



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

I. PURPOSE

To establish policy on the acceptable use of Southern Utah University computer systems, networks, and Internet resources. To define the responsibilities of individuals and of Information Technology (IT) staff to maintain appropriate security measures covering university networks on campus.

Implementation and Review

CIO is responsible for the implementation of this policy and for its periodic review, for network security needs appropriate to the campus, and for general oversight of the elements of network security. The committee will invite the academic and administrative user groups to participate.

II. REFERENCES

SUU Policy and Procedures, 5.8, Computer Software Licensing

SUU Policy and Procedures, 5.46, Student Responsibilities and Rights

SUU Policy and Procedures, 6.6, Academic Freedom

SUU Policy and Procedures, 5.27, Sexual Harassment

SUU Policy and Procedures, 5.19, Personnel Records and Privacy Rights

SUU Policy and Procedures, 5.39, Records Access and Management

SUU Policy and Procedures, 5.52, Intellectual Property

Utah State Board of Regents Policy and Procedures, R341, Computing Systems Program

Utah State Board of Regents Policy and Procedures, R343, Information Management

Utah Code 63-2-206, Government Records Access and Management Act (GRAMA)

Acknowledgments: Ohio State University and Cornell University resources on computer policy and law (www.cuinfo.cornell.edu/CPL/policies/)



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

III. INTRODUCTION

A. Glossary of Terms and Acronyms

AUDITING AND REVIEW: To insure that all components and employees are in compliance with this policy, periodic audits of equipment, configurations, and systems will be performed by the IT staff. Account authorizations, id and password protections, and file protective measures will be part of the audit. Peripheral networks, such as housing and some notebook subnets, may be established outside the campus firewall, and they will be periodically reviewed.

CIO: Chief Information Officer

DNS Domain Name Service: A network protocol for determining a computer's Internet address

DUE PROCESS: As with other university policies, appropriate notice and an opportunity for discussion or hearing will be provided. Where applicable, grievance policies are also provided.

ENCRYPTION: As an extra protection when using the university's networks, and to protect sensitive information sent over insecure lines, some data may be encrypted. IT staff will support, in coordination with appropriate software vendors, encryption as applications may require. Digital certification will be a responsibility of the CIO.

FIREWALL: A dedicated security system to protect access to networks.

HACKER: Someone who attempts to compromise computer or network security.

HOST: Roughly, a computer.

INCIDENT RESPONSE & DISASTER CONTINGENCY PLAN: SUU employs security measures for intercepting virus attacks, backing up servers for data recovery, and other standard network security measures. The CIO is responsible for contingency planning and for implementing data security measures in case of a disaster or emergency.



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

ILLEGAL ACTIVITIES: Pertinent laws include, but are not limited to:

- *Copyright:* (See SUU policy 5.52)
- *Disruptive Activities:* (Section 76-8-703 U.C.A.)
(Section 76-8-704 U.C.A.)
(Section 76-8-705 U.C.A.)
- *Sexual Harassment:* (See SUU policy 5.27)
- *Threats:* 18 U.S.C. 875
- *Libel:* (Section 76-9-502 U.C.A.)
- *Public Displays:* (Section 76-10-1228 U.C.A.), (Section 76-10-1227 U.C.A.)
- *Pyramid Schemes:* Utah law (Section 76-6a-3 U.C.A.)

INORDINATE: Determined by affected system administrators. Including, but not limited to: affecting available disk space, CPU time, e-mail system, printing facilities, and dial-up access lines.

INTERCEPTION: Utah law (Sections 77-23a-1 to 16 U.C.A.) allows for interception of communications.

- SUU, may provide information/technical assistance to persons authorized by law to intercept communications if they are provided with a court order or authorization from the Attorney General's office stating that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.
- System administrators may intercept electronic communications if one of the parties to the communication has given prior consent to the interception (unless it is intercepted to commit a crime or a tort) or if the electronic communication is made through a system that is readily accessible to the public. System administrators may divulge the contents of any communication:



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

- as authorized under Utah Law Section 77-23a-4 or 77-23a-9;
- with lawful consent of the originator or any addressee or intended of the communication;
- to a person employed or authorized or whose facilities are used to forward the communication to its destination;
- that is inadvertently obtained by system administrators and to pertain to the commission of the crime (contents can then be revealed only to law enforcement).

