B. MOBILE DEVICE POLICY FOR CITY OWNED DEVICES

The purpose of this policy is to define accepted practices and responsibilities for use of City of Redlands-owned mobile devices for which authorization is given to connect to enterprise systems and the city' network. This policy defines user eligibility and commitment requirements, provides guidance for the secure use of mobile devices. This policy applied to and provides guidelines for all mobile devices, including mobile phones, smart phones and tablets. This policy is intended to be used as a supplement to the Computer and Electronic Communications Policy.

The objective of the City's mobile device policy is to establish the required measures for using mobile devices owned or managed by the City to do business and to access enterprise information or IT resources. This policy is operationalized in a Mobile Device Management (MDM) software used by the Department of Innovation and Technology for the management and administration of mobile devices owned by the city. Software is installed prior to deployment.

Mobile devices are valuable tools used to conduct business. It is the policy of the City to protect and maintain user safety, security and privacy, while protecting enterprise information assets at the same time allowing employees to use these tools. Use of mobile devices supplied by, or funded by, the City shall be primarily for City business.

1. Policy Application

This policy applies to all City of Redlands employees, interns, volunteers, and affiliates that are considered authorized users of the City's systems as defined in the Computer and Electronic Communications Policy.

2. Definitions

Tablet

A tablet is an open-face wireless device with a touch screen display and with or without physical keyboards. The primary use is the consumption of media; it also has messaging, scheduling, email, and Internet capabilities. Diagonal screen dimensions are typically between 5 inches and 18 inches. Media tablets may have open-source operating systems (such as Android) or a closed operating system under the control of the operating system vendor and/or device make (such as Apple's iOS and Windows). Media tablets may or may not support an application store.

Mobile Device

This refers to any mobile phone, cellular modem, Smartphone, laptop or tablet.

Mobile Applications

This refers to software designed for any or all the mobile devices defined in this policy.

3. User Roles and Responsibilities

a. Responsibilities

- Users must ensure that they comply with all sections in this policy.
- Users must agree to take responsibility for the security of their mobile devices and the information they contain.
- Acceptable forms of security for mobile devices include: configuring a passcode to gain access to and use the device. This helps prevent unauthorized individuals from gaining access to the City's systems and data.
- Set an idle timeout that will automatically lock the device when not in use. This also helps prevent unauthorized individuals from gaining access to the device.
- Mobile devices are issued for business purposes and remain the property of the City.
- When the mobile phone, laptop or portable computing device is allocated, the user assumes responsibility for the physical security of the equipment and information contained within.
- Users are not permitted to authorize purchases or services for their mobile devices, unless such purchases are for City oriented purposes; or if for personal use, the purchases must be made from and linked to a private, non-city account.
- Users must notify The Department of Innovation and Technology and their respective department immediately of loss, theft or damage to a City-owned mobile device.
- Users consent that if the device is lost/stolen the Department of Innovation and Technology (DoIT) may wipe and completely erase all data from the mobile device so as to not jeopardize the security of City data and systems that are accessed from the device. This applies to all City-owned mobile devices, whether or not they are password and lockout protected.

b. Condition

Users must take proper care of their mobile device(s).

c. Cost Control

Users should support efforts to manage device operation costs by ensuring that call minutes, text messages and data usage do not exceed usage plan limits.

When traveling abroad, users should avoid using mobile phones. If mobile phones are used abroad users should:

- Contact the Department of Innovation and Technology prior to travel, if use of the device is essential during their trip.
- Exercise caution to avoid incurring excessive charges and roaming fees when using the mobile device.
- Connect to mobile data networks only when essential.
- Choose Wi-Fi hot spots as the preferred manner of connecting to data networks.

Note: If you have a choice, select those hot spots that use some form of encryption. Be sure and set the location to "Public Network."

- When connected to public Wi-Fi hot spots be cognizant of the fact that any data transferred can easily be intercepted by other Wi-Fi hotspot patrons.
- Use a soft phone or other voice over Internet Protocol (VoIP) solutions when possible.

d. Loss or Theft

It is the user's responsibility to take appropriate precautions to prevent damage to or loss/theft of the device.

If the device is lost, stolen or suspected to be compromised in any way, the user must notify the City's Department of Innovation and Technology and the any carrier for telecom services within 12 hours. The Department of Innovation and Technology then has the authority to wipe the device so as to not jeopardize the security of City data and systems.

e. Applications and Downloads

Users must take all reasonable steps to protect against the installation of unlicensed or malicious applications.

All software on the device must either be provided and installed by The Department of Innovation and Technology or approved for installation by the employee's supervisor. Unmanaged or unapproved installations can constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.

