

TABLE OF CONTENTS

General Mobile Device Best Practices	1
iPad/iPod/iPhone Specific Best Practices	2

GENERAL MOBILE DEVICE BEST PRACTICES

- Use a passcode/passphrase/pattern to lock the device after inactivity – typically no more than 10 minutes of inactivity should trigger this
- Encrypt the device if the option is available, using the highest encryption possible (minimum 128-bit). If encryption is unavailable, never store highly confidential data on the device.
- When choosing between unsecured Wi-Fi and 3G/4G/CDMA service, always opt for the cellular data service, as it is typically significantly more secure than unsecured Wi-Fi. If accessing sensitive/protected data, never use unsecured Wi-Fi unless you have access to a VPN client.
- Use the Marquette Cisco VPN if the device will support it
- Report stolen/lost devices as soon as possible. Note your device serial number, ESN (Electronic Serial Number, if applicable), and other identifying information for your own records and to facilitate law enforcement or other recovery. Marquette tracks this for university supported devices.
- Utilize remote wipe capabilities if possible (can be enforced through Microsoft Exchange)
- Carefully select applications to install on the device, taking into account the type of data the application will access, whether or not the application is believed to be secure, and whether or not the vendor typically collects information from users through the application (leading to possible data leakage).
 - In addition, it is recommended to avoid use of Remote Desktop programs via a mobile device
- Disable options and applications that you do not use
- If Bluetooth is enabled, do not allow the device to be discovered automatically, and secure it with a password to prevent unauthorized access.
- Never leave the mobile device unattended
- Utilize antivirus/anti-malware software if supported
- Regularly back-up data – preferably in an encrypted fashion
- Update the device’s software per the manufacturer’s instructions. Typically updates tend to fix security holes and improve device functionality.
- Limit use of the device by 3rd parties to protect your personal data and facilitate accountability for potential misuse
- If the device is no longer in use, ensure that all of the data on it is wiped, and it is disposed of properly.

IPAD/IPOD/IPHONE SPECIFIC BEST PRACTICES

- In addition to/in conjunction with the above practices
 - Use Marquette configuration templates (coming soon) to set up the device with Marquette's network, and to enforce University suggested policies on the device, including:
 - Use of a passcode (strength dependent on the potential data the device may contain)
 - Allow device wipe if 10 failed passcode attempts
 - Use of Cisco AnyConnect VPN – Available in the Apple App Store
 - Encryption of device configuration profile
 - Forced encryption of device backups
- If multiple users will be accessing the device, the native mail program should not be used, to protect the primary users email account. Web access to eMarq is the suggested alternative.