# Oklahoma County

## ACCEPTABLE USE POLICY

Information Technology Resources

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

| | |
|---|---|
| **Document ID:** | IT-POL-AUP-001 |
| **Version:** | 1.0 |
| **Effective Date:** | [Date] |
| **Last Reviewed:** | [Date] |
| **Classification:** | Internal Use |
| **Document Owner:** | Director of Information Technology |
| **Approved By:** | Board of County Commissioners — Resolution No. [____] |

**CONFIDENTIAL — FOR OFFICIAL USE ONLY**

# Table of Contents

# 1. Purpose

This Acceptable Use Policy (AUP) establishes rules and guidelines governing the use of Oklahoma County information technology resources. The purpose of this policy is to:

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.

- Protect the confidentiality, integrity, and availability of County information systems and data
- Define acceptable and prohibited behaviors when using County IT resources
- Ensure compliance with applicable federal, state, and local laws, regulations, and standards
- Establish a foundation for information security aligned with the CJIS Security Policy, NIST SP 800-53, and CIS Controls v8
- Reduce organizational risk arising from misuse or unauthorized use of County technology

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.

> ***Framework Alignment:*** *NIST SP 800-53: PL-4 (Rules of Behavior) | CIS Control 14 (Security Awareness and Skills Training)*

# 2. Scope

## 2.1 Applicability

This policy applies to all individuals who access, use, or interact with Oklahoma County information technology resources, including but not limited to:

- All County employees, whether full-time, part-time, temporary, or seasonal
- Contractors, consultants, vendors, and third-party service providers
- Volunteers and interns working in any County department or Office
- Elected officials and appointed board members using County IT resources
- Any individual granted access to County networks, systems, or data

**Multi-Department Scope:** This policy applies uniformly across all County Offices, including those with independent IT staff for any use of County IT resources or any system connected to the County core network managed by MIS. Departmental IT operations retain authority over Office-specific systems as defined in the IT Governance Charter, but all systems connected to shared infrastructure must comply with this policy.

## 2.2 Covered Resources

This policy covers all County-owned, leased, or managed information technology resources, including but not limited to:

- Desktop computers, laptops, tablets, and mobile devices
- Servers, network infrastructure, and telecommunications equipment
- Email systems, cloud services (including Microsoft 365 / Google Workspace), and collaboration platforms
- Internet and intranet access, VPN connections, and remote access solutions
- Shared workstations and public-facing kiosks
- Personally owned devices (BYOD) when used to access County systems or data
- Software, applications, databases, and electronic records
- Telephony systems including desk phones, mobile phones, and voicemail

***Framework Alignment:*** *NIST SP 800-53: PL-4, AC-20 (Use of External Systems) | CIS Control 1 (Inventory and Control of Enterprise Assets)*

**CJIS** Personnel accessing Criminal Justice Information (CJI) are subject to additional requirements defined in Section 14 of this policy, in accordance with the FBI CJIS Security Policy.

# 3. Definitions

| Term | Definition |
|---|---|
| Authorized User | Any individual who has been formally granted access to County IT resources through an approved process. |
| County IT Resources | All hardware, software, networks, data, and services owned, leased, or operated by Oklahoma County. |
| Criminal Justice Information (CJI) | All data provided by the FBI CJIS Division, including biometric data, identity history, person/property/organization records, and case/incident data. |
| BYOD | Bring Your Own Device — a personally owned device used to access County systems or data. |
| Privileged Access | Elevated system permissions beyond standard user access, including administrator, root, or domain admin rights. |
| Sensitive Data | Any information that requires protection due to legal, regulatory, contractual, or ethical obligations, including PII, CJI, HIPAA data, and financial records. |
| VPN | Virtual Private Network — an encrypted connection used to access the County network remotely. |
| MFA / 2FA | Multi-Factor Authentication / Two-Factor Authentication — requiring two or more verification methods for system access. |

# 4. General Acceptable Use

## 4.1 Authorized Use

County IT resources are provided for the purpose of conducting official County business. All users are expected to exercise sound judgment, act professionally, and use County resources responsibly. Users shall:

- Use IT resources primarily for authorized County business purposes

- Comply with all applicable federal, state, and local laws when using County systems
- Protect the confidentiality of information they access in the course of their duties
- Report any suspected security incidents, policy violations, or system compromises to the MIS department immediately
- Complete required security awareness training within 30 days of onboarding and annually thereafter

