Dallas County Information Technology Mobile Device Management Policy

1. Scope

The Dallas County Mobile Device Management Policy applies to all Users (County employees, elected officials, contractors, subcontractors, part-time and temporary workers , individuals telecommuting, and who have been granted access to County's network or email messaging platform). Because Dallas County owns the network, this Policy applies to all mobile devices that connect to Dallas County's network.

This policy supersedes all other policies on this topic either written or verbal.

2. Purpose

This document defines the policy necessary for governing connectivity to the Dallas County network and services from mobile devices.

3. Policy

Definition

The mobile device policy applies to all devices and accompanying media that fit the following classifications:

- Laptop
- Tablet computers
- Wearable technology
- Microsoft Surface Book
- Smartphones (Android and Apple) including BYOD* (bring your own device)
- Any mobile device capable of storing County data and connecting to a network (including Wi-Fi connection)

County Issued Mobile Devices

Any mobile device or portable hardware that is owned, acquired by or supplied by the Dallas County Office of Information Technology that could be used to access County resources with a network connection to conduct official County business.

Privately Owned Mobile Devices (i.e., BYOD)

Any mobile device or portable hardware that is owned, acquired by or supplied by a Dallas County user that could be used to access County resources with a network connection to conduct official County business. Users issued a County-owned mobile phone cannot use personal phones (privately owned) for County business.

Governance from the County Mobility Policy

Conducting County Business on Privately Owned or BYOD Mobile Devices

(a) All county-owned mobile devices are required to have the Dallas County MDM (mobile device management) client. Users must remain signed into the Comp Portal application (MDM client). User are prohibited to delete the Comp Portal application (MDM Device Management app) under the phone Setting.

(b) It is strongly recommended that Users do not conduct official County business on their personal electronic devices including, but not limited to, utilizing County email, discussing official County business via text message, or using personal electronic devices to make County related telephone calls. As such, the County shall not reimburse Users for use of their personal electronic devices to conduct official County business.

(c) Elected officials, department heads, managers, and supervisors should not require Users to use their privately owned mobile devices. Should a User need to conduct substantial official County business using a personal electronic device, the County will issue the User a County owned cellular telephone based on a demonstrated need and the approval process as detailed in Section 114-182 of the Dallas County Code.

(d) Should a User choose to conduct official County business on their personal electronic device, the employee will be required to download the County Mobile Device Management client in order to secure and ensure the availability of the County Data. Further, the User shall be required to sign an acknowledgement and agree that the County data may be remotely removed from their personal electronic device should the need arise. The User must also comply with Section 74-136 of the Dallas County Code regarding their obligations under the Public Information Act and applicable records retention guidelines.

(e) In the event a User's privately owned mobile device that contains the County owned phone number is lost, stolen or misplaced, irreparably damaged or otherwise compromised, the User shall notify their supervisor, manager, department head or elected official and the ServiceDesk within 2 hours of such occurrence or discovery so that appropriate steps can be taken to remove the County's data from that device. The department head or elected official is responsible for immediately notifying the Service Desk with regards to the termination of employment so that appropriate steps can be taken to remove the County's data from privately owned mobile devices.

(f) All Users are advised that if a User chooses to use their privately owned mobile device to conduct official County business, they become a temporary custodian of the public information received, created, or maintained on their privately owned mobile device for purposes of compliance with the Texas Public Information Act. All Users using their privately owned mobile devices and are not using a separate County owned phone number to conduct official County business are required to:

(1) forward all public information in whatever form to the Public Information Officer for Dallas County or their elected official, or

(2) preserve all the public information on their privately owned mobile device for the applicable records retention period under Texas law; and

(3) provide all public information relating to official County business in whatever form maintained on their privately owned mobile device to the Public Information Officer for Dallas County or their elected official upon request for the County to comply with the Texas Public Information Act.

(4) any County data stored on the device classified as "protected" or "confidential" must be encrypted.

(g) If a User chooses to use their privately owned mobile device and separate County owned phone number to conduct official County business, they are required to inform all other

employees and persons with whom they conduct official County business of the new County owned telephone number to be used for conducting official County business and shall have an ongoing duty to forward any communications received on their privately owned mobile device or telephone number to the County owned phone number.

(h) All Users are advised to create a separate account for Apple ID or Google Cloud to be used with Dallas County credentials. Official County business shall not be combined with personal Apple ID or Google Cloud accounts.

(i) Users who fail to comply with this Policy, Texas Senate Bill 944, 86th Legislature, Regular Session 2019, and subsection (f) above may be subject to disciplinary action up to and including termination, monetary fines, and/or potential civil or criminal liability pursuant to the Texas Public Information Act.

Mobile Operating Systems

Android and Apple mobile operating systems are the only operating systems that will be permitted to connect to the Dallas County network and services. Operating systems from both platforms (Android and Apple) are expected to be kept up-to-date and free of vulnerabilities that would make Dallas County non-compliant or put the network at risk. Supported mobile devices will not have an operating system that is more the 2 revisions behind the most currently supported version of the operating system by the vendor. Mobile operating systems that are rooted or jailbroken will not be permitted to connect to Dallas County resources.

Access Control

County Issued Mobile Devices attempting to connect to the Dallas County network will automatically be enrolled in the mobile device management platform used by Information Technology Services before initial use. Enrollment requires the installation of a software client on the mobile device that will permit the Information Technology Services Department to remove Dallas County information stored on the device in the event the device is lost, stolen or misplaced, irreparably damaged, or otherwise compromised. Access to the Dallas County network or to offsite services such as Microsoft Outlook Online and Office 365 will be governed by the mobile device management platform.

