NUMBER: IT 3.00

SECTION: Information Technology

SUBJECT: Information Security

DATE: September 2, 2010

REVISED: January 19, 2012

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

I. Policy

The University of South Carolina (USC) is committed to appropriately protecting the confidentiality, integrity and availability of its data and information technology assets. The University Information Security Office is therefore directed to develop, implement and maintain the University-wide Information Security Program.

A. Policy Statement

Principles of information security must be treated as fundamental to any function or activity of USC. The principles and framework for USC's approach to information security are outlined in USC's Information Security Program, which is administered by the University Information Security Office under specific authority granted by the University. Response to all compromises or breaches of the confidentiality, integrity or availability of University information technology assets or data will be centrally coordinated by the University Information Security Office.

B. Definitions

1. The University's voice, video, and data systems and other systems defined below will be referred to generally as "University information technology assets" in this document.

2. "User(s)" refers to any person(s) accessing University information technology assets or data, including but not limited to: students, faculty, staff, contractors, clients, consultants, invited guests, and others working at or for the University.

3. "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 personal digital assistants (PDAs) and laptop computers; 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 handheld mobile devices or home computers that interface with University information technology assets will be subject to this policy.

5. “University data” and “data steward” are defined in University Policy UNIV 1.50 Data Access.

6. 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.

7. The “University Information Security Incident Response Team” is defined as the operational group assigned to respond to compromises or breaches of confidentiality, integrity or availability of University information technology assets or data.

8. "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.

9. "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 are officially assigned to.

10. The term "authorization" is defined as a means to determine whether a user is permitted access to specific University information technology assets or data.

II. Procedure

A. Procedure for All Campuses

1. The University Information Security Office will develop, implement and maintain the University-wide Information Security Program. The published program can be found in the “Information Security Program” section of the University security website (http://security.sc.edu).

2. The University Information Security Office also will develop, implement and maintain the University-wide Information Security Incident Response Procedure. The published procedure may be found in the “Information Security Program” section of the University security website (http://security.sc.edu). Due to the sensitive nature of this procedure the full document may not be publicly available. A summary or outline of the procedure may be posted instead while full copies will be made available as necessary.

3. Any University information technology assets or personally owned technologies that pose a security threat may be disconnected from the network. If a security breach is discovered in progress, the University Information Security Incident Response Team may take immediate actions to isolate and deny access to the user, data or information technology asset. Any attempt to interfere with, prevent, obstruct, or avoid information security measures, or any attempt to dissuade a member of the University community from reporting a suspected information security incident is prohibited and may be cause for investigation and disciplinary action.

4. If a user suspects his/her access credentials, information technology assets, or data have been compromised, the user must immediately cease using the information technology asset in question and contact the University Information Security Office, designated security contact or the University helpdesk.

5. The management and staff of each organizational unit of USC is responsible and accountable for ensuring the appropriate security of data and information technology assets as outlined in the Information Security Program and associated policies, standards and procedures.

6. Each user is responsible and accountable for appropriately securing and protecting the confidentiality, integrity and availability of University data and information technology assets as outlined in the Information Security Program and associated policies, standards and procedures.

7. Each organizational unit will designate and advertise a qualified security contact and an alternate who will act as the security liaison between the respective organization and the University Information Security Office. A qualified security contact is: someone who is knowledgeable about security principles and current issues; is aware of Information Security Program requirements; and has full knowledge of the information technology assets and data for which he or she is responsible.

8. Any exceptions to published Information Security Program requirements must be: approved by the appropriate data steward if University data is involved; documented and maintained on file at both the University Information Security Office and the organizational unit level with a Risk Acceptance Waiver that acknowledges acceptance of responsibility by the head of the organizational unit and outlines any alternate security measures implemented to help mitigate the risk.

III. Related Policies

See also:

University Policy IT 1.06 Acceptable Use of Information Technology
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

IV. Reason for Revision

This revision removes ambiguity regarding applicability to personally owned technology.