AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Data Security for Mobile Devices

Policy Category: Information Technology Policies

Subject: Safeguarding university data on mobile devices.

Office Responsible for Annual Review of this Policy: Office of Information Technology

Related University Policies: IT Security Policies, Computer Use and Copyright, Privacy Policy, Health Insurance Portability and Accountability Act Privacy Policy, Confidentiality of Student Records, University Records Retention and Disposal Policy, Data Classification Policy

---

I. SCOPE

This policy covers staff and faculty and their usage of both personal and university-owned mobile devices attaching to the American University network and server infrastructure that may store, display, or process University data.

II. POLICY STATEMENT

Mobile devices that combine computing power and telephony are on the rise. While the portability makes these devices useful, it also makes them a potential security risk to users and to the University when they access University data. These risks include but are not limited to the ease of mobile devices getting lost, stolen, or misplaced and weak user authentication. The technology is new; but, the responsibility remains the same and should stay focused on the data. Protecting the confidentiality, privacy, and integrity of American University data is each of our responsibilities. We must physically protect our devices and take the necessary precautions to protect the data that we interact with. The purpose of this policy is to clearly state the user requirements necessary to mitigate these risks and to protect the University data accessed on mobile devices.

III. DEFINITIONS

Jailbreaking is commonly used to describe the process of removing the limitations on devices, running the iOS and Android operating systems. Jailbreaking permits root access to the operating system, allowing the download of additional applications, extensions, and themes that are unavailable through the official Apple store or Android Marketplace sites. For this policy, we use the term broadly to refer to any unsanctioned operating system changes made to a mobile device.

Mobile devices are any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Examples include, but are not limited to: Blackberries, Android based devices, iPhones, and iPads (iOS) devices.

Registered devices are mobile devices that have been registered with the Office of Information Technology's (OIT) Blackberry Enterprise Server (BES) or Lotus Notes Traveler service.

Users are faculty or staff who use mobile devices, university or personally owned, which utilize University network resources.

IV. RESPONSIBILITIES

All staff and faculty mobile devices must be registered with the Office of Information Technology's (OIT) Blackberry Enterprise Server (BES) or Lotus Notes Traveler service, if they access University services.

Users must abide by the University's IT Security Policies and Computer Use and Copyright Policy.

Users must routinely follow the mobile device manufacturer's recommendations to update and patch the operating system and applications, as soon as practical after receiving notification.

Users must set a password/PIN on the mobile device that must be at least 4 characters in length. There will be no expiration set.

The OIT will enforce the use of PIN and inactivity settings for all devices registered through Lotus Notes Traveler and the BES. Registered devices, can be wiped if the they are lost or stolen.

Users will set the password lock (screen saver) on their mobile devices to activate at the maximum time frame. To achieve a higher security level, OIT recommends that Users set the shortest window as possible.

Users must not jailbreak their devices.

Users must not store confidential data as defined by the University's Data Classification Policy.

Violations of this policy may result in disciplinary action up to and including termination of employment.

VI. EFFECTIVE DATE

June 1, 2014

VII. FREQUENCY OF REVIEW AND UPDATE

Annually. Last reviewed August 2015, no updates.

VIII. SIGNATURE, TITLE, AND DATE OF APPROVAL

The policies herein are effective June 1, 2014. This policy needs to be signed by the appropriate officer (listed below) before it is considered approved.

This document was approved and signed by

Doug Kudravetz
CFO, Vice President & Treasurer