C. MOBILE DEVICE POLICY

PURPOSE

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's network. This policy defines user eligibility and commitment requirements, provides guidance for the secure use of mobile devices. This policy applies 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.

POLICY

Policy Application

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

1. 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.
- Users must agree not to tamper with or otherwise interfere with the City-installed mobile device management software.
- User must agree not to change the City-issued Apple ID or other unique device identification on a City-issued device.
- 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, such as apps. 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.
- Authorization to order the devices and cellular/data services from a telecommunications carrier must be administered through the procedure below.
- Users must notify The Department of Innovation and Technology and their respective department within no less than 12 hours 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).

PROCEDURE

This procedure is to help with the acquisitions, upgrades and replacements for mobile devices deployed to the various City staff.

Mobile Device Order Procedure

Steps (Note steps 1-3 must be completed prior to #4 before orders are place.)

1. Create a helpdesk ticket, stating a need for a mobile device to be purchase, with the make and model.

   a. If you do not know which make or model to choose, please ask IT for assistance.

   b. IT will get back to you with pricing. Requests will be addressed within 2 business days. If urgent, please note in your helpdesk ticket and staff will prioritize accordingly.

2. Complete a City Cell Phone form which:

   a. Confirms user assignment, request type, plan & equipment information.

   b. Confirms employee personal use.

   c. Obtains approval from employee supervisor/department head

   d. Serves as approval form for monthly recurring service charge.

   e. Cell Phone Forms can be found here: \\files\Shared\DoIT Forms\Cell Phones\VERIZON WIRELESS and here: J:\DoIT Forms

3. Complete a Short Form for equipment:
    a. Confirms make and model of device to be purchase
    b. Confirms any accessories to be purchase
    c. Confirms pricing of items
    d. Confirms account number to which charges will be applied
4. Email Copies of completed Cell Phone and Short forms to the assigned helpdesk technician and CC. Elizabeth (Lizzie) Ramirez eramierz@cityofredlands.org
5. Forward original forms to Finance, attention Lizzie Ramirez.

Employee Separation

1. Departments are responsible for collecting mobile devices (including chargers and cables) and notifying IT to disconnect or suspend service.
    a. Please create a helpdesk ticket to disconnect or suspend service.
2. Service & Monthly charges, may be suspended for a maximum of 90 days per instance, and no more than 180 days in any 12-month period. Service and charges will automatically resume at the end of each 90-day suspension.

Phone Reassignment

1. If an existing line of service is reassigned to a new employee, a new City Cell Phone form must be completed and send to IT as a helpdesk ticket, and CC. Elizabeth (Lizzie) Ramirez eramierz@cityofredlands.org

Once a City-owned mobile device is in use, employees must adhere to the following requirements:

- 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 Division 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.
- City-issued Apple ID’s should not be removed from any City-device.
- Users must take proper care of their mobile device(s).

- 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 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.

a. 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 a 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 Department of Innovation and Technology staff to make the purchase.

b. 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 outline in Section VII. 4 of the Computer and Electronic Communications Policy.

c. User Safety

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

d. 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.
- 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.

All forms for this policy can be found here: J:\DoIT Forms