APPLICABILITY/ACCOUNTABILITY:

This policy applies to all employees of the University of Central Florida.

POLICY STATEMENT:

It is the policy of the University of Central Florida to protect assets, such as mobile computing and communication devices, from loss or theft and to protect restricted data that may reside in such devices from unauthorized access.

DEFINITIONS:

Data. Numerical or other information represented either in a physical form or a form suitable for electronic processing or storage.

Mobile communication device. Cellular telephones, smart phones, and mobile computing devices equipped with wireless or wired communication capability.

Mobile computing device. Laptop computers, tablet PCs, personal digital assistants, and similar mobile electronic devices that are capable of storing, processing, displaying, and communicating data.

Mobile data storage device. USB storage devices, floppy disks, CD-ROMs, DVDs, mobile music players, and any other mobile electronic device or medium that is capable of storing data.

Restricted data. Data that are considered sensitive, as defined in UCF Data Classification and Protection policy 4-008.
Strong password. A password that is difficult to guess, consisting of six or more characters including numbers and special characters.

Virtual private network. A secure means of connecting to a private network, such as the UCF network, from or through an insecure public network, such as the Internet or a wireless network. VPNs encrypt data during transmission.

BACKGROUND INFORMATION:

Laptop computers, cell phones, mobile music players, mobile data storage devices, and similar mobile computing and communication devices have become very popular because of their convenience and portability. However, the use of such devices is accompanied by risks that must be recognized and addressed to protect both the physical devices and the information they contain. The most effective way to secure restricted data is not to store it on mobile devices. A second secure technique is to keep sensitive data only on secure central university servers and access it remotely using secure communication techniques outlined in this policy. However, university business requirements may on occasion justify storing restricted data on mobile computing devices. In those limited cases, users are required to observe this policy to assure that all possible steps have been taken to keep the university’s restricted data secure.

Mobile computing, communication, and storage devices are subject to five areas of risk. It is the responsibility of all university employees who use such devices to contain, process, transmit, or access university restricted data to recognize these risks and take the necessary steps to protect the devices and the sensitive information they may contain or to which they may have access. The risk areas are as follows.

1. Physical risk. Theft or loss.

2. Unauthorized access risk. Login or network access by an unauthorized person or computer

3. Operating system or application risk. All computer operating systems and applications contain both known and unknown vulnerabilities that can be exploited to gain control of the device or access to its data.

4. Network risk. Computing and communication devices can be accessed through the networks to which they are connected without detection. Viruses, worms, and other malware can enter a computer or other electronic device through networks, Web sites, e-mail attachments, and mobile storage media.

5. Mobile data storage device risk. Any mobile device that can be used to store data (USB drives, Personal Digital Assistants (PDAs), mobile music players, floppy disks, CD-ROMs, DVDs, etc.) are subject to loss or unauthorized access.
PROCEDURES:

The following procedures must be followed by all university employees to protect university computing and information assets.

1. Physical risk
   a. All university portable computers must be registered in the UCF asset management system and the serial numbers and property tag numbers recorded.
   b. Users must not leave portable computers or data storage devices in view in an unattended vehicle, even for a short period of time, must not leave mobile devices in vehicles overnight, and must secure unattended portable computers with a cable lock or store them in a locked cabinet or locked private office.
   c. All data on mobile devices must be erased before the device is transferred or surplused.
   d. Users must inform their departmental security coordinator, the UCF Police, and their departmental property management person if a laptop computer is lost or stolen. In addition, users must contact the UCF information security officer immediately if the missing computer contains or is suspected to contain restricted data.
   e. Mobile computer asset recovery software is recommended to enable authorities to locate and return the asset. For recommendations, go to http://www.infosec.ucf.edu/computer_security_standards.htm.

2. Unauthorized access risk
   a. Users must not grant access to their mobile devices to unauthorized individuals.
   b. Users must use strong passwords
   c. Passwords must be changed at least once every 60 days.
   d. When entering passwords, users must take precautions to prevent others from observing.
   e. If the user's mobile computing device is equipped with a biometric device, such as a fingerprint reader, it should be enabled and used with a strong password.
   f. Users must use a non-administrative account for regular use of their mobile device; i.e., laptop. This account type restricts the installation and alteration of programs thus protecting the system from malicious applications and activity. An administrative account should be used to install, alter, and set up programs to be used by the non-administrative account. Users can consult with their departmental information technology professional for assistance in setting up these accounts.
   g. Storage of restricted data on a mobile computing device must be approved in writing by the employee’s dean, director, or vice president and based on a legitimate business need. All restricted data thus approved must be protected by encrypting it with an approved encryption technology. For additional information, go to http://www.infosec.ucf.edu/computer_security_standards.htm.
h. If restricted data are stored on a mobile computing device, the device should be equipped with disk encryption software so that if the device is stolen or accessed, the data cannot be recovered. The latest versions of Windows and OS-X include disk encryption software.

i. All mobile electronic devices, including laptops, smart phones, and PDAs must be configured with a password-protected screen saver that activates after five to ten minutes of idle time.

j. Care must be taken to securely preserve access keys and passwords to recover data.

3. Operating system or application risk

   a. Users must configure their computers to automatically receive and install operating system and application updates from vendors.

   b. Users must take all reasonable steps to protect against the installation of unlicensed or malicious software.

   c. All laptops and, if appropriate, other mobile devices must have anti-virus software installed, and antivirus signatures must be kept up to date.

   d. All laptops and, if appropriate, other mobile devices must have anti-spyware software installed, and malware signatures must be kept up to date.

   e. All laptops and, if appropriate, other mobile devices must have personal firewall software installed and enabled. Major operating system vendors provide firewall software at no cost.

4. Network risk

   a. Users must use the UCF virtual private network to access UCF resources from insecure networks, such as wireless and public Internet service providers.

   b. All wireless communication technologies, i.e., WiFi, Bluetooth, infrared, etc., must be disabled when not in use.

5. Mobile data storage device risk

   a. Restricted data must not be stored on mobile data storage devices.

   b. Backups or archival copies made from systems containing restricted data must be encrypted.

   c. Mobile data storage devices must be kept in a secure location when not in use.

RELATED DOCUMENTS:

4-008 Data Classification and Protection policy

CONTACTS:

INITIATING AUTHORITY: Provost and Executive Vice President

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-007
Initiating Authority: [Signature] Date: 12/4/07
Policies and Procedures Review Committee Chair: [Signature] Date: 12/3/07
President or Designee: [Signature] Date: 12/4/07