### 4.2 Personal Use

Oklahoma County permits limited, incidental personal use of IT resources, subject to the following conditions:

- Personal use must not interfere with job performance, County operations, or the productivity of others
- Personal use must not consume excessive network bandwidth, storage, or system resources
- Personal use must not involve any activity that would violate this policy, County policy, or applicable law
- Personal use must not create additional costs to the County beyond normal operational expenses
- Personal use of County IT resources does not create any expectation of privacy (see Section 12: Monitoring)

**Excessive personal use** is a violation of this policy. Examples include but are not limited to: streaming entertainment media during work hours, operating a personal business using County resources, extensive personal social media browsing, online shopping during business hours, or any personal use that degrades system performance for others.

***Framework Alignment:*** *NIST SP 800-53: PL-4 (Rules of Behavior), AC-2 (Account Management) | CIS Control 14.1*

## 5. Account and Password Management

### 5.1 Account Responsibilities

Each user is personally accountable for all activity performed under their assigned credentials. Users shall:

- Never share their username, password, PIN, security token, or any authentication credential with any other person, under any circumstance
- Never use another person’s credentials to access any system, even with their permission
- Lock their workstation or device when leaving it unattended, even briefly (Windows+L or equivalent)
- Log off or lock shared workstations and kiosks immediately after completing their session
- Notify MIS immediately if they suspect their credentials have been compromised

**Sharing credentials is a serious policy violation** and may result in disciplinary action up to and including termination. For personnel with access to CJI, credential sharing constitutes a CJIS Security Policy violation reportable to the Criminal Justice Agency.

### 5.2 Password Requirements

All passwords for County systems must meet the following minimum standards:

| Requirement | Standard |
|---|---|
| Minimum Length | 14 characters (20+ required for admins and service accounts) |
| Complexity | At least 3 of 4 character types: uppercase, lowercase, numbers, special characters |
| Password History | Cannot reuse last 24 passwords |
| Maximum Age | 90 days (No expiration if MFA is enforced) |
| Lockout Threshold | Account locks after 5 consecutive failed attempts |
| Lockout Duration | Minimum 30 minutes or until unlocked by IT |
| Multi-Factor Authentication | Required for: VPN, remote access, privileged accounts, cloud services, and all CJI systems |

***Framework Alignment:*** *NIST SP 800-53: IA-2, IA-5 | CIS Controls 5.2, 6.3, 6.4, 6.5 | CJIS Policy 5.6.2.1*

**CJIS** CJIS Security Policy 5.6.2.1 requires advanced authentication (MFA) for all users accessing CJI from any location. Password standards for CJI systems must meet or exceed the minimums in this section.

# 6. Email and Electronic Communications

## 6.1 Acceptable Email Use

County email accounts are provided for official business communications. Users shall:

- Use their County-assigned email address for all official business communications
- Not auto-forward County email to personal or external email accounts
- Not use County email to send or receive material that is obscene, harassing, discriminatory, threatening, or otherwise in violation of County personnel policies
- Not open suspicious attachments or click links in unsolicited emails — report suspected phishing to MIS immediately
- Not use County email to send sensitive or confidential data without appropriate encryption or approved secure file transfer methods

## 6.2 Messaging and Collaboration Platforms

Use of County-provided messaging and collaboration tools (e.g., Microsoft Teams, Slack, Google Chat) is subject to the same standards as email. Communications on these platforms:

- Are County records and may be subject to public records requests, e-discovery, or legal hold
- Must not include sensitive data unless the platform has been approved for that data classification
- Must remain professional and appropriate for a government workplace

***Framework Alignment:*** *NIST SP 800-53: SC-8 (Transmission Confidentiality and Integrity), AU-2 | CIS Control 9 (Email and Web Browser Protections)*

# 7. Internet and Web Usage

## 7.1 General Internet Use

Oklahoma County provides internet access to support County business functions. All internet activity conducted through County networks or devices is subject to monitoring and web content filtering. Users shall:

- Use internet access primarily for County business purposes
- Not attempt to bypass, disable, or circumvent web content filtering or monitoring systems
- Not access, download, or distribute material that is illegal, obscene, sexually explicit, hateful, or in violation of County harassment/discrimination policies
- Not use County internet access for unauthorized commercial activity, political campaigning, gambling, or cryptocurrency mining
- Not use County systems to engage in peer-to-peer file sharing or torrenting

## 7.2 Web Content Filtering

Oklahoma County employs web content filtering to protect the County network and ensure compliance with applicable policies and regulations. The web filtering system:

- Blocks categories of websites determined to be high-risk or inappropriate for a government work environment
- Logs all web traffic for security monitoring and investigation purposes
- May be configured differently for specific departments based on legitimate business needs

Requests for website exceptions must be submitted to MIS with a documented business justification and department head approval.

