Mobile Device Security Policy

IT Communication to Faculty and Staff

From: Tyler Pitts <PittsT@mobap.edu>

Subject: New Mobile Device Security Policy

Date: May 29, 2015 at 4:10:43 PM CDT

Good afternoon,

I wanted to take a minute to inform you all of a change that is taking place on June 15, 2015, in regards to mobile device security.

Mobile device security refers to enabling a set of basic security settings to protect data residing on a smartphone or tablet in the event that the device is lost or stolen. We are requiring this change because many of our MBU faculty and staff access University business information on mobile devices. Many of these people store email messages with sensitive MBU business data such as financial, donor, contract, student, or employee information. In addition, a number of regulations require the protection of certain types of data. FERPA protects student information, HIPAA protects health information, and PCI protects credit card information. Nearly every state has expensive notification requirements for its citizens in the event MBU loses any personally identifiable information (PII), such as a person's name along with his or her birth date, social security number, financial, and other information.

There are three things that you need do to prepare for the Mobile Device Security Policy:

- Update your device. Ensure your device is running the most current operating system software. Check with your device manufacturer for updates.
- Back up your device. While it's unlikely that you'll have any problems, personal data should always be backed up on mobile devices to guard against information loss in the event of theft, device loss, or catastrophic damage.
- Choose a four-digit PIN (passcode) you can remember, cannot contain sequential numbers, must have at least three unique digits, and that is difficult for someone else to guess. For more information on how to setup your PIN, please see the FAQ.

After deployment of this policy, the first time you use your device to connect to Exchange, you will be prompted to create a passcode (if one has not been previously set) which will be needed to unlock the device and gain access to email and other data. You'll also notice that the screen will lock after 15 minutes of inactivity. Other features of the policy will generally be invisible.

If your device is lost or stolen, please contact IT immediately so we can make sure the information on your device is secure.

On this page:

Frequently Asked Questions

What is Mobile Device Security?

"Mobile Device Security" refers to enabling a set of basic security settings to protect data residing on a smartphone or tablet in the event that the device is lost or stolen.

Why is MBU requiring Mobile Device Security?

Many of our MBU faculty and staff access University business information on mobile devices. Many of these people store email messages with sensitive MBU business data such as financial, donor, contract, student, or employee information. In addition, a number of regulations require the protection of certain types of data. FERPA protects student information, HIPAA protects health information, and PCI protects credit card information. Nearly every state has expensive notification requirements for its citizens in the event MBU loses any personally identifiable information (PII), such as a person's name along with his or her birth date, social security number, financial, and other information.

How does Mobile Device Security protect MBU's data?

The settings enabled on the device will protect the data from unauthorized exposure by placing a screen lock timeout of no longer than 15 minutes, encrypting data stored on the device, and allowing the user (or an authorized IT staff member) to remotely wipe the device of all data. These simple settings will protect MBU's and your personal data in the event that the device is lost or stolen.

What devices are affected by Mobile Device Security?

The mobile device security implementation affects all iOS devices (iPhones, iPads, iPod touch), Android devices (both phones and tablets), Windows mobile devices, and BlackBerry devices that connect to MBU's Exchange email system.

Why should I care about this?

The fact that you work at MBU means that you could receive sensitive MBU business data on your mobile device at any time via email. In addition, your personal data on the device will be protected. Do you access your Facebook or other social network site from your phone? Do you carry pictures of your family that you wouldn't want to lose? Do you have any online accounts like Dropbox or Evernote that someone who found your phone would have access to? These security settings with specific configuration will protect your personal data, too.

Do I have to participate in the Mobile Device Security Policy?

The easiest, and preferred, way to opt out is to remove your MBU Exchange account— and delete any sensitive MBU information—from your mobile device. Then you won't be storing sensitive MBU information on your device and the Policy will not apply. You may still check your e-mail by using your browser, and log in at https://mail.mobap.edu. For all other users, opting out of the Policy is highly discouraged and anyone who stores sensitive MBU information on their mobile device (including email) is expressly prohibited from opting out.

