Agenda Item No. B-5

DATE SUBMITTED	10/29/2025
SUBMITTED BY	R. ALEJANDRO ESTRADA
DATE ACTION REQUIRED	11/5/25

COUNCIL ACTION	(X)
PUBLIC HEARING REQUIRED	( )
RESOLUTION	( )
ORDINANCE 1ST READING	( )
ORDINANCE 2ND READING	( )
CITY CLERK'S INITIALS	( )

IMPERIAL CITY COUNCIL
AGENDA ITEM

SUBJECT: DISCUSSION/ACTION:

1. Approve and adopt the Bring Your Own Device Policy.

DEPARTMENT INVOLVED: DEPARTMENT OF INNOVATION & TECHNOLOGY

BACKGROUND/SUMMARY:

The City of Imperial Department of Innovation & Technology's (DoIT) intentions for publishing a Bring Your Own Device Policy are not to impose restrictions that are contrary to the City's established culture of openness, trust, and integrity. DoIT is committed to protecting the City's assets while providing a secure and effective method of conducting City business.

A Bring Your Own Device (BYOD) Policy enables approved employees to access their City of Imperial email account using an approved personal mobile device in lieu of a department-issued phone.

FISCAL IMPACT: There is no fiscal impact associated with this action.	FINANCE INITIALS VMG
STAFF RECOMMENDATION: Recommendation to approve and adopt the Bring Your Own Device Policy.	DEPT. INITIALS
MANAGER'S RECOMMENDATION: Approve	CITY MANAGER's INITIALS

MOTION:

SECONDED:
AYES:
NAYES:
ABSENT:

APPROVED ( ) REJECTED ( )
DISAPPROVED ( ) DEFERRED ( )

REFERRED TO:

POLICY NAME: Bring Your Own Device	AUTHORITY: City of Imperial
APPLICATION: All Employees	DATE APPROVED: November 5, 2025

City of Imperial

Department of Innovation & Technology

Bring Your Own Device (BYOD) Policy

Adopted: 11/05/2025

1. Overview

The City of Imperial Department of Innovation & Technology's (DoIT) intentions for publishing a Bring Your Own Device Policy are not to impose restrictions that are contrary to the City's established culture of openness, trust, and integrity. DoIT is committed to protecting the City's assets while providing a secure and effective method of conducting City business.

A Bring Your Own Device (BYOD) Policy enables approved employees to access their City of Imperial email account using an approved personal mobile device in lieu of a department-issued phone.

This policy is not intended to replace the current City Cellular Phone Policy dated August 17, 2011, nor the Mobile Devices Policy dated 12/15/2021.

2. Purpose

This policy outlines the acceptable use, security requirements, and responsibilities associated with using personal mobile devices (e.g., smartphones, tablets, laptops) to access City of Imperial government networks, applications, and data.

3. Scope

This policy applies to all employees, elected officials, contractors, and third-party vendors who access or use City of Imperial government data or systems on their personally owned devices.

4. Definitions

- BYOD: "Bring Your Own Device" refers to using personally owned computing devices to access government resources
- Device: A personally owned smartphone, tablet, laptop, or other mobile computing device.

5. Eligibility

Employees and contractors may be eligible for BYOD participation. Final approval rests with the Department of Innovation & Technology Director.

6. Security Requirements

All BYOD participants must adhere to the following guidelines:

- Use a strong device passcode and enable device encryption
- Report lost or stolen devices immediately
- Allow remote wipe of City of Imperial data in case of loss, separation from employment, or compromise.
- Do not store sensitive or confidential City data on personal devices unless explicitly authorized.

7. Access Control

- Devices may only access City of Imperial systems and network via secure VPN, or other approved tools.
- Access rights may be revoked at any time based on security risk or administrative discretion.

8. IT Support Limitations

- IT support will be limited to ensuring secure access to the City of Imperial network.
- IT will not provide full support for personal apps or non-City-related issues on BYOD devices.

9. User Responsibilities

Users must:

- Maintain compliance with all security configurations.
- Notify IT of any security incidents or potential data breaches
- Understand that City of Imperial data on personal devices remains subject to public records laws and may be discoverable under FOIA or similar statutes.

10. Data Ownership and Privacy

- City of Imperial retains ownership of all government data.
- The user understands that personal data may be visible during troubleshooting or audits.
- Users waive expectation of privacy on government-related activity conducted via BYOD devices.

11. Reimbursement

- The City of Imperial is not liable for data or messaging charges while conducting City business.

12. App Restrictions

- The installation of unapproved applications that access or store City of Imperial data is prohibited. Only applications vetted and approved by the DoIT department may be used for business-related purposes on BYOD devices.

13. Public Records Compliance

- All communications, documents, and data related to City of Imperial business on BYOD devices are subject to applicable public records laws. Users must comply with requests for records and understand that personal devices may be subject to legal discovery if used for business-related purposes.

14. Violations

- Non-compliance with this policy may result in disciplinary action, including revocation of BYOD privileges.

15. Acknowledgment

- All participants must sign a BYOD Agreement Form before being granted access to City of Imperial systems or data using a personal device

EMPLOYEE ACKNOWLEDGMENT

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

I have read the City of Imperial's policy on the use of e-mail, network, and internet/intranet 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