PROCEDURE NUMBER:	IT 3.00 Procedure
SECTION:	Division of Information Technology
SUBJECT:	Information Security
DATE:	July 31, 2020
REVISION:	July 31, 2020
Procedure for:	USC System
Authorized by:	Vice President for Information Technology and Chief Information Officer
Issued by:	Division of Information Technology – VPCIO Office

Procedure

The Division of Information Technology, VPCIO Office, will ensure compliance with IT 3.00. This procedure is applicable to campuses, units, departments, centers, and administrators at the University who are involved with the USC System. The purpose of this procedure is to supplement the associated policy by providing additional detail regarding Information Security.

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

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). University Policy 1.52 (Responsible Use of Data, Technology, and User Credentials) 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.

History of Revisions:

DATE OF REVISION	REASON FOR REVISION
July 31, 2020	Revised to match updated policy template, related university policy references

\