Mobile Device Security Standard

Syracuse University – Information Technology and Services
Information Security Standard – S0103 v1.1

1.0 Scope

This standard applies to any mobile computing device to include but not be limited to smartphones, tablets, or iPod touch type devices, either owned by Syracuse University or privately owned, used by SU faculty/staff and store SU data classified as "confidential" or "enterprise".

2.0 Purpose

To improve security of Syracuse University data that resides on a mobile device and help prevent data from being lost or compromised. Enacting this standard helps to protect Syracuse University from costly breach notification requirements in the event of a device loss or theft.

3.0 Standards

Syracuse University Information Technology and Services (ITS) requires the following security settings on all mobile devices that store any SU data classified as "confidential" or "enterprise" as defined by the "*Syracuse University Information Security Standard"*. Note that access to the SU Exchange e-mail system through any protocol other than using web based access means the device is storing at least confidential data. The settings are as follows:

- A non-trivial numeric passcode with a minimum required length of four characters. Simple passcodes consisting of consecutive or sequential characters such 0000, 1234, 9876 etc. are strongly discouraged. Passcodes consisting of additional character sets or greater lengths are recommended
- An inactivity timeout to automatically lock the device after a maximum of 15 minutes
- Enable device encryption (on supported devices)
- Automatic data wiping after ten failed passcode entry attempts or as supported by the devices operating system.
- Enable the ability to remotely wipe data from lost/stolen devices
- Disable IMAP on user mailbox
- Prohibit users from modifying or disabling security safeguards

These requirements will be enforced by IT'S THE Exchange ActiveSync Server (EAS).

Users with devices that are capable of performing ActiveSync connections must use the Exchange ActiveSync Server (EAS) for the same. This ensures proper connection with the SU Exchange servers and enforces the required security settings.

Rooting or jailbreaking a mobile device is not allowed, as it would render the device highly insecure. Such devices are not allowed to access or store any sensitive data.

3.1 Exception

Any device that is not capable of meeting all the requirements is prohibited from being used to retrieve and store any sensitive data classified as confidential or enterprise data by the IT Security Standard #6, V 1.5. Users can alternatively view their SU Exchange email on a mobile device through Outlook Web Access using any browser.

Exceptions for mobile devices that are unable to meet the aforementioned standards can only be granted by the SU's Information Security Officer (ISO) (see contact information below). The end user of the device as well as their local IT support staff must schedule a meeting with the ISO to discuss the need for the exception and possible alternative protections.

3.2 Lost or Stolen devices

Employees are responsible for the physical security of their mobile device and the device should be kept in their physical presence whenever possible.

Users are required to immediately report a lost or stolen mobile device incident to their local IT support staff so that a remote wipe of the device may be initiated. Users must also immediately change their NetID credentials to protect against unauthorized access to other SU IT resources.

The wiping of a mobile device will result in the loss of ALL data on the device, including contacts, pictures, notes, applications, music files, text messages, etc. Mobile device users should always maintain a current backup of their device(s) so that data may be easily restored in the event that a device must be wiped.

4.0 Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Standard:	http://its.syr.edu/security/standards/MobileDeviceStandard.pdf
Standard: *Syracuse University Information Security Standard* - IT Security Standard #6, V 1.5	http://its.syr.edu/security/standards/ITSecurity-standard.pdf
Contact: Information Security Officer	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.1
Effective Date:	January 7, 2013
Date of Last Review	August 26, 2015
Date of Next Mandatory Review	August 26, 2016