

Number: IT 1.06
Section: Information Technology

Subject: Network Access and Acceptable Use

Date: January 5, 1999
Latest Revision: August 17, 2004

Policy for: All Campuses
Procedure for: All Campuses
Authorized by: William F. Hogue
Issued by: Office of Information Technology

I. Policy

The University operates and maintains voice, video, and data systems which are connected by networks and communications systems of many types. Network connections are maintained to University sites and to off-campus networks such as the Internet. The Office of Information Technology has established procedures, described below, regarding access to, and acceptable use of, these systems.

II. Procedure

A. Overview and Definitions

1. The University's voice, video, and data systems, as described above, and those systems as defined below, will be referred to generally as "University network" in this document.
2. The term "user" refers to any person accessing the University network, including, but not limited to, students, faculty, staff, contractors, clients, consultants, invited guests, and others working at the University.
3. The phrase "systems and equipment" is defined as workstations, servers, printers, telephones, switches, routers, wiring, hubs, wireless and cellular components, personal digital assistants (PDAs), and other devices and software components that access the University network.
4. The term "user account" refers to the user identification, logon/login identification, or other system-specific means granted to a user permitting access to the University network.
5. The term "authentication" is defined as a means to determine whether a user has a valid account for general access to the University network. The term "authorization" is defined as a means to determine whether a user is permitted access to specific

systems, resources, or services available via the University network.

6. "Private access" is defined as access to a single entity or finite group of entities that is controlled or limited by authentication or authorizations. "Public access" is defined as access that is unlimited and/or anonymous.
7. "University airspace" is defined as the wireless radio emissions generated from University owned, leased, or occupied buildings and outdoor spaces.
8. The "University IT Security Department" is defined as the group led by the University Information Technology (IT) Security Officer to address the on-going operational security concerns of the University.
9. The "University IT Security Council" is defined as the working team which develops security policies and procedures. The Council includes the University IT Security Department and security experts representing the academic units and the regional and four year campuses.
10. The "University Information Security Oversight Committee" (UISOC) serves to address the University's strategic and policy issues regarding network access, including - but not limited to - security, privacy, confidentiality, and copyright. UISOC is appointed by the Provost and chaired by the Chief Information Officer (CIO). In addition to the CIO, membership includes, but is not limited to, senior administrators representing the offices of Academic Affairs, Student Affairs, Human Resources, General Counsel, Regional Campuses and Continuing Education, Research and Health Sciences, and Business and Finance; a senior administrator representing the four-year campuses; the University IT Security Officer; a member of the University Information Technology Council; and, the Chair of the Council of Academic Deans.
11. This policy applies to all wired, wireless, cellular, and emerging network technologies.

B. Access to the University Network

1. The University network is available to the faculty, staff, and students of the University. The University network may be made available to other users by arrangement. Access to the University network may be revoked if the user violates policy or law.
2. The University IT Security Council will establish and maintain a set of requirements that must be met if equipment and systems are to be connected to the University network.
3. The University IT Security Department may delegate authority to information technology management groups or individuals at the unit level to authorize

connection of equipment in their areas of responsibility. Units and individuals are required to register all systems and to obtain authorization from the University IT Security Department or the unit designee before connecting any systems or equipment to the University network.

4. Access to the University network is provided in support of University-related activities. Unauthorized commercial use is not permitted. Incidental personal use by faculty, staff, contractors, clients, consultants, invited guests, and others working at the University is governed by University Policy IT 2.01.
5. Access to telecommunication facilities and equipment therein is restricted to personnel authorized by the University Information Security Oversight Committee or its designee(s). Access is regulated by published procedures.

C. Remote Access to the University Network

1. An encrypted channel or method is required for private access to internal systems.
2. All inbound and outbound traffic is regulated by firewalls. All University Internet services must be registered and approved by the University IT Security Department to gain access through the firewalls. The Security Department may also limit outgoing connections on a case-by-case basis as the need arises.
3. A remote system used for private access to internal systems must meet the same requirements as those specified for internal access to internal systems. Machines connected simultaneously to the University network and any external third party networks may not route traffic between systems on the external networks and the University network unless authorized by the University IT Security Department.

D. Wireless Access

1. Equipment causing interference, disruptions, or conflicts in University airspace will be identified and may be disconnected from the University network.
2. All data being transmitted through University wireless networks must be encrypted to limit exposure of institutional data to unauthorized viewers. All wireless devices must support minimum encryption and authentication standards published by the University IT Security Council. Unauthorized sharing of encryption keys is prohibited.

E. Authentication

1. Identification and authentication are required for users to access equipment attached to the network. Authorization is provided by system administrators or their designees; authorization generally is in the form of a user account issued in the name of the user as the primary means of identification. Authentication methods will be

system dependent, but should validate the individual identity of the user.

2. The authentication requirement may be waived, upon the approval of USC General Counsel, for information access in the campus libraries if, and only if, those workstations designated for public information access are completely isolated from the remainder of the USC network.
3. Users may not access the University network through a user account that is not their own. In some cases shared user accounts are either necessary or unavoidable due to limitations of technologies or processes being used. For those specific cases, the shared user account must be authorized by at least the next level of supervisory authority, and should be used only when the activities requiring the shared user account are ongoing.

