

NUMBER: IT 1.06
SECTION: Information Technology
SUBJECT: Acceptable Use of Information Technology
DATE: January 5, 1999
REVISED: September 21, 2012
Policy for: All Campuses
Procedure for: All Campuses
Authorized by: William F. Hogue
Issued by: Office of Information Technology

I. Policy

All users of University information technology resources must adhere to applicable state and federal laws, statutes, and regulations; must comply with applicable policies, standards and procedures as defined by the University; must understand and acknowledge that information technology assets and data are for authorized use only; and must not compromise the confidentiality, integrity and availability of these assets and data.

The University provides information technology resources for use by faculty and staff for University-related duties and responsibilities. The use of information technology resources for personal or other non-university purposes that results in costs to the university is strictly prohibited.

A. Policy Statement

The Office of Information Technology has established this policy regarding access to, and acceptable use of, these assets. In order to successfully carry out its mission, the University will act to protect the confidentiality, integrity and availability of information technology assets in accordance with applicable policies, standards and procedures; or as appropriate.

The University operates and maintains many information technology assets, including but not limited to: voice, video, and data systems. These assets are connected by networks and communications systems of many types. Connections are maintained to University sites and to non-University networks such as the Internet.

B. 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 information technology assets" in this document.
2. The term "user(s)" refers to any person(s) accessing University information technology assets, including but not limited to: students, faculty, staff, contractors, clients, consultants, invited guests, and others working at or for the University.
3. The phrase "University information technology assets" includes University owned, operated or maintained: workstations, servers, printers, telephones, switches, routers, wiring and hubs; wireless and cellular components; mobile devices such as smart phones, tablets, laptops and other portable computing devices; or any University owned, operated or maintained technology, software, components or devices that store, process or transmit information or data.
4. Personally owned technology such as mobile devices (e.g., smart phones, tablets, portable computing devices, etc.) or home computers that interface with University information technology assets will be subject to this policy.
5. The "University Information Security Office" is defined as the group assigned to implement University-wide information security strategy and is led by the senior information security person as appointed by the University.
6. The term "access credentials" refers to the user identification, logon/login identification, or other system-specific means granted to a user permitting access to University information technology assets or data.
7. The term "authentication" is defined as a means to determine whether a user attempting to gain access to University information technology assets by means of particular access credentials is in fact the user those credentials were officially assigned to.
8. The term "authorization" is defined as a means to determine whether a user is permitted access to specific University information technology assets.
9. The term "consumable software" refers to University-purchased software that provides insignificant business value, as determined by the acquiring department, in terms of overall function relative to the original purchase price of the software; or to software that would cost the University more to track, reclaim, or redistribute than the original purchase price.

II. Procedure

A. Procedure for All Campuses

1. The University Division of Information Technology will establish and maintain a set of requirements -- in the form of standards and procedures -- that must be met for University information technology systems and assets. Information security-specific standards, procedures, and guidelines can be found in the “Information Security Program” section of the University security website (<http://security.sc.edu>); all other information technology standards, procedures, and guidelines can be found in the “Standards, Procedures and Guidelines” section of the University Technology Services website (<http://uts.sc.edu>).
2. All users are responsible for complying with this policy and established IT standards and procedures. Users are responsible and accountable for all activity initiated or conducted through the use of assigned access credentials. Dissemination of unofficial, unsolicited mass communications via University information technology assets is prohibited. Violation of any portion of this policy may result in immediate loss of access to University information technology assets, initiation of legal action by the University, and/or disciplinary action. Users are responsible for reporting any actual or suspected violation of this policy to the University Information Security Office and designated security contact immediately.
3. System administrators or staff assigned the responsibility of maintaining or supporting University information technology systems or assets will be responsible for implementing requirements outlined in this policy and established standards and procedures. This includes monitoring vendor and public disclosure forums that report vulnerabilities, incidents, and other information of interest that could affect the confidentiality, integrity, or availability of the system or assets for which they are responsible and disseminating relevant information and/or recommended actions to their users.
4. NOTE: All levels of management are responsible for ensuring that all users within their area of accountability are aware of responsibilities as defined in this policy and for ensuring a secure office environment. The head of each unit will authenticate the need for individual access to information technology assets and must request and obtain authorization for access to University data from the appropriate Data Steward. The terms “data” and “Data Steward” are defined in University Policy UNIV 1.50 Data Access.
5. Administrative and academic unit heads are responsible for taking the necessary steps to ensure that access to University information technology assets and data is appropriately limited or restricted for employees who transfer to another department within the University or are no longer employed by the University.
6. Consumable software shall not be tracked, reclaimed or redistributed, unless otherwise directed by an appropriate authority.

III. Related Policies

A. This policy supersedes the following policies:

University Policy IT 1.08 Computer Software Licensing and Distribution
University Policy IT 2.01 Telephone, Computer, Communication and Photocopy Equipment Use by Employees
University Policy IT 2.03 Telephone Equipment
University Policy IT 2.04 Pager Services
University Policy IT 2.06 Telephone Equipment Repair
University Policy IT 2.09 Telephone Services Billing
University Policy IT 2.10 Telephone Credit Cards
University Policy IT 2.12 Telephone Work Requests – Moves and Changes
University Policy ACAF 7.04 Web Sites
University Policy ACAF 7.05 Data Change Notification

B. See also the following related policies:

University Policy IT 3.00 Information Security
University Policy BUSF 4.11 Credit/Debit Card Processing Policy
University Policy HR 1.39 Disciplinary Action and Termination for Cause
University Policy STAF 1.02 Carolinian Creed
University Policy STAF 4.12 Procedures for Responding to Violations
University Policy STAF 6.26 Student Code of Conduct
University Policy UNIV 1.50 Data Access
University Policy BUSF 2.18 (formerly IT 2.18)

IV. Reason for Revision

This revision supersedes IT 1.08 and provides an additional location for supporting standards and procedures.