Purpose:

To establish standards for the use of mobile computing and storage devices, and to specify minimum configuration requirements for them at the University of Florida consistent with the Mobile Computing and Storage Devices Policy.

Standard:

All mobile computing and storage devices that access the University of Florida Intranet and/or store University of Florida Restricted data must be compliant with University of Florida Information Security Policies and Standards.

1) Encryption of data

a) All laptops and portable personal computers storing restricted data must utilize whole disk encryption. In addition, any laptops and portable personal computers purchased after August 17, 2011 must utilize whole disk encryption. All other laptops and portable personal computers shall have whole disk encryption installed by August 17, 2013;

i) The encryption passphrase must meet or exceed University of Florida Gatorlink password strength rules, must not be shared, and not stored in a visible or plaintext form on or with the device.

ii) The encryption system must include a management component that provides key recovery and proof that the device is encrypted.

b) All smartphones and PDAs that access University of Florida data must be configured to encrypt any restricted data in persistent storage. In addition, any smartphones and PDAs purchased after August 17, 2011 must utilize encryption. All other smartphones and PDAs shall have encryption installed by August 17, 2013.

c) All smartphones and PDAs must include the ability to remotely wipe stored data in the event the device is lost or stolen.

d) All portable storage devices must include built-in encryption. The following exceptions apply:
Standard: Mobile Computing and Storage Devices

i) Specific uses where no Restricted Data will be stored and encryption would interfere with the device’s intended use. Devices used in this way must be clearly marked as not for use with Restricted Data.

ii) Specific uses in which devices are used for marketing and public relations, no Restricted Data will be stored, and the intended recipient is not a member of the UF Community. Devices used in this way must be clearly marked as not for use with Restricted Data.

e) The encryption and key management methods used must have the approval of the UF Information Security Officer or designee.

f) Restricted Data must be protected by encryption during transmission over any wireless network and any non-University of Florida wired network.

2) Authentication

a) The portable computing device must be configured to require a strong password of its user and administrator, consistent with or exceeding UF GatorLink password requirements. Small portable computing devices where keyboard entry is cumbersome (ex. Smartphones) may use reduced password complexity if the device is configured to allow no more than 10 failed password entry attempts before preventing use by locking for a significant amount of time or erasing all storage.

b) The portable computing device must be configured with an inactivity timeout of not more than 30 minutes, which requires re-authentication before use.

3) Disposal

a) Disposal of mobile computing and storage devices must be in compliance with the University of Florida Information Security Reuse and Disposal Standards for IT Workers.

4) Backup

a) Users must maintain a copy of data needed for UF activities, including research, teaching and business processes, on a secure server when the UF data are stored on a mobile computing or storage device.

5) Physical Security
Standard: Mobile Computing and Storage Devices

a) The mobile computing device must have a durable physical or electronic label with contact information sufficient to facilitate an expedient return in the event that a lost device is found.

b) Mobile computing and storage devices must be used and stored in a manner that deters theft.

c) Devices should use tracking and recovery software to facilitate return if lost or stolen.

References:

NIST Special Publication 800-53 revision 3: AC-19