SUBJECT:	Effective Date	Policy Number
Security of Mobile Computing, Data Storage, and Communication Devices	8-27-2015	4-007.1
	Supersedes	**Page** **Of**
	4-007	1 5
	Responsible Authority	
	Vice Provost for Information Technologies & Resources	

APPLICABILITY/ACCOUNTABILITY

This policy applies to all individuals working for or on behalf of the University of Central Florida who maintain or use university data. This includes all full-time and part-time employees, adjuncts and others on temporary or time-limited appointments, all volunteers and courtesy appointees, student workers, and all persons paid by or through the university such as contractors, consultants, or employees of direct support organizations.

BACKGROUND INFORMATION

Laptop computers, tablets, cell phones, mobile music players, mobile data storage devices, and similar mobile computing 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 to store it only on secure central university servers and access it remotely using secure communication techniques outlined in this policy.

POLICY STATEMENT

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

Highly restricted data must not be stored on mobile devices or personally owned Internet cloud storage services. Restricted data (e.g., student grades identified by emplIDs) can be saved on

university-owned mobile devices or in a university-sanctioned Internet cloud data storage service only if encrypted and protected by a strong password.

Mobile computing and storage devices are subject to five areas of risk including physical risk, data security risk, operating system or application risk, network risk, and mobile device or cloud data storage 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.

Any violation of this policy and procedures may result in immediate loss of network and computer access privileges, seizure of equipment, loss of research laboratory access, or removal of inappropriate information posted on university-owned computers or university-supported Internet sites. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination.

DEFINITIONS

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

Data security risk. Login or network access by an unauthorized person or computer.

Encryption. The encoding of data into a form that cannot be easily decoded by unauthorized parties.

Internet cloud storage. Data stored in third party data centers, e.g., OneDrive, CrashPlan, Dropbox, iCloud, Google Drive, Box, etc.

Mobile computing device. Cellular telephones, smartphones, laptop computers, tablets, PCs, personal digital assistants, and similar mobile electronic devices that are capable of storing, processing, displaying, or 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.

Mobile or cloud data storage device risk. Any mobile device that can be used to store data (USB drives, flash drives, tablets, mobile music players, floppy disks, CD-ROMs, DVDs, or cloud data storage service (Dropbox, Box, etc.) are subject to loss or unauthorized access.

Network risk. Computing devices can be accessed without detection through the networks to which they are connected. Viruses, worms, and other malware can enter a computer or other electronic device through networks, websites, email attachments, and mobile storage media.

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.

Physical risk. Theft or loss.

Restricted data. Confidential or personal data that are protected by law or policy as defined in UCF *Data Classification and Protection* policy 4-008.1.

Strong password. A password that is difficult to guess, consisting of eight (8) or more characters, including lower case and upper case letters, numerals, and special characters. Longer passwords, or passphrases are, in general, more secure than shorter passwords.

Virtual private network (VPN). A secure means of connecting to a private network, such as the UCF network, through an insecure network, such as the Internet or a public wireless network. A VPN connection encrypts data during transmission.

PROCEDURES

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

1. Physical risk

    a. 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.
    b. All data on mobile devices must be wiped and rendered not readable (not just deleted) before the device is transferred or leaves the university.
    c. All university owned mobile devices should be backed up in a secure manner to preserve data in the event the device is lost or stolen.
    d. Users must inform their departmental security coordinator, the UCF Police, and their departmental property management person if a mobile computing device is lost or stolen. In addition, users must contact the UCF Information Security Office immediately if the missing mobile device contains or is suspected to contain highly restricted or restricted data.
    e. Mobile computing device asset recovery software is recommended to be installed in order to remotely wipe or lock a lost or stolen mobile computing device and enable the university to work with authorities to locate and return the asset. For recommendations, go to *www.infosec.ucf.edu*.
    f. The university reserves the right to wipe data from a university owned mobile device in the event of loss, employment separation, or termination.
    g. University-owned mobile devices are subject to open records requests or authorized investigations.

h. Users should label mobile computing devices with contact information to facilitate recovery if lost.

2. Data security risk

   a. Users must protect university data under their control.
   b. Users must not grant access to their mobile computing devices to unauthorized individuals.
   c. Users must use strong passwords to protect their computer accounts and, where appropriate, PINs with a minimum of six (6) digits to protect their devices from unauthorized access.
   d. Passwords must be changed at least once every 60 days according to the UCF password standard.
   e. When entering passwords, users must take precautions to prevent others from observing.
   f. If the user's mobile computing device is equipped with fingerprint reader or other biometric device, it should be enabled and used along with a strong password.
   g. A non-administrative account restricts the installation and alternation of programs thus helping to protect a computer system and data from malicious applications and activity. User accounts on mobile computing devices must be non-administrative accounts, where technically possible (e.g., laptops). 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 professionals for assistance installing or updating software.
   h. Mobile computing devices that support screen savers must have them configured to require passwords and activate after five to ten minutes of idle time.

3. Operating system or application risk

   a. Users must configure their computers, smartphones, and tablets 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 possible, other mobile computing devices must have antimalware software installed, and antimalware signatures must be kept up-to-date.
   d. All laptops and, if possible, other mobile computing devices must have firewall software installed and enabled. Major operating system vendors provide firewall features at no cost.

4. Network risk

   a. Users must use the UCF virtual private network (VPN) to access UCF resources from insecure networks, such as free public wireless (e.g., coffee shops) and from Internet service providers.

b. All wireless communication technologies, e.g., WiFi, Bluetooth, infrared, Radio Frequency Identification (RFID), Near-Field Communications (NFC) etc., must be disabled when not in use.

5. Mobile data storage device risk

   a. Backups or archival copies made from systems containing restricted data must be encrypted.
   b. Mobile data storage devices must be kept in a secure location when not in use.

RELATED DOCUMENTS

Policy 4-008.1 - *Data Classification and Protection* Policy
Policy 4-002 - *Use of Information Technologies & Resources Policy*
Policy 2-103 - *Use of Copyrighted Material Policy*
Policy 3-206.1 - *Cardholder Information Security Procedures Policy*

UCF Password Standards - http://www.cst.ucf.edu/wp-content/uploads/501-101-Password-Standards.pdf

CONTACTS

Computer Services and Telecommunications Information Security Officer, 407-823-3863.

INITIATING AUTHORITY Provost and Executive Vice President

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

Policy Number: 4-007.1

Initiating Authority: _____ Date: 8/24/2015

University Policies and Procedures Committee Chair: _____ Date: 8/21/2015

President or Designee: _____ Date: 8/27/15