Policy # 5.51
SOUTHERN UTAH UNIVERSITY **Date Approved: 10/21/11**
Date Amended:
Policies and Procedures **Reviewed w/no Changes:**
Office of Responsibility: CIO
Page 1 of 8

SUBJECT: INFORMATION TECHNOLOGY RESOURCES

I. PURPOSE

To outline the University's policies for students, faculty, staff and others, concerning the use of the University's computing and communication resources, including those dealing with voice, data, and video. This policy governs all activities involving the University's computing facilities and Information Technology (IT) Resources, including electronically or magnetically stored information. Every user of these systems is required to know and follow this policy.

II. REFERENCES

A. SUU Policy and Procedures, 5.27, Sexual Harassment
B. SUU Policy and Procedures, 5.39, Records Access and Management
C. SUU Policy and Procedures, 5.46, Student Responsibilities and Rights
D. SUU Policy and Procedures, 5.52, Intellectual Property
E. SUU Policy and Procedures, 5.8, Computer Software Licensing
F. SUU Policy and Procedures, 5.55, Web Services
G. SUU Policy and Procedures, 5.57, Information Technology Resource Security
H. SUU Policy and Procedures, 5.58, University E-mail
I. SUU Policy and Procedures, 6.22, Faculty Due Process
J. SUU Policy and Procedures, 8.3.5, Termination of Non-Academic Staff Employees and Disciplinary Sanctions
K. SUU Policy and Procedures, 11.2, Student Rights, Responsibilities and Conduct
L. 18 U.S.C. § 2510: Electronic Communications Privacy Act
M. Utah Code Ann. § 76-6-703: Utah Computer Crimes Act
N. Utah Code Ann. § 76-10-1801: Communications Fraud
O. Utah Code Ann § 63-2-101 et seq.: Government Records Access and Management Act (GRAMA)
P. Acknowledgments: University of Utah Information Technology Resources Policy (Policy 4-002)

III. DEFINITIONS

A. Information Technology (IT) Resources include any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage, transfer, and use of information. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, web sites, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

B. Best Practices is a set of guidelines and procedures governing how the IT department installs, configures and supports Users and IT Resources. It is found on the IT department web site and is continually evaluated and updated.

C. User includes anyone who accesses and uses Southern Utah University Information Technology Resources.

D. Chief Information Officer (CIO): The Chief Information Officer is responsible for Southern Utah University's IT planning, budgeting, and performance including its information security components.

E. Utah Government Records Access and Management Act (GRAMA).

IV. APPLICABILITY

This policy applies to all Users of University Information Technology Resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations.

V. POLICY

A. General

1. Southern Utah University makes available Information Technology Resources which may be used by University students, faculty, staff and others. These resources are intended to be used for educational purposes and the legitimate business of the University and in a manner consistent with the public trust. Appropriate use of the resources includes instruction, independent study, authorized research, independent research and the official work of the offices, departments, recognized student and campus organizations of the University.

2. Access to computer systems and/or networks owned or operated by Southern Utah University imposes responsibilities and obligations on its Users. Access is granted subject to University and Board of Regents policies, and local, state, and federal laws. Appropriate use is ethical, reflects academic honesty, and shows restraint in the utilization of shared resources. Appropriate use is consistent with academic freedom, intellectual property rights, ownership of data, system security mechanisms, and rights to privacy and to freedom from intimidation, harassment, and annoyance.

3. It is the University's policy to maintain access to local, national and international sources of information, and to provide an atmosphere that encourages access to knowledge and sharing of information. The University also strives to create an intellectual environment in which students, staff, and faculty feel free to create individual intellectual works as well as to collaborate with other students, staff, and faculty without fear that the products of their intellectual efforts will be violated, misrepresented, tampered with, destroyed, stolen or prematurely exposed. Nothing in this policy guarantees that violations of this policy will not occur or imposes liability on the University for any damages resulting from such a violation.

4. The University retains the right to allocate its Information Technology Resources and to control access to its electronic communications systems.

5. In order for the University to maintain a stable, reliable and secure computing environment, and to make the most efficient use of IT Resources and staff, the IT department will maintain a Best Practices document governing the installation, configuration and use of IT Resources. The Best Practices document will be available on the IT department’s web site. Users are encouraged to familiarize themselves with the various sections of the document that may impact their use of IT Resources.

B. Privacy

1. Electronic communications systems have inherent limitations. No computer security system can absolutely prevent a determined person from accessing stored information that he/she is not authorized to access. Moreover, electronic documents may be disclosed pursuant to public records law or in the litigation / administration discovery process.

2. Users should be aware that their uses of University Information Technology Resources are not completely private. While the University does not routinely monitor individual usage of its Information Technology Resources, the normal operation and maintenance of the University’s computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for rendering reliable service. The University may also specifically monitor the activity and accounts of individual Users of University Information Technology Resources, including individual login sessions and communications, without notice, when (a) the User has voluntarily made them accessible to

the public; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other Information Technology Resources or to protect the University from liability; (c) there is sufficient cause to believe that the User has violated, or is violating, this policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in “(a)”, required by law or necessary to respond to perceived emergency situation, must be authorized in advanced by the CIO or designees.

