Corporate Mobile Device Management (MDM)

August 8, 2018

Objectives & Goals

- What is Mobile Iron and Mobile Device Management:
  - Mobile Iron is an application that manages mobile devices (phones and tablets).
- Our goal is to:
  - Securely manage and strategically contain data/ information on Company and non-Company owned devices i.e. (bring your own device) with no end user impact.
- Our objectives are to:
  - Install MobileIron on all work-related mobile devices
  - Maintain and manage compliance with Information Technology (IT) Acceptable Use Policy.
  - Align Corporate and its subsidiaries for mobile device management.

BYOD vs Corporate Owned Devices

Bring Your Own Device (BYOD)

- Requires manager approval
- Authorization to install Company software on personal device(s)
- IT Acceptance Use Policy acknowledgment
- Will be provided link to install with registration
- For email communication only unless approved
- Works with multiple mobile device operating systems (OS)

Company Owned Devices

- Mandatory installation as part of the IT Acceptance Use Policy
- If not issued with device, a link will be provided to install and register software
- Based on approval can utilize all the features which include Mobile@Work, Web@Work and Docs@Work.
- Native email client will be utilized (iPhone email client)

What's in it for me

- Ability to utilize and save data on home drive if desired from a phone or tablet. e.g., I-drive.
- Ability to access internal web sites not accessed by the public. e.g., EAR.
- Mobile applications necessary for business function can be pushed to the device. e.g., Concur.
- Devices can be locked or unlocked remotely (both personal or Company Devices).
- Remotely wipe stolen or lost devices; quickly remove Company confidential information (Company Data only through the App).
- Employees can use the device of their choice (with approval).
- Newly purchased Company mobile devices will have MobileIron installed.

Impacts

- Users may face a small learning curve after installing the applications needed to access Company data. Some instruction may be required.
- Access to Company resources will be restricted to secure applications approved by the company. The primary applications used to provide secure access are Mobile@Work, Docs@Work and Web@Work. These applications will need to be installed on the device (Manager approval required).
- The IT Acceptable Use Policy has been updated and users will have to read and accept it before MDM access is granted.
- Manager approval is required to before MDM access is granted.

Impacts (continued)

- To understand the impacts, pilot groups are being identified with both Company and subsidiary users.
- Current users with email access will no longer have access once the MDM program has been accepted. A date will be determined and notifications sent to current users to ensure employees have time to install MDM.