# Mobile Device Policy

## 1. Overview

Mobile computing devices (smartphones, tablets, convertible laptops, and various other personal computing devices) are becoming an implementation standard in today's computing environment. Their size, portability, and ever- increasing functionality are making the devices desirable in replacing traditional desktop devices. However, the portability offered by these devices can also increase security exposure to individuals using the devices.

## 2. Purpose

The purpose of this policy is to establish the procedures and protocols for the use of mobile devices and their connection to the network.

## 3. Scope

This policy applies to all City of Turlock staff who use personal devices for business purposes or business-issued mobile computing devices.

## 4. Policy

### A. GENERAL

All mobile devices, whether owned by City of Turlock or owned by staff, that have access to systems and applications are governed by this policy. Applications, including cloud storage software used by staff on their own personal devices are also subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

- Mobile computing devices must be protected with a password required at the time the device is powered on
- Personal mobile computing devices that require network connectivity must conform to all City of Turlock standards for use and configuration
- City owned mobile devices will have location services enabled at all times.
- Unattended mobile computing devices shall be physically secured
- Mobile computing devices that access the City of Turlock network shall have active and up-to-date anti-malware and firewall protection
- Lost and stolen devices will be locked and location services will be used to locate the device. If the device cannot be located, it will be wiped of all information.

### B. USER DEVICE RESPONSIBILITIES

The following procedures and requirements shall be followed by all users of mobile devices:

- Staff shall immediately report any lost or stolen devices
- Unauthorized access to a mobile device or company data must be immediately reported

- Mobile devices shall not be “rooted” or have unauthorized software/firmware installed
- Staff shall not load illegal content or pirated software onto any mobile device
- Only approved applications are allowed on mobile devices that connect to the City of Turlock network
- Mobile devices operating system software and applications shall be kept up-to-date
- Staff shall use City of Turlock corporate email system when sending or receiving City of Turlock data
- Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis
- Mobile Device Management (MDM) will be used to enforce common security standards and configurations on devices
- Staff shall not modify configurations without express written authorization from the Information Technology Manager.

### C. ADMINISTRATIVE RESPONSIBILITIES

The Information Technology Manager or their designee shall ensure:

- Annual security training is provided to users of mobile devices. The content and form of that training shall be decided by the City of Turlock or their designee. Periodic security reminders may be used to reinforce mobile device security procedures.
- MDM software is used to manage risk, limit security issue, and reduce costs and business risks related to mobile devices. The software shall include the ability to inventory, monitor (e.g. application installations), issue alerts (e.g. disabled passwords, categorize system software (operating systems, rooted devices), and issue various reports (e.g. installed applications, carriers).
- MDM software enforces security features such as encryption, password, bricking, and key lock on mobile devices.
- MDM software shall include the ability to distribute applications, data, and global configuration settings against groups and categories of devices.
- Procedures and policies exist to manage requests for exemptions and deviations from this policy.

Information Technology Division shall implement procedures and measures to strictly limit access to sensitive data moving to and from mobile computing devices since these devices generally pose a higher-risk for incidents than non-portable devices.

## 5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of City of Turlock. Satisfactory examples of evidence and compliance include:

- Spot user checks for compliance with mobile device computing policies
- Readily available processes and procedures for staff use of mobile devices
- Configuration and support guidelines and procedures for mobile devices
- Communication and device logs of attached units showing appropriate management and monitoring protocols are in place
- Anecdotal and archival communications showing regular implementation of the policy

## 6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## 7. Distribution

This policy is to be distributed to all City of Turlock staff and contractors using City of Turlock information resources.

## 8. Policy Version History

| Version | Date | Description | Approved By |
|---|---|---|---|
| 1.0 | 08/24/2021 | Initial Policy Drafted | |
| | | | |
| | | | |

I, _____ HEREBY ACKNOWLEDGE THAT I HAVE READ AND UNDERSTAND THE MOBILE DEVICE POLICY.

_____

Signature of Employee

_____

Date

_____

Witness

_____

Date