> ***Framework Alignment:*** *NIST SP 800-53: SC-7 (Boundary Protection), AU-2, SI-4 | CIS Controls 9.2, 9.3*

# 8. Social Media

## 8.1 Official Social Media Accounts

Only personnel specifically authorized by their department head or Elected Official may operate official County social media accounts. Official accounts must:

- Be registered using a County email address and managed through a County-approved platform
- Have at least two authorized administrators to prevent single points of failure
- Comply with all applicable records retention requirements

## 8.2 Personal Social Media Use

Users must exercise caution when using personal social media, particularly as it relates to their role as a County employee:

- County systems and work hours must not be used for personal social media activity beyond limited incidental use

- Users must not imply they are speaking on behalf of Oklahoma County unless specifically authorized to do so
- Users must not post confidential, sensitive, or non-public County information on any social media platform
- Users must not post information that could compromise an ongoing investigation, legal proceeding, or County operation
- Users must not post content that harasses, discriminates against, or threatens other County employees or members of the public

**Misuse of social media** in a manner that reflects negatively on Oklahoma County, discloses sensitive information, or violates any provision of this policy may result in disciplinary action.

***Framework Alignment:*** *NIST SP 800-53: AC-22 (Publicly Accessible Content) | CIS Control 14*

# 9. Software and Hardware

## 9.1 Prohibited Software Activities

To protect the integrity and security of County systems, the following activities are strictly prohibited:

- Installing, downloading, or running any software that has not been approved by MIS
- Using portable applications or browser-based tools to circumvent software installation restrictions
- Installing personal software, games, or browser extensions on County devices
- Modifying, disabling, or tampering with any security software, including antivirus, endpoint detection, or encryption tools
- Using unauthorized remote access tools (e.g., TeamViewer, AnyDesk, personal VPN clients)
- Downloading or using pirated, unlicensed, or illegally obtained software

## 9.2 Hardware and Device Integrity

Users must not modify County-owned hardware or connect unauthorized devices to County systems:

- Do not connect personal USB drives, external hard drives, or portable storage devices to County computers without MIS approval
- Do not connect personal routers, switches, wireless access points, or any network equipment to the County network
- Do not open, modify, or repair County hardware — submit a service request to MIS
- Do not relocate or disconnect network infrastructure (cables, patch panels, switches) MIS coordination

**Connecting unauthorized devices to the County network** creates significant security risk and is a serious policy violation. Unauthorized devices will be disconnected immediately and may be confiscated for forensic analysis.

***Framework Alignment:*** *NIST SP 800-53: CM-7 (Least Functionality), CM-11 (User-Installed Software) | CIS Controls 2.3, 2.5, 2.6*

# 10. Bring Your Own Device (BYOD)

## 10.1 BYOD Authorization

Oklahoma County permits the use of personally owned devices to access certain County systems and data, subject to the following requirements. BYOD access is a privilege, not a right, and may be revoked at any time.

## 10.2 BYOD Requirements

All personal devices used to access County resources must:

- Be registered with MIS prior to use
- Have an active, supported operating system with all current security patches applied
- Have a device lock enabled (PIN, password, or biometric) with a maximum 5-minute auto-lock timeout
- Have full-disk or device-level encryption enabled
- Have the County-approved Mobile Device Management (MDM) solution installed as required by MIS
- Not be jailbroken, rooted, or have any security controls disabled

## 10.3 BYOD Restrictions

- County data must not be stored locally on personal devices unless the data is encrypted and the device is MDM-enrolled
- Users must not use personal devices to photograph, screenshot, or otherwise capture restricted or CJI data unless explicitly authorized
- MIS reserves the right to remotely wipe County data from a personal device if the device is lost, stolen, compromised, or the user separates from County employment
- Users accept that MIS may have limited visibility into personal device usage as part of MDM enrollment

