The City *of*
WAUKESHA
Information Technology

ITMDM-0.1 MOBILE DEVICE MANAGEMENT POLICY

Responsible Business Unit: IT
Affected Business Unit: All
Created by: Chris Pofahl

Creation Date: 4/26/17
Effective Date: [Effective Date]
Expiration Date: [Expiration Date]

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the City of Waukesha (City) in order to achieve its goals.

However, mobile devices represent a significant risk to data security. 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 leakage and system infection.

The City is required to protect its information assets in order to safeguard itself and its reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

Definitions

a. **Mobile Device:** A mobile device is defined as: ~~Cell phone,~~ Smartphone, ~~Internet broadband air card,~~ Laptop or Notebook computer, Tablet computer, ~~Global Positioning Service (GPS), or any electronic portable device. This includes any City owned electronic devices being used by Employees at office, home or while traveling.~~

Commented [CP1]: Updated

b. **Mobile Device Management (MDM):** Mobile Device Management Software, or MDM, is the software used to manage mobile devices by setting up software policies around the device(s).

c. **Jail-breaking or Root/Rooting Devices:** "Jail-breaking or Root/Rooting Devices" is defined as modifying a mobile device to remove controls put in place by the device manufacturer, leaving the device vulnerable to malware and/or virus and/or Trojan and stability issues.

Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by the City of Waukesha and to reduce the risk of acquiring malware infections on the network.

Scope

1. **Policy Justification**
   a. This policy related document insures the integrity, availability, and security of the City of Waukesha Wisconsin's digital assets.
   b. All mobile devices, whether owned by the City or owned by employees, inclusive of smartphones and tablet computers, that have access to the City network, data and systems are governed by this mobile device security policy. The scope of this policy does not include City owned and IT-managed laptops/notebooks.
   c. Applications used by employees on their own personal devices which store or access City data, such as cloud storage applications, are also subject to this policy.
   d. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other City requirements) a risk assessment -authorized by security management must be conducted and approved by the IT Director in conjunction with the ITB.

2. **Affected Staff**
   a. All City departments, offices, divisions, and agencies
   b. All represented and non-represented employees, contractors, and temporary workers
3. **Significantly Related Documents and Policies**
   a. ~~???~~ Cell Phone Use Policy
4. **Policy Maintenance**
   a. Review this policy annually by Information Technology Board
5. **Policy Statement**
   a. Devices must use an operating ~~OS~~system that is in compliance with the approved OS list maintained by the IT Department.
   b. Devices must store all user-saved passwords in an encrypted password store.
   c. Devices must be configured with a secure password or PIN that complies with City's password policy . ~~This password must not be the same as any other credentials used within the City.~~

Commented [CP2]: IF we can integrate with AD, we should

d. Only devices managed by IT will be allowed to connect directly to the internal City network.
e. Devices, as listed in the Policy Scope,   will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management (MDM) software.

6. User Requirements

a. Users may only load corporate data that is essential to their role onto their mobile device(s).

b. Users must enroll their device in to the Mobile Device Management System

c. Users must report all lost or stolen devices to City IT immediately by calling the IT helpdesk number (24x7): 1-262-524-3577.

d. If a user suspects that unauthorized access to City data has taken place via a mobile device, they must report the incident to the IT and HR department immediately by calling the IT helpdesk number (24x7): 1-262-524-3577.

e. Devices must not be “jail broken” (or rooted) or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

f. Users must not load pirated software or illegal content onto their devices (as described in City of Waukesha software acceptable use policy).

g. Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is not permissible. If you are unsure if an application is from an approved source contact City IT helpdesk at 1-262-524-3577.

h. 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.

i. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with City policy.

j. Devices must be encrypted in line with City security standards.

k. Users must be cautious about the merging of personal and work email accounts on their devices as any work related email may be subject to open records laws. Users must have their devices, personal or city provided, enrolled in the mobile device management system to ensure that City data is only sent through the City email system. If a user suspects that City data has been sent from a personal email account, either in body text or as an attachment, they must notify City IT helpdesk immediately at 1-262-524-3577.

l. The above requirements will be checked regularly and should a device be noncompliant that will result in the loss of access to email, a device lock, or in particularly severe cases, and if city owned, a device wipe.

m. The user is responsible for the backup of their own personal data and the City will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

7. Only devices that have the City MDM device manager installed on them will be authorized to access the City network / City applications (Apps).

