# Mobile Internet Device Security Guidelines

*Version 2.0: October 2015*

## *Introduction*

This document is designed to help you develop mobile Internet device security policy, standards, guidelines or procedures. It is organized into steps you can follow to define your objectives and develop a plan to move forward. Included in this document is supporting information to help you think through, and hopefully answer, some of the questions or issues you may encounter along the way.

## Step 1: What are you trying to accomplish? Define your scope.

- Is your goal: Establishing rules people must follow (i.e., policies, standards, procedures) or non-binding recommendations (i.e., guidelines)? Some of both?
- Do you have a clear definition of what a "mobile Internet device" is for your institution?
    - What Is A Mobile Internet Device?
    - Understand Your Environment
- Does ownership (i.e., personally owned vs. institutionally owned) of the device matter?
- Is your goal: Requirements for the protection of physical university assets?
    - Fake or Stolen Hardware
    - It's A Hard World Out There
- Is your goal: Requirements for the protection of digital university data?
    - What Mobile Internet Devices Should You Support?
    - What About Enterprise Device Management?
    - What About Mobile Device App Choices, Web Site Readiness and New Features?
    - Spam and Malware Management On Mobile Internet Devices
    - How About Hardware Encryption?
    - And Remote Wipe Capabilities?
    - Jailbreaking or Rooting
    - Fake or Stolen Hardware
    - Institutional Contact With Users' Mobile Devices
- Is your goal: Requirements for the protection of personal privacy?
    - What About Mobile Device App Choices, Web Site Readiness and New Features?
    - Spam and Malware Management On Mobile Internet Devices
    - Privacy, Health and Safety
    - Institutional Contact With Users' Mobile Devices
- Is your goal: Requirements for use in a classroom or other pedagogical setting?
    - What Mobile Internet Devices Should You Support?
    - Mobile Internet Devices and Academic Courtesy in the Classroom
    - What About Mobile Device App Choices, Web Site Readiness and New Features?
    - Institutional Contact With Users' Mobile Devices

- Is your goal: Defining acceptable use in general? You will likely want to treat employee devices differently from student devices. What about guests?

## Step 2: Does existing physical asset, technology or data-specific policy cover all or part of your defined scope?

- If not, consider revising existing policy. Doing so may be easier or more desirable than crafting new policy. If at all possible, implement a technology-agnostic policy framework that allows you to create more specific standards, procedures or guidelines without having to modify policy.

## Step 3: Communicate what you are trying to accomplish and a high-level implementation plan with your constituents.

- Help your executives understand residual risks associated with your chosen approach and why/how mobile Internet devices may be different from more familiar computing technologies.

### Step 4: Begin implementation.

### Step 5: Monitor progress, evaluate feedback, make modifications to steps 1 through 3 as necessary and continue with implementation.

### Step 6: Regularly report progress to management.

Top of page

## *Supporting Information*

### What Is A Mobile Internet Device?

To help get you started, your institution may wish to define "mobile Internet devices" as any portable technology running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple's iOS, Windows Mobile, and Symbian. To avoid confusion, your definition should exclude technology running traditional/classic or more general-purpose operating systems such as any of the Microsoft Windows desktop or server operating systems, versions of MacOS, or Linux. Your institution likely already has policies, standards, procedures or guidelines in place for those technologies.

### Understand Your Environment.

Strive to understand what mobile Internet devices your users actually have and use (including personally owned devices). There may be more of them out there than your expect!

### What Mobile Internet Devices Should You Support?

It is hard to support "everything" well, and your users may end up more-or-less randomly selecting a mobile Internet device based on word-of-mouth or aggressive salesmanship. Should you be making some specific recommendations? In fact, should you have a standardized list of supported mobile Internet devices?

Does the cellular connectivity matter from a security point of view? Do you want to standardize on GSM? CDMA? How about iDEN? Do you have opinions about 3G and 4G protocols?

If you want influence over mobile device selection, are you willing to pay to obtain that influence (e.g., by subsidizing some mobile Internet device choices), or do you just want to try influencing those decisions via policy?

### What About Enterprise Device Management?

Some sites require all institutional personal computers to be centrally managed. If you're from one of those sites, will you be comfortable if mobile Internet devices aren't *also* centrally managed? Central management of institutionally owned mobile Internet devices may allow you to do things such as:

- setting minimum device password length, complexity, maximum time between changes, max failures before wiping, etc.
- adding or removing root certificates
- configuring institutional WiFi and VPN
- controlling installation of third party applications, recreational uses, etc.

If you're planning to centrally manage mobile Internet devices, you may want to review device enterprise management feature support options as part of deciding what mobile Internet devices you want to endorse and support. Specifically, what options are available for securely and scalably pushing policy to your users' mobile Internet devices?

Also consider that it may be desirable to use different policies for students than for employees. Network access control policies on your residence hall networks as compared to faculty and staff networks may be a good illustrative example of how some institutions treat these populations differently.

If your intention is to enforce policy on *any* mobile Internet device connecting to your infrastructure (however you define that), be aware that this will almost certainly include personally owned devices. Decide in advance how you will address inevitable questions, challenges and concerns regarding this decision. Unless your institution is requiring use of personally owned devices to perform official duties, there is likely no obligation for anyone to do so. In other words, it may be entirely at the discretion of the device owner to connect to your institution's infrastructure. If an individual does not agree with or accept your institution's terms for doing so they can choose not to use their mobile Internet device to interact with your institution. This may be similar to how many organizations explicitly prohibit the use of personal computers in designated areas, for specific roles or when accessing specific systems or data.

In short, you may wish to think of mobile Internet devices connected to your institution's network in the same way as laptops. That is, if you have specific requirements (e.g., network access control enforcement; no unauthorized Internet connection sharing; etc.) for laptops connecting to your wireless (or wired) network, you will very likely want those same requirements enforced on mobile Internet devices for the same (or similar) reasons. Similarly, you may wish to think about mobile Internet devices *not* connected to your institutions wired or wireless networks as any other non-trusted computer on the Internet, even though these devices may be physically present on your campus.

### How About Hardware And Data Encryption?

Personally identifiable information ("PII") is a material concern at many sites. Do the mobile devices you've chosen to support have hardware encryption? Is that encryption solid enough to meet your PII protection requirements?

Similarly, some mobile Internet devices may forgo the use of on-device storage and store all data "in the cloud." You likely already have requirements in place to protect sensitive or important institutional data. Make sure devices that store institutional data in the cloud meet applicable security and privacy requirements for doing so.

### And Remote Wipe Capabilities?

If you lose control over an institutionally owned mobile Internet device, do you need the ability to remotely send the device a magic "kill code?" (Note that even if you can remotely wipe the device, there may still be off-site backups floating around, or the device may get taken offline before the kill code can be sent and processed by the device, so don't depend too much on being able to send remote kill codes)

### What About Mobile Device App Choices, Web Site Readiness and New Features?

Mobile Internet devices have a far more constrained application development environment than traditional desktops and laptops. Thus, for example, while you may have standardized on one web browser for use on desktops and laptops, such as Firefox, perhaps, you may be surprised to find that choice may not even be available on some mobile Internet devices. Is this a problem for you or your applications?

You should also take time to look at how critical local institutional online resources look on a mobile Internet device. A home page that's optimized for a large screen and a high-speed connection may not work well on a mobile device with more modest capabilities. For example, try viewing important institutional sites via simulators such as http://www.testiphone.com/ -- are your web pages still usable? Should you create a mobile version of your home page? (If www.example.edu is your normal home page, you might create a simplified home page at m.example.edu for mobile users)

Recognize, too, that mobile devices bring some new capabilities, such as QR ("quick response") codes, the square dot-like codes that are readable by camera-equipped mobile Internet devices. They're cool, aren't they? But how do you know what a code points to? Should you be using them yourself to increase ease of use for your mobile Internet device users? Or do they represent a security threat that should be discouraged?

You should begin having these conversations at your site.

### Spam and Malware Management On Mobile Internet Devices.

Recognize that spammers will still target users even if they're on mobile Internet devices. What spam management options do users have for a given service? How can they report spam that slips through? Malware may still target users of mobile devices, but due to the device architecture, traditional antivirus software may not be needed (or may not even be available!) Your site's security team and/or operational support staff should talk about how they want to approach issues such as spam and malware on supported mobile Internet devices.

### Jailbreaking Apple iPhones, Rooting Android Devices.

Normally only Apple-approved applications run on the iPhone. However, some users have developed hacks (NOT blessed by Apple!) that will allow users to "break out of that jail" and run whatever applications they want. Jailbreaking your iPhone violates the license agreement and voids its warranty, but it is estimated that 5-10% of all iPhone users have nonetheless done so.

Because jailbreaking is operating system version specific, many users of jailbroken iPhones hesitate to upgrade their iPhones even when important patches are released, because upgrading will reverse the jailbroken status of their phone. Users who want to jailbreak their iPhones may also be specifically targeted by malicious applications masquerading as jailbreaking tools. For that matter, any sort of application for a jailbroken iPhone obtained from a third party source may not have been subject to any security review or auditing, unlike applications from Apple's official AppStore, and may include malicious routines.

"Rooting" can be understood as the Android equivalent of jailbreaking. As described above, rooting Android based devices can introduce new or unexpected security and/or privacy risks to data stored on the device.

For all these reasons, your site may want to discourage or forbid jailbreaking or rooting of institutionally supported mobile devices, even if you may be specifically permitted to do so here in the United States.

### Fake or Stolen Hardware.

Sites and users should also be alert that they may encounter fake or stolen mobile Internet devices. These devices may not work at all, or may break, or may stop working at the next operating system upgrade. Only purchase mobile Internet devices from reputable authorized dealers.

### It's A Hard World Out There.

Mobile Internet devices live in the real world, and are subject to a panoply of environmental threats ranging from being dropped to getting wet, or getting cooked in hot cars or frozen in cold ones. You may want to encourage users to keep their device on their person, and to consider purchasing and using a case or holster to minimize at least some of those threats.

### Privacy, Health and Safety.

Mobile Internet devices can potentially have profound privacy implications. By way of example, almost all mobile Internet devices have the ability to have their physical location tracked by a variety of means, a wonderful invention if you're having a heart attack and have just called 911 for an ambulance, but potentially a huge invasion of your privacy if this service gets abused by a stalker, or by an intrusive marketer.

Mobile Internet devices also emit cellular radiation. While those emissions are limited by law, and are believed to be at safe levels, some phones emit less radiation than others, and use of hands-free devices may also reduce (or shift) the amount of radiation you receive. If this issue is important to you, we encourage you to make appropriate choices.

We'd also urge users of mobile Internet devices to be careful when it comes to where and when they use their devices. In particular, please do NOT use your mobile Internet device while you're driving. Driving while distracted can be as bad as driving while under the influence of alcohol, and we don't want to see cool mobile Internet devices result in totally avoidable tragic accidents. Many institutions may want to explicitly forbid use of mobile Internet devices while driving.

### Mobile Internet Devices and Academic Courtesy in the Classroom.

Colleges and universities strive to provide a civil environment in which to learn and work. As a matter of courtesy to those you're with, please be responsible in how you interact with your mobile Internet device in the classroom. If possible, turn your phone off while you're in class, or at least set it to vibrate only. Now that we all have mobile Internet devices, if even ten percent of those devices ring during any given class session, it can be hugely disruptive.

On the other hand, we encourage faculty members to be flexible; do your best to accommodate students who may have job-related or family-related responsibilities which require them to carry a mobile Internet device with them at all times (although we recognize that obviously examination periods and other special circumstances may require more restrictive policies).

### Institutional Contact With Users' Mobile Devices.

Many schools ask students, faculty and staff to register their mobile numbers with the school for purposes such as emergency notification during extreme weather or active-shooter-on-campus scenarios. Be careful not to abuse the numbers entrusted to you solely for emergency purposes for unrelated activities, such as routine campus announcements or push marketing purposes.

Expectations should also be set for work-related contacts over mobile devices. That is, unless an employee is officially on call (and paid for that status), or it's a *real* emergency, avoid calling employees outside of work hours. Let employees have some time off to spend with their families and their friends, or to just sleep and recuperate! Please don't treat employees as if they're on unpaid call status 24x7, or you may find a sudden increase in "cellular connectivity issues" spontaneously arising, potentially at some very inopportune times.

### Selection of Mobile Device Management On-Line Resources at the time of Publication

- Mobile device management (Wikipedia)
- Exchange ActiveSync (Wikipedia)
- Understanding Exchange ActiveSync (Microsoft)
- Mobile Email with Exchange ActiveSync (Microsoft)
- iPhone/iPad/iOS Enterprise Support (Apple)
- Android Enterprise Management: An indication of the level of maturity for Android enterprise management may be deduced from the number of third party players in this field.
    - www.zenprise.com/Manage_Android
    - www.sybase.com
    - www.maas360.com/Free_MDM_Guide
    - www.inquso.se
    - http://www.mobileiron.com/
    - http://www.citrix.com/English/ps2/products/product.asp?contentID=1689163
- RIM Announces Multi-Platform BlackBerry Enterprise Solution for Smartphones and Tablets

Top of page

### Examples of Higher Education IT Policy Frameworks

- Cornell University
- University of South Carolina

### Examples of Higher Education Mobile Internet Device Guidelines

- Carnegie Mellon University
- Duke University
- Indiana University
- Kansas State University
- New York University
- Northwestern University
- Purdue University
- Rochester Institute of Technology
- Stanford University
- University of Michigan
- University of Notre Dame
- University of South Carolina
- Vassar College
- Villanova University

### Examples of Federal Government Policies

- Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs (includes several sample policies)

Top of page

---