Privately Owned Mobile Devices attempting to connect to the Dallas County network or to offsite services such as Microsoft Outlook Online or Office 365 will not be permitted to connect without a waiver. Users of privately owned mobile devices will be asked to sign a mobile device waiver if they wish to have the mobile device management software client installed on their device. Access to the County's network and services will not be authorized without the mobile device waiver and a proper installation of the mobile device management software client.

County Issued or Privately Owned Mobile Devices traveling abroad must seek authorization prior to accessing confidential County data abroad. The device must be inspected by IT Operations prior to going and then after return from abroad, to ensure that all controls are in place and functioning properly in accordance with this and other data protection policies and procedures.

Security

The mobile device management software client will enable the following security safeguards on County Issued or Privately Owned Mobile devices:

- Remote device accessibility – Unconditional for both DC and BYOD devices.
- Ability to locate the device - Unconditional for County Issued – Upon request by employee (when the device is lost or event such as termination or any security incident.
- Remote locking - Unconditional for County Issued – Upon request by employee when the device is lost or event such as termination or any security incident.
- Remote wipe encrypted container - Unconditional for County Issued – Upon request by the employee when the device is lost or events such as termination or any security incident.
- Auto screen lock + password - Unconditional for County Issued – Upon request by the employee when the device is lost or events such as termination or any security incident.
- Jailbreak and root detection - Unconditional for both DC and BYOD devices.
- Container encryption (at rest) - Unconditional for both DC and BYOD devices.
- Encryption in transit (cell or Wi-Fi) - Unconditional for both DC and BYOD devices.
- Malicious software detection – Unconditional for both DC and BYOD.
- Automated application patching - Unconditional for both DC and BYOD.
- Block non-compliant OS versions – Unconditional for DC. Do not allow DC n/w access for BYOD.
- Disallow copy and paste – Unconditional for DC devices and Limited to DC applications such as Outlook etc. for BYOD.
- Disallow screen capture - Unconditional for DC devices and Limited to DC applications such as Outlook, etc. for BYOD.
- Disallow printing Unconditional for DC devices and Limited to DC applications such as Outlook etc. for BYOD.
- Users issued County-owned mobile phone are required to back up their data, a minimum of once a week.
- Every 90 days, all the county-issued mobile devices are required to change the passcode and must do so when prompted.
- Users are prohibited from downloading and installing unapproved and unauthorized software applications on County-owned mobile devices.

In the event of a lost, stolen or misplaced, irreparably damaged or otherwise compromised mobile device the User is required to notify their supervisor, manager, department head or elected official and the ServiceDesk within 2 hours of such occurrence or discovery to report the incident. The County issued mobile device or County owned phone number/app will be remotely wiped of all Dallas County data to prevent unauthorized access*. The remote wipe will not destroy or alter any personal data on the privately owned mobile device*. If the device is recovered, it can be submitted for re-enrollment.

Audit Protocol

The Dallas County Office of Information Technology will be authorized to establish audit trails, which will be accessed and used without notice to the Users.

The audit trail logs will track the attachment of an external device to the County network, and the resulting reports may be used for investigation of possible breaches and/or misuse. Additionally, the audit logs will record dates, times, duration of access and the IP address of the device in order to identify unusual usage patterns or other suspicious activity.

Users agree to immediately report to his/her supervisor, manager, department head, or elected official and the Service Desk **any incident or suspected incident of unauthorized data access**, data loss, and/or disclosure of Dallas County data.

Prohibited Activities and No Expectation of Privacy
There is no expectation of privacy for any employee or user using County-owned devices, or when accessing the County's network or data from a BYOD. Mobile device access is a privilege. Transmission and viewing of any material in violation of any federal or state regulation is strictly prohibited. This includes, but is not limited to, plagiarizing copyrighted material, threatening or obscene materials, or materials protected by trade secret or that are classified government information. Moreover, the viewing, transfer, solicitation, use or storage of pornography or other sexually harassing information is strictly prohibited except in the pursuit of bona fide law enforcement or Human Resources investigations. Initiation of electronic mail and the Internet for commercial ventures, religious or political causes or other non-County sanctioned activities is also prohibited.

4. Periodic Reviews

This policy will be reviewed and updated on an annual basis.

5. Enforcement and Exception Handling

All the Users must follow the Dallas County Code of Conduct for Mobile Devices. Failure to comply with the Criminal Justice Information Policy (CJIS), Dallas County Code, and Dallas County Security Policies can result in a loss of access and/or disciplinary actions, up to and including termination of employment, contracts and/or other relationships. Additional legal actions may also be taken in response to violations of applicable regulations and laws.

Requests for exceptions to Dallas County security policies should be submitted to the ServiceDesk and routed to the Security Team. Exceptions will be permitted only upon receipt of written approval from the Dallas County CIO, with deference to the security processes as determined by the Compliance Committee.

6. References

NIST SP 800-53 Revision 4 - Moderate Baseline Control Objectives
FBI Criminal Justice Information Services (CJIS) Version 5.9
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended
Payment Card Industry-Data Security Standard Version 3.2.1
Dallas County - Information Technology Security Policy
Dallas County Code

7. Revision History

Date:	***version #:***	***Description:***	***Updated by:***
06/07/21	1.0	Initial Draft	Security Team
07/21/22	1.1	Adds BYOD Attestation for CellTrust/SL2 Project, revises context to include BYOD, updates MDMP requirements, revisits references to Sec. 174-136, and other minor updates to verbiage.	Sheila Campbell, PM
04/05/2023	1.2	Additions from the Dallas County Code	Security Team
4/19/2023	1.3	Policy review and changes	Chief Privacy Officer
8/29/23	1.4	Updates and changes	Chief Privacy Officer