# RIVERSIDE: AUDIT & ADVISORY SERVICES

July 25, 2018

To: John Virden, Chief Information Security Officer

 Information Technology Solutions

Subject: Internal Audit of Campus Mobile Devices

Ref: R2017-07

We have completed our audit of Campus Mobile Devices in accordance with the UC Riverside Audit Plan. Our report is attached for your review. We will perform audit follow-up procedures in the future to review the status of management action. This follow-up may take the form of a discussion or perhaps a limited review. Audit R2017-07 will remain open until we have evaluated the actions taken.

We appreciate the cooperation and assistance provided by your staff. Should you have any questions concerning the report, please do not hesitate to contact me.

 Gregory Moore

 Director

cc: Ethics & Compliance Risk and Audit Controls Committee

UNIVERSITY OF CALIFORNIA AT RIVERSIDE

AUDIT & ADVISORY SERVICES

MEMBER OF ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INTERNAL AUDIT REPORT R2017-07

CAMPUS MOBILE DEVICES

JULY 2018

 Approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Noahn Montemayor Rodolfo L. Jeturian, Jr.

Principal Auditor Assistant Director

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Gregory Moore

 Director

**UC RIVERSIDE**

**CAMPUS MOBILE DEVICES**

**INTERNAL AUDIT REPORT R2017-07**

**JULY 2018**

**I. MANAGEMENT SUMMARY**

Based upon the results of work performed within the scope of the audit, it is our opinion that, overall, the system of internal controls over mobile device use, management, and security is operating satisfactorily and is generally in compliance with University policies and procedures.

We observed some areas that need enhancement to strengthen internal controls and/or effect compliance with University policy.

Information Technology Solutions (ITS) has disseminated mobile security guidelines, technical information, and how-to procedures to aid campus users in understanding risks and threats and protecting mobile devices. However, some critical measures to mitigate mobile device security vulnerabilities are not strictly enforced by management or thoroughly adopted by all users. These include requiring operating system updates, disabling location services when not needed, immediately reporting lost devices to ITS, safeguarding synchronization and backup of campus mobile devices and data, and encrypting data stored on mobile devices.

1) Specific compliance requirements designed to support mobile computing and secure mobile devices against a variety of threats have not been written into campus policy and procedures. (Observation III.A.)

2) To mitigate mobile device security vulnerabilities, implementing certain mobile device management technologies and administrative controls may have to be considered. (Observation III.B.)

These items are discussed below. Minor items that were not of a magnitude to warrant inclusion in the report were discussed verbally with management.

**II. INTRODUCTION**

 **A. PURPOSE**

UC Riverside Audit & Advisory Services (A&AS), as part of its Audit Plan, performed a review of campus mobile computing device use, management, and security standards and practices. Review procedures were designed to evaluate compliance with certain University policies and procedures, efficiency and effectiveness of selected operations, and adequacy of controls implemented to mitigate risks associated with allowing mobile devices to access campus data and information systems.

 **B. BACKGROUND**

Mobile computing devices, such as smartphones, tablets, personal digital assistants, smartwatches, and data storage devices are important tools for productivity and their use is supported to achieve business goals. However, these devices also present significant risks to data security and information systems security. If appropriate security measures and control procedures are not effectively applied, mobile devices can be channels for unauthorized access to UCR data and IT infrastructure.

**Mobile device** as considered in this audit and as used throughout this document is defined 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. It excludes 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 – technologies for which policies, standards, procedures, and guidelines are separate and already in place.

 **C. SCOPE**

Audit procedures were performed to evaluate whether Campus, ITS, and various department policy, standards, guidelines, and procedures that direct the use, management, and security of mobile devices are adequate and appropriate, operating as intended, and effective to mitigate risks of impairing the integrity, availability, and confidentiality of University data and information systems.

The scope of the audit was limited to activities during the fiscal year (FY) July 1, 2016 through June 30, 2017 and focused on the following conceptual areas of mobile computing device management and security:

**Governance / Policy Framework**

* Determined whether a governance framework and/or security policy exists for campus mobile devices;
* Evaluated existing organizational structure, leadership, and management processes as well as mobile device security policy and procedures for clarity, adequacy, and effectiveness in ensuring the security of mobile devices, data, information systems, and university resources.

**Risk Management**

* Assessed management processes that ensure risks associated with mobile computing are appropriately evaluated and that mobile computing security risks are minimized;
* Determined if risk assessments are performed prior to implementation of new mobile computing devices, and if a continuous risk monitoring program evaluates changes in or new risks associated with mobile devices.

**Mobile Device Security Awareness**

* Reviewed cybersecurity awareness and related training programs for adequacy and effectiveness in addressing risks and policies associated with specific mobile computing technologies/devices and their security components as well as accountability, responsibility, and communication processes between device users and management.

**Mobile Computing Operations**

* Evaluated existing administrative controls and practices to manage mobile computing operations for compliance with applicable policy and procedures, adherence to relevant standards, best practices, and generally accepted security principles, and adequacy of certain internal controls;
* Reviewed operating procedures and control activities in the following procedural areas:
	+ Device Management – device tracking, device provisioning / de-provisioning;
	+ Access Control – access control rules;
	+ Stored Data – Encryption technology, data transfer, data retention;
	+ Malware Avoidance – Malware prevention technology;
	+ Secure Transmission – Secure connections.

**D. INTERNAL CONTROLS AND COMPLIANCE**

As part of the review, internal controls were examined within the scope of the audit.

Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the achievement of objectives in the following categories:

\* effectiveness and efficiency of operations

\* reliability of financial reporting

\* compliance with applicable laws and regulations

Substantive audit procedures were performed during March through June 2017. Accordingly, this evaluation of internal controls is based on our knowledge as of that time and should be read with that understanding.

