In support of the this policy, the following procedures are applicable:

Reporting Violations

Taking Disciplinary Action

Use of Technology Resources Guidelines

In support of this policy, the following are included:

Guidelines for Using Information Technology Resources .

Guidelines for Using Information Technology Resources

- ⌨ Use e-mail, computers, and networks only for legally authorized purposes. Unauthorized or illegal uses include, but are not limited to, harassment, destruction of or damage to equipment, software, or data belonging to the University or others; unauthorized reproduction of copyrighted materials; private or personal business unrelated to the University's business or activities.

- ⌨ Users are warned not to share the account information or password assigned to you. Select an obscure password and change it frequently.

- ⌨ Users are responsible for all activities utilizing their user name/account ID and/or originating from their system. If a user has reason to believe that his/her user name/account ID or password has been compromised, the user should contact the System/Network Administrator immediately.

- ⌨ Users should never disclose information to which they have access but not ownership or the authority or permission to disclose.

- ⌨ Users should only access accounts, files, and data that is their own or that is publicly available, or to which they have been given authorized access.

- ⌨ Users should use only legal versions of copyrighted software on Southern University and A&M College owned computer or network resources in compliance with vendor license requirements.

- ⌨ Users should not engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized or unapproved changes to data files.

- Southern University's prohibition against sexual, racial, religious, and other forms of harassment is extended to include the use of electronic and communications systems.

- Use of Southern University's computers and information systems must conform with all other university policies related to harassment, discrimination, and conduct in the workplace.

- University employees and other authorized users are prohibited from sending and receiving harassing and/or offensive messages, pictures, files, etc. using University technology resources.

- Employees may not use university equipment or university time to visit sexually explicit and/or other questionable websites.

- All computer equipment and software are property of the university and shall not be used in any way that is illegal, harmful to university operations, and/or pose potential embarrassment to the university or place it in a negative light.

- Southern University reserves the right to periodically inspect and audit the use of university computer(s), E-mail and Internet access to ensure compliance with university policy. Disciplinary action shall be taken against an employee who is found to have violated these policies.

- Southern University reserves the right to enter and inspect the contents and to deactivate an authorized account when the user leaves or is no longer associated with the University and has not taken the appropriate steps to formally decommission the account or to secure authorization for its continued use

- Users are cautioned to: 1) be aware of conditions of services and encouraged to consult with the System Administrator relative to any questions about system workload(s); and 2) refrain from monopolizing and overloading systems or networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

- For situations not covered by these provisions, users should contact their system/ network administrator or departmental data custodian.

Reporting Violations

Violations of this policy may involve any of the issues described in Appendix A of this policy. Violations should be reported to the appropriate office from the list below or to the department's designated technology steward:

Violence or threats or damaging acts in the workplace

- Contact University Police regarding threats to personal safety: for emergencies, call 911; for non-emergencies, call (225) 771-2770. For consultation on potential threats to personal safety, call the Southern University Police Department at (225) 771-2770.

Computer misuse/unauthorized use

- Contact the departmental system/network administrator or technical support staff. In an emergency, during an in-progress attack, contact the Office of Technology and Network Services at (225)-771-3935. For after-the-fact or non-emergency reports, send logs and other pertinent information to the Office of Technology and Network Services. Report account misuse (such as spamming* by account-holders at the University) to webmaster@subr.edu. Report spamming from outside of the University to the originator's ISP.

Activities with potential legal consequences

- Report activities with potential legal consequences for the University to the Office of the General Counsel at (225) 771-4680.

Taking Appropriate Disciplinary Action

1. Student
   Follow the standards set forth in the Code of Student Conduct.

2. Faculty and Staff
   Follow the appropriate employment manual or handbook or <u>Bylaws and Regulations of the Board of Supervisors.</u>

3. Other Authorized Users
   Follow the provisions for sanctions in the agreement authorizing the use of the university's technology resources.