What should I do to prepare?

There are three things that you need do to prepare for the Mobile Device Security Policy:

• Update your device. Ensure your device is running the most current operating system software. Check with your device manufacturer for updates.

• Back up your device. While it's unlikely that you'll have any problems, personal data should always be backed up on mobile devices to guard against information loss in the event of theft, device loss, or catastrophic damage.

• Choose a four-digit PIN (passcode). Make sure to choose a PIN you can remember, however:

- It cannot contain sequential numbers.
- It must have at least three unique digits.

Refer to the following articles for setting up a passcode on your Android or Apple device.

Setting up a Passcode on an Android Device

Setting up a Passcode on an Apple Device

What will I notice when the Policy is activated?

After deployment of the Policy, the first time you use your device to connect to Exchange you will be prompted to create a passcode (if one has not been previously set) which will be needed to unlock the device and gain access to email and other data. You'll also notice that the screen will lock after 15 minutes of inactivity. Other features of the Policy will generally be invisible.

Wait... You're going to wipe my phone?!?

Remotely wiping the device is not done by default, nor is it a new feature. It has been enabled by default for a number of years on any device that connects to MBU's Exchange system via Microsoft's ActiveSync protocol. The protocol does not allow any selectivity in wiping data; only the entire device is erased back to a factory default state. A device will only be wiped in the event of loss or theft, or after 16 incorrect attempts at entering a PIN (passcode).

There isn't a practical method for remotely identifying the ownership of a device that connects to MBU's systems. MBU is responsible for its data—and for costly breach notification requirements in the event of device loss or theft—whether the device on which it resides belongs to the University or to one of its employees.

Can I wipe my own device? How do I do that?

Yes, you can wipe your own device. **BE CAREFUL, this is NOT reversible**.

1. From the Outlook Web App (https://outlook.office.com), click the **settings gear**, and then click **Options**.
2. Under **General**, click **Mobile Devices.**
3. Select the device you want to wipe and click the **Wipe device** icon.
4. Click **Yes**.

For a detailed tutorial and more information on how to wipe your mobile device please contact the IT Department.

Under what circumstances will my device be wiped?

After 16 attempts at typing in an incorrect PIN (passcode) we assume that the device has been stolen and someone is trying to guess the PIN that you assigned to the device. In order to protect sensitive MBU data, the device must be wiped and restored to factory defaults.

NOTE: With iOS devices, there are forced timeouts between incorrect tries that will prevent someone (such as a child) from quickly erasing your device.

Will the policy apply to all of my mobile devices?

Yes, the policy is applied to your Exchange e-mail account and not to specific devices. Any device that is configured to connect directly to your MBU Exchange account will be affected.

If you do not check MBU email on your device, then the standard will not be automatically enforced on your device. However, if you store sensitive non-email data on your device you are still required to manually apply the security settings. If you choose to add your MBU email account to your device in the future the security settings will be enforced the first time you connect to Exchange.

Will MBU be able to access data on my device?

No, MBU cannot access data on your device or monitor your activities. Mobile Device Security only ensures that data is secured in the event that your device is lost or stolen.

Why did I see a message about my camera being disabled?

Your camera will not be disabled. The message that you're seeing is static and reflects what the Policy could be set to do, but does not reflect what is actually being done.

If locked out, can I place emergency calls?

Nearly all phones have an "Emergency Call" feature that you can access from the lock screen. You can choose this option to call 911 or other phone numbers that are memorized on your device.

What if my device is "jailbroken" or "rooted"?

Devices that are "rooted" or "jailbroken" are not allowed to access MBU data since these devices are highly insecure.

I already have a PIN code, what will happen?

Nothing. Your device will continue to work as you have been using it (as far as the PIN is concerned).

Are you installing software on my device?

No. All we are doing is enabling the security features already built into your device's operating system. These features are being activated through the existing ActiveSync protocols used between your device and the Exchange Server. We will not be able to monitor the use of your device in any way.