I. **INTRODUCTION** (Purpose and Intent)

Identity theft is a growing problem throughout the world and the University of South Florida System (University/USF) must take appropriate steps to limit and protect personal identity information which it collects in its technology systems. In support of its mission of teaching, research, and public service, USF has connections to the Internet and thereby its technology systems are exposed to threats from the global community. USF must take all actions possible to protect the identity information that it maintains in its technology systems. Personal identity information must be protected from proliferation to technology systems and media that are not properly secured and authorized.

The purpose of this policy is to define the policy, process, procedures, and requirements that all persons and entities shall follow for the security and protection of personal identity information that is stored electronically at the University. The policy relates to the storage and access of personal identity information and the protections required, not the usage of personal or confidential data which is covered by other policies and statutes.

II. **DEFINITIONS**

Identity theft is the unauthorized use of another person’s personal identifying information to fraudulently obtain goods, services, money, or to take other actions which might affect the individual or is otherwise unlawful.

Personal Identity Information (PII), for the purposes of this policy is that information stored on electronic media which individually identifies someone in a manner which enables
identity theft or fraud. Such information includes social security number, driver’s license number, Florida Identification Card number, date of birth, and personal financial information but may be redefined by the Office of Information Security through its published standards and procedures.

For purposes of this policy, PII does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

III. STATEMENT OF POLICY

A. Personal identity information shall be collected, stored and accessed only when required for official University business purposes.

B. Personal identity information shall be stored in the authoritative technology systems and Systems of Record maintained by the Division of Information Technology, with access controls carefully monitored through the data custodians and the Office of Information Security.

C. All technology systems seeking permission to store PII, other than those addressed in section III.B., must register with the Office of Information Security (OIS). The OIS will coordinate the approval process by the Information Technology Management Council (ITMC). This permission to store PII granted by the ITMC may be reviewed and revoked at any time.

D. As part of the approval process, system owners and data custodians must be able to justify the business reason for the storage and use of each data element. They also must ensure that appropriate access and audit controls are in place, following industry standards and those published by the Office of Information Security in the web site http://security.usf.edu. These controls will be reviewed by the OIS no less than annually.

E. University units must limit authorization for the use of mobile devices to store PII to
employees with an official business need. Storage of PII on mobile devices must be approved in advance by USF IT Office of Information Security. Authorization forms are published on the University Security web site, http://www.usf.edu/it/services/data-security.aspx. A signed agreement by the appropriate Vice President and employee responsible for storing the data must be submitted to USF IT Office of Information Security for approval before any data is removed from protected University technology systems.

F. University units storing PII on mobile devices must abide by the following minimum requirements:

• Units must maintain a log of all mobile computing devices used to store PII to include model number, serial number and a listing of all approved applications installed.

• All such devices shall be retrieved and the log/inventory updated in case of termination of user duties.

• Sensitive data shall not be removed from the department network or protected technology systems and saved to the mobile computing device unless the data remains encrypted.

• All mobile devices containing PII shall contain virus protection, a personal firewall and access control logging.

• PII data must be removed immediately when an official business need for storage no longer exists. All data shall be securely removed from the mobile storage device.

• Prior to any mobile storage and use of PII data, employee(s) must receive training on potential risks to theft, fraud, misuse or unauthorized access for mobile devices. This training also shall reinforce the duty to protect the privacy and confidentiality of sensitive data.
G. Additional requirements are published on the Security web site, 

H. When required for University business purposes, transfer of PII between approved technology systems shall be conducted with secure, encrypted transmission methods as defined by the Office of Information Security.

I. Should PII be disclosed or otherwise compromised, the breach shall be immediately reported to the University’s Information Security Manager who will then invoke the incident handling procedures established by the Office of Information Security.

IV. VIOLATION OF POLICY

Violation of this policy may result in disciplinary action including dismissal.

The University of South Florida is a system of higher education composed of multiple campuses and separately accredited institutions located in Tampa, St. Petersburg, and Sarasota-Manatee. Regional campuses and separately accredited institutions may have unique characteristics. Students, faculty and staff must check with their individual campuses and apply System-wide policies in conjunction and consistent with the specific characteristics and guidelines applicable to those campuses.

*Current Responsible Office: Information Technology

*Refer to the appropriate Responsible Office website for a current name of the Vice President or other Responsible Officer.