Enterprise Mobile Technology Policy

Policy No. D-02[1]

The Scope of this policy includes the following individuals:[2]

- ✓ Employees (including Appointed Officials, Probationary Employees, Full-Time At-Will Employees, Part-Time Employees, Temporary Employees, Civil Service Employees, Teamsters Employees, HPOA, HPSA, and IAFF Employees)
- ✓ Full-Time Elected Officials
- ✓ Volunteers

I. PURPOSE

To outline the City's rules regarding acquiring, administering, and using mobile technology.

II. POLICY APPLICATION

A. City-Owned Mobile Devices

Mobile devices, such as but not limited to, cell phones, laptops, tablets, smartphones, and mobile hotspot devices, may be issued to employees based upon substantial business needs, such as performing job tasks away from City facilities, emergency callouts and remaining in communication with other City staff. A mobile device will only be issued with approval of the department director or designee and upon signing a form acknowledging financial responsibility for the device if the device is damaged or lost as a result of the employee's negligent care or intentional misuse. Accessories such as cases, chargers and headphones may be purchased with City funds at the department director or designee's discretion.

---

[1] This policy is not to be construed as a contract or an implied contract concerning any employment-related decision or term or condition of employment. The City reserves the right to revise, delete or add to any and all policies, procedures, work rules or benefits stated in this policy at its sole discretion. See Introduction, Administrative Policy No. A-01.

[2] The relevant definitions for the individuals identified in the Scope of this policy are defined in Introduction, Administrative Policy No. A-01.

Each department will budget for and manage the capital and operating costs for mobile devices within their department. Each department is responsible for accurately maintaining an inventory of cellular devices and smartphones as well as regularly auditing bills for accuracy and cost management.

Departments will select a phone and/or data plan which provides the most economical and efficient option for the City based on need and anticipated usage. Departments will communicate the selected plan's allowable minutes, data usage, or text messaging limits to employees upon issuance of a mobile device. The City will not pay for any overages if an employee exceeds the allowable minutes, data usage or text messaging of the plan, unless it is clear that the overages occurred as a result of work related purposes. The departments have sole discretion in making this determination.

Departments should consult with the Department of Information Technology (DoIT) prior to changing to a different mobile technology carrier. The selected carrier must comply with the National Association of State Procurement (NASPO) pricing.

Employees are not allowed to upgrade their mobile devices without City approval. Upgrading of City-owned mobile devices will be at the City's sole discretion and will generally take place only if the mobile device is not functioning. Requests for upgrades must be made through and approved by the employee's supervisor and the DoIT.

For City-owned mobile devices, the City owns any corresponding telephone number. The City may access and monitor mobile device usage. Employees have no expectation of privacy when using City-owned mobile devices, as such, location services can be utilized as a means to locate an employee. Upon request, employees are required to provide IT with any password(s) associated with their City-owned mobile device. This may include, but not limited to: a) 6-digit Lock pin, b) AppleID/password OR Google Account/password, and/or c) City userID and password.

Employees are strongly discouraged from using text messaging as a means of communicating about official City business. Rather, text messages should be limited to transitory communications, versus substantive communications related to official City Business. Transitory records do not pertain to a City decision, policy, guideline, procedure, discuss a business matter, discuss a decision, certify a transaction, or act as evidence of receipt. Employees are strongly encouraged to use their City email or converse on the telephone for official City business and should only use text messaging as a last resort (i.e., in an emergency and when no other communication alternative is available) when communicating about a substantive matter. Employees should be aware that official City business generated on a mobile device may be subject to Nevada's public record laws.

Employees who are assigned a mobile device are responsible for caring for the device. Employees are required to produce the mobile device for inspection at any time at the

City's request. Employees will be responsible for the repair and replacement costs for damage caused by negligent care or intentional misuse. Employees must notify the DoIT and their immediate supervisor if a City-owned mobile device is lost or stolen. All City-owned mobile devices must be returned to the City immediately upon upgrade to a different device, or upon an employee's separation of employment. For devices to be factory reset and reissued at the City's discretion, employees are required to provide IT with any password(s) associated with their City-owned mobile device. This may include, but not limited to: a) 6-digit Lock pin, b) AppleID/password OR Google Account/password, and/or c) City userID and password. Employees who fail to return the City-owned mobile device upon termination or who leave their employment with the City with outstanding debts for equipment loss or unauthorized charges will be responsible for payment of such expenses and charges.

City-owned mobile devices are issued for business purposes. All personal business conducted on City-owned mobile devices should be kept to a minimum. Employees who are issued mobile devices are responsible for complying with all other related policies.

