NUMBER:	IT 3.00
SECTION:	Information Technology
SUBJECT:	Information Security
DATE:	September 2, 2010
REVISED:	October 18, 2016
Policy for:	All Campuses
Procedure for:	All Campuses
Authorized by:	Vice President for Information Technology and Chief Information Officer
Issued by:	Office of Information Technology

I. Policy

The University of South Carolina (USC) strives to provide a safe computing environment, and is committed to securing its data and information technology (IT) resources per state and federal laws, statutes, and regulations. In order to support risk management and compliance efforts, the University Information Security Office (UISO) is authorized to administer the university-wide Information Security Program.

The UISO develops and publicizes the Information Security Program and coordinates all security incident response. Users and managers of university data and IT assets follow the Information Security Program.

USC prohibits interference with–or avoidance of–security measures. Such actions may be grounds for investigation and disciplinary action.

A. Definitions

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

2. "University IT assets" includes any technology, software, or device that stores, transmits, or processes university data. Personal devices that access university data or IT assets are subject to this policy.

II. Procedure

A. The UISO will:

1. Develop and maintain the Information Security Program. The program will focus on the most significant threats to university data and IT assets, weighing the impact of requirements on university operations.

2. Develop, implement and maintain the Security Incident Response Procedure. The UISO may omit internal details due to the sensitive nature of some incident response practices.

3. Act to protect users, data and IT assets, including interruption of access until a threat or vulnerability is resolved.

B. The management and staff of each organizational unit (OU) will:

1. Operate per state and federal laws, statutes, and regulations governing data and IT assets. Any costs from non-compliance or data breach are the responsibility of the culpable OU(s).

2. Name and advertise a security contact with the UISO. This Security Liaison will remain knowledgeable about current security issues, Information Security Program requirements, and the unit's IT assets.

3. Carry out all provisions of the Information Security Program. Provisions may include, but are not limited to, reporting current protections, implementing safeguards, documenting improvement plans, and maintaining approved exceptions to program requirements.

C. Each user will:

1. Protect university data and IT assets according to OU and UISO instructions. The UISO publishes its requirements and guidance on the security website (http://security.sc.edu). The university policy on Responsible Use of Data, Technology, and User Credentials (forthcoming) defines appropriate use of data and IT assets.

2. Stop using an IT asset if he or she suspects a compromise and report the incident. Users may report incidents to the UISO, a unit's Security Liaison, or the university technology Service Desk.

III. Related Policies

University Policy FINA 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 1.51 Data and Information Governance
University Policy UNIV 1.52 Responsible Use of Data, Technology, and User Credentials

IV. Reason for Revision

This revision updates the Related Policies section to reflect changes in policy.