**III. OBSERVATIONS, COMMENTS, AND RECOMMENDATIONS**

1. **Mobile Computing Considerations in Information Security Program**

Although UCR has disseminated mobile computing and mobile device security procedures, standards, and guidelines, compliance has not been strictly enforced. Specific compliance requirements designed to support mobile computing and secure mobile devices against a variety of threats have not been written into campus policy and procedures.

COMMENTS

University policy (IS-3 Electronic Information Security) requires campuses to establish an Information Security Program that comprises a comprehensive set of strategies with a range of related technical and non-technical measures. As the use of mobile devices proliferates, UCR must address the unique security concerns that the use of these devices brings.

A robust and comprehensive policy provides not only the starting point of an overall mobile computing and security program but also the guidelines for acceptable use of mobility technologies and information resources. The policy need not lay out the technical details, but should instead focus on desired results. A set of detailed standards and procedures should support the implementation of policy and aid in ensuring compliance by all mobile device users.

RECOMMENDATIONS

Management should develop and implement specific policy and procedures for the use of mobile computing devices to access campus information resources and conduct University business. Policy and procedures should be supplemented by specific standards or rules that must be followed for supported mobile devices to be granted access to campus data and information systems.

Some of the questions that these standards should address include:

* What mobile devices are supported?
* Do manufacturers / brands matter?
* How will personally-owned devices be supported differently than University-owned equipment?
* Does cellular connectivity matter? GSM? CDMA? iDEN?
* What about 3G, 4G, LTE, or LTE-Advanced protocols?
* How are the rules different when the mobile device users are faculty, staff, or students?

MANAGEMENT RESPONSE

The UC Riverside Information Technology Solutions (ITS) Office will create a UCR campus guideline specific to mobile device management following new UC IS-3 Electronic Information Security Policy and UC Minimum Security Standard which cover mobile inventory, anti-malware, patching, encryption, etc., and maps to ISO 27002:2013. Will include standards or rules applicable to specific protocols (3G, 4G, LTE, etc.) as applicable. Guidelines and standards will be formalized through UCR policy approval process (ITEG) and implemented across campus.

Expected completion date: June 30, 2019

Additionally, the UC Riverside Information Technology Solutions (ITS) Office will initiate research, consideration and implementation of formalized organizational account requirements with suppliers, such as Apple. A resulting policy or guideline will allow organizations to fully manage the device when an employee leaves. Currently when an employee leaves who had an Apple device assigned to him/her and locked with a personal Apple ID, the device becomes locked as the former employee leaves without signing out of the account. Having a corporate account with Apple, will help to facilitate an unlock of these devices as they will be associated to UCR and not the individual.

Expected completion date: June 30, 2019

1. **Mobile Device Management**

To mitigate mobile device security vulnerabilities, implementing certain mobile device management technologies and administrative controls may have to be considered.

COMMENTS

Centralized mobile device management technologies are increasingly used as a solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users. In addition to managing the configuration and security of mobile devices, these technologies offer other features, such as providing secure access to enterprise computing resources. There are two basic approaches to centralized mobile device management: use a messaging server’s management capabilities (sometimes from the same vendor that makes a particular brand of mobile device operating system), or use a product from a third party, which is designed to manage one or more brands of mobile device operating system.[[1]](#footnote-1)

Mobile device management (MDM) is a way to ensure users stay productive and do not breach enterprise policies. By controlling and protecting the data and configuration settings of all mobile devices in a network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime. [[2]](#footnote-2)

MDM software enables corporate IT departments to manage the many mobile devices used across the enterprise. There are plenty of features depending on which MDM product is chosen:

* Policy enforcing – There are multiple types of policies which can be enforced on MDM users.
	+ Personal policy – According to corporate environment, highly customizable
	+ Device platform specific – Policies for advanced management of Android, iOS, Windows and Blackberry devices.
	+ Compliance Policies/Rules
* Secure email
* Secure browser
* Application catalogue
* VPN configuration
* Predefined WiFi and hotspot settings
* Jailbreak/Root detection
* Remote wipe of corporate data
* Remote wipe of entire device
* Device remote locking
* Remote messaging/buzz
* Disabling native apps on device

RECOMMENDATIONS

Management should consider implementing centralized mobile device management technology for University-owned mobile devices and conceivably for personally-owned devices as well. MDM software will enable ITS and/or department IT managers to better manage the many mobile devices used across campus.

MANAGEMENT RESPONSE

The UC Riverside Information Technology Solutions (ITS) Office, since the time of this audit, has initiated a pilot MDM program using a single shared instance of AirWatch, an MDM solution recently integrated into the Workspace One suite. AirWatch is being used to manage and secure 44 institutionally owned mobile devices in the following customer departments: TAPS, Student Health Center, Counseling & Psychology, UCPath – HR, Student Affairs Case Management and the HUB Union. Through customer demand, adoption of this service offering continues to grow organically. ITS is confident that this solution will be able to service customers with both institutionally and personally owned devices. AirWatch offers many of the features listed above.

ITS is currently exploring how to implement a scalable campus-wide license or subscription model and improve its support model so this service can be deployed in a cost effective and sustainable manner. Currently, customers are funding their own subscriptions. ITS will conduct an implementation and budget requirements analysis along with campus mandates for use and enforcement.

Expected completion date: June 30, 2019.

1. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Murugiah Souppaya and Karen Scarfone, NIST Special Publication 800-124 Revision 1 June 2013 [↑](#footnote-ref-1)
2. *BYOD Requires Mobile Device Management* (<http://www.informationweek.com/news/mobility/business/229402912>). Information Week. [↑](#footnote-ref-2)