Data Protection Standard for Mobile Devices (ISSP-012)

Definition

**Restricted Data** is defined by Information Security Standard ISSP-001, posted on the security web site [http://security.usf.edu](http://security.usf.edu). It includes **Restricted Personal Data** (Social Security Numbers, Student GPA, grades, and financial information) as well as **Restricted Limited Data** (internal audit results, research data, departmental budget projections, etc).

Scope

This standard covers all mobile devices and storage devices used to store University data, included but not limited to laptops, PDAs, and removable storage of any type.

Laptop Encryption

According to the *Information Technology Management Council (ITMC)*, all laptops purchased by the University must have approved whole disk encryption software installed. A list of approved software is available at Information Technology web site, [http://www.it.usf.edu](http://www.it.usf.edu).

Additional Safeguards for Restricted Personal Data

In addition to whole disk encryption, users storing Restricted Personal Data on mobile devices or portable storage devices must agree that:

- There is a compelling business or academic reason to store such data on the mobile device;
- It is impossible or impractical to de-identify the data; and
- It is impractical for the device to connect to the data through the internet using a secure transport method (such as VPN or SSL).

If all three bullets listed above apply to this situation and Restricted Personal Data will be stored in the mobile device, the following requirements must be followed:

- The initial secure setup and configuration of the device shall be verified by USF Information Security staff or designee.
- The end user shall not be allowed to download and install any software application after this initial verification without the explicit consent from a USF Information Security staff or designee.
- The device must be setup for timely operating system and application updates (if applicable). The appropriate configuration for these updates must be verified by USF IT or designee on a yearly basis.
- The device must set up with anti-virus protection, anti-spyware, and a personal firewall (if applicable).
- The data on the device must be encrypted with software approved by the *University Technology Standards Board (UTSB)*
- The password or key to the above encryption must be stored safely, separately from the device.

Personal Identifiable Information

In addition to the requirements listed in the previous section, if the mobile device will store Restricted Personal Data known as **Personal Identifiable Information** (PII), such as social security number, driver's license number, Florida Identification Card number, date of birth, or personal financial information, ISSP-013 must be filed with the Office of Information Security. The form can be downloaded from the IT website at [http://it.usf.edu/standards/procedures](http://it.usf.edu/standards/procedures).

Exceptions

For exceptions to this standard, a request can be made to the University Technology Standards Board by going to the following link and filling out the online form: