OKLAHOMA COUNTY

BRING YOUR OWN DEVICE POLICY

Information Technology Operations

Aligned with CJIS Security Policy | NIST SP 800-53 | CIS Controls v8

Document ID:	IT-POL-BYOD-001
Version:	1.0
Effective Date:	[Date of BOCC Resolution]
Last Reviewed:	[Date]
Classification:	Internal Use
Document Owner:	Director of MIS
Approved By:	Board of County Commissioners — Resolution No. [____]

CONFIDENTIAL — FOR OFFICIAL USE ONLY

Table of Contents

1. Purpose

This Bring Your Own Device (BYOD) Policy establishes the requirements, responsibilities, and security controls governing the use of personally owned devices to access Oklahoma County information systems, networks, and data.

This policy is adopted under the authority of the Oklahoma County Information Technology Governance Charter (IT-GOV-CHARTER-001), as approved by the Board of County Commissioners. It is binding on all County Offices, departments, and agencies as defined in the Governance Charter.

This policy expands the BYOD provisions in the Acceptable Use Policy (IT-POL-AUP-001, Section 11) into a comprehensive standalone policy. BYOD access is a privilege, not a right, and may be revoked at any time by MIS or the user's department head.

> ***Framework Alignment:*** *NIST SP 800-53: AC-20 (Use of External Systems), MP-7 (Media Use) | NIST SP 800-124 Rev. 2 (Guidelines for Managing the Security of Mobile Devices) | CIS Controls 1.2, 1.4 | CJIS Security Policy 5.13*

2. Scope

2.1 Covered Devices

This policy applies to all personally owned devices used to access any Oklahoma County system, network, data, or service, including but not limited to:

- Smartphones (iOS, Android,)
- Tablets (iPad, Android tablets, Windows personal devices)
- Laptops and personal computers (Windows, macOS, Linux, ChromeOS, etc.)
- Smartwatches and wearable devices that receive County notifications or data

2.2 Covered Access

This policy applies whenever a personal device is used to:

- Access County email (Outlook, Exchange Online) or collaboration tools (Teams, SharePoint, OneDrive)
- Connect to the County network via VPN
- Access County cloud services (Microsoft 365, Azure-hosted applications)
- Access any County application or portal that contains Internal Use, Confidential, or Restricted data
- Receive County push notifications, calendar invitations, or voicemail

2.3 Organizational Scope

This policy applies to all personnel covered by the Acceptable Use Policy, across all County Offices, including employees, contractors, and vendors of departments with independent IT operations.

3. Definitions

Term	Definition
BYOD	Bring Your Own Device — a personally owned device used to access County systems or data.
MDM	Mobile Device Management — the County-approved platform used to manage, secure, and monitor devices that access County resources.
MAM	Mobile Application Management — management of County applications and data on a device without full device management. Allows a managed container for County data while leaving personal data untouched.
Managed Container	A secured, encrypted partition or application set on a personal device that separates County data from personal data. County data within the container can be remotely wiped without affecting personal content.
Remote Wipe	The ability to remotely erase County data (container wipe) or all data (full wipe) from a device.
Jailbroken / Rooted	A device whose manufacturer security controls have been bypassed, disabled, or modified, making it ineligible for BYOD enrollment.

4. BYOD Enrollment

4.1 Enrollment Process

All personal devices must be enrolled with MIS before accessing any County system. The enrollment process is:

1. The user submits a BYOD Enrollment Request through MIS' ITSM Platform, specifying the device type, operating system version, and intended use
2. The user's supervisor approves the request, confirming a legitimate business need for BYOD access
3. MIS verifies the device meets the minimum requirements (Section 5).
4. The user reviews and signs the BYOD User Agreement (Appendix A) acknowledging the terms of this policy
5. MIS configures the managed application or device workspace using the MDM/MAM solution.
6. The device is registered in the County asset inventory as a BYOD device

4.2 Enrollment Denial

MIS may deny BYOD enrollment if:

- The device does not meet minimum requirements (Section 5)
- The device is jailbroken, rooted, or has tampered security controls
- The device is running an unsupported operating system
- The user declines to accept the BYOD User Agreement
- The user's role does not require mobile access to County systems

4.3 Device Changes

When a user replaces their personal device, they must:

- Notify MIS and unenroll the old device before enrolling the new one
- Ensure County data has been removed from the old device (MIS will perform a container wipe during unenrollment)
- Complete the enrollment process for the new device

Framework Alignment: *NIST SP 800-124: Section 4 (Mobile Device Management Technologies) | CIS Controls 1.2, 1.4*

5. Minimum Device Requirements

Personal devices must meet the following minimum standards to be eligible for BYOD enrollment:

Requirement	Standard	Notes
Operating system	Current or previous major version (e.g., iOS 18/26, Android 14/15, Windows 11, macOS 15/26)	Devices more than two major versions behind are ineligible
Security patches	All available OS security patches applied	Device must be current at enrollment and remain current
Device lock	PIN (minimum 6 digits), password, or biometric (fingerprint, face recognition) enabled	Pattern locks are not accepted
Auto-lock timeout	5 minutes maximum	Enforced by MDM policy
Encryption	Full-device encryption enabled	Default on modern iOS; must be verified on Android and laptops
Jailbreak / root status	Not jailbroken or rooted	MDM detects jailbreak/root; device will be blocked automatically
MDM/MAM enrollment	County-approved MDM/MAM agent installed and active	Required for all enrolled devices
Personal firewall	Enabled (laptops/desktops only)	Built-in OS firewall must be active
Antivirus/anti-malware	Active and current (laptops/desktops only)	Windows Defender or approved equivalent for Windows/macOS laptops

MIS reserves the right to update minimum device requirements as threats evolve and new OS versions are released. Updates to minimum requirements are communicated at least 30 days before enforcement.

6. Security Controls

6.1 Managed Container

The County's BYOD program uses a managed container approach (MAM) where technically feasible. This model:

- Creates a secured, encrypted container on the personal device for all County applications and data
- Separates County data from personal data — MIS does not access, monitor, or manage personal content outside the container
- Allows MIS to remotely wipe the County container without affecting personal photos, apps, or data
- Enforces encryption, copy/paste restrictions, and data sharing controls within the container

Privacy commitment: MIS does not monitor personal calls, texts, browsing, photos, personal email, or app usage on BYOD devices. MDM/MAM visibility is limited to: device OS version, encryption status, jailbreak status, MDM compliance state, and the County-managed container. MIS cannot read personal data.

6.2 Network Access

- BYOD devices access County resources through cloud services (Microsoft 365) — not by connecting directly to the internal County network or with VPN
- Personal devices must not be connected to County internal wired or wireless networks designated for County-managed devices
- A dedicated BYOD wireless SSID may be provided where available, segmented from the internal production network
- All remote access from BYOD devices requires MFA per the Password and Access Management Policy

6.3 Data Protection

- County data must remain within the managed container and approved County applications
- Users must not copy, forward, or transfer County data from managed applications to personal applications, personal email, personal cloud storage, or unmanaged apps
- Screenshots or screen recordings of Confidential or Restricted data on personal devices are prohibited
- County documents downloaded for offline access within managed apps must remain encrypted within the container
- Printing County data from personal devices requires the same handling protections as printing from County devices (per the Data Classification and Handling Policy)

6.4 Application Controls

- Only County-approved applications provisioned through the managed container may be used to access County data
- Users must not configure personal email clients, personal browsers, or unapproved apps to access County email, SharePoint, or other County services
- MIS publishes the list of approved BYOD applications and updates it as needed

6.5 Prohibited Data Types for BYOD

- Unless explicitly approved, the following data types are prohibited from BYOD devices.
- Records covered by CJIS requirements
- Records covered by HIPAA requirements

- Records covered by PCI requirements
- Classified and Restricted records covered by the Data Classification and Handling Policy
- Sealed court documents
- Evidence files or media
- Network diagrams or administrative credentials.

Framework Alignment: *NIST SP 800-53: AC-19 (Access Control for Mobile Devices), AC-20, SC-7, SC-13, SC-28 | CIS Controls 3.6, 3.10, 12.6*

7. CJI and Restricted Data

Personal devices must not be used to access, store, process, or transmit Criminal Justice Information (CJI) unless they meet ALL CJIS mobile device requirements and are explicitly approved by the LASO. As a general rule, CJI access is restricted to County-managed devices.

7.1 CJIS BYOD Requirements (If Authorized by LASO)

- The device must meet all minimum requirements in Section 5 PLUS all CJIS mobile device requirements per CJIS Security Policy 5.13
- Full device encryption must use a FIPS 140-3 validated cryptographic module
- Advanced authentication (MFA) must be enforced for all CJI access
- Full remote wipe capability (not just container wipe) must be enabled and tested
- The device must be capable of being remotely wiped within 24 hours of being reported lost or stolen
- The LASO must specifically authorize each device for CJI access in writing

7.2 Restricted Data (Non-CJI)

Access to other Restricted data (as classified in IT-POL-DCH-001) from personal devices requires:

- MIS Operations Manager approval in addition to supervisor approval
- Full MDM enrollment (not MAM-only) with remote wipe capability
- Enhanced logging of access events
- Quarterly review of continued access need

Framework Alignment: *CJIS Security Policy 5.13 (Mobile Devices) | NIST SP 800-53: AC-19, SC-13, MP-5*

CJIS	CJIS Security Policy 5.13: Mobile devices used to access, store, or transmit CJI must employ advanced authentication, FIPS 140-3 encryption, remote wipe capability, and meet all CJIS mobile device security requirements. The LASO must authorize all mobile device access to CJI.

8. User Responsibilities

- Keep the device's operating system and security patches current at all times — devices that fall out of compliance will be blocked from accessing County resources automatically
- Maintain a working device lock (PIN, password, or biometric) at all times
- Do not disable, circumvent, or uninstall the MDM/MAM agent or managed container
- Do not jailbreak, root, or otherwise modify the device's security controls
- Report a lost or stolen device to MIS immediately — within 1 hour during business hours, within 4 hours after hours
- Do not allow other individuals (family members, friends) to use the device while it is connected to County resources or while the managed container is unlocked
- Do not use the device for County business while the device is connected to untrusted or public Wi-Fi networks
- Cooperate with MIS on remote wipe if the device is lost, stolen, or compromised
- Comply with all provisions of the Acceptable Use Policy, Data Classification and Handling Policy, Password and Access Management Policy, and any other applicable policy when using a personal device for County business

9. MIS Responsibilities

- Provide a clear and efficient BYOD enrollment process
- Communicate minimum device requirements and any changes with adequate notice (minimum 30 days)
- Limit MDM/MAM visibility to the minimum necessary for security compliance — MIS does not monitor personal content
- Provide technical support for the managed container and County applications on enrolled devices
- Execute container wipes promptly upon device unenrollment, employee separation, or security incident
- Maintain the approved BYOD application list and communicate updates to enrolled users
- Conduct quarterly compliance checks on enrolled devices and notify users of non-compliance

10. Lost, Stolen, or Compromised Devices

10.1 Reporting

Users must report a lost, stolen, or potentially compromised device to MIS immediately:

- **Business Hours - Contact MIS helpdesk by phone or in person — within 1 hour**
- **After-Hours - Contact the on-call engineer — within 4 hours**
- **If CJI Access was provisioned - Report immediately, regardless of time — the LASO must also be notified**

10.2 MIS Response

7. MIS initiates a remote container wipe (or full wipe if CJI-authorized or full MDM enrolled) immediately upon notification
8. MIS disables the device's access to County resources (Conditional Access block, MDM compliance flag)
9. If the device had access to Confidential or Restricted data, the Senior Security Analyst assesses potential data exposure
10. If data exposure is confirmed or suspected, the incident is escalated per the Incident Response Plan
11. If the device is recovered, MIS verifies its integrity before re-enrolling it

10.3 User Cooperation

By enrolling in the BYOD program, the user acknowledges and consents to:

- Remote container wipe of County data at any time, without prior notice, if MIS determines it is necessary to protect County data
- Full device wipe ONLY if the device was enrolled under full MDM (CJI or Restricted data access) AND the device is confirmed lost or stolen — full wipe requires MIS Operations Manager authorization except in CJI emergencies

MIS will always attempt a container-only wipe first. Full device wipe is a last resort and is only performed when the device is enrolled under full MDM, the device is confirmed lost/stolen, and the risk to County data justifies it. MIS will communicate with the user before a full wipe whenever possible.

11. Separation and Offboarding

When a BYOD user separates from County employment or their BYOD access is revoked:

12. MIS performs a container wipe to remove all County data and applications from the personal device
13. The device is unenrolled from MDM/MAM
14. The user's access to County resources (VPN, M365, cloud apps) is revoked per the account deprovisioning process
15. The user confirms that no County data remains on the device
16. The device is removed from the County asset inventory

Users who are involuntarily separated have their BYOD access revoked and container wiped simultaneously with their account deprovisioning — within 4 hours of notification per the Password and Access Management Policy.

12. Enforcement

12.1 Non-Compliance

Devices that fall out of compliance with this policy are automatically blocked from accessing County resources by the MDM/MAM platform. Common compliance failures include:

- OS version or security patches out of date beyond the grace period
- Device lock disabled or weakened below minimum requirements
- Jailbreak or root detected
- MDM/MAM agent uninstalled or tampered with

Users are notified of non-compliance and given 7 calendar days to remediate. If remediation does not occur, the device is unenrolled and a container wipe is performed.

12.2 Policy Violations

Violations of this policy are subject to the enforcement provisions of the Acceptable Use Policy (IT-POL-AUP-001). Examples of violations include:

- Accessing County resources from a non-enrolled personal device
- Transferring County data outside the managed container to personal apps or storage
- Failing to report a lost or stolen device within the required timeframe
- Allowing unauthorized individuals to access County resources through the enrolled device
- Accessing CJI from a personal device without LASO authorization

Violations involving Confidential or Restricted data are treated as serious violations per the AUP enforcement matrix.

13. Policy Administration

This policy is reviewed at least annually by MIS and the IT Council. Amendments follow the IT Governance Charter (Section 8) and require BOCC approval. MIS may update the minimum device requirements, approved application list, and MDM/MAM configuration standards without BOCC action, provided no substantive policy changes are involved.

14. Related Policies and Documents

Document	ID	Relationship
IT Governance Charter	IT-GOV-CHARTER-001	Authorizing framework
Acceptable Use Policy	IT-POL-AUP-001	Parent usage policy; BYOD Section 11 superseded by this policy
Data Classification and Handling Policy	IT-POL-DCH-001	Data handling requirements apply to BYOD
Password & Access Management Policy	IT-POL-PAM-001	MFA and authentication requirements for BYOD access
Information Security Policy	IT-POL-ISP-001	Parent security policy
Incident Response Plan	IT-POL-IRP-001	Governs response to incidents involving BYOD devices
IT Security Baseline Standard	IT-STD-SEC-001	Device hardening requirements

Document	ID	Relationship
FBI CJIS Security Policy	External	Mobile device requirements for CJI access
NIST SP 800-124 Rev. 2	External	Guidelines for managing security of mobile devices

Appendix A: BYOD User Agreement

I acknowledge that I have read, understand, and agree to the terms of the Oklahoma County Bring Your Own Device (BYOD) Policy (IT-POL-BYOD-001). By signing below, I agree to the following:

- My personal device will be enrolled in the County's MDM/MAM solution and must remain enrolled while I have BYOD access
- I will maintain my device's operating system, security patches, and device lock per the minimum requirements
- I will not jailbreak, root, or tamper with my device's security controls
- I will report a lost, stolen, or compromised device to MIS immediately per the timeframes in the policy
- County data on my device is County property and subject to remote wipe at any time MIS determines it necessary to protect County data
- I consent to container wipe (removal of County data and apps only) upon separation, policy violation, or security incident
- I consent to full device wipe ONLY if my device is enrolled under full MDM (CJI/Restricted data) AND the device is confirmed lost or stolen
- MIS does not monitor my personal content — MDM/MAM visibility is limited to device compliance status, OS version, encryption, and the managed container
- I will comply with all provisions of the Acceptable Use Policy, Data Classification and Handling Policy, Password and Access Management Policy, and any other applicable policies when using my personal device for County business
- I understand that BYOD access is a privilege that may be revoked at any time
- Violation of this policy may result in revocation of BYOD access, disciplinary action, and/or other consequences per the Acceptable Use Policy

Field	
Printed Name	
Department	
Device Type / Model	
Device OS	
Signature	
Date	
Supervisor Signature	
Supervisor Date	

This agreement is retained by MIS for the duration of the user's BYOD enrollment and for 1 year after unenrollment.