IT. Information Technology department

KEY MANAGEMENT. Keys are used to encrypt and decrypt data and are the responsibility of the CIO who will determine key length, changes, key escrow, generation and distribution.

PASSWORDS AND AUTHENTICATION. Passwords provide access to individual user accounts and other restricted areas within the computer system, and must be kept confidential. Passwords are not to be shared and are the user's primary assurance of privacy within the computer system. In addition to user id and password authentications, there may be need to go to a token-based authentication. The Network Manager or CIO will determine the level of authentication. If a modem is necessary for dial-in access, it will be installed by IT support personnel who will set up the proper security.

ROUTINE MAINTENANCE of the system includes, but is not limited to: security checks, deletion of temporary files, verification of E-mail delivery, regular back ups, and assurance of available disk space.

SECURITY BREACH:

1. Unauthorized use of an account.
2. Unauthorized access or unauthorized changes to system resources.
3. Unauthorized attempts to use or acquire others' passwords.



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

SOFTWARE SECURITY. The University uses both commercial and non-commercial software on servers, workstations and the network. Purchasing and installing software for campus-wide use is the responsibility of the IT staff. Downloading software from the Internet onto university servers or computers is not authorized without coordination with the IT staff. However, faculty may download “shareware” software for use in their own environments. Computer software protected by copyright is not to be copied from, into or by using university computers, except as permitted by law or by the license or contract with the owner of the copyright. The software license or contract will define number of copies, simultaneous users, machine exclusivity, etc.

SPAM: Unsolicited bulk electronic mail e.g., broadcast announcements, chain letters, surveys, etc.

SPAMMING: The distribution of unsolicited bulk electronic mail (spam).

SYSTEM FILES: Any files that control or otherwise affect the startup or operation of a computer system.

TLT. Teaching, Learning, Technology committee—an advising committee of campus constituencies on technology-related issues.

B. General Statement

As a part of the physical and social learning infrastructure, Southern Utah University acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for university-related purposes, including direct and indirect support of the university’s instruction, scholarly/creative, and service missions; of university administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the university community and between the university community and the wider local, national, and world communities.

The rights of academic freedom and freedom of expression apply to the use of university computing resources and university-hosted web sites of faculty and students. So, too, however, do the responsibilities and limitations associated with those rights. The use of university computing resources, like the use of any other university-provided resources and like any other university-related activity, is subject to the normal requirements of legal and ethical behavior within the university community. Thus, legitimate use of a computer, computer system, or network does not extend to what ever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Computers and networks are ubiquitous at SUU. Electronic mail, payroll, submitting homework, processing financial aid, and scholarly/creative efforts—all involve computers and networks. In the near term, digital transactions and signatures, wireless technology, and other “enhancements” to university operations will be implemented.

The benefits of electronic information and communication come with commensurate risks. Confidential information can be intercepted on the networks. Access to critical business systems can be compromised. A hacker from the other side of the world (or the lab next door) can do irreparable damage. A key communication medium on campus is e-mail. Additionally, web access has become a key to good communication and information dissemination, and more and more student services transactions (admissions, registration, tuition payment, and grade review) are web based. E-commerce in higher education is ever-expanding, and all these applications depend on the networks of the university.

C. Incident Detection and Response

Open access to campus networks without adequate traffic control and security exacerbates security incidents and exposes the university to the wholesale compromise of data. Examples of network security incidents include using sniffer software to invade someone else’s network transactions, spamming, forging e-mail return addresses, e-mail harassment, using SUU computers for private commercial purposes, using the network as a courier site for commercial software, generating or transmitting viruses (often unwittingly), and packet-flooding (dispersing information packets for fraudulent purposes so that they appear to be coming from a variety of hosts). . Have these incidents happened at SUU? Yes. Indeed, recent global viruses have destroyed university hardware, costing thousands of dollars. In response the university has acquired a comprehensive virus detection system. It intercepts two to three dozen viruses each day. Rebuilding drives, replacing equipment, fixing software applications, and other system failures are costly to the university and divert the efforts of IT staff.

IV. APPLICABILITY

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations.