***Framework Alignment:*** *NIST SP 800-53: AC-20 (Use of External Systems), MP-7 (Media Use) | CIS Controls 1.2, 1.4*

| | |
|---|---|
| **CJIS** | CJIS Security Policy 5.13 (Mobile Devices): Personal devices used to access, store, or transmit CJI must meet all CJIS mobile device requirements, including advanced authentication, encryption, and remote wipe capability. |

# 10. Artificial Intelligence and Generative AI

Artificial intelligence (AI) tools, including generative AI platforms, large language models (LLMs), AI-powered assistants, and machine learning services, present both opportunities and risks to County operations. This section establishes requirements for the acceptable use of AI technologies by all personnel covered under this policy.

## 10.1 Authorized AI Use

The use of AI tools in the course of County business must be authorized by MIS and the user's department head. Authorized use of AI tools is subject to the following requirements:

- Only AI platforms and tools that have been reviewed and approved by MIS may be used for County business purposes
- Users must not create accounts on or submit County data to unapproved AI platforms, including free or trial-tier services
- AI tools must be used as an aid to human judgment, not as a substitute for it — all AI-generated output must be reviewed, validated, and approved by a qualified human before being used in any official capacity
- Users are personally responsible for the accuracy, completeness, and appropriateness of any work product they submit or publish, regardless of whether AI tools were used in its creation
- The use of AI tools must not violate any other provision of this Acceptable Use Policy, including data handling, privacy, copyright, and records retention requirements

## 10.2 Prohibited AI Activities

The following activities involving AI tools are strictly prohibited:

- Entering, uploading, pasting, or otherwise submitting Confidential, Restricted, or Sensitive data into any AI tool that has not been explicitly approved by MIS for that data classification level
- Submitting Criminal Justice Information (CJI), law enforcement case data, personally identifiable information (PII), HIPAA-protected health information, or any other legally protected data into any generative AI platform
- Using AI tools to generate official County communications, legal documents, policy language, or public-facing content without supervisory review and approval prior to release
- Using AI tools to draft or fabricate evidence, reports, affidavits, or any document intended for use in legal, administrative, or investigative proceedings
- Using AI tools to impersonate individuals, generate deepfake images or audio, or create misleading or deceptive content
- Using AI tools to circumvent security controls, generate malicious code, or probe for system vulnerabilities
- Using AI tools to make automated decisions that affect individuals' rights, benefits, employment, or legal status without documented human oversight and approval
- Installing, running, or deploying AI models, agents, or automation scripts on County infrastructure without MIS authorization

**Submitting CJI or law enforcement data to any AI platform is a CJIS Security Policy violation** and may constitute a reportable security incident. The CJIS Security Policy does not currently authorize the use of generative AI platforms for processing, analyzing, or storing Criminal Justice Information.

## 10.3 Data Protection and AI

AI platforms often retain, log, or use submitted data for model training or improvement purposes. Users must understand and account for these risks:

- Assume that any data entered into an AI tool may be retained, logged, or used by the AI provider unless MIS has confirmed otherwise through vendor agreement review
- Data submitted to AI tools may be stored outside the County's control and may be subject to the AI provider's privacy policy, terms of service, and applicable jurisdiction — not the County's
- County data classification requirements (Section 16) apply to all data submitted to AI tools — treat AI input fields the same as any external system for data handling purposes
- MIS will evaluate AI platforms for data handling practices, retention policies, and compliance posture before approving them for County use
- Users must not submit data that combines individually non-sensitive data points in ways that could reveal Confidential or Restricted information when aggregated

***Framework Alignment:*** *NIST SP 800-53: AC-22 (Publicly Accessible Content), SA-4 (Acquisition Process), SI-12 (Information Management and Retention) | NIST AI 100-1 (AI Risk Management Framework) | CIS Controls 3.2, 3.7*

## 10.4 AI Output Accuracy and Accountability

AI-generated content may contain inaccuracies, fabrications (commonly known as "hallucinations"), bias, or outdated information. Users must:

- Verify all facts, citations, legal references, statistics, and technical claims generated by AI tools against authoritative sources before relying on them
- Not represent AI-generated content as their own original work in contexts where the use of AI would be material to the recipient's understanding (e.g., grant applications, sworn statements, expert testimony)
- Disclose the use of AI tools when required by applicable federal or state regulations, grant requirements, court rules, or County policy
- Understand that AI tools may reflect bias in their training data — AI-generated analyses or recommendations involving personnel decisions, benefits determinations, law enforcement, or public-facing services must receive additional scrutiny for fairness and equity