F. Network Monitoring and Expectation of Privacy and Confidentiality

1. As guided by the University Information Security Oversight Committee, the University reserves the right, but is not required, to monitor and examine the type and content of electronic communications sent or received using the University network at any time and without prior notice for the purpose of discharging security duties, responding to duly authorized law enforcement requests, and maintaining network integrity. Every effort will be made by security personnel to avoid violation of privacy of individuals or groups.
2. If the privacy of individuals or groups is breached by authorized University security personnel in the performance of their duties, maintenance of strict confidentiality is a legal requirement. See “Interception of Wire, Electronic, or Oral Communications,” Title 17, Chapter 30, Code of Laws of South Carolina for further information.
3. Unauthorized users may not use hardware or software tools that have the ability to evaluate or compromise security on machines other than those that they own or for which they are responsible. If such tools are discovered, the user responsible for employing the tools may immediately lose network privileges and may face disciplinary action. Authorization to use such tools must be obtained through the University IT Security Department or its designees.
4. By making use of computing resources, users consent to allow information to be divulged to authorized law enforcement or other relevant agencies, in accordance with law.

G. Security

1. Any equipment or systems that pose a security threat may be disconnected from the network. If a security breach is discovered in progress, the University IT Security Department may isolate and deny access to the individual, device, or service

immediately.

2. Any attempt to interfere with, prevent, obstruct, or avoid network or system security, or any attempt to dissuade a member of the University community from reporting a suspected security problem is prohibited and may be cause for investigation and disciplinary action.
3. Overall security of a work area is the responsibility of the user and departmental management. Equipment that accesses the University network is required to be secured when the operator is absent or when the system is connected to a network.
4. Each departmental subnet will have a single point of contact for security. Furthermore, each organizational unit will designate and advertise a qualified security contact and a backup who will act as the security liaisons between the organization and the University IT Security Department. A qualified security contact is one who is knowledgeable about security issues and requirements and the machines and networks for which he or she is responsible.
5. If a user suspects his/her account, equipment, or data have been compromised, the user must keep copies of all relevant documents or files; disable the computer network connection; and contact the system administrator, designated security contact, or the University IT Security Department.
6. Systems and security administrators will maintain records from security incidents and preserve evidence when required as outlined in incident handling procedures published by the University IT Security Council. The University IT Security Department, the Internal Audit Department, the Office of the General Counsel, or law enforcement may be consulted for incident resolution and policy violations.
7. Users may not intentionally create, execute, forward, or introduce any computer code designed to self-replicate, damage or otherwise impede the performance of computing resources. See "Computer Crime Act," Title 16, Chapter 16, Code of Laws of South Carolina.
8. Users are prohibited from misrepresenting their identity or attempting to gain access to computing resources for which they are not authorized, or in any way damaging, altering or disrupting the operations of computing resources. Interception of traffic for unauthorized purposes is prohibited. See "Interception of Wire, Electronic, or Oral Communications," Title 17, Chapter 30, Code of Laws of South Carolina.
9. Users may only access, modify, or destroy files, data, and resources for which they are authorized and that lie within the scope of their responsibilities. Malicious destruction or modification of data or resources is not permitted. Accessing data through channels that are a result of failure of security protections or weaknesses in such protections is not permitted.

10. Appropriate measures must be taken when decommissioning media (hard drives, print-outs, magnetic tape, etc) to prevent University data from being disclosed to unauthorized persons.
11. Any exceptions to published security policies or requirements must be documented and maintained on file at the department level with a Risk Acceptance Waiver that acknowledges acceptance of responsibility and outlines any alternate security measures implemented to help mitigate the risk.

H. User Responsibilities

1. To obtain access to the University network, each user is responsible for supplying current information to the appropriate system administrator. This information may vary from system to system but will include specifying or verifying affiliation with the University or department. Providing false or misleading information for the purpose of obtaining access is prohibited.
2. Users are responsible for all activity initiated by their accounts.
3. Dissemination of unofficial, unsolicited mass email (spam) is prohibited.
4. Use of computing resources for harassment is prohibited. This includes transmission of violent, threatening, discriminatory, defaming, obscene, or unlawful material. If a user feels that he/she has been harassed, he/she must keep all relevant documents or files and notify the system administrator, the designated security contact, or the University IT Security Department.
5. Copyright, obscenity, libel, and other laws governing communication and publication apply to electronic media as well. Unauthorized copying or distribution of software or other copyright material is prohibited. Individual users are responsible and liable for such infringing activities.
6. Users are responsible for selecting secure passwords for their accounts and for keeping those passwords private at all times. Users should follow published password standards.
7. Users must ensure that virus protection is installed as applicable and maintained, and that all relevant security patches are installed on all computing devices and equipment for which they are responsible.
8. System administrators are required to monitor vendor and public disclosure forums that report bugs, incidents, and other problems that could affect the security or viability of the systems or software for which they are responsible and disseminate relevant information to their users.

9. Users will not divulge any proprietary or sensitive organizational or personnel data to persons not directly associated with the University, without a demonstrated need to know.
10. Some computing resources are made available on an unmonitored basis. It is the responsibility of every user to act in such a manner as not to cause damage to the equipment and systems. Accidental damage or damage caused by other parties should be reported as soon as possible so that corrective action may be taken.
11. Users are responsible for obeying all official notices regarding network access and security. Users are responsible for understanding and complying with all policies, procedures, and standards dealing with information security and appropriate network use. Users may be required to participate in a security awareness training program. University information technology professionals may also be required to take additional training before obtaining increased access or privileges, as required by their jobs.
12. Users are responsible for reporting any actual or suspected system security violation to their system administrator or designated security contact immediately.

III. Sanctions

- A. Users found violating this policy may be disconnected immediately from the network. Following established University policy and procedure, revocation of network access may remain in effect until an appropriate review and final disposition can be made.
- B. Violation of any portion of this policy may result in loss of account or network privileges, initiation of legal action by the University, and/or disciplinary action. See:
<http://www.sc.edu/policies/hr139.html>
<http://www.sc.edu/policies/staf/staf412.html>
<http://www.sc.edu/policies/staf/staf626.html>

Send comments to William F. Hogue