CITY OF NORWALK TECHNOLOGY DEPARTMENT

POLICY: MOBILE DEVICE SECURITY AND BRING YOUR OWN DEVICE POLICY

EFFECTIVE DATE: 10/1/2018

With advances in computer technology, mobile computing and storage devices have become useful tools to meet the business needs of the City of Norwalk. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere.

Bring-Your-Own-Device or BYOD refers to the policy of permitting users (this includes: employees, elected officials, appointed officials, volunteers who serve on agencies, boards and commissions) to bring personally owned mobile devices (smart phones, etc.) to their workplace, and to use those devices to access privileged City information and applications.

The City of Norwalk seeks to protect its mobile devices and the data stored on such devices, from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal. City mobile devices are the property of the City of Norwalk and must be appropriately secured to prevent sensitive and confidential data from being lost or compromised, or from posing any other potential threat to the City’s infrastructure.

I. Terms

This Mobile Device Security Policy and procedures apply to all users who may access City information or information systems.

A. Devices & Terminology Defined:

1. **Mobile Device** includes portable devices that allow for non-fixed using within the City’s facilities, including: Laptop/Notebook computers, Tablet PCs, iPhones, iPads, Smartphones, and any portable devices or removable media, such as thumb/flash drives, that contain a hard drive or high-capacity storage.

2. **City-Owned Mobile Devices** are those mobile devices purchased by the City of Norwalk and configured and distributed to approved users by the Department of Information Technology for the purpose of conducting City business.

3. **Personal Mobile Devices** are those devices independently purchased and owned by City users but approved for use in accessing City email and/or other authorized information assets.

4. **Remote Data Wipe** is a procedure initiated and executed by the Information Technology Department on all lost or stolen City-owned or personally-owned mobile devices to ensure the security and confidentiality of Norwalk data. The remote wipe process may delete all data on the phone/device, whether it is City data or personal data.
II. Responsibilities

Users of the City who have been authorized to use a mobile device for City business are responsible for safeguarding any City-issued mobile device and the data contained therein as defined in this policy.

- The Information Technology Department will determine which mobile device types can be used for City business, configuring City-owned devices and initiating a remote data wipe as defined in this policy.

- All authorized users of mobile devices are required to read and comply with the requirements and guidelines outlined in this Mobile Device Security Policy.

- All authorized users of mobile devices are required to immediately report the loss or theft of a mobile device that contains City information to the Information Technology Department.

- All mobile devices must be configured and managed according to the safeguards outlined in this policy.

- Anyone observing what appears to be a breach of security, violation of this policy, violation of state or federal law, theft, damage, or any action that might place City resources at risk must immediately report the incident to the Information Technology Department.

III. Requirements

The following safeguards apply to all mobile devices with access to City information.

1. All users of mobile devices must be authorized and approved by the Information Technology Department.

2. All authorized personal mobile device users shall sign a form acknowledging his/her responsibility for notifying the Information Technology Department and granting the City the right to remotely wipe the device in case it is lost, stolen or the end user’s employment is terminated.

   In the case of remote wipe, personal data including photos, videos, applications, or anything else stored on the device may also be wiped. For this reason, it is imperative that users ensure they are backing up their personal phones, tablets, and devices on a regular basis. The Information Technology Department is not responsible for the backing up or protection of a user’s personal data.

3. City of Norwalk cellular phones may not be used in any manner that may be construed to violate any law, statute, rule, regulation or code, nor may it be used to violate any City of Norwalk policy, including, the Harassment Free Workplace Policy. City of Norwalk cellular phones also may not be used to harm or damage any other property or person.

4. Personal mobile device users shall only connect to City email, under the directions of (and after approval by) the Information Technology Department.

5. All mobile devices must be configured to use whole disk encryption and use encrypted file storage containers as necessary to secure City data.
6. All mobile devices must be protected by a password or PIN with a minimum length of 4 characters. Specialized mobile software is installed on all City-owned devices which will enforce a passcode.

7. Mobile devices shall be kept with the user whenever possible. Whenever a device is stored, it shall be stored in a secure place, preferably out-of-sight.

8. In the event the mobile device is lost or stolen, the user must immediately report the incident to the Information Technology Department. The Information Technology Department will initiate a remote data wipe.

9. For City-owned devices, any options, software and applications that are not required as part of the job function or business need should be disabled or removed.

10. All mobile devices should have screen locking and screen timeout functions enabled whenever possible.

11. If the mobile device is used for transitional storage (for example copying data between systems), the data shall be removed from the mobile device immediately upon completion.

12. Laptop locks and cables should be used to secure laptops when in the City buildings or other fixed locations whenever possible.

13. An industry standard data destruction tool must be used when destroying or disposing of mobile device storage or removable media that may have contained City sensitive data.

14. Multifactor authentication may be required for certain administrative or privileged users.

15. Only City Information Technology Department-approved Mobile storage and USB storage devices are allowed. Under no circumstances are personal devices to be used.

16. Creating shares to or from the mobile devices or allowing access to the mobile device from another non-City device is prohibited.

17. Installation of software on a City-issued mobile device is prohibited. Only Information Technology staff with proper approval is permitted to install approved business software.

18. Connecting personal non-authorized hardware is prohibited unless otherwise authorized by the Information Technology Department.

19. Industry standard encryption will be deployed for data transport communications on mobile devices.

20. When your employment with the City of Norwalk is terminated, you must return your City-issued technologies and equipment and all accessories in good working condition to your Department Head or the Information Technology Department before your last day of employment. If you do not return the equipment and accessories prior to your departure or you return them in less than good working condition, you will be responsible for the cost of replacement or repair of equipment.

IV. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
V. Document Distribution & History

This document is the property of the City of Norwalk and is distributed to all users, contractors, and vendors with network access privileges for reference. Questions regarding this Mobile Device document can be directed to the Norwalk Information Technology Department at (203) 854-7714.

Approvals:

ITT Committee: June 6, 2018

Director, Information Technology

Director, Personnel and Labor Relations

Corporation Counsel

Mayor Harry W. Rilling
Mobile Device Security / Remote Wipe
Acknowledgement and Waiver

WHEREAS:

- The City has established a Mobile Device Security Policy to ensure the security and confidentiality of City data that may be contained on a City-owned or personal mobile device. I have read and understand the requirements.

- I wish to access City email and information assets on my personal mobile device. I will notify the City Information Technology Department immediately in the event that my personal device is lost or stolen, or my employment is terminated. I understand that the Information Technology Department will then initiate a remote data wipe of my mobile device, which may delete all City and personal data contained on the device. I understand that the backup and recovery of personal data is solely my responsibility. I authorize the City to initiate the remote wipe and accept responsibility for any loss of personal data.

My signature below indicates I have read and understand the requirements of the Mobile Device Security and Bring Your Own Device Policy, including my responsibilities for immediately notifying the Information Technology Department. I understand that failure to follow the requirements may result in disciplinary action, up to and including termination of employment.

User Signature ____________________________________________

Date: ________________