B. Employee-Owned Mobile Devices

Employees are expected to use their City-owned mobile device to perform official City business. Employees are prohibited from using text messaging as a means of communicating about official City business from an employee-owned mobile device. If an employee receives and/or sends a text message related to official City business on an employee-owned mobile device, then the text messages may be subject to Nevada's public record laws. Employees should respond to any text message sent to their personal device and related to official City business by providing their City-owned mobile device number or City email address, and then continue any related communications via their City-owned device or City email address. Further, if an employee receives a text that pertains to official City business on an employee-owned device, then the employee is required to maintain the text in accordance with the Clerk's Office's Records Directives (concerning preservation) referenced in F-01.

If the City receives a public records request seeking all text messages related to official City business to and from an employee's personal mobile device, the employee will be required to review their texts on their personal mobile device for responsive information, timely provide the City with any responsive information, and sign a declaration stating that they have reviewed their personal mobile device and (1) has provided all responsive information, or (2) if no responsive information exists, state that no responsive texts exist on their personal mobile device.

Employees may access their City-email using the website mail.cityofhenderson.com on their employee-owned mobile devices, laptops, tablets, and home workstations. Employees are also permitted to install the mobile Outlook/client application on their employee-owned device. Employees may also use their personal mobile devices, laptops,

tablets, and home workstations to connect to the City's data network via an approved Virtual Private Network (VPN) method using a two-factor authentication.

Installation of City-owned software onto employee-owned devices is prohibited unless first approved the DoIT. Employees are responsible for all financial obligations relating to their mobile device.

C. Security and Acceptable Use

The City reserves the right to deny any level of access to devices that pose a risk to the computing environment, including the right to remotely wipe information from any City-connected devices without notification.

Mobile devices should not connect to City services when travelling internationally. Data usage charges will not be paid by the City unless approved by the employee's department director or designee prior to travel.

Employees may not engage in inappropriate material activity (i.e., visit inappropriate websites, send inappropriate text messages, etc.) at any time on their City-owned mobile devices or during work hours on employee-owned mobile devices. Employees' conduct when using City-owned phones, or employee-owned mobile devices during work hours, must be consistent with the City's policies. The failure to comply with any City policy when using a City-owned mobile device or employee-owned mobile device during work hours may subject an employee to discipline, up to and including termination. Excessive personal communication during the workday, regardless of the mobile device used, can interfere with employee productivity and be distracting to others.

Employees should not use a cell phone or mobile device while operating a City Vehicle or personal or rental vehicle on City business, unless the employee's job requires him/her to do so. When a cell phone conversation is necessary, an employee must pull off to a safe location and cease operating the vehicle. The employee must be sure to select an area which will not jeopardize the employee's safety or cause a hazard for the employee or other drivers. Employees required to use a cell phone as part of the employee's job duties while operating a vehicle, such as public safety personnel, must use a hands-free device. Under no circumstances may the employee input, view messages, retrieve voice messages or type any information while operating a City Vehicle or personal or rental vehicle on City business. This includes the use of all cellular telephones, blackberries, PDAs and monitors (including but not limited to text messaging, checking emails, and web browsing, etc.)

Non-exempt employees should not be performing any work away from their regular work site and outside regular working hours unless they have been scheduled for overtime, are serving in a standby status, and/or have been called back to work. The City does not expect non-exempt employees to check e-mail or return phone calls or text messages

outside of their normal working hours, unless prior authorization from their manager or supervisor has been granted and all other requirements set forth by a department's policy/procedure has been complied with.

All non-exempt employees must accurately record and immediately report all time worked to their supervisor or manager. This includes work performed off of the City's premises and time spent on work-related e-mail, text or phone communication that occurs after working hours. The City reserves the right to verify the work performed and assess the duration and business necessity of any communication reported to be completed outside of regular work hours.

III. APPROVAL

APPROVED BY:
Richard Derrick, City Manager/CEO

REVIEWED BY:
Nicholas Vaskov, City Attorney
Brooke Stream, Director of Human Resources

Record of approved document can be obtained through the Human Resources Department.

Relevant Form(s):
Acknowledgment of Financial Responsibility & Auth for Deduction from Wages Form
Acknowledgment of Financial Responsibility & Auth for Deduction from Wages-Cellular Devices
City Cell Phone Reset Instructions

ORIGINAL EFFECTIVE DATE: 2/16/2016
REVISION DATE(S): 10/17/2016; 11/8/2021