TITLE: Mobile Device Policy & Acknowledgement	POLICY NO. 34
EFFECTIVE: Immediately	REVISED:

(For employees in positions eligible for a mobile device)

Employee: _____

Position: _____

The City of Hilliard understands that a mobile device can be a vital component of effective operations and at times are needed by employees in the course of their work. To that end, if a substantial business reason exists for a position to use a mobile device, a Department Director, in conjunction with the Human Resources Director, shall determine which positions are eligible for reimbursement within the applicable Department. The City will provide an employee in an approved position with a stipend for a mobile device as described below.

All *mobile devices* that connect to the *City network* must comply with this policy, regardless of whether they are personal (*BYOD)* or City-issued devices. The purpose of this policy is to provide criteria for mobile device access to the City network in a manner that protects the confidentiality, availability, and integrity of City *information assets.* This policy describes acceptable methods for a mobile device to connect to the City network. It is irrelevant of the individual technology or protocol used to make the connection, this policy provides guidelines that cover all mobile devices and methods of connection. Policy scope is limited to consumer-grade computing and communication devices (smartphones, tablets, etc.) that run a mobile operating system.

This policy applies to all mobile devices. Registration with IT is required for any personal (BYOD) or City-owned mobile device that connects to the City network. Registration is per user/per device.

- **Definitions**
  1. **BYOD**: Bring Your Own Device, permitting employees to use personally owned mobile devices in the workplace and to use those devices to access resources (calendar, e-mail, file services, applications, etc.) in the City network.
  2. **Corporate Container**: The compartment of a mobile device designated specifically for work purposes. For City-owned mobile devices, this is the entire device. For personal (BYOD) mobile devices, this is a separate container setup on the device for work use, distinct from the container for personal use. In other words, it is a separately segregated digital space.
  3. **Information Assets**: Business applications, system software, development tools, utilities, etc.
  4. **Mobile Device Management (MDM)**: is the software that provides the following functions: software distribution, policy management, inventory management, security management, and service management for devices running a mobile operating system.
  5. **Mobile Devices:** Computing and/or communication devices, running a mobile operating system (such as Google Android, Apple iOS, Microsoft Windows Phone, BlackBerry OS, etc.), as opposed to desktop-class operating system (such as Windows, Mac OS, Ubuntu, etc.).
  6. **Personal Identifiable Information (PII):** Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

7. **City network**: The City of Hilliard Wide Area Network, City of Hilliard Demilitarized Zone (DMZ) networks, and any other secure network managed by the City of Hilliard.

Please note the following:

- If an employee is issued a City-owned phone/mobile device, they are not eligible for reimbursement.
- All reimbursements are subject to review from the City IT Department and the Director of Human Resources.
- The City will not reimburse an employee for the following charges: roaming, plan overages, etc.

Several acknowledgments are required to accept a mobile device stipend for mobile device use:

- A substantial business reason exists for your position to warrant use of a mobile device for business purposes.
- Public records laws apply to the use of mobile devices and your phone records, texts, data, etc. may be considered public records. Retention of public records on your mobile device shall comply with the City's Record Retention Policies.
- Users must protect the mobile device from theft, damage, abuse and unauthorized use.
- If a separate *corporate container* is setup for any personal (BYOD) mobile device, any access to the City network must take place only through the corporate container. All City data must remain in the corporate container. If no corporate container is setup on a personal (BYOD) device, then City data cannot be stored on the personal device.
- Users must ensure that they remain the only user of the corporate container of any mobile device that they use to connect to the City network.
- All users should attest that you have read and accept the terms and conditions of this policy.
- A user must ensure no modifications occur to either the mobile device or its operating system that could potentially violate or void the manufacturer's warranty or alter the manufacturer's standard security configuration. This includes, but is not limited to "jail breaking" an iOS device or "rooting" an Android device.
- Immediately notify IT Customer Support at **614-334-2549** of any lost, misplaced, or stolen mobile device with City network access.
- (For non-police officer employees): You are prohibited from using a mobile device, unless hands-free, while driving a City vehicle or a personal vehicle while conducting City business. As an employee, you must safely pull over to the side of the road if using a mobile device unless you are able to safely use the phone in a hands-free manner. Non-hands free texting while driving a City of Hilliard or personal vehicle on City of Hilliard business is strictly prohibited.
- (For police officers): Pursuant to ORC § 4511.204, if you are operating an emergency vehicle, you may only use a mobile device if you are involved in an urgent situation and should, where practicable, stop the vehicle at an appropriate location to use the mobile device. Except in an emergency, if you are operating a non-emergency vehicle you shall not use a mobile device unless it is specifically designed and configured to allow hands-free use. Hands-free use should be restricted to business-related calls or calls of an urgent nature. Non hands free texting while driving is strictly prohibited.
- Mobile device operating systems supported include currently supported versions (by the original equipment manufacturer) of Google Android, Apple iOS, Windows Phone, and Blackberry
- Mobile devices (regardless if City-owned or personal) must have passwords or six (6) digit PINs. For personal BYOD mobile devices, the password for the corporate container must be at least eight characters in length, with at least one uppercase alpha, one lowercase alpha, and one numeric character. A non-

expiring password is acceptable. The pure phone feature will always remain unlocked. For personal BYOD mobile devices, a six (6) digit PIN is required (a fingerprint is also an acceptable password).

