Mobile Device Security Standard

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 Thiel College or privately owned, used by Thiel College faculty/staff and store Thiel College data classified as “confidential” or “enterprise”.

2.0 Purpose

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

3.0 Standards

Thiel College Information Technology and Services (ITS) requires the following security settings on all mobile devices that store any Thiel College data classified as “confidential” or “internal” as defined by the “Thiel College Data and Classification Policy”. Note that access to the Thiel College Office 365 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

Thiel College’s Office 365 Exchange ActiveSync Server (EAS) will enforce these requirements along with Cisco Merki MDM Management.

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 Thiel College Office 365 Servers.

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 Policy. Users can alternatively view their Thiel College Exchange email on a mobile device through Outlook Web Access using any browser.

The Thiel College's Director of Information Systems grant exceptions for mobile devices that are unable to meet the aforementioned standards can only. The end user of the device as well as their IT staff must schedule a meeting with the Director 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 Public Safety and the IT Department so that a remote wipe of the device may be initiated. Users must also immediately change their ID credentials to protect against unauthorized access to other Thiel College 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.

The IT Department upon report will wipe data using Cisco Meraki MDM Solution. It is also possible for the user to do the same when they device is reported stolen by going to one of the following links.

Apple's Find My iPhone

Android's Find My Device

Meraki Self Service Portal

4.0 Related Standards, Policies and Processes

- Acceptable Use Policy
- Security Policy