Procedure Guideline

Index No: 8035
Date: 1/2/2013
Reviewed: 12/1/13

MOBILE DEVICE SECURITY

I. PURPOSE:

This document describes the minimum security policy for City of Little Rock mobile devices. Mobile devices must be appropriately secured to prevent sensitive or confidential data from being lost or compromised, to reduce the risk of spreading viruses and to mitigate other forms of abuse of the City's computing and information infrastructure.

The City of Little Rock Information Technology Department seeks to protect City mobile devices from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and removal. These devices are to be used strictly for business purposes. This security policy applies to the user of any City-owned mobile device which connects to any City managed network/resource.

II. RESPONSIBILITY:

A. All users accessing City data services on any mobile device are covered by this policy, as well as any related policies or procedures put in place by the City Manager and their Department Director.
B. The Information Technology Department (LRIT) will be responsible for device management and compliance enforcement through a mobile device management (MDM) system.
C. Each Department will be responsible for their devices' monthly subscription fee for the MDM system in order to have access to the City's network. The subscription fee is a per device monthly charge.
D. Each Department will be responsible for maintaining a list of approved applications (apps) for City-owned devices. In addition, Departments will be responsible for notifying LRIT in a timely fashion when changes are made to these lists.
E. Each Department will maintain an inventory of all City-owned mobile devices and accessories in use. This list will be provided to LRIT for management purposes and any additions or deletions made to it will be communicated to LRIT in a timely fashion.
F. Each Department will be responsible for any issues related to mobile device management caused by their failure to notify LRIT of changes to either approved apps lists or their device inventories.

G. Department Managers and Supervisors are responsible for ensuring that users are aware of and understand this policy and all related procedures.
H. Non-compliance with this policy and its resulting procedures may be cause for disciplinary action.

III. POLICY:

A. All requests to add a device to the City's network must be accompanied by the attached Acknowledgment form with a justification for the business use and signature from the respective Department Director.
B. Device user must read, sign and agree to the terms of this policy before the device will be placed on the City's network.
C. City-owned devices will be configured by LRIT Staff to ensure compliance with all applicable policies and procedures prior to being given access to the City's network.
D. All devices will be protected by passwords that meet LRIT standards.
E. Non-Exempt employees must follow all applicable FLSA (Fair Labor Standard Act) procedures to retain mobile access to City data services.
F. No CJIS (Criminal Justice Information Services) information will be accessed or stored on any mobile device without prior approval from the Little Rock Police Department.
G. LRIT reserves the right to terminate access to City data services at any time without prior warning or notification.
H. All devices will have Mobile Device Management software installed for policy enforcement purposes. Removal of this software will result in immediate termination of access to City data services.
I. User must immediately notify both their supervisor and LRIT in the event of device loss or theft. LRIT will then remotely wipe the device.
J. LRIT will maintain both a whitelist and blacklist of applications for devices. These lists will take precedence over all department level lists. City-owned devices will be subject to both lists.
K. User must not download and install apps that are not approved for use on City-owned devices.
L. User must abide by all City, State and Federal Laws regarding mobile device use while driving.
M. Users must adhere to other applicable City Policies as they relate to acceptable use.
N. All City-owned devices must be synced to a Networked City computer and not on a personal one.
O. LRIT maintains the right to limit access to WiFi networks on City-owned devices for security reasons.

Freedom of Information Act: Employees who use a mobile devices to access City data services, particularly email, should be mindful that public records stored on a mobile device are subject to disclosure pursuant to a request under the Arkansas Freedom of Information Act unless they are covered by

an exemption. The creation of a record of communications about public business is no less subject to public access because it was transmitted over a mobile device. Therefore, employees who maintain public documents on mobile devices may be required to provide copies of public records stored on such devices.

IV. DEFINITIONS:

A. *Mobile Devices:* These include, but are not limited to: tablet PCs, Blackberrys and smart phones.
B. *User:* Anyone with authorized access to the City's network, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants and other parties with valid City network accounts.
C. *Screen Lock:* A security feature that prevents the device from responding to touch or gestures until it is unlocked with a password.
D. *Screen Timeout:* A lower power state that dims the display to conserve battery life after a period of device inactivity.
E. *Remote Wipe:* A security procedure that removes all City related data from a device in the event of loss or theft. City owned devices will be subject to a complete wipe.
F. *City Data Services*: All information technology resources maintained by LRIT (email, Internet access, servers, stored data, etc.)

Approved:

Bruce T. Moore
City Manager

Employee Acknowledgement of City's Mobile Device Security Policy

User Information	
Employee Name:	
City Department:	
Division:	
Justification/Business Need for Device:	
Device Information	
Manufacturer:	
Model:	
Serial Number:	
Telephone Number:	
City Asset Number:	
Service Provider Information	
Service Provider:	
Account Number:	

I have received a copy of the City's Mobile Device Security Policy. I agree to abide by the requirements of these policies and understand that failure to do so may result in revocation of a City owned device. I assume full responsibility for the proper care and usage of the mobile device and understand that if the equipment is lost, damaged or stolen I may be personally responsible for the cost of reimbursement to the City. I also agree to immediately notify my supervisor and LRIT if the device is lost or stolen.

By signing below, I also agree to comply with the City's Electronic Communications Policy, including the restriction for non-exempt employees working without prior approval during non-work hours. This includes checking voice mail at home or using a City mobile device to make work related phone calls or check City email after hours.

_____

Print Name

_____

Signature of Employee **Date**

I authorize the assignment of this mobile device to the employee identified above and certify that this request is in compliance with the City's policy.

_____

Print Name

_____

Signature of Department Director **Date**