Background to this policy

City of Waukesha IT faces two challenges when contemplating a Mobile Device Management (MDM) policy: a mix of city and employee owned devices accessing the city's network and data, and the use of those devices for both professional and personal purposes.

With data flowing across public networks, to and from devices that are easily lost or stolen, protecting data becomes a paramount concern and the primary driving force for implementing MDM systems and policies. Security must be central to the city's workforce mobility strategy in order to protect city data, maintain compliance, mitigate risk and ensure mobile security across all devices.

This policy gives a framework for securing mobile devices and should be linked to HR policies which support's the City of Waukesha posture on IT and data security.

As a BYOD program can only be successfully implemented if certain security policies are enforced, the city would expect a MDM solution to be a prerequisite for this policy.

1. 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.

1.1 Definitions

"City" is defined as: (The City of Waukesha).
"Employee" is defined as: all personnel working in the City full time or part time.

"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.

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

"IT Dept." is defined as Information Technology Department

"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.

To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

City of Waukesha – Mobile Device Management Policy

2. Scope

1. 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.
2. 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 City Administrator.
3. 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.

3. Policy

3.1 Technical Requirements

1. Devices must use the following Operating Systems: Android 2.2 or later, iOS 4.x or later, Windows 7 or later. <This is a living requirement - add or remove as necessary>
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with City's password policy. This password must not be the same as any other credentials used within the City.
4. Only devices managed by IT will be allowed to connect directly to the internal City network.
5. These devices 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.

3.2 User Requirements

1. Users may only load corporate data that is essential to their role onto their mobile device(s).
2. Users must enroll their device in to the Mobile Device Management System

Commented [CP1]: Revise and include laptops/notebooks.

Commented [CP2]: Revise who can authorize.

Commented [CP3]: Change this to "within one revision of the latest OS"

Commented [CP4]: Not sure about this

Commented [CP5]: Password or PIN

Commented [CP6]: What devices?

Commented [CP7]: Added for reinforcing item 3.1-4

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

3.4. 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.

4.5. 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.

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

6.7. 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.

7.8. 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.

8.9. 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.

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

10.11. 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.

11.12. 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.

12.13. 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.

13.14. 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.

~~14.~~15. The City requires its employees to adhere to all federal and state laws and regulations regarding the use of Mobile Devices.

3.3 Use While Operating a Motor Vehicle

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.

3.4 Personal Use

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.

3.5 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.

3.6 Actions which may result in a full or partial wipe of the device

1. A device is jail-broken/rooted,
2. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user),
3. A device is lost or stolen, and
4. A user has exceeded the maximum number of failed password attempts.

City of Waukesha – Mobile Device Management Policy

3.7 Use of particular applications which have access to City data

1. Only devices that have the City MDM device manager installed on them will be authorized to access the City network / City applications (Apps).
2. 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.
3. 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.

City of Waukesha – Mobile Device Management Policy

Mobile Device Management User Agreement

Return signed copy to: Information Technology Department (Help Desk)

Employee Last Name:	**First Name:**	**Email Address:**
Work Phone Number:	**Supervisor Name:**	
Mobile Device Phone Number:	**Make/Model/OS of Mobile Device:**	

Employee's Signature: _____ Date: _____

Supervisors Signature:_____ Date: _____

By signing above, I agree to the following:

1. I have read and will adhere to the City of Waukesha (City) Mobile Device Management policy.
2. I will assist in protecting devices issued by the City or that store or utilize City data.
3. Devices must have encryption installed and enabled.
4. The City reserves the right to remotely wipe all City owned data on mobile devices.
5. Passwords are required for access to all mobile devices and you must safeguard your password based on the City Passwords policy.
6. Never leave mobile devices unattended for any reason while in use; always lock. Protect classified information or other protected data at all times from improper access or disclosure.
7. The MDM must be on the mobile device(s) in order to access the City network/ City applications.
8. Report any lost mobile devices to IT and the HR department is required by policy. Call: (IT department 1-262-524-3567) (HR department 1-262-524-3744)
9. The City is not liable for the loss or damage of personally owned mobile devices used to conduct City business.

DRAFT