***Framework Alignment:*** *NIST AI 100-1: Map 1.5 (Impacts to Individuals), Measure 2.3 (AI Bias) | NIST SP 800-53: SI-5 (Security Alerts and Advisories)*

## 10.5 AI Governance and Approval

MIS is responsible for evaluating, approving, and maintaining a register of AI tools authorized for County use. The AI governance process includes:

- Departments requesting the use of a new AI tool must submit a request to MIS that includes the intended use case, the data types involved, and the anticipated business benefit
- MIS will conduct a risk assessment of each requested AI platform, evaluating data residency and retention, security posture, vendor terms of service, and compliance with County policy and applicable regulations
- Approved AI tools will be added to a maintained AI Tools Register, specifying authorized use cases, data classification limits, and any conditions of use
- The AI Tools Register will be reviewed at least semi-annually and updated as tools are added, removed, or as vendor terms change

- Departments must not enter into contracts, subscriptions, or licensing agreements for AI services without prior review and approval by MIS and, where applicable, the County procurement office

***Framework Alignment:*** *NIST SP 800-53: SA-4 (Acquisition Process), SA-9 (External System Services), PM-9 (Risk Management Strategy) | NIST AI 100-1: Govern 1.1, Govern 1.3 | CIS Control 2.3 (Authorized Software)*

# 11. Remote Access and VPN

## 11.1 Remote Access Requirements

Remote access to County systems is provided through the County VPN and approved remote access solutions. Users accessing County resources remotely must:

- Use only County-approved VPN or remote access solutions — personal VPN services must not be used to access County systems
- Authenticate using multi-factor authentication (MFA) for all remote connections
- Ensure that the device used for remote access meets minimum security standards (current OS patches, active antivirus, encryption enabled)
- Not allow family members or other unauthorized individuals to use a device while connected to the County network
- Ensure that remote work environments provide reasonable physical security — screens should not be visible to unauthorized individuals

## 11.2 VPN Usage

The County VPN provides encrypted access to internal County resources. VPN users must:

- Disconnect from the VPN when access to County resources is no longer needed
- Not use split-tunneling unless the configuration is approved by MIS
- Not use the VPN connection to route personal internet traffic through the County network

***Framework Alignment:*** *NIST SP 800-53: AC-17 (Remote Access), SC-10 (Network Disconnect), SC-12 | CIS Controls 3.10, 6.4*

| | |
|---|---|
| **CJIS** | CJIS Security Policy 5.5.6 (Remote Access): All remote access sessions involving CJI must be encrypted using FIPS 140-3 validated cryptographic modules and require advanced authentication. |

# 12. Monitoring, Logging, and Privacy

## 12.1 Monitoring Notice

**Oklahoma County reserves the right to monitor, log, audit, and inspect all use of County IT resources without prior notice.** Users should have no expectation of privacy when using County-owned systems, networks, or devices, or when accessing County systems from personal devices.

Monitoring may include but is not limited to:

- Web browsing history and content filtering logs
- Email content, metadata, attachments, and routing information
- File access, modification, and transfer activity
- Authentication events (successful and failed login attempts)
- Application and software usage
- Network traffic analysis and intrusion detection logs
- VPN connection logs and remote access session data
- Physical access logs for secure areas

### 12.2 Purpose of Monitoring

Monitoring is conducted for the following purposes:

- Protecting the security and integrity of County IT infrastructure
- Detecting and investigating security incidents, policy violations, and unauthorized access
- Ensuring compliance with this policy and applicable regulations
- Supporting legal, audit, compliance, and law enforcement inquiries
- Managing system performance and capacity

Monitoring data is retained in accordance with applicable records retention schedules and may be disclosed to law enforcement, legal counsel, or management as necessary.