3. The University, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made by means of University Information Technology Resources are also generally subject to GRAMA statutes to the same extent as they would be if made on paper.

4. Appropriate administrators and network managers may require access to records and data typically regarded as private. In particular, individuals having official computer or network responsibilities, such as system administrators, network supervisors, system operators, electronic mail postmasters, or others who cannot perform their work without access to documents, records, electronic mail, files or data in the possession of others, may access such information as needed for their job responsibilities. Whenever practical, prior notice should be given for other than trivial intrusions on privacy.

C. Individual Responsibilities

1. Users shall respect the privacy and access privileges of other Users both on the University campus and at all sites accessible through the University's external network connections.

2. Users shall treat institutional data, files maintained by other Users, departments, or colleges as confidential unless otherwise classified pursuant to state or federal statutes, regulation, law, or University policy. Users shall not access files or documents belonging to others, without proper authorization or unless pursuant to routine system administration.

3. Users shall not knowingly falsely identify themselves and will take steps to correct misrepresentations if they have falsely or mistakenly identified themselves.

4. In making appropriate use of Information Technology Resources, Users must:

   a. Use only those Information Technology Resources that they are authorized to use and use them only in a manner and to the extent authorized. Ability to access Information Technology Resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

   b. Protect their user-ID from unauthorized use. User-IDs and passwords should not be shared with, or used by, persons other than those to whom they have been assigned by the University. Users are ultimately responsible for activity conducted using their account. If a User suspects that their account has been compromised, he/she should change their password immediately.

   c. Be considerate in their use of shared resources and refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources. The University may require Users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

   d. Comply with all federal, Utah, and other applicable law; all applicable University policies; and all applicable contracts and licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

5. Users must respect the integrity of computing systems and networks, both on the University campus and at all sites accessed by the University's external network connections. As such, in making appropriate use of Information Technology Resources Users must NOT:

   a. Gain, attempt to gain, or help others gain access without authorization.

b. Use or knowingly allow other persons to use University Information Technology Resources for personal gain, for example, by selling access to their User-ID's, or by performing work for profit or contrary to University policy. Personal use of University Information Technology Resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the User’s job or other University responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

c. Destroy, damage, or alter any University Information Technology Resource or property without proper authorization.

d. Waste computing resources, for example by implementing or propagating a computer virus, using destructive software, or inappropriate game playing; or monopolizing Information Technology Resources for entertainment or personal use.

e. Harass or intimidate others in violation of law or University policy.

f. Violate laws or University policy prohibiting sexual harassment or discrimination on the basis of race, color, religion, gender, national origin, age, disability, sexual orientation, or veteran status.

g. Attempt to monitor or tamper with another User's electronic communications or copy, change, or delete another User's files or software without the explicit agreement of the owner(s); or

h. Violate state and federal laws pertaining to electronic mailing of chain letters and other unauthorized use of computing resources or networks.

i. Make or use illegal copies of copyrighted or patented software, store such copies on University systems, or transmit such software over University networks.

j. Attempt, without authorization, to circumvent or subvert normal security measures or engage in any activity that might be harmful to systems or information stored thereon or interfere with the operation thereof by disrupting services or damaging files. Examples include but are not limited to: running "password cracking" programs, attempting to read or change administrative or security files or attempting to or running administrative programs for which permission has not been granted, using a telnet program to connect to system ports other than those intended for telnet, using false identification on a computer or system or using an account assigned to another, forging mail or news messages.

k. Transfer software, files, text, or pictures in violation of copyright and/or pornography laws, or transfer software or algorithms in violation of United States export laws.

l. Send email in violation of the University Email Policy, Policy 5.58.

VI. Enforcement

A. A violation of the provisions of this policy or departmental policy is a serious offense that may result in the withdrawal of access and in addition may subject the User to disciplinary action or academic sanctions consistent with University Policies and Procedures. Violation of University policy or federal, state, and/or local law may lead to University disciplinary action and/or prosecution or other appropriate legal action. Members of the University community who violate this policy may be subject to disciplinary action as described in SUU Policy 6.22, Faculty Due Process; SUU Policy 8.3.5, Termination of Non-Academic Staff Employees and Disciplinary Sanctions; and/or SUU Policy 11.2, Student Responsibility and Rights.

B. A systems administrator may immediately suspend the access of a User when the administrator reasonably believes:

1. the User has violated University policies or law; and

2. the User's continuing use of Information Technology Resources will result in: (1) damage to the Information Technology Resources systems, (2) further violations of law or policy, or (3) the destruction of evidence of such a violation.

3. the User shall be informed of his/her right to immediately appeal such a suspension to the cognizant head of the department or unit. Permanent revocation of privileges shall be imposed solely through the disciplinary processes set forth in paragraph A above. (Section VI.A)

4. Users who are not faculty, staff or students may have their access to Information Technology Resources unilaterally revoked if they violate this policy.