Android Mobile Device Management

Mobile devices are widely used by faculty, staff, students and other authorized individuals to access a variety of MUSC systems that contain sensitive data, including administrative and financial records, educational records, and protected health information. While mobile access can provide valuable benefits, there is a significant risk of unauthorized access to sensitive MUSC data if a mobile device is lost or stolen, or otherwise leaves the control of its owner or authorized user.

Who: Mobile Device Management is required for ALL users who connect to the MUSC Exchange server (MUSC email) from a smart phone.

Why: By requiring Mobile Device Management (MDM) software on smartphones, the following goals will be achieved:
- Force Password Lock
- Require Inactivity Timeout
- Enforce Encryption of MUSC data including email, contacts, and calendar information.
- Push <muscsecure> wireless and VPN settings to our users' devices and remove them if necessary.
- Push Exchange Email, Contacts, and Calendar settings to users devices and remove them if necessary.
- Add the Ability to Wipe, Selectively Wipe MUSC Data only, Locate lost devices if users choose to allow their device to be located. The physical security of mobile devices must be maintained at all times. In particular, these devices should not be left unattended in any location where loss or theft, or any access to the device by an unauthorized party, would be a reasonably anticipated and avoidable risk.

If devices are lost, users will have the ability to log into a self-service portal at http://www.musc.edu/myphone and do the following:
- Lock their device
- Locate their device (If they have location services turned on and GPS enabled on their device)
- Wipe their device completely
- Wipe only MUSC data from the device (Exchange Email, Exchange Contacts, Exchange Calendar, MUSC VPN Settings, muscsecure wireless settings, passcode policy)

Please Note: MDM does NOT allow administrators to see users' private data stored on their phone such as messages in MUSC or personal email accounts, pictures, videos, phone calls, and text messages. MDM does allow administrators to see device data such as Battery Life, UDID, Phone Number of Device, Location of Device (only with written permission of the user when users allow their device to be located), Applications installed on the device, and Passcode and Encryption Compliance.

ALL users who connect to the MUSC Exchange server from their phone will be required to install the Xen Mobile MDM client. Please email any questions and/or suggestions to endpointsecurity@musc.edu.
Getting Started: Android
**Please have your Google Play password accessible.**

**MDM and TouchDown minimum space requirements:** 40MB of free space.

In the steps below, you will be instructed to delete all Email, Contacts and Calendar information. PLEASE NOTE that this information is stored on MUSC’s ‘Exchange’ server and will be downloaded to the TouchDown application. If you do not currently have your MUSC Email, Contacts or Calendar on your Android, then you can skip the ‘removal’ step below (Removing MUSC Email...) and instead proceed to the “Installing MDM and TouchDown application on your Android Device”.

**Different Android versions**
The instructions below may not match exactly to your device as there are many different versions of the Android operating system. Please call the OCIO Help Desk at 792-9700 or send an email to endpointsecurity@musc.edu if you have any questions.

Removing MUSC Email, Contacts and Calendar Information
1. Open your Email application, go to Settings, and select your email account.
2. Scroll down and select Remove Account. Please note that your Email, Contacts, and Calendar will be reloaded by following the instructions below.

Installing MDM and Touchdown on your Android Device
1. Open your device’s Settings then select [Security] or [Applications] depending on your Android version.
2. Scroll down to Unknown Sources and check the box next to it then press OK if prompted.
3. Open the Play Store app and search for Citrix Secure Hub.
4. Select the free Citrix Secure Hub app. Select [Install] then press [Accept]. This may take several minutes.
5. Once finished, select [Open].
6. Enter the server address mdm.musc.edu when prompted then press [Next].
7. Enter your NetID and password, then press [Next], then press [Activate] when prompted. Enrollment is complete. The Citrix Secure Hub app will open but no further action is needed in it, press the home button on your phone to exit.
8. Create a Pattern, PIN, or Password for your device when prompted. If this screen disappears before you have a chance to create a pattern, PIN, or password you need to go Settings->Security->Screen Lock (location of this setting varies between different devices) to create it.
9. When prompted (you may have to select Package Installer), install the Touchdown app (Email app) by pressing [Next], [Next], [Install], [Accept], [I Accept], then [I Accept] again. Enter your password on the configuration page that will display afterward.
10. You will now use the TouchDown app to access your MUSC Email, Contacts, and Calendar. If the TouchDown icon is not already on one of your home screens, you can drag it there from your list of applications.
11. If you want to turn off notification sounds from Touchdown, open the Touchdown app and go to [Settings] then select [Advanced]. Scroll down and press the [Email Alerts] button. Select [Customize Settings], check [Enable Lights], press [Configure Lights] and then select the color of the small flashing light that will notify you of a new email message. Or select any of the notification methods you prefer.