City of New Orleans
Chief Administrative Office

POLICY MEMORANDUM No. 60(R) **May 12, 2014**

TO: **All Departments, Boards, Agencies and Commissions**

FROM: **Andrew D. Kopplin, First Deputy Mayor/ Chief Administrative Officer**

SUBJECT: **Wireless Communications Device Policy**

I. Purpose

To retitle and reestablish the policy governing the use of approved wireless devices and rules of behavior associated with the use of City provided wireless devices and personally-owned wireless devices and to establish rules for the connection of these devices to the City of New Orleans' network. These rules are necessary to preserve the integrity, availability and confidentiality of the City's network.

II. Scope

This policy applies to all wireless devices (cell phones, smart phones, tablets, air cards, mobile hot spots, laptops, net books and any other wireless device) in use by City of New Orleans employees or those who connect through a wireless device to any City of New Orleans network.

III. Policy

A City employee is a candidate for a wireless device if the nature of his or her job requires that the employee have access to email, voice and web services while away from their office or in a mobile situation (e.g., the employee works "in the field"). The determination of whether the employee's job requires such mobile access is made by the director of the department for which the employee works. Primary use of the wireless device is for official City business.

As a general guideline, eligible employees include:

- Employees available for emergency contact (e.g., duties require them to be contacted anywhere/anytime).
- Employees on the road or in the field (e.g., typically out of the office on business 60 or more days annually) who are required to remain in touch with others.

IV. City-Provided Device Policy and Rules of Behavior

The following policy and guidelines inform City provided wireless device users of their allowable usage and features available for business and limited personal use. This document also serves to clarify the employee's responsibility to take proper care of the equipment provided to them by the City. Wireless device care is the responsibility of each employee entrusted with a City provided wireless device. Failure to adhere to the guidelines listed below may result in personal liability and/or retraction of device privileges. All employees who receive a wireless device must sign or electronically accept the attached City-Provided Wireless Communication Device User Acknowledgment and Agreement.

A. Overall Requirements:

The City of New Orleans expects employees using wireless devices to:

- Protect their City-issued device from theft, damage, abuse, and unauthorized use;
- Abide by all applicable laws of the state of Louisiana (or laws of local governments when traveling for City business) governing the use of wireless cell phones and/or smartphones while driving (e.g., hands-free use and/or texting); and
- Notify the City of New Orleans Service Desk (504-658-7800 or ServiceDesk@nola.gov) if the device is lost or stolen within one hour or as soon as practical after noticing the device is missing. The City of New Orleans Department of Information Technology & Innovation ("ITI") will lock and disable the device upon notification. ITI will also remotely wipe the device to protect the City's information. The employee will be responsible for any costs associated with replacing the device. In order for departments to determine the replacement value, the department should provide the service vendor with the required device information and request a written quote for the replacement cost. This replacement cost may then be deducted from the employee's pay using the appropriate transaction in the payroll system.

B. Privacy Expectations:

City employees do not have a right to, nor should they have an expectation of privacy while using City provided devices at any time, including while accessing the Internet, e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the City provided device for personal use. By acceptance of the City provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained on or passed-through that device.

C. Additional Guidelines:

While ITI will not have complete oversight and management of device usage and expenses, the Chief Administrative Officer authorizes ITI and the Department of Finance, Bureau of Purchasing access to each City department's wireless bills for the regular review of charges and approved devices.

- City employees are permitted limited use of IT equipment for personal needs if the use does not interfere with official business and imposes no additional expense upon the City. Since minutes on the City's voice plans may be limited, personal phone calls should be limited to occasional brief calls.
- Assistance or support is available through ITI's Service Desk by calling (504) 658-7800 or emailing servicedesk@nola.gov.
- The City reserves the right to recall/disconnect City provided wireless devices due to budget restrictions or changes to deployment priorities.
- If an employee's employment is terminated for any reason, the employee shall turn over the wireless device in good working condition to the City on the employee's last day worked. If the device is not received then the cost of the device will be deducted from the last paycheck and the device will be disconnected. If desired, the employee can transfer their number to their personal device (refer to CAO Policy 109).

