Baker County Extension Service
Michael A. Davis, Ph.D.
Director / Agriculture Agent
1025 W. Macclenny Ave.
Macclenny, FL 32063
[904-259-3520] michael.davis@ufl.edu
http://baker.ifas.ufl.edu

University of Florida Data Security Policies and Mobile Devices – What it Means to Extension Personnel

Newer mobile devices such as smartphones and tablets, along with traditional portable devices such as laptops and notebooks provide the Extension professional with an easy means to access data when away from the office. However, these devices also pose a security risk in cases where they are lost or stolen or if the data is access by an unauthorized person. To this end, the University of Florida has implemented policies and standards concerning mobile devices and the data that is stored upon them. Definitions of some terms are included with this document. For definitions of additional technology terms, please see 'Technology and Mobile Devices – Glossary of Terms', a fact sheet from the Baker County Extension Service (http://baker.ifas.ufl.edu). The full text of the UF Mobile Computing and Storage Devices Policy and the Mobile Computing and Storage Devices Standard can be found online at http://www.it.ufl.edu/policies/mobilecomputingpolicy.html and http://www.it.ufl.edu/policies/mobilecomputingstandard.html, respectively.

UF email on Smartphones and Tablets

Using the built-in email service on your smartphone or tablet is an easy way to keep up with email on the go. Most devices also allow the synchronization of your Exchange calendar and contacts. However, there are certain requirements that you need to be aware of before you set up your device to receive University email.

- Microsoft Exchange ActiveSync is the most common way to sync your email. There are other services available such as Blackberry, but these services require annual fees. Instructions for configuring your mobile device can be found at https://info.mail.ufl.edu/mobile-devices/.
- Using this service requires that you allow the UF Exchange security policies to be placed on your device. This allows UF IT to have administrative control over the device.
- At minimum, a 4-digit PIN (Personal Identification Number) must be used to unlock the device.
- The maximum timeout period for the PIN is 15 minutes. This means that if you unlock the device and then don't use it for 15 minutes, the device will relock and you will have to re-enter the PIN. You can adjust this time to be shorter than 15 minutes.
- There is a set number of retries to enter the PIN correctly. Failure to enter the PIN and unlock the device in the correct number of tries will result in a Hard Reset (Factory Reset) of the device. **This will erase all data stored by the user on the device and restore it to the state when it was new. You will lose all files, photos, music, etc. on the device if this happens.**

Encryption

Due to the possibility of loss of data, UF has implemented a Mobile Computing and Storage Device Policy and a Mobile Computing and Storage Device Standard that specifies that all mobile 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.

The Mobile Computing and Storage Device Policy states that:

1. **Restricted Data** (see definition below) stored on mobile computing and storage devices must be encrypted.
2. Any and all mobile computing devices used within the University of Florida information and computing environments must meet all applicable UF encryption standards. Mobile computing devices purchased with University of Florida funds, including, but not limited to contracts, grants, and gifts, must also be recorded in the unit's information assets inventory.
3. University of Florida information security policies applicable to desktop or workstation computers apply to mobile computing devices.

Restricted Data – Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities, which are subject to specific protections under federal or state law or regulations or under any applicable contracts. Examples include, but are not limited to: medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records, research protocols and export control technical data.

This means that if your device has access to or stores data that is defined as restrict4ed, then you must use encryption on that device. Most newer models of smartphones and tablets have the ability to encrypt the data on the device. Note that encryption is not reversible and the only way to take encryption off the device is to perform a hard reset (factory reset) that erases all data on the device. Please consult with your IT representative to determine if your device(s) contains **Restricted Data**.