UF UNIVERSITY of FLORIDA
Information Technology

Standard: Mobile Computing and Storage Devices

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, store, process or transmit **University Data, regardless of ownership,** must be compliant with University of Florida Information Security Policies and Standards.

1) Encryption of data

   a) All persistent storage within mobile computing devices will be encrypted

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

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

      iii) Whenever possible, devices will include the ability to remotely wipe stored data in the event the device is lost or stolen.

   b) All portable storage devices must be fully encrypted. The following exceptions apply:

      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.

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

d) Restricted Data must be protected by encryption during transmission over any wireless network and any non-University of Florida 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 password complexity 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. Shorter timeout durations should be implemented when appropriate based on risk and usage.

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 backup or copy of data needed for UF activities, including research, teaching and business processes, when UF data are stored on a mobile computing or storage device.

5) Physical Security

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

SEC-AC-002.02 Password Complexity Standard

Revisions:

March 1, 2013: Original

March 10, 2015: Removed deadlines for encryption, consolidated encryption requirements, minor clarifications.