Boston Water and Sewer Commission

WIRELESS MOBILE DEVICE POLICY AND AGREEMENT

Contents

I. Policy Statement

The purpose of this Policy is to define accepted practices and responsibilities for use of Boston Water and Sewer Commission's ("Commission") mobile devices issued to employees and contractors. This Policy defines employee eligibility and commitment requirements. Additionally, it provides guidance for the secure use of a mobile device.

The objective of the Commission's Wireless Mobile Device Policy is to establish the requirements when using mobile devices owned and/or managed by the Commission and to protect and maintain employee safety, security, and privacy while protecting Commission information and assets. Employees and contractors shall use Commission mobile devices primarily for the Commission's business.

II. Penalties

The inappropriate use or neglect of mobile devices may result in discipline up to and including termination. In addition, a violation of this Policy may result in criminal penalties when appropriate.

III. Scope

This Policy applies to all employees and contractors who have access to Commission devices.

IV. Responsibilities

A. Employee's Responsibility

Employees must ensure that they comply with all sections of this Policy and adhere to the Mobile Device Agreement. See Appendix A. Employees must sign the agreement and take shared responsibility for the security of their Commission-owned mobile devices. When employees receive a mobile device, the employee assumes responsibilities for its physical security and the information contained within.

The Commission shall issue mobile devices for business purposes, and those devices remain the property of the Commission.

The Commission does not authorize employees to purchase services or applications for their mobile devices.

The Commission reserves the right to reclaim Commission-owned mobile devices at any time. Employees will be responsible for the return of all equipment upon a request from the IT Department. In the case of a disciplinary hearing before the Executive Director or his designee, employees should return Commission equipment prior to that hearing.

1. Security Criteria for Mobile Devices

All mobile devices connecting to the network or accessing Commission information must meet the following security criteria:

- All Commission employees must select strong passwords and change passwords regularly.

- Employees may not share passwords to their mobile device.
- The IT Department configures mobile devices with an appropriate password or pin. The length and complexity will vary by device.
- The IT Department will configure mobile devices to lock automatically after a predefined period of inactivity, when applicable.
- Mobile devices must be running Commission-approved antivirus software and firewalls, when applicable.

2. Cost Control

Employees should support efforts to manage device operation costs by ensuring that call minutes, text messages and data usage do not exceed usage plan limits.

When employees are traveling, employees should:

- Exercise caution to avoid incurring excessive charges and roaming fees when using the mobile device.
- Connect to mobile data networks only when essential.
- Use reasonable care when choosing Wi-Fi hot spots.
- Prior to traveling abroad on Commission business, contact the IT Department regarding accessibility issues.

3. Care/Loss/Theft

Employees must follow the manufacturer's guides regarding the care of their mobile devices. See http://help.apple.com/iphone/8/#/iphbbe12ba1 and http://help.apple.com/ipad/8/#/iPadab498ed1.

If the device is lost, stolen, or compromised, the employee must notify the Help Desk immediately at (617) 989-7555. This notification must take place prior to any cancelation of the mobile services associated with the device. The Commission's IT Department reserves the right, at its discretion, to delete remotely ("wipe") all data contained in the device.

4. Application and Downloads

Employees must take all reasonable steps to protect against the installation of unlicensed or malicious applications. Employees must abide by all provisions of the Digital Millennium Copyright Act. Employees should understand that unmanaged or unapproved installations compromise the operating environment and constitute a security risk, including the intentional or unintentional spreading of malware.

Employees may only connect Commission-issued mobile devices with Commission-owned IT resources. Employees should never connect Commission-owned mobile devices to personally

owned or other third-party devices unless job duties require such a connection with either a contractor or government entity.

5. Security and Privacy Obligations for Business Data

Employees should recognize the Commission may monitor the use of or access to data provided at any time. Employees should presume that the Commission might also monitor personal data downloaded on a Commission-owned device. Employees should not expect to have any personal privacy while using IT resources.

The Commission will only use location information that may be obtained as part of the normal management of the device for locating the device if lost or stolen with the express permission of the employee, or to assist an employee in distress or an employee who is believed to be in distress. The Executive Director may authorize the review of location data for any other business use.

6. System Security

Employees must comply with security requirements when equipment is at the employee's workstation and when traveling. Employees must take the following physical security preventative measures defined in this Policy to protect the Commission's data and systems:

- All employees shall abide by the Commission's standard information security directives for the device at all times.
- Employees must comply within 24 hours with directives from IT Department to update or upgrade system software, and must otherwise act to ensure the security and system functionality.
- Employees must not leave mobile devices in plain view in an unattended vehicle or other vulnerable position, even for a short period.
- Employees must not leave mobile devices in a vehicle overnight.
- When leaving a mobile device unattended for any extended period (e.g., on lunch breaks or overnight) employees must physically secure it.
- Employees should carry mobile devices as hand luggage when traveling and never check the mobile device as luggage to be stored anywhere, thus prohibiting immediate access or visual contact with the device.

B. IT Responsibilities

The IT Department's responsibilities include:

- Publishing IT standards that document the type of approved use/connection to the Commission's IT resources, including specific requirements governing the equipment's configuration/control and connection/operational changes.
- Making employees aware of any changes to technologies that will affect daily use.
- Ensuring that optimized applications are available for devices.
- Handling operating management functions that control Commission information assets on devices.

