PHDC

MAKING PHILADELPHIA BETTER, BLOCK BY BLOCK

# MEMORANDUM

TO: PHDC EMPLOYEES
FROM: DAVID S. THOMAS, PRESIDENT AND CEO
SUBJECT: PHDC MOBILE DEVICE POLICY
DATE: SEPTEMBER 15, 2022

## MOBILE DEVICE POLICY

### INTRODUCTION

Mobile devices such as tablet computers are important tools for PHDC, and their use is supported to achieve business goals. However mobile devices also represent a risk to information security and data security in that if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organizations and city's data and IT infrastructure.
This document outlines a set of practices and requirements for the safe and appropriate use of mobile devices owned and/or provided by PHDC ("devices") which are used to or have access to PHDC or city networks, data, and systems.

### POLICY

#### DEVICE SECURITY

- Devices shall have a PHDC or City of Philadelphia property tag which shall not be removed as long as the device remains in the PHDC or City of Philadelphia inventory.
- End user is to responsibly care for all Devices in his or her possession.
    - Unless explicit approval is given by the Deputy Director or his designee to retain Devices overnight, Devices shall be turned in at the end of each workday to the designated administrator for overnight storage and charging
    - Devices shall not be left unattended but shall be either in the possession of the end user or shall be locked and secure, whether in the field or in the office.
- If the Device is lost or stolen, the end user shall notify his or her supervisor and Director immediately. If the Director is not available, the loss or theft shall be reported to the Deputy Director.

- Devices will have location services enabled to (a) locate misplaced or lost Devices and enable remote wiping if the Device is lost or stolen. End user shall not disable location services settings or software at any time.

**DATA SECURITY**

- A passcode (PIN) to gain access into the Device is required and shall be set by PHDC. This helps prevent unauthorized individuals from gaining access to the Device. End user shall not disable or change PIN.
- An idle timeout lock is required to ensure that the Device will automatically prompt for the PIN when left idle or unattended. The idle lockout time is set for 15 minutes and shall not be changed or disabled by the end user.
- If an end user suspects that unauthorized access to PHDC's network or data may have occurred via their Device, the end user shall report the incident immediately to the Administrator. If the Administrator is not available, the incident shall be reported to the Deputy Director.
- Software to access PHDC networks or data shall not be installed on personal devices without express permission of the Deputy Director.

**DEVICE INTEGRITY**

- Devices shall be maintained in base configuration.
- End users shall not download any of the following without prior approval:
    - Music
    - Videos
    - Applications (free or paid)
    - Executable files of any type
- End users shall not download any of the following at any time:
    - Pirated software
    - Illegal content
    - Content which is prohibited under any other PHDC or City of Philadelphia OIT policy
- Devices shall not be connected to end users personal (non-PHDC) computers at any time.
- Devices shall not be "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the end user.
- Each end user will be provided with a Device, hard case, soft case and car charger. The Device shall remain inside the hard case at all times and inside the soft case when not in use.

**EMAIL ACCOUNTS**

- Email accounts on the Devices are separate from your phila.gov email accounts. They shall be used only for the following purposes:
    - Updating HIP software

    - Communicating with other PHDC staff when telephone service is not available
- Because these emails accounts do not follow the same archive and retrieval standards as phila.gov accounts, they shall not be used to communicate with anyone outside of PHDC or for non-PHDC business.
- Use of these email accounts shall be subject to the existing PHDC and City of Philadelphia email policy.  This policy can be found in Lotus Notes at any time.
- End users shall not change passwords on mobile device email accounts.

**INTERNET USAGE**

- Internet usage on the Devices shall be subject to existing PHDC and City of Philadelphia policies.

**HIP MOBILE APPLICATION USAGE**

- End user shall log on and “Check In” at the beginning of each workday.
- End user shall remain logged in until the end of the workday.
- End user shall “check out” at the end of the workday.
- Because forms completed and photographs taken using other methods do not become part of the PHDC electronic record, inspections, forms and photographs shall be completed using the HIP Mobile Application only, except with permission from your Director or Deputy Director.

**DEVICE USAGE**

- Devices shall only be used by the corresponding authorized end users
- Devices shall not be used while the end user is operating a motor vehicle
- Devices shall be secured while the end user is traveling in a motor vehicle so that it will not fly about in the event of an accident and potentially result in injury to occupants
        - Any PHDC employee issued a mobile device is accountable for maintaining the device in a safe, secure, and responsible manner at all times while the device is assigned to the employee.