- Mobile devices must lock after a maximum of 15 minutes of inactivity. Password is required to unlock.
- After ten (10) consecutive unsuccessful login attempts, the mobile device will automatically be locked. For personal (BYOD) mobile devices, automatic locking is of the corporate container only, not the entire device.
- Mobile devices reported as lost, misplaced, or stolen must be wiped (formatted). For personal (BYOD) mobile devices, automatic wiping is of the corporate container only, not the entire device.
- When City network access is via a personal (BYOD) mobile device, the Directors of Human Resources and IT may initiate a forensic audit on the corporate container of such devices. It is not IT's intent to conduct forensic investigation on the personal container. Additionally, while connected to the City network, applications not relevant to City business may be quarantined so they cannot operate.
- Should the mobile device store, even temporarily, *PII* or any other high-risk data, the device must be encrypted to the AES-256 strength.
- For the purpose of access audit to City IT assets, the corporate container of each device must have one, and only one, designated user. All mobile device holders must acknowledge that they do not share the corporate container of their device with any other person (including family members) as a condition of using the device to access City resources
- IT does not maintain mobile devices. IT's troubleshooting assistance can only be on a best-effort basis. Users will have to coordinate assistance from IT and the wireless carrier, if applicable. The only IT deliverable is access to the City network.
- Should statutory restrictions forbid stakeholders from accessing specific City information assets from non-City devices, then this policy does not change that.
- Except as identified in collective bargaining agreements, the City is held harmless for any damage resulting from a personal mobile device being used for City business, having MDM software installed, and/or accessing the City network.
- Failure to comply with any of the above provisos may lead to termination of access to the City network, in addition to discipline up to and including termination.

The City of Hilliard Information Technology Department will:

- Register and manage City-owned and personal (BYOD) mobile devices that connect to the City network.
- Assist users with mobile device configuration so that they can access the City network. IT's troubleshooting assistance can only be on a best-effort basis, since IT does not maintain mobile devices. Users will have to coordinate assistance from IT and the wireless carrier, if applicable.
- Utilize *MDM* software for all mobile devices connecting to the City network. This includes installing client *MDM* software to each mobile device.
- Wipe (format) or lock the mobile device in the event of a security issue. This includes, but is not limited to wiping City data and applications from the device, and locking devices exceeding the maximum number of consecutive unsuccessful device login attempts.

A City stipend is to be used to pay for the portion of business-related costs incurred on a personal mobile cellular.

Device Model: _____ Phone #: _____

Service Provider: _____

Policy Date: 7.23.2019

- I understand that I am responsible for paying all costs related to the device including monthly or other service charges.
- I agree to maintain an adequate level of service sufficient for necessary email access, call minutes, texting, calendar access, voicemail and any other service needs. Minimally, this includes:
  - Monthly data – 1 Gig or more, with at least 3G coverage
  - Phone, text – sufficient to allow incoming and outgoing phone calls and text messaging in expected work, travel, and home locations as relevant.
  - Service coverage – sufficient to provide adequate coverage for email, phone and text access in expected work, travel, and home locations as relevant.
- I agree to adhere to the City's administrative policies in the use of my mobile device as outlined in the Information Technology Use and Security Policies.
- I agree to keep the device secured and follow the passcode requirements of this document at all times.
- I agree to notify City IT staff immediately if the device is lost, stolen, or damaged to the level of inhibiting needed functionality.
- The City will reimburse an employee $25 or $40 per month toward the cost of the device plan.
  - ◯ $25/month shall reimburse voice and text requirements.
  - ◯ $40/month shall reimburse voice and data requirements.
- I understand and agree that false confirmation or failure to adhere to the above confirmations as determined solely by the City may result in disciplinary action taken by the City, pursuant to policy or the applicable collective bargaining agreement, up to and including termination from employment.

I understand that the City of Hilliard has the right to change this program at any time. All City employees will be provided updates to this policy if and when any changes are made.

Employee Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

Department Director Signature: _____ Date: _____

ADMIN/IT USE ONLY:

◯ Statement received (i.e. mobile phone bill) ◯ Stipend created in Payroll

◯ Adequacy of coverage confirmed

I certify the adequacy of the above and hereby approve the issuance and adequacy of the coverage for stipend purposes.

IT Signature: _____ Date: _____

HR Signature: _____ Date: _____