CITY OF WAUKESHA
Administration
201 Delafield Street, Waukesha, WI 53188
Tel: 262.524.3701 fax: 262.524.3899
www.ci.waukesha.wi.us

Committee: **ITB**	**Date:** **5/6/2015**
Common Council Item Number: **15-2512**	**Date:** Click here to enter a date.
Submitted By: Bret Mantey, IT Director	**City Administrator Approval:** Kevin Lahner, City Administrator Click here to enter text.
Finance Department Review: Click here to enter text.	**City Attorney's Office Review:** Click here to enter text.
Subject: ITB agenda item 15-2512 (Mobile Device Management Policy)	

The IT department faces two challenges when contemplating a Mobile Device Management (MDM) policy: It is a mix of city and employee owned devices accessing the city's network and data; 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 will build 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.

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

The MDM policy will strike a balance between establishing a safe and secure framework for city resources to be accessed remotely without diminishing the ability of the mobile worker to do their job.

Options & Alternatives:
Currently there are no policies within the city that cover mobile device management. One option is to continue with no policy in place as the city is currently doing. IT feels this is not an option.

The MDM policy is being proposed in order to start implementing policies to protect the device and the city from harm. Other policies that can be mixed/incorporated into the MDM policy as it matures, they are:

Bring Your Own Device (BYOD) policies – These outline the level of support the IT department offers for employees' personal devices. Every organization's BYOD policy is different. Some companies give employees a stipend to purchase and maintain devices of their own, but companies usually just agree to support personal devices as well as corporate devices. BYOD policies usually include more than just mobile devices and may be referred to as bring your own technology (BYOT) policy.

Consumerization policies outline how IT will manage consumer devices in a company and define rules for acceptable use. They usually list which devices employees can use, how much control admins will have over those devices, how much (if any) of the bill the organization will cover and how IT will support devices.

End user policy lists directives that applies to end users is an end user policy. That includes BYOD policies, consumerization policies, acceptable use policies, corporate mobile device policies, mobile security policies and/or social networking policies. Usually, employees must agree to the terms of the policy, and the violation of those terms can result in consequences, such as termination.

Corporate mobility policies set out to protect data from prying eyes and make sure that the company is compliant with regulatory guidelines. The policies define how data will be secured, both at rest and in transit. Much of the time, a company also lists how it will enforce the terms of its mobility policy, including use of encryption and secure connectivity to prevent unauthorized devices from accessing the network.

Acceptable use policy- Users must agree to acceptable use policies if they want access to a network or to the Internet. Usually employees must agree not to use the Internet to break the law, spam people or break the security of other computers or users. Organizations may personalize their acceptable use policies.

Financial Remarks:
None

Executive Recommendation:
None at this time

Committee Recommendation:
Review and comment on first draft of a Mobile Device Management Policy, moving it forward towards policy adoption.

City of Waukesha – Mobile Device Management Policy

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.

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.

City of Waukesha – Mobile Device Management 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 report all lost or stolen devices to City IT immediately.
3. 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.
4. 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. Users must not load pirated software or illegal content onto their devices.
6. 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.
7. 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. 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. Devices must be encrypted in line with City security standards.
10. Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care 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 immediately.

11. The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
12. 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. 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.

**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.*

3.3 Actions which may result in a full or partial wipe of the device, or other interaction by IT

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.

3.4 Use of particular applications which have access to City data

1. Only devices that have the City MBM 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.

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 262-524-3567) (HR department 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