CITY OF DURANGO MOBILE DEVICE ADMINISTRATIVE POLICY

Approved By: Ron Letkeman Date: 11/8/17

Effective Date: 1-1-2018 or at time of issuance of City owned mobile device if device issued prior to January 1, 2018.

Subject: City of Durango Mobile Device Policy

Applicability: All City of Durango employees.

Policy Issued: November 8, 2017

Revision History: November 7, 2017

Purpose: Mobile devices are powerful tools that can be utilized to increase the efficiency and effectiveness of City government. However, to maintain adequate security, public records, ensure a productive exchange of information and a positive morale, and consistency across the City of Durango this policy governs use of mobile devices used for City business.

1. Definitions:

Mobile Devices: Include, but are not limited to City Mobile Devices and Personal Mobile Devices, including cell phones, smartphones, tablets, laptops and other similar devices.

MDM: Mobile Device Management. The administration of mobile devices such as cell phones, smartphones, tablets and laptops.

Network Access: Secured access to any City of Durango data including applications, databases and file shares.

Strong Password: A password designed to be hard for a person or program to discover. Two things make a password stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper and lower-case letters and special characters ($, #, etc.).

Two Factor Authentication: A method of confirming a user’s claimed identity by utilizing a combination of two different components, one of which is usually a password.
Remote Wipe: A system where an administrator has the ability to remotely delete data on a hardware device or system.

Personal Mobile Device: A Mobile Device that is owned by an employee of the City.

City Mobile Device: A Mobile Device that is secured and owned by the City and issued for use by employees or other authorized persons for City business only.

2. Policy:

Employees for the City of Durango may have the opportunity to use a City Mobile Device for work purposes, when required to perform job duties and when authorized in writing, in advance, by the Department Director, Information Services, Human Resources and Finance.

When a City Mobile Device is assigned to an employee or work group, it is required to be used for all City business; Use of personal devices by employees is prohibited for the purpose of conducting any City business, except as otherwise provided herein.

3. Procedure

3.1 Device Protocols

To ensure the security of the City of Durango information and network, authorized employees are required to keep all City Mobile Devices updated with the latest operating system version and to allow mobile device management (MDM) functionality on the device. MDM requires, but is not limited to, a strong password and remote wipe capability.

Attachments, files and documents may be downloaded for viewing and may be downloaded and saved to the City Mobile Device.

Employees must use extreme caution when connecting to unsecure internet sites, including utilizing public Wi-Fi. The use of City Mobile Devices in public places and transmitting information through public telecommunication networks, presents a significant risk of unauthorized persons observing/gaining access to the information that is being processed.

3.2 Restrictions on authorized use

The use of Personal Mobile Devices to photograph and/or record confidential, non-public City information, or conversations, phone calls and/or or other information related to City business is prohibited. Relatedly, recording of another City employee without his or her knowledge and express consent, whether via a Personal Mobile Device or a City Mobile Device, is expressly prohibited.¹

¹If there is a valid and legitimate reason for recording another City employee the individual wishing to record must advise the individual(s) to be recorded and obtain consent from the individual(s) before proceeding. Secret recording is not in accordance with City values as it is not respectful of privacy expectations of employees and guests; not conducive to the free flow of ideas and exchange of frank discussion within the City; and secret recording creates disruption, discord, lack of trust and lack or morale in the workplace.
City of Durango Personnel Regulations and policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of all Mobile Devices for activities that are in any way connected to the employee’s employment with the City. Nonexempt employees may not use City Mobile devices for work purposes outside of their normal work schedule without authorization in advance from their supervisor or department director. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls, excluding calls related to work attendance. Nonexempt employees using electronic communications for work-related correspondence during unauthorized times may be subject to disciplinary action up to and including dismissal for violations of this policy. Supervisors requiring nonexempt employees to use electronic communications for work-related correspondence at unauthorized times are also subject to disciplinary action up to and including dismissal. City of Durango reserves the right to deactivate the network access from the employee’s City Mobile Device during periods of leave or outside scheduled work hours.

Personal Mobile Devices may be used by an employee for the limited purpose of contacting other City personnel regarding work attendance or scheduling issues or in the case of a bona fide emergency. No other City business may be conducted on a Personal Mobile Device.

Limited use of Personal Mobile Devices (phone and text only, no access to City Network) by part-time Parks and Recreation employees and volunteers who are working and who are required to use those Personal Mobile Devices for specific purposes designed for the convenience of the public and the department related to Parks and Recreation Activities will be exempt from portions of this policy. These employees and volunteers understand that theses exemptions do not include exemptions from Privacy /City access section of the policy.

3.3 Privacy/City access

No employee using a City Mobile Device is entitled to expect any privacy except which is governed by law. The City of Durango has the right, at any time, to monitor and preserve communications that use the City of Durango’s networks or any City Mobile Device in any way, including data, stored photos/videos, voice mail, telephone logs, text messages, instant messages, internet use and network traffic, to determine proper use or to carry out the functions of the City.

The use of City Mobile Devices for business purposes may result in the creation of public records, which must be maintained in accordance with records retention requirements. Personal and City related data on City Mobile Devices may be reviewed, retained or released to government agencies or third parties during records request, an investigation or litigation. The City may review the activity and analyze use patterns and may choose to publicize this data to ensure the City of Durango’s resources in these areas are being used according to this policy.

Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool. The use of a Personal Mobile Device for City business in contravention of this policy or as allowed in limited circumstances by this policy may also create a public record which may be subject to disclosure under Colorado Law, and to the extent such a record is found
to have been created, the employee shall cooperate in allowing the City to have access to necessary records to comply with any required disclosure.

4. Safety

Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using a Mobile Device while driving, per established safety policies.

Employees who are charged with traffic violations resulting from the use of mobile devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using mobile devices while at work in those areas if such use can potentially be a safety hazard.

4.1 Lost, Stolen, hacked or damaged equipment

Employees are expected to protect City Mobile Devices from loss, damage or theft. Employees must immediately notify their supervisor and the IS Division in the event their City Mobile Device is lost or stolen.

To secure sensitive City data, all employees will be required to have MDM software installed on their City Mobile Devices by the IS division prior to using the device.

City of Durango will not be responsible for loss or damage of any applications or data resulting from the use of City applications or the wiping of City information.

Personal responsibility for replacement costs for damages caused to City Mobile Devices will be determined on a case-by-case basis. Employees may receive disciplinary action up to and including dismissal for damage to City Mobile Devices caused willfully by the employee.

4.2 Security

City Mobile Devices that store City information must be strong password protected with two factor authentications.

5. Supervisory Responsibilities

Supervisors are responsible for ensuring employees are adhering to this policy and reporting violations of this policy.

6. Termination of employment

All City Mobile Devices must be returned to City custody upon termination of employment.
7. Violations of policy

Employees who have not received authorization in writing from City of Durango and who have not provided written consent will not be permitted to use mobile devices for work purposes. Abuse of the program or failure to follow City of Durango policies and procedures may result in disciplinary action, up to and including dismissal of employment.