Policy Statement

SUBJECT: City of Detroit Mobile Device Policy

Table of Contents

I. Overview

A. Purpose:

Mobile devices, such as smart phones and tablet computers, are important tools for the City of Detroit and their use is supported to achieve business goals. However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the city's data and IT infrastructure. This can subsequently lead to data and information leakage and system infection. The City of Detroit has a requirement to protect its data and information assets in order to safeguard its constituents, intellectual property and reputation.

B. Audience/Scope

All mobile devices, whether owned by the City of Detroit or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smart phones and tablet computers.

II. Policy

A. Technical Requirements

Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later. <add or remove as necessary>

Devices must store all user-saved passwords in an encrypted password store.

Devices must be configured with a secure password that complies with the City's password policy. This password must not be the same as any other credentials used within the organization.

With the exception of those devices managed by ITS, devices are not allowed to be connected directly to the internal corporate network.

B, User Requirements

City of Detroit sensitive data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive City of Detroit data and information must be encrypted using approved encryption techniques and password protected.

City of Detroit sensitive data and information must not be transmitted via wireless communication to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized. .

Whenever possible all mobile devices should enable screen locking and screen timeout functions.

If a user suspects that unauthorized access to company data and information has taken place via a mobile device they user must report the incident in alignment with City of Detroit incident handling process

Devices must not be “jailbroken”* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

Users must not load pirated software or illegal content onto their devices. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact City of Detroit ITS department.

Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.

All mobile computing devices must have approved virus and spyware detection/protection software along with personal firewall protection (where applicable).

The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee’s physical presence when ever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.

If a mobile device is lost or stolen, promptly report the incident to the City of Detroit Help Desk and proper authorities. Also, be sure to document the serial number of your device now, for reporting purposes, in the event that it is lost or stolen.

Devices must be encrypted in line with City’s compliance standards.

A “remote wipe” option must be available.

Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data and information is only sent through the corporate email system. If a user suspects that company data and information has been sent from a personal email account, either in body text or as an attachment, they must notify city ITS immediately.

(If applicable to your organization) Users must not use corporate workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

III. Exceptions:

The City Information Technology Services Director and City Corporation Counsel must approve any exceptions to this policy.

Approval Block

Mobile Device Policy	
Approval Date: 3/19/2014	**Review: Bi-Annual**
Effective Date: 3/19/2014	**Last Review =**