- ITI will provide a list of approved wireless devices to City departments. Departments shall only purchase approved devices. All other devices will require special approval by the Chief Administrative Officer and the Department Director.
- The City of New Orleans will pay the monthly recurring cost subject to the City provided Device Policy and Rules of Behavior.
- ITI shall approve, test and certify for use and operation all applications allowed on City wireless devices. If a department requires an application on a wireless device which has not been certified by ITI, the department shall submit a request to the ITI Service Desk with an explanation for the use of the application to be certified and approved.
- City employees are not permitted to dial 411 or any other pay toll numbers on the City provided wireless device. Employees shall only use free toll free numbers. Fee based emergency services that enhance reliability of communications are exempt and may be activated on a per call basis at the direction of the department director or EOC leadership.
- City Employees are not permitted to download applications that are not approved by ITI. Upon departmental request, ITI will certify applications for use. Once certified, ITI will remotely install ("push") applications to wireless devices.
- All City wireless devices will be supported through mobile device management software providing the City the capability to manage configuration, applications and security, monitor City property and protect the City's information and infrastructure.
- If the employee loses or misplaces the City provided device or it is stolen, the employee must notify ITI immediately so your device can be remotely wiped, locked and/or disconnected from the City's network.
- The employee is responsible for the care and upkeep of the device on a daily basis to ensure that it stays in good working condition for the term of the device.
- The employee shall not loan or give the City provided device to any other person
- The employee shall not make international calls unless the employee is specifically required to for his or her job (approved on a case by case basis). If there are unapproved international dialing charges on the employee's City provided device, at the discretion of the department director, the employee shall reimburse the City within 30 days of notification by their department.

V. Bring Your Own Device Policy and Rules of Behavior

This document provides policies, standards, and rules of behavior for the use of smart phones and/or tablets personally owned by City employees to access the City's network resources. Access to and continued use of network services is granted on condition that each user reads, signs, respects, and follows the City's policies concerning the use of these devices and services. All employees who participate in the Bring Your Own Device program must sign or electronically accept the attached Bring Your Own Device User Acknowledgement and Agreement.

The Bring Your Own Device (BYOD) program permits personnel to use personally owned cell phones, smart phones and tablets for business purposes.

A. Overall Requirements:

- The employee understands that participation will require registration and installation of a mobile device management application which provides the City the capability to protect the City's information. The installation of the mobile device management software may result in data or text messaging charges. Depending on the applicable data plan, the use of the application may increase applicable rates. The employee is responsible for confirming any impact on rates as a result of the installation or use of this application and will not be reimbursed for any such costs.
- The employee shall not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual, the outcome of a charge/complaint/case, proprietary information, or agency financial operations. This excludes city email and apps that are protected through various security controls enabled by the installed mobile device management application;
- The employee will password protect the device;
- The employee agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not modify a device to enable or disable features ("Jail Break"), install alternative kernels or operating systems, install non-manufacturer or non-carrier provided modifications ("mods") or otherwise install software that allows the user to alter the device's original operation or bypass built-in or mobile device manager enabled security features and controls;
- The employee agrees that the device shall not be shared with other individuals or family members. Employees shall comply with CAO Policy No. 83, Standards of Behavior;
- The employee agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments or other regular use. ITI will provide instructions for identifying and removing these unintended file downloads.

B. Privacy Expectations:

The City will respect the employee's privacy as it relates to the employee's personal device and will only request access to the device to implement security controls. This differs from policy for City provided equipment/services, where City employees do not have the right to, nor should they have the expectation of privacy while using City equipment or services. While City access to the employee's personal device is restricted, the City's Policy and Rules of Behavior regarding the use and access of City email and other City systems and services remains in effect. If there are concerns related to compliance with the security requirements, the employee may opt to leave the BYOD program instead of providing the device to technicians for compliance verification. Leaving the BYOD program does not change an employee's obligation to respond to Law Department requests.

C. Additional Guidelines:

- The employee may use their personal device if it is on the City's list of approved devices. If the City employee does not have a City approved device and is approved to participate in the BYOD program, the employee can either contact ITI for information concerning any add-on applications

which may bring the non-approved device into compliance or purchase one of the approved devices from a wireless carrier via links on the City's wireless website. ITI can also provide information on monthly service discounts offered by wireless carriers.

- All devices will need to be registered in order for the City to protect access to City resources, enforce policy and properly secure information. Any attempt to circumvent ITI security or management will result in the device being de-enrolled from the mobile device management software. This will result in loss of access to City services through the device. The employee may contact ITI for information on how to re-enroll the device.
- If the employee leaves for any reason, any device management measures implemented by ITI or access to services through the device will be removed, including City emails, contacts, applications and calendar events. These services and any installed City applications will be remotely wiped from the device.
- The City is not responsible for any maintenance of the device being used in the BYOD program.

VI. Enforcement

Since improper use of wireless technology and wireless communications can open the City's network to additional sniffing and intrusion attacks, authorized and proper use of wireless technology is critical to the security of the City and all City employees. Employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

VII. Inquiries

Should you have any questions relative to this policy, please contact the Chief Administrative Office at (504) 658-8600. For further information, please refer to Policy No. 61 Internet Use & Access Authorization, Policy No. 83 Standards of Behavior and Policy No. 109 Regulations Pertaining to Assignment, Usage and Care, and Return of City Property by Employees.

ADK/ALS

Attachments