City of Milwaukee

Mobile Device Management Standard

NIST Reference:	Implementation Date:	Revision Number:
AC – Account Access AT – Account Training and Awareness	June 6, 2018	1.0

WEBSITE LINKING

PURPOSE

Mobile devices are commonly being used in almost all departments to increase performance in the field and extend communications beyond the office. The City is committed to provide and promote this technology as appropriate to add value to the community by delivering high quality services at the lowest possible cost.

SCOPE

This Policy establishes the rules and conditions for City-supplied cell phones and privately-owned mobile devices being used to conduct City business. Mobile devices are defined as any electronic device with the ability to transmit or receive data, text, and/or voice, via a cellular network. This includes but is not limited to smartphones, cellular equipped tablets, laptops, and mobile hot spots.

All City employees and contractors issued and accepting City mobile devices and services from the Information and Technology Management Division will be expected to maintain compliance with this policy. Public Safety (MPD & MFD) and the following elected officials' departments (City Clerk/Common Council, City Treasurer, City Comptroller and City Attorney) maintain their own vendor contracts and are therefore excluded from this policy. However, these department should review and consider including in their departmental work rules items #1-6 below or other pertinent items under 'General Policy'.

GENERAL POLICY

1. Employees may use a City device for incidental personal use, however a City mobile device is intended for business use. Employees should be cautious about the merging of personal and work activities on their devices. See other policies that may apply such as Email Use Policy and the City of Milwaukee Internet Use guidelines.

2. If an employee elects to use his or her personal device for City business they should be aware that they could be required to share their usage in an open records request or in the event of litigation. The City does not offer per-call reimbursement or provide stipends for personal monthly cellular service or data usage.

3. Mobile devices that access email and other City services must be secured using a passwords or pin. Devices may not be "rooted" or "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

4. Employees must not load pirated software or illegal content onto their devices. If you are unsure about any specific application, contact ITMD.

NIST Reference:	Implementation Date:	Revision Number:
AC – Account Access AT – Account Training and Awareness	June 6, 2018	1.0

5. Any non-City of Milwaukee e-mail, instant messaging, social media, or other accounts must not be used to conduct City-related business. If an official record is received or generated using text-messaging or any other third-party service, the employee must save the record to City systems that are routinely backed up and archived to comply with open records laws.

6. In situations where job responsibilities include regular driving and acceptance of business calls, hands-free equipment may be provided to facilitate the provisions of this policy. Under no circumstances are employees required to place themselves at risk or break the law to fulfill business needs. Employees who are charged with traffic violations resulting from the use of their phone while driving will be responsible for all financial liabilities and associated penalties that result from such actions.

7. Department or division telecommunications coordinators will recommend who qualifies for a City issued cellular device based on department needs.

8. With proper authorization, a City employee may be issued multiple mobile devices with enabled cellular service. Employees needing to connect multiple devices to either the Internet or a cellular service provider should work with ITMD for alternative solutions and technologies. Such technologies may include smart phone tethering or a temporarily assigned Mi-Fi access point.

9. All City device service usage records produced by assigned mobile devices are property of the City and managed by the City. Usage summary reports (i.e. number of minutes or GB of data used) are distributed to department telecommunications coordinators regularly and are periodically reviewed by ITMD. Detailed usage reports, including call history, are available to any supervisor upon request by contacting ITMD.

10. Mobile device management software is used to enforce mobile device security requirements for ITMD-issued mobile devices and personal devices that access City resources. This software may include the ability to require passwords, limit installation of software, push security updates, locate the device, and remotely wipe (erase all data and reset to factory defaults) mobile devices. A wipe removes everything on the device. The City of Milwaukee is not responsible for any personal data on the device lost in this process.

11. Employees in possession of ITMD-issued mobile devices are expected to secure the equipment from loss or damage. If the cellular device is lost or damaged, the employee should report this to ITMD. ITMD will remotely reset the cell phone to factory defaults (remote wipe the device) and the device will be replaced with a device that can perform similar City business as the original device. There is no guarantee that such a replacement device will be the same make or model device that was lost or damaged. Under circumstances where it is determined that the employee is responsible for damage to, or misuse of, their issued mobile device, disciplinary action may be taken. Free software downloads needed to access information on the City of Milwaukee web site

12. Purchase of and billing for mobile devices and services will be coordinated by ITMD with the department or division telecommunications manager. Purchases without the knowledge and involvement of ITMD is not allowed for ITMD-supported departments.

City of Milwaukee

Mobile Device Management Standard

NIST Reference:	Implementation Date:	Revision Number:
AC – Account Access AT – Account Training and Awareness	June 6, 2018	1.0

COMPLIANCE

ITMD or the Department Telecommunications Coordinator will notify the Employee if there is a compliance concern, so the Employee may rectify any inadvertent breaches of policy expeditiously. Any continued or serious compliance concerns will be immediately referred to the Employee supervisor for potential disciplinary action.

City records are prohibited from being permanently stored on a mobile device. Only copies of documents may be stored on a mobile device for extended periods. City records (including documents, photos, videos, or any other City record) created on a mobile device are to be transferred by the user as soon as practical to City systems that are routinely backed up and archived.

City-issued mobile devices are City owned property. If the device is no longer needed for City business, it is to be returned to ITMD. Mobile devices deemed excess property are re-sold through the City's established excess property disposal procedures and methods. Departments or Divisions may not sell, trade-in, or give-away new or used City cellular or communication devices.

Upon resignation or termination of employment, employees are expected to promptly return the mobile device. Employees who separate from employment without returning City equipment or who incur charges after separation may be subject to legal action for recovery of the loss.

Individual departments may have additional restrictions, based on specific needs or policies of the department.

REMOVAL OF PROHIBITED FOREIGN PRODUCTS

Using information gathered through state, federal, and industry-led intelligence, certain vendors and products currently present an unacceptable level of cybersecurity risk to the City including products and applications where the City has a reasonable belief that the manufacturer or vendor may participate in activities such as but not limited to:

- Collecting sensitive citizen, financial, proprietary, intellectual property, or other business data.
- Enabling email compromise and acting as a vector for ransomware deployment.
- Conducting cyber-espionage against government entities.
- Conducting surveillance and tracking of individual users; and
- Using algorithmic modifications to conduct disinformation or misinformation campaigns.

In alignment with the State of Wisconsin Standard 290 – Removal of Prohibited Foreign Products, the following vendors and/or software are prohibited from being used in or connected to any City network or installed on any City-issued device, including but not limited to desktop computers, laptops, tablets, cellular phones and other mobile devices.

NIST Reference:	Implementation Date:	Revision Number:
AC – Account Access AT – Account Training and Awareness	June 6, 2018	1.0

- TikTok
- Huawei Technologies
- ZTE Corp
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dashua Technology Company
- Tencent Holdings, including but not limited to:
- Tencent QQ
- QQ Wallet
- WeChat
- Alibaba products, including but not limited to:
    - AliPay
- Kaspersky Lab

This list will be updated corresponding to applications and vendors identified by the State and Federal government based on risk to the City of Milwaukee information systems.

ENFORCEMENT

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REVISION HISTORY

Revision	Date	Changes
0.0	June 6, 2018	Initial Release
0.1	July 8, 2019	Format Revision.
1.0	March 2023	Addition of Prohibited Foreign Products