WOODBURY COUNTY BOARD OF SUPERVISORS AGENDA ITEM(S) REQUEST FORM

Date: 05/08/2025 Weekly Agenda Date: 05/20/2025

ELECTED OFFICIAL / DEPARTMENT HEAD / CITIZEN: Melissa Thomas HR Director

WORDING FOR AGENDA ITEM:

Approval of the Mobile Device Management Policy

ACTION REQUIRED:

Approve Ordinance ☐	Approve Resolution ☐	Approve Motion ☑
Public Hearing ☐	Other: Informational ☐	Attachments ☑

EXECUTIVE SUMMARY:

The Mobile Device Management Policy ensures the secure use of mobile devices within the organization, and provides guidelines for mobile device use when accessing County data.

BACKGROUND:

County data may be accessed on county issued devices or authorized personally owned devices. The device accessing the data must be enrolled in the Mobile Application Management (MAM), which is installed by WCICC. Staff with personally owned devices must sign a Personal Smartphone Usage Waiver and follow the other requirements of this policy (see attached).

FINANCIAL IMPACT:

$0

IF THERE IS A CONTRACT INVOLVED IN THE AGENDA ITEM, HAS THE CONTRACT BEEN SUBMITTED AT LEAST ONE WEEK PRIOR AND ANSWERED WITH A REVIEW BY THE COUNTY ATTORNEY'S OFFICE?

Yes ☐ **No** ☐

RECOMMENDATION:

Approve the Mobile Device Management Policy

ACTION REQUIRED / PROPOSED MOTION:

Motion to approve the Mobile Device Management Policy

Approved by Board of Supervisors April 5, 2016.

Mobile Device Management Policy

Purpose

The Mobile Device Management Policy is to ensure the secure use of mobile devices within the organization. This IT policy provides guidelines for managing mobile devices that access Woodbury County resources.

Scope

This policy applies to all employees who use mobile devices to access Woodbury County systems, networks and data. Mobile devices include, but are not limited to:

- Organization-issued mobile devices.
- Personally owned devices authorized to access County resources.

Policy

All organization-issued mobile devices accessing County organizational data must be enrolled in the Mobile Application Management (MAM) solution.

All employees approved to use their personal use mobile device and accessing County organizational data must be enrolled in the Mobile Application Management (MAM) solution.

If an eligible Employee requests to access organizational data from their personal-use smartphone, they must sign the Personal Smartphone Usage Waiver. The waiver can be found on the Employee Portal or by contacting IT. Only after completing the Personal Smartphone Usage Waiver may an employee request IT to setup MAM on their smartphone device.

If an Employee has not been issued a business smartphone or has not been given permission by their department supervisor, organizational data is not allowed to be accessed from their device.

The Employee is responsible for notifying IT when they are replacing their personal use smart device that has access to organizational data.

If a smartphone device with organizational data access is lost or stolen, it is the user's responsibility to promptly report this event to their direct supervisor and the IT Security Team.

If an Employee leaves employment, and the Employee had access to organizational data on their personal smartphone the employee's direct supervisor is responsible for reporting to IT.

Mobile devices must be configured to enforce strong passcodes and inactivity timeouts.

Jailbroken or rooted devices are prohibited from accessing organizational systems.

Personal data on MAM devices will remain private, while organizational data and apps will be managed separately through containerization.

Policy Compliance

When an end-user is found in violation of this policy, access to organizational resources is revoked and the end-user's supervisor is notified.

Exceptions

Any exception to the policy must be approved by the IT Security Coordinator or designee in advance.

Definitions and Terms

Mobile App Management – MAM

A platform that secures and enables IT control for enterprise applications on end users' personal mobile devices. MAM allows IT administrators to apply and enforce corporate policies on enterprise applications only, leaving the users personal apps and data untouched.

IT Security Team

The IT Security Team consists of the IT Security Coordinator and other IT employees. Members of the IT Security Team collaborate to manage security for the IT aspects of network resources. Contact the IT Helpdesk for a member of the IT Security Team.

Organizational Data

Includes but is not limited to; Microsoft 365 data, Outlook items, OneDrive and SharePoint files, Teams data, GIS maps, images, any data that is used for County business.

Revision History

Date of Change	Responsible	Summary of Change
1/21/2025	Chandra Chase	Creation
4/9/2025	Chandra Chase	Revision