Title: Mobile Device Management Policy
Effective Date: February 17, 2026
Amended:
Issuing Authority: Board of Commissioners
Responsible Officer: Director of Information Technology

Category: 500
Number: 504

Purpose

The purpose of this policy is to establish guidelines for the secure use and management of County owned mobile devices, including smartphones, tablets, and other portable devices, that access County resources. This policy ensures the protection of County data, compliance with security standards, and appropriate use of mobile devices.

Responsibility

County of Saginaw Information Technology (COSIT) is responsible for all Mobile Device Management (MDM) functions. All mobile devices must be configured by COSIT prior to their issuance.

Scope

This policy applies to all County of Saginaw Elected Officials, Judges, employees, contractors, third-party vendors, or anyone else who has access to or uses County mobile devices.

Policy

Enrollment

- All County owned mobile devices must be enrolled in the company's MDM solution.
- Devices not enrolled in MDM will not be granted access to company systems.

Security Requirements

- A passcode/PIN must be enabled on all devices.
- Use of encryption on all devices is mandatory (iPhones & Pixel devices use encryption by default).
- COSIT reserves the right to enforce security settings remotely through MDM.
- Jailbroken or rooted devices are strictly prohibited.

Access Control

- Access to County data via mobile devices is limited to approved applications deployed to mobile devices by COSIT.
- County, ePHI, PII, or CJI data must never be stored in unapproved third-party applications or cloud services.
- Lost or stolen devices must be reported to COSIT & Department Head immediately.

Monitoring and Management

- Requests to have applications remotely installed or removed from a county device can be made through the COSIT Service Desk.
- The MDM platform will monitor device compliance, including operating system version, installed applications, and security settings.
- COSIT will remotely wipe a county device in cases of loss, theft, or termination of employment.
- Users shall not attempt to disable or circumvent County MDM controls.

County Administrator / Legal Counsel Review

The County Administrator has determined that this Policy, as submitted to the Board of Commissioners, contains the necessary substance in order to carry out the purpose of the policy. County Civil Counsel has determined that this Policy, as submitted, contains content that appears to be legal activities of the Saginaw County Board of Commissioners.

Approved as to Substance:
Saginaw County Administrator

Approved as to Legal Content:
Saginaw County Civil Counsel

Definitions

Criminal Justice Information (CJI) refers to all data collected, stored, transmitted, or exchanged by criminal justice agencies that is necessary for the administration of criminal justice.

ePHI or PHI are any of 18 HIPAA identifiers used in conjunction with a person's physical or mental health condition, health care, or a person's payment for health care, which can be stored on paper or electronically.

Jailbroken or rooted refers to a mobile device that has been modified to remove the manufacturer's built-in restrictions and security controls. Jailbreaking gives the user elevated or "root" access to the operating system, allowing them to install unauthorized applications, change system files, and bypass security protections.

Mobile Device(s) are portable, electronic computing equipment designed to support wireless communication, data processing, and application functionality. Mobile devices typically operate on battery power, utilize cellular and/or wireless networks for connectivity, and may include features such as touchscreens, cameras, sensors, and integrated storage.

Mobile Device Management (MDM) is a type of security and administrative technology used by organizations to monitor, manage, and secure employees' mobile devices—such as smartphones, tablets, and laptops—that access corporate systems and data.

PII is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.