Mobile Computing | Storage Devices Policy

Developmental Research School
at the University of Florida

Effective August 2013, the University requires that all mobile computing devices owned or purchased by the University have acceptable encryption installed. Mandating the use of acceptable encryption on mobile computing devices helps reduce the level of risk to which the university is exposed.

This policy is designed to prevent unauthorized access to restricted data saved on or accessed by computers, tablets, mobile phones, and other devices. **Restricted Data** is data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records (e.g. student grades), research protocols and export controlled technical data.

All mobile computing and storage devices:

- All laptops and portable personal computers storing restricted data must utilize whole disk encryption.
- Any and all mobile computing devices used within the University of Florida information and computing environments must meet all applicable UF encryption standards.
- University of Florida information security policies applicable to desktop or workstation computers apply to mobile computing devices.

Smartphones, PDA's, and Other Personally-owned Devices:

Due to the pervasive nature of smart phones, tablets, and other highly portable devices, users are not exempt from compliance with relevant aspects of the Mobile Computing and Storage Devices policy. All members of the University of Florida constituency who are currently using personally-owned mobile computing and storage devices that access the University of Florida intranet and/or store University of Florida restricted data are required to **bring their personal device into compliance with University of Florida policies and standards.**

- All smartphones and PDAs that access University of Florida data must be configured to encrypt any restricted data in persistent storage.
- All smartphones and PDAs must include the ability to remotely wipe stored data in the event the device is lost or stolen.
- **All portable storage devices must include built-in encryption or password protection.**
    - includes accessing business email and TEAMS.
- Personally-owned mobile computing devices must encrypt restricted data in persistent storage.

For a more detailed explanation of University of Florida's mobile computing and storage devices standard: https://it.ufl.edu/policies/information-security/mobile-computing-and-storage-devices-policy/

I have read the policy on mobile computing and storage devices and personally-owned devices.

☐ My personally-owned mobile computing devices have password protection or encryption in compliance with all relevant requirements.

Signature: _____ Date: _____

Printed Name:_____

1200 SW 6th Street, Gainesville, FL 32601
P: 352.392.1554 ■ F: 352.392.9559 ■ pkyonge.ufl.edu