~~**8.** Cloud storage solutions: The City currently does not support or recommend any cloud storage solutions as they have been known to be insecure. The City IT department only supports devices connected through MDM.~~

Commented [CP3]: We do use cloud solutions now

~~9.~~8. The use of solutions other than the above will lead to a compliance breach and the loss of access to the City network for the user. Discipline for actions found to be intentional can lead to discipline, up to and including termination.

~~**10. Use While Operating a Motor Vehicle**~~

Commented [CP4]: Covered by the Cell Phone Policy

~~The safety of City employees is critical to our ongoing success. Therefore, the City encourages all employees with a City issued Mobile Device to utilize hands-free equipment when using the Mobile Device while operating a City owned vehicle, personal vehicle, or rental vehicle for business.~~

~~Only voice calling with hands-free equipment is permitted. When dialing a number, employees should pull over to the side of the road for safety. Employees may also use voice activated calling or pre-programmed numbers providing it does not distract from safe driving. Any other Mobile Device enabled activity that prevents an employee from focusing on driving such as surfing the internet, text messaging, checking email, use of applications, or other activities, is prohibited.~~

~~**11. Personal Use**~~

Commented [CP5]: Covered by the Cell Phone Policy

~~Charges associated with using a City provided Mobile Device for personal communications, including text messages, email and voice calling, will count~~

~~towards the City's monthly mobile device plan from the wireless carrier. Therefore, personal use of a City provided Mobile Device should be minimized if possible. Employees may be held accountable of any abuse or misuse of a city provided mobile device.~~

~~**12. Loss or Damage**~~

~~Employee holds all responsibility for safe keeping of Mobile Device. Employees may also be held accountable for lost or damaged Mobile Device. Employees are not allowed to jailbreak or root any City owned device.~~

Commented [CP6]: Covered by the Cell Phone Policy

~~13.~~9. **Actions which may result in a full or partial wipe of the device**

a. A device is jail-broken/rooted,

b. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user),

c. A device is lost or stolen, and

d. A user has exceeded the maximum number of failed password attempts.

~~14.~~10. **Use of particular applications which have access to City data**

a. Only devices that have the City MDM device manager installed on them will be authorized to access the City network / City applications (Apps).

b. Cloud storage solutions: The City currently does not support or recommend any cloud storage solutions as they have been known to be insecure. The City IT department only supports devices connected through MDM.

c. The use of solutions other than the above will lead to a compliance breach and the loss of access to the City network for the user. Discipline for actions found to be intentional can lead to discipline, up to and including termination.

~~15.~~11. **Enforcement**

a. Process Violation – See City of Waukesha HR Policy *B20 - Software Usage and Standardization* approved this 2nd day of February 2010.

b. Wis. Stat. § 19.31

c. Criminal Justice Information Services (CJIS) Security Policy

d. Additionally, see related regulation enforcements (governance, security, regulatory, HIPAA, SOX, ITIL, ISO, COBIT, Homeland Security, State of Wisconsin, Federal Government, etc.) as applicable.

~~16.~~12. **Procedures Enforcing this Policy**

ITMDM-0.1 MOBILE DEVICE MANAGEMENT POLICY Approval

The Person(s) listed below approve this ITMDM-0.1 MOBILE DEVICE MANAGEMENT POLICY for IT use on the date specified.

Approver Name	**Approved On**

[Approved by] [Approved]