If for personal use, as allowed under the Mobile Device Management software and Computer and Electronic Communications Policy, user will perform due diligence to verify downloads are not malicious in nature or would not otherwise expose the City's systems to a security risk. Downloading applications from the platform's (e.g., Apple's, Android's) general application store is acceptable, insofar as the application complies with this policy, The Department of Innovation and Technology protocols and the Computer and Electronic Communications Policy.

Unless approved for work-related use, City procurement credit cards shall not be used for app store purchases nor entered into an app store account. In most cases, work- related apps will be provided under a volume purchase to City employees using an App Store Front for the City. Should a work-related app not be contained in the storefront, the user should contact The Department of Innovation and Technology to make the purchase.

f. Backup and File Sharing or Synchronization

Users are required to use approved software for backing up all devices.

The use of a non-City authorized cloud-based service, such as Apple iCloud, is not permitted for backing up or sharing any City data.

g. Functionality and Feature Management

The device operating system shall not be modified, unless required or recommended by the City. The use of devices that are jailbroken, "rooted" or have been subjected to any other method of changing built-in protections is not permitted and constitutes a breach of this policy.

At the City's request, users are responsible for delivering the mobile device to the Department of Innovation and Technology if and when the device is selected for a physical security audit or is needed for purposes outlined in Section VII. 4 of the Computer and Electronic Communications Policy.

h. User Safety

Users should comply with the safety guidelines defined in the City Employee Policy Manual when using mobile phones in their vehicles.

i. Security and Privacy Obligations for City Data

Users should recognize that their use of, or access to, data provided by or through the City

may be monitored by the City. If personal information is stored on a City device, users should presume that that information may also be monitored, but every attempt will be made to compartmentalize personal data.

The City will only use mobile device location information in accordance with Section VII.4 of the Computer and Electronic Communications Policy.

Users must take appropriate precautions to prevent others from obtaining access to their mobile devices.

- Users should not share passwords, PINs or other credentials with anyone.
- Users should not share City-issued mobile devices with anyone, unless the department has explicitly intended those devices to be shared among multiple staff.

j. Exit Obligations for Employees Taking Absence or Separating from the City

Any employee who will be taking leave from the City for a period of four (4) or more consecutive weeks shall be notified in writing from the HR Department of the need to surrender to the City any and all City-owned mobile devices in their possession.

Any employee separating from the City permanently is responsible for surrendering any City-owned mobile device in their possession before the end of their last day of service to the City.

4. Prohibited Uses

Users are strictly prohibited from using the City of Redlands's information technology and electronic communications systems to transmit, receive, download, view or copy any communication that is fraudulent, harassing, discriminatory, racially offensive, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. Employees encountering or receiving this type of material should immediately report the incident to the user's supervisor. The City of Redlands recognizes, however, that certain employees may have valid City business reason to use the Internet to access otherwise inappropriate materials in the course of performing their duties. The Mobile Device Management software used by the City may be used to track the use of prohibited content on mobile devices.

The City reserves the right to deploy industry standard Mobile Device Management (MDM) software for the express purpose of monitoring and managing city owned devices to ensure the integrity of the city's network and data resources.

5. Data and System Security

a. Data Security

All mobile devices connecting to the City's network or accessing City information must meet the following security requirements:

- It is highly encouraged that all City mobile devices must be secured with a PIN, password or a pattern-screen lock when powering on the device or when left unattended, wherever possible.
- It is highly encouraged that all City mobile devices must be configured to automatically lock after a period of inactivity, wherever possible.
- Device users must comply with The Department of Innovation and Technology directives regarding updating or upgrading system software, and must otherwise act to ensure security and system functionality.

b. Physical Security

Mobile device users must comply with physical security requirements when equipment is at the user's workstation, when traveling, or when working in the field or at a job site. Users must take the following preventative measures defined in this policy to protect City data and systems:

- Mobile devices must not be left in plain view in an unattended vehicle, even for a short period of time.
- Mobile devices must not be left in a vehicle overnight.
- A mobile device displaying sensitive information being used in a public place must be positioned so that the screen cannot be viewed by others.
- The device must be physically secured when it is left unattended outside the immediate work area for any extended period.
- In vulnerable situations (e.g., public areas), the mobile device must not be left unattended under any circumstance.
- Mobile devices should be carried as hand luggage when traveling and never checked as baggage.
- The employee will be responsible for the replacement or repair of the City-owned mobile device if it is damaged or lost as a result of the employee's negligent or intentional conduct.
- The employee's department will be financially responsible for the replacement or repair of the City-owned mobile device if it is damaged, stolen or lost.