V. POLICY



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

- A. All users of university computing resources must:
- comply with all federal, Utah, and other applicable law; all applicable university policies; and all applicable contracts and licenses. Examples of such laws, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud Abuse Act, which prohibit “hacking”, “cracking”, and similar activities; the university’s code of student responsibilities and rights; the university’s sexual harassment policy; and the university’s software licensing policy. 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.
 - use only those computing resources that they are authorized to use and use them only in a manner and to the extent authorized. Ability to access computing 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. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university.
 - respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Ability to access other persons’ accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
 - respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of university computing 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.
 - refrain from using those resources for personal commercial purposes or for personal financial or other gain. Personal use of university computing resources for other



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

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.

- refrain from stating or implying that they speak on behalf of the university or from using university trademarks and logos without authorization to do so. Affiliation with the university does not, by itself, imply authorization to speak on behalf of the university. Authorization to use university trademarks and logos on university computing resources may be granted, as appropriate. The use of suitable disclaimers is encouraged.

The University does not grant permission or authority to use the system in violation of this policy. This policy does not limit or supercede any other University policies. Access to the University's computer systems is a privilege granted to authorized users.

B. Elements of Network Security

1. **Physical Security.** The network depends on the integrity and security of interconnections. Communications rooms, wiring closets, and server rooms, are to be protected and access restricted. The CIO and designees, as well as campus security and plant operations staff, are granted access to these rooms.
2. **Network Security.** The University has implemented a variety of devices and security measures to protect its networks. The measures include firewalls, access controls, network auditing, Internet services, and file system directory structures. The CIO is responsible for engaging security measures that protect network security.
3. **Access Control.** Access controls such as passwords and domain security ensure that people have access to their own information or services. Traffic will be controlled and channeled in the following manner:
 - a. **Outgoing traffic.** All network traffic originating from the University will be permitted without constraint to leave campus. For any connections to the Internet that originate on campus, the replies will be permitted to return. However, pursuant to this policy, illegal activities will be blocked, as will any attempts to hack another computer.
 - b. **Incoming traffic.** Network connections originating off-campus will be permitted under these conditions: (1) Web services will be permitted to



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

approved web servers, (2) FTP will permitted to approved FTP servers, (3) Telnet will be permitted to approved telnet hosts, (4) Mail will be permitted to approved mail servers, (5) Domain Name Service (DNS) requests will be permitted to the campus DNS servers, and (6) when an off-campus vendor needs access to a particular machine they support or maintain, access will be granted from their IP address to the address of the machine they support.

- c. IP addresses and domain names. Individual users or departments needing new addresses should contact IT support staff. New addresses are authorized only by IT staff. Similarly, internet domain names associated with the University's networks are to be established and maintained by the IT staff.

VI. ENFORCEMENT

In order to protect the security of the University's networks, and the integrity of the information against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper use, the University reserves the right to limit, restrict or terminate any account holder's usage. The University also reserves the right to periodically check (diagnose) any University system on the campus network, and to take such other actions are necessary to protect University networks and computers.

If a violation of policy is suspected, system administrators are authorized to immediately take action such as locking or disabling accounts when the safety and well-being of students, faculty, staff, or university property are at risk. The Assistant Provost for Information Technology (or designee) will then authorize an investigation. The means of investigation will include, but not be limited to, interception, monitoring traffic and files, including the contents thereof.

- A. Violation of University policy or federal, state and/or local law may lead to revocation of computing privileges and/or prosecution or other appropriate legal action. (Note: Intentional and/or malicious violations or conduct by employees will cause them to forfeit any right they may have otherwise had to legal representation by University counsel and/or the Utah Attorney General's Office. Students are not entitled to such representation in any case.)
- B. Violations of this policy are referred to the appropriate academic, administrative, and/or legal authority.



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

- C. Due process is afforded users charged with violations. Disabling the account constitutes appropriate notice and the user is then entitled to discuss the circumstances with the Assistant Provost for Information Technology or other appropriate administrator authorized to make disclosure to legal authorities, to make a final decision on behalf of the University, or to re-institute computer privileges.
- D. Grievances may be filed upon any adverse decision
 - 1. Students see SUU policy 5.46, Student Responsibilities and Rights.
 - 2. Faculty see SUU policy 6.22, Faculty Grievances
 - 3. Staff see SUU policy 8.4, Employment Grievances.

The University will not be liable for, and the user assumes the risk of, loss of data or interference with files resulting from the University's efforts to maintain the privacy and security of the University's computers and network facilities.