> ***Framework Alignment:*** *NIST SP 800-53: AU-2 (Audit Events), AU-6 (Audit Review), SI-4 (Information System Monitoring) | CIS Controls 8.2, 8.5, 8.11*

| CJIS | CJIS Security Policy 5.4 (Auditing and Accountability): Systems processing CJI must generate audit logs that capture sufficient detail to reconstruct events, with logs reviewed at minimum weekly. |
|---|---|

## 13. Shared Workstations and Kiosks

Some County Offices and Departments use shared workstations or public-facing kiosks. Additional controls apply to these environments:

### 13.1 Shared Workstation Requirements

- Users must log in with their own credentials — shared or generic accounts are prohibited
- Users must log off completely when finished — do not simply lock the screen for the next user
- Do not save passwords, bookmarks, or personal files on shared workstations
- Do not change system settings, desktop configurations, or default browser settings on shared machines
- Report any shared workstation that appears to be malfunctioning, compromised, or displaying unexpected behavior

### 13.2 Kiosk-Specific Controls

- Kiosks are configured with restricted functionality and are intended for a specific purpose — do not attempt to access systems or websites outside the kiosk's intended function
- Do not connect personal devices to kiosks via USB, Bluetooth, or other interfaces
- Do not enter sensitive personal information into public-facing kiosks unless the kiosk is specifically designed and approved for that purpose

***Framework Alignment:*** *NIST SP 800-53: AC-11 (Device Lock), SC-10 (Network Disconnect) | CIS Controls 4.3, 6.2*

## 14. Criminal Justice Information Services (CJIS) — Additional Requirements

This section applies to all personnel who access, process, store, or transmit Criminal Justice Information (CJI) as defined by the FBI CJIS Security Policy. This includes personnel in law enforcement agencies and any County staff who support systems that process CJI.

**Note:** Requirements in this section supplement all other provisions of this policy. Where this section imposes a more restrictive standard than the general policy, the more restrictive standard applies.

### 14.1 CJIS Personnel Security

- All personnel with access to CJI must have a completed fingerprint-based background check on file prior to access being granted
- Background checks must be reviewed and renewed at a minimum every five (5) years
- All personnel must complete CJIS Security Awareness Training within three (3) months of initial access and annually thereafter
- Contractor or vendor personnel with unescorted access to CJI or CJI systems must sign a CJIS Security Addendum

### 14.2 CJIS Access Control

- Access to CJI is granted on a need-to-know and need-to-have basis, validated by the responsible Criminal Justice Agency (CJA)
- Advanced authentication (MFA) is required for all access to CJI, regardless of physical location
- Session inactivity timeout must not exceed 30 minutes for systems processing CJI
- Unsuccessful login attempts must lock the account after a maximum of 5 consecutive failures

### 14.3 CJIS Data Protection

- CJI must be encrypted in transit using a FIPS 140-3 validated cryptographic module (minimum 128-bit)

- CJI at rest on any device (including mobile devices, laptops, and removable media) must be encrypted using a FIPS 140-3 validated module
- CJI must not be transmitted via unencrypted email, personal email accounts, or unapproved messaging platforms
- CJI must not be stored on personally owned devices unless those devices meet all CJIS mobile device requirements and are approved by the County CJIS Local Agency Security Officer (LASO)
- Physical media containing CJI (printouts, USB drives, DVDs) must be stored in a physically secure location with controlled access and must be destroyed in accordance with CJIS media disposition standards

### 14.4 CJIS Incident Response

- Any suspected or confirmed security incident involving CJI must be reported to the County LASO and MIS within one (1) hour of discovery
- The LASO is responsible for reporting CJIS security incidents to the CJIS Systems Officer (CSO) within the timeframe specified by the State CJIS Systems Agency
- CJI security incidents must be documented, investigated, and retained in accordance with FBI CJIS Security Policy requirements

### 14.5 CJIS Media Disposition

- Electronic media previously containing CJI must be sanitized prior to disposal using methods approved by the FBI CJIS Security Policy (e.g., clearing, purging, or physical destruction)
- Hard copy CJI must be cross-cut shredded or incinerated
- Media sanitization records must be maintained for audit purposes

***Framework Alignment:*** *CJIS Security Policy v5.9.5: Sections 5.1–5.13 | NIST SP 800-53: MP-6 (Media Sanitization), SC-13 (Cryptographic Protection) | CIS Controls 3.6, 3.9*

## 15. Data Handling and Classification

### 15.1 Data Classification

Oklahoma County classifies data into the following categories. Users must handle information according to its classification:

| Classification | Description | Examples |
|---|---|---|
| Public | Information approved for unrestricted public release | Press releases, public meeting minutes, published budgets |
| Internal