Adopted: 06/02/2015
Revised:

UNIVERSITY OF CENTRAL ARKANSAS
MOBILE DEVICE SECURITY POLICY

RATIONALE

The University seeks to protect its mobile devices and the data stored on either University owned or privately owned devices holding institutional data from unauthorized access, use, alteration, modification, disclosure, deletion, destruction and/or removal.

This document describes the minimum necessary security policy for mobile devices. Mobile devices must be properly secured in order to:

1. Prevent sensitive or confidential data from being lost or compromised;

2. Reduce the risk of spreading viruses or other malware that adversely affect the integrity of data, devices, or network resources;

3. Prevent abuse of the University's computing and information infrastructure.

This policy is subject to revision annually or as needed.

SCOPE

This policy applies to all mobile computing and storage devices used by UCA faculty and staff in the performance of their duties, and to all sensitive information when accessed through, or stored on, mobile computing and storage devices, regardless of the device's ownership. Sensitive data may not be released for storage on, or access through, devices that do not meet these requirements.

Applications used by employees on their own personal devices that can store or access sensitive data (cloud storage providers, etc.) are also covered by this policy.

DEFINITIONS

1. Mobile Device – Any handheld or portable device with an operating system optimized or designed for mobile computing. Examples include, but are not limited to, laptop computers running Microsoft Windows, Apple OS X, or other hardware running Android, Blackberry OS, Apple iOS, or Windows Phone.

2. User – Anyone with authorized access to University information systems. This includes permanent and temporary employees or third-party personnel such as contractors, consultants, and other parties with valid access to University resources.

3. Sensitive data – Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities, that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical

records, social security numbers, credit card numbers, financial account information, and education records.

POLICY

A. UCA Board Policy 412 - Computer Use

This policy does not supercede or replace UCA Board Policy 412. Employees should also be familiar with Board Policy 412.

1. Board Policy 412 - http://uca.edu/board/files/2010/11/412.pdf

B. Physical Security

Physical security of a mobile device is the responsibility of the user to whom the device has been assigned. Devices will be kept in the employee's presence whenever possible and stored in a secure location when the user cannot have the device with them.

1. Users must report all lost/stolen devices to the University's IT staff immediately.

2. Laptop/notebook computers must be configured to require a password that meets the University's requirements for length and complexity.

3. Mobile device screen locks must be set to automatically activate and use an access control mechanism such as a PIN, pattern, fingerprint or password to allow unlocking.

C. Platform / Operating System / Application Security

1. Mobile devices used to store or access University data must, at a minimum, run on the following hardware/operating system combinations:

    a. Android (minimum version specified by UCA Information Technology)
    b. Apple iOS (minimum version specified by UCA Information Technology)
    c. Windows Phone (minimum version specified by UCA Information Technology)
    d. BlackBerry OS (minimum version specified by UCA Information Technology)

2. Devices must not be "jailbroken" or "rooted" or have any software/firmware installed that will provide the user with access to functions or configuration options not intended to be exposed to the user.

3. Users must not load pirated software or illegal content onto their devices.

4. Applications must be only installed from official sources provided by the manufacturer of the mobile device, such as the Apple App Store or Google Play Store. Installation of code/applications from untrusted sources is forbidden.

5. Mobile devices must be kept current with all manufacturer or network provided updates and patches.

D. Data Security

1. Users may only load sensitive data onto mobile devices if such data is necessary and essential to the role of their employment with the University.

2. Users should ensure that any sensitive data resident on a device is the absolute minimum necessary to perform the user's required tasks.

3. Mobile devices should only be used for temporary storage of sensitive data. Users should delete any sensitive information from the mobile device as soon as the work that requires it is completed.

4. Sensitive data should never be copied to any online storage service.

5. Mobile devices must not be connected to a host computer that does not have current and enabled anti-malware protection as specified by the UCA IT department.

6. Mobile devices must use a secure connection encrypted with the WPA or WPA2 protocols when accessing sensitive data over a wireless network.

7. Mobile devices used to store sensitive data must support and use file system data encryption.

8. The user is responsible for the backup of any personal data that may be stored on the device, and the University will accept no responsibility for the loss of any personal files due to the device being wiped for security reasons.

9. A device may be subject to a full or partial remote wipe and erasure for reasons including, but not limited to:

    a. The device being jailbroken or rooted;
    b. The device containing an application that is known to contain a security vulnerability;
    c. The device being lost or stolen.

10. Upon termination of employment, the user must present their device to a member of the UCA Information Technology Department to ensure that all sensitive information, including the user's access to their UCA email account has been removed from the device. In the event that a user is involuntarily terminated, the user's device may be subject to remote wipe to ensure removal of sensitive UCA information.

E. Enforcement

Failure to comply with this policy will be investigated in accordance with UCA disciplinary procedure. Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including (but not limited to):

1. Forfeiture of University-owned mobile device(s)
2. Suspension of network account and/or email privileges
3. Administrative disciplinary action
4. Suspension of employment with or without pay
5. Termination of employment
6. Civil action initiated by the University and/or other parties
7. Referral to appropriate law enforcement agencies

ACKNOWLEDGEMENT

All employees who have been or will be issued UCA owned mobile devices, must provide documentation of receipt of this policy.