VII. SECURITY AND PRIVACY

- A. The university employs various measures to protect the security of its computing resources and of users' accounts. Users should be aware, however, that the university cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for, their accounts, guarding their passwords, and changing them regularly.
- B. Users should also be aware that their uses of university computing resources are not completely private. While the university does not routinely monitor individual usage of its computing 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 computing resources, including individual login sessions and communications, without notice, when (a) the use has voluntarily made them accessible to the public, as posting to Usenet or a web page; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing 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



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

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.

- C. 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 computing resources are also generally subject to GRAMA statues to same extent as they would be if made on paper.
- D. Electronic Mail (E-Mail)
1. E-Mail is made available to authorized users as a convenience for personal communication. Users are advised that E-mail messages on the University system constitute "public records" and/or "student records" and SUU is authorized and may be obligated to disclose E-mail messages to law enforcement officials, or others under the Government Records Access and Management Act (GRAMA), or the Family Education Rights and Privacy Act (FERPA), without prior notice.
 2. The proliferation of spam abuses the mail system and the network infrastructure because spam requires large amounts of disk space and CPU cycles. This results in fewer resources for University purposes. Sending e-mail messages unrelated to University business to more than 10 users, whether as a single message or as a series of related messages, is expressly prohibited by this policy. Only the public relations, human resources, and President's offices may send messages to the entire faculty, staff, and administration. The IT staff may send bulk e-mail as needed to information the campus community of computing-related issues. Further, e-mail messages to the entire student body are prohibited. Those persons wishing to reach all students should use the campus pipeline systems. Faculty members are permitted to send e-mail message to large groups of students enrolled in university courses if the e-mail content is relevant to the course.
- E. Finally, users should be aware that:



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

1. Students who wish to have their personal information removed from directory databases, {as provided by the Family Education Rights and Privacy Act (FERPA)}, need to contact the Registrar's office, and submit an appropriate request.
2. Individual users are primarily responsible for judging from the circumstances what level of privacy they may expect, and to what extent other users may view their work and react to it.
3. In all matters relating to general issues of privacy and security of individual accounts and communications, along with requests for release of information, University personnel will abide by appropriate laws, including the {FERPA} Family Education Rights and Privacy Act, or where applicable, the {GRAMA} Government Records Access and Management Act. These generally regard student records as private and confidential to most external inquiries. However, they allow for disclosure of student records in response to a proper subpoena or court order from external attorneys, police, and/or administrative agencies. Personally identifiable attributes of employee records are treated confidentially under GRAMA, disclosable only on properly authorized warrant, subpoena, or other court process; other information constitutes a public record and must be disclosed upon proper request by a newspaper, citizens, etc.
4. Employees of the University who retire, resign, or leave the institution for more than one academic year will be given 60 days to arrange for alternate internet services and to back up data. After 60 days or upon notification of termination of service by the CIO or designee, campus internet service and computing accounts will be closed.
5. During regular hours of the work week the University supports computers of employees that are located in the employee's home and that are used for official University business. This support will be on a carry-in basis. The CIO will coordinate necessary support and maintenance, as well as any exceptions to this policy provision.

Appendix A



SUBJECT: COMPUTING, INTERNET USE, AND NETWORK SECURITY

The growth of the Internet, the freedom of information exchange, recent case law, and the development of similar use policies at other universities were key factors in the design of this policy. As with all university policies, many academic and administrative bodies were involved in the creation of the policy before its recommendation to the Board of Trustees.

Concurrent with adoption of this policy, SUU endorses the following statements:

- A. The Educom [now Educause] Code for Software and Intellectual Rights was developed through a non-profit consortium of colleges and universities committees to the use and management of information technology in higher education, and the Information Technology Association of America (ITAA), a computer software and services industry association. The code states:
1. Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publications and distribution.
 2. Because electronic information is volatile and easily reproduced respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasions of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.
- B. An excerpt for the Joint Statement on Rights and Freedoms of Students created by the American Association of University Professors (AAUP) pertaining to student due process:
- Pending action on the charges, the status of a student should not be altered, or his right to be present on the campus and to attend classes suspended, except for reasons relating to the student's physical or emotional safety and well being, or for reasons relating to the safety and well being of students, faculty, or university property.