The Commission's IT Department must provide all software on the device. The employee's department will distribute standard applications, or the Commission will approve the software, which the IT Department will then install.

V. Related Federal and Massachusetts Laws

The following is not a comprehensive list of laws that affect mobile device usage. Employees should direct their questions to the IT Department regarding this Policy and their device.

United States Code Chapter 17 Section 106 gives the owner of a copyright in any medium the exclusive right to reproduce the material. Do not use Commission mobile devices to reproduce protected work.

Massachusetts General Law Chapter 56 Section 25 makes it illegal to allow others to see a ballot marked at a polling center. Do not use Commission mobile devices to memorialize a completed or partially completed ballot.

Massachusetts General Law Chapter 90 Section 13 makes it illegal to distract a driver with a mobile device.

Massachusetts General Law Chapter 272 Section 99 makes it a criminal offense to audibly record someone without his or her consent.

VI. EFFECTIVE DATE OF POLICY

The Commission approved this Policy as of November 20, 2015.

This Policy shall remain in effect until amended or rescinded by a vote of Board of Commissioners.

APPENDIX A

MOBILE DEVICE AGREEMENT

I, _____, agree to the following terms and conditions in connection with the use of a mobile device issued to me by the Boston Water and Sewer Commission, regardless of whether I connected the device to the Commission's network:

Scope

This agreement applies to employees and contractors who use Commission-issued devices.

Agreement

The employee or contractor noted on this form acknowledges and understands the following:

1. The Commission retains complete ownership and control over any mobile device that it issues to employees or contractors. The Commission may and will exercise the right to inspect/ or reclaim any Commission-owned mobile device that is or has been connected to IT Resources, any data contained therein, and any data sent or received by the device in pursuit of legitimate needs for supervision, control, security, and assistance with criminal investigations.

2. Authorized employees and contractors may access programs and applications from Commission mobile devices. The Commission is not responsible for materials viewed, sent, downloaded or received to or by employees, contractors or third parties.

3. No employee or contractor shall have any expectation of privacy in any message, file, image, or data created, saved, viewed, sent, retrieved, or received using the Commission's mobile devices. The Commission reserves the right to monitor or inspect the Commission's mobile devices at any time without notice or warning.

4. The employee or contractor consents to allow the Commission to monitor and/or inspect their issued mobile device while using Commission IT Resources (including without limitation the network and systems). This consent covers any data that he or she creates or receives, any messages they send or receive, and any web sites that they access, insofar as such data, messages, or access relate to the work with respect to the Commission or the security of Commission's IT Resources.

5. Employees and contractors may only use the mobile device that the Commission issued to them. Employees or contractors are not permitted to share devices, even those to whom the Commission issued the same or substantially similar mobile devices. Users may not share mobile devices or passwords associated with either the Commission-issued mobile device or the Commission's IT Resources. Any damage to the Commission's device will be the responsibility of the authorized employee or contractor who must report any damage immediately to their supervisor. After consultation with the IT Department, the damage may lead to the user reimbursing for the device's repair or replacement and/or disciplinary action as determined by the user's supervisor.

6. Subject to any changes to state or federal law regarding mobile device use, employees and contractors may not actively dial Commission mobile devices while operating Commission vehicles or their personal vehicles on Commission business. By signing this agreement, the user acknowledges that he or she will not actively dial Commission mobile devices and operate Commission vehicles or heavy

equipment at the same time. Employees and contractors agree that they will always use the mobile devices in a safe and reasonable manner and in conjunction with Massachusetts laws and regulations. Employees and contractors also agree not to use Commission hardware to distract another employee or contractors while operating the Commission's vehicles or heavy equipment. Breach of this agreement may lead to revocation of mobile device privileges and possible disciplinary action.

Employees and contractors may not tamper with or alter any security controls configured for a Commission-owned mobile device including but not limited to:

a. Authentication (Logon)

b. Authorization

c. Cryptographic techniques

d. Back-ups

e. Malware protection

f. Mobile device management

g. Network configuration

7. Highly sensitive Commission data can only be stored on Commission-owned mobile devices connected to the Commission's network as long as the data is secured and explicitly allowed on the mobile device by the employee's or contractor's supervisor.

8. Users must report a lost or stolen Commission-owned mobile device immediately upon realization that the device is missing, by contacting the Helpdesk at (617) 989-7555. **If a user loses such a device, or it is stolen, the Commission IT Department reserves the right, at its discretion, to remotely delete ("wipe") all data contained in the device, in order to secure Commission data and information technology resources.**

User Signature & Date	CIO Approval (or designee) & Date
Printed Name & Title	Printed Name & Title

BWSC Minimum Password Complexity Requirements

- Cannot contain significant portions of your employee account name or full name
- Must be at least eight characters in length
- Must contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Employees must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, employees must not employ passwords like “X34JAN” in January and “X34FEB” in February.

Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in data communications software, in web browsers, on hard drives, or in other locations where unauthorized persons might discover them.

Employees must not write down their passwords and leave them in a place where unauthorized persons might discover them. Aside from initial password assignment and password-reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized employee, the password must be changed immediately.

Passwords must never be shared or revealed to anyone else besides the authorized employee. If employees need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms. This policy does not prevent the use of default passwords, typically used for new employee ID assignment or password reset situations, which are then immediately changed when the employee next logs onto the involved system.