




DATE SUBMITTED 12/08/2021  
 SUBMITTED BY R. Alejandro Estrada  
 DATE ACTION REQUIRED 12/15/2021

COUNCIL ACTION (x)  
 PUBLIC HEARING REQUIRED ( )  
 RESOLUTION ( )  
 ORDINANCE 1<sup>ST</sup> READING ( )  
 ORDINANCE 2<sup>ND</sup> READING ( )  
 CITY CLERK'S INITIALS em

**IMPERIAL CITY COUNCIL  
 AGENDA ITEM**

SUBJECT: DISCUSSION/ACTION: 1. APPROVE AND ADOPTION OF THE CITY OF IMPERIAL MOBILE DEVICES POLICY	
DEPARTMENT INVOLVED: DEPARTMENT OF INFORMATION TECHNOLOGY	
BACKGROUND/SUMMARY: The City of Imperial staff is requesting the Council's consideration in the adoption of the updated Mobile Devices Policy.  It is the responsibility of the City of Imperial to implement procedures for effective use of City-issued mobile devices, communication services, and electronic equipment to increase the City's operational efficiencies. Mobile devices such as smart phones and tablets offer great flexibility and improved productivity for employees. However, they can also create added risk and potential targets for data loss. As such, their use must be in alignment with appropriate standards and encryption technology should be used when possible.	
FISCAL IMPACT:	FINANCE INITIALS 
STAFF RECOMMENDATION: It is staffs recommendation to approve the updated Mobile Devices Policy .	DEPT. INITIALS 
MANAGER'S RECOMMENDATION: The City Manager agrees with staffs recommendation.	CITY MANAGER'S INITIALS 
MOTION:	
SECONDED: AYES: NAYES: ABSENT:	APPROVED ( )      REJECTED ( ) DISAPPROVED ( )      DEFERRED ( )  REFERRED TO:



## 1. Overview

It is the responsibility of the City of Imperial to implement procedures for effective use of City-issued mobile devices, communication services, and electronic equipment to increase the City's operational efficiencies.

Mobile devices such as smart phones and tablets offer great flexibility and improved productivity for employees. However, they can also create added risk and potential targets for data loss. As such, their use must be in alignment with appropriate standards and encryption technology should be used when possible.

## 2. Purpose

This document describes the Department of Information Security's (DoIT's) requirements for employees of the City of Imperial that work outside of an office setting.

## 3. Scope

This policy applies to any mobile device, or endpoint computer issued by the City of Imperial which contains stored data owned by the City of Imperial. e.g. email, text, videos and photos.

## 4. Policy

All employees shall assist in protecting devices issued by the City of Imperial or storing the City of Imperial data. Mobile devices are defined to include desktop systems in a telework environment, laptops, PDAs, and cell phones.

Users are expressly forbidden from storing City of Imperial data on devices that are not issued by the City of Imperial, such as storing the City of Imperial email on a personal cell phone, personal laptop or PDA.

### 4.1 Anti-Virus, Windows Defender

City of Imperial will issue devices with Windows Defender and Endpoint security installed. Employees are to notify the DoIT immediately if they see error messages for these products. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with City of Imperial policy.



### 4.2 Mobile Device Modifications

Staff shall not modify configuration without express written authorization from the DoIT. Devices must not be “jailbroken” or “rooted” or have any software /firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

### 4.3 Applications

Applications that are not approved by DoIT are not to be used within the workplace or in conjunction with corporate data. Users must not load pirated software or illegal content onto their devices.

### 4.4 Keys

All encryption keys and pass-phrases must meet complexity requirements described in the City of Imperial’s AUP.

### 4.5 General Care

Devices that malfunction or are damaged must be reported to the DoIT. The City will be responsible for repairing tablets or phones that malfunction.

### 4.6 Loss and Theft

The loss or theft of any mobile device containing City of Imperial’s data must be reported immediately.

### 4.7 Driving

A mobile phone shall never be used under any circumstances, to text, receive or place calls, surf the web, email or instant message or to take pictures or video while driving a vehicle. Employees may place or receive calls only with the use of an approved hands-free device and in accordance with applicable laws. Employees who are charged with traffic violations resulting from the use of their City-issued mobile devices while driving will be solely responsible for all liabilities including any fines, penalties, or any actions taken by law that result from such violation.



## Mobile Devices Policy

Department of Information Technology

### 5 Policy Compliance

#### 5.1 Compliance Measurement

The DoIT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

#### 5.2 Exceptions

Any exception to the policy must be approved by the DoIT and City Manager's Office in advance.

#### 5.3 Non-Compliance

The City reserves the right to inspect any and all files stored on mobile devices in order to ensure compliance with this policy. Individuals do not have any personal privacy right in any information created, received, stored in, or sent from any City issued mobile device. Any data stored or recorded by a City-issued mobile device is the sole property of the City. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### EMPLOYEE ACKNOWLEDGMENT

If you have additional questions about this policy, please contact Human Resources and/or DoIT before signing the following agreement.

I have read the City of Imperial's policy on the use of mobile devices and agree to abide by it. I understand that violation of any of the above policies may result in discipline, up to and including termination.

---

User Name (Printed)

---

User Signature

---

Date