Weill Cornell Medicine
Information Technologies & Services

Service Policy

Mobile Devices

Responsible Executive: Chief Information Officer, WCM
Original Issued:
Last Updated: November 14, 2022

Contents

1. What is considered a mobile device?

A mobile device, such as a smartphone or tablet, is generally a small form factor device with local built-in storage, network access, and the ability to run one or more applications from various sources, such as the web or an application repository.

2. User Responsibilities

Mobile devices that are used to access the internal WCM network or to synchronize WCM data to the device (e.g., email, contacts, calendars, etc.) must be centrally managed by Information Technologies & Services (ITS) through the certified mobile device management (MDM) platform. WCM faculty or staff who wish to purchase a mobile device must contact their division or department administrator. ITS can provide recommendations on the appropriate device to meet the user's needs and assist the department in contacting the appropriate vendor.

The user is responsible for:

- Settling any service or billing disputes with the carrier
- Purchasing any required software not provided by the manufacturer, wireless carrier, or ITS under a site license agreement
- Registering the device and maintaining any necessary warranty information
- Battery replacement due to failure or loss of ability to hold a charge
- Backing up all data, settings, media, and applications
- Maintaining compliance with the Minimum Security Requirements
- ITS will not provide support for:
    - Third-party or "beta" release software, unless explicitly listed as being a supported application
    - Non-approved mobile devices using WCM synchronization and application services

3. Minimum Security Requirements

Any mobile device that synchronizes information with WCM resources must be registered with ITS and configured with the ITS MDM platform. The following minimum requirements will be enforced by the MDM platform:

3.01 Device Passcode

All mobile devices must enforce at least a six-digit complex PIN that adheres with the below requirements:

- The PIN may not consist of three or more consecutive ascending or descending digits (e.g., 123456 or 654321).
- The PIN may not have more than two repeated consecutive digits (e.g., 143333).
- The passcode may not be one of three previously used passcodes.

Biometric authentication, such as fingerprint or facial recognition, is permitted when combined with a compliant PIN. Pattern unlocks and other authentication methods are not permitted.

After 10 invalid passcode attempts, the mobile device will be reset to factory defaults and all data will be lost.

3.02 Device Timeout

The maximum amount of time before the mobile device requires a passcode to unlock is 30 minutes.

3.03 Device Encryption

In accordance with ITS policy 11.06 – Device Encryption, all mobile devices must be encrypted.

3.04 Device Operating System

Mobile devices must be running a version of the operating system that is under active support and receiving regular security updates from the manufacturer to synchronize WCM data. Please note, while a particular phone model may be able to run the latest operating system, it may not necessarily be receiving regular security updates.

Please refer to the following articles for manufacturer support information:

- Apple iOS and iPadOS devices
- Google Pixel devices
- Samsung devices
- Motorola devices
- OnePlus devices
- vivo devices
- Xiaomi devices
- LG devices

If a mobile device is not listed on the above websites, the manufacturer may no longer be providing security updates and the phone cannot be used to synchronize WCM data. Contact ITS Support for further assistance.

3.05 Device Configuration and Inactivity

The MDM application must be installed on all mobile devices to ensure compliance with this policy. In addition, all mobile devices must check in with the MDM server at least once every 30 days.

3.06 Device Quarantine

Mobile devices that fail to meet the above requirements may be temporarily quarantined. Users will receive notifications when quarantining has occurred and instructions on how to correct the compliance issues.

4. Lost or Stolen Devices

If your mobile device is misplaced, stolen, believed to be compromised, or its whereabouts are otherwise unknown, promptly report it to ITS Support. ITS may be able to assist you in locating your mobile device. When this is not possible or if the device is not retrievable, ITS will issue a remote wipe command to attempt to remove all WCM data from the device. At your request, we can also attempt to issue a full wipe command, which will remove all personal data.

5. Other Guidelines

5.01 Install Antivirus Software

Although rare, mobile devices are just as susceptible to viruses as desktop or laptop computers. Industry analysts expect viruses, Trojans, spam, and all manner of scams to increase dramatically as the demand and use of mobile devices grow. Not all mobile devices have antivirus software, but many vendors do offer antivirus and antispam solutions for some devices. Contact ITS Support if you wish to learn more.

5.02 Use Protected Wi-Fi Networks

Where possible, connect to known secure (password-protected) Wi-Fi networks. By registering your mobile device, you will be able to connect to the secure WCM wireless network. Exercise caution when connecting to public hotspots.

5.03 Disable Unused Options and Applications

Reduce security risk by limiting the use of your device to only necessary applications and services. In addition, other benefits are extended battery life, increased memory storage, increased application performance, efficient synchronization

time and reduced management of security updates for applications. Bluetooth and infrared (IR) are services that should be configured properly or turned off when not in use because they can potentially pose a risk to your device and data.

5.04 Perform Regular Data Backups

Back up your data on a regular basis in case your mobile device is lost, damaged, or loses battery life. Multiple backup mechanisms are available to fit your needs.

5.05 Dispose of Your Device Safely

When you are ready to dispose of your device or return it to the vendor, be sure to remove all sensitive information first. Apple users should be sure to deactivate “Find My iPhone” or similar feature to remove the security activation lock. The device should be restored to "factory defaults" which can be accomplished by a "hard reset." Contact ITS Support if you need assistance in resetting the device.

Revision History:

Date	Author	Revision
⋮		
May 11, 2021	Brian J. Tschinkel	Device Passcode section updated
November 14, 2022	Brian J. Tschinkel	Device Operating System section updated