UNIVERSITY OF ROCHESTER
Mobile Computing Device Security Standards

Overview

As mobile devices further incorporate features traditionally found in a personal computer, their smaller size and affordability make these devices a valuable tool in a wide variety of applications. However, these devices are also subject to increased risk of loss, theft, and unauthorized use.

Purpose

The purpose of these standards are to establish base configurations and management guidelines for mobile computing devices (cellular phones, personal digital assistants (PDAs), netbooks, iPads, etc.) owned and/or operated by the University of Rochester or its workforce. As there are a wide variety of mobile device operating systems, software, and system configurations used across the University, this document is NOT intended to be a definitive and comprehensive guide to device security.

Compliance with these standards does not exempt a device from meeting federal, state, or local laws and regulations. For example, if the device is collecting or storing credit card data, then the application and server must comply with all Payment Card Industry (PCI) standards.

Effective implementation of these standards will minimize the likelihood of unauthorized access to University computing resources and legally restricted and/or confidential information. All security events (ie., loss of, or unauthorized access to device) must be reported to the appropriate Chief Information Security or Privacy Officer as soon as they are discovered, in order to ensure compliance with legal obligations.

Scope

These standards apply to all University of Rochester faculty, physicians, staff, students, volunteers, vendors, contractors and any others who utilize a mobile device to access or store the University of Rochester's nonpublic information, including email and other electronic data, regardless of ownership of the device.

Definitions

Mobile device: includes any device that is both portable and capable of collecting, storing, transmitting, or processing electronic data or images. Examples include, but are not limited to, laptops or tablet PCs such as iPads and netbooks, personal digital assistants (PDAs), and "smart" phones such as Blackberry, iPhones, Android devices, etc.. This definition also includes storage media, such as USB hard drives or memory sticks, SD or CompactFlash cards, and any peripherals connected to a mobile device.

UNIVERSITY OF ROCHESTER
Mobile Computing Device Security Standards

Minimum Requirements for Mobile Devices:

- **Physical Protection**: Individuals must keep mobile devices with them at all times or store them in a secure location when not in use.

- **Password Protection:** Access to the mobile device must be protected by the use of a password.

- **Encryption:** University data classified as Legally Restricted Information must not be stored on a storage card or the device (including within cached email) without proper encryption, password protection and inactivity timeout.

- **Inactivity time out Protection:** Inactivity timeout must be set. The recommended inactivity timeout is 15 minutes but must not exceed 60 minutes.

- **Proper Disposal:** Any residual settings, data, and applications on the mobile device must be removed or wiped prior to disposal or transfer to another user. All attached storage cards that contain Legally Restricted Information must be destroyed or wiped so no data recovery is possible.

- **Lost or Stolen Device:**
  If a mobile device containing University of Rochester information is lost or stolen, report the loss immediately to University of Rochester Security, the University or Medical Center Chief Information Security Officer, and a Privacy Officer (if it was used to access or store Medical Center information). These individuals will determine whether there is any requirement to report the security incident to state or federal agencies or others. In addition, the incident must also be reported immediately to the appropriate information technology helpdesk to determine if the device can be wiped remotely.

Additional Recommendations for Mobile Devices:

- Invalid Password Attempts: The device should be set to wipe after 10 invalid password attempts.

- Disabling unused services: Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.

- Remote wipe capability: The mobile device should support the ability to remotely reset the device, including the deletion of all locally stored data.

- Secure connectivity: Any Legally Restricted information transmitted to or from the mobile device (e.g. wireless or the Internet) should be encrypted.

UNIVERSITY OF ROCHESTER
Mobile Computing Device Security Standards

Need Help?

For additional information or assistance with configuring your device:
University IT Help: 585-275-2000 or send an email at Univithelp@rochester.edu.
Medical Center IT Help: 585-275-3200 or email at Helpdesk_ISD@URMC.Rochester.edu

Related Policies

I. **University of Rochester Information Technology Policy**

http://www.rochester.edu/it/policy/

II. **Patient Protected Health Information (PHI) covered by Health Insurance Portability and Accountability Act HIPAA)—Privacy and Security Policies**

https://intranet-secure.urmc.rochester.edu/policy/HIPAA/PolicyManual/

III. **Social Security Number (SSN) and Personally Identifying Information (PII)**

http://www.rochester.edu/it/policy/SSN-PII.html

IV. **Student Information covered by Family Educational Rights and Privacy Act FERPA)[1]**

http://www.rochester.edu/registrar/policies.html

V. **Financial Account, Credit and Debit Card Information**

http://www.rochester.edu/adminfinance/treasury/nocard.html

http://www.rochester.edu/adminfinance/treasury/docs/ecommerce.pdf

VI. **Employee Personnel Records**

http://www.rochester.edu/working/hr/policies/pdfpolicies/108.pdf
http://www.rochester.edu/working/hr/policies/pdfpolicies/404.pdf

VII. **Legally Restricted or Confidential (http://www.rochester.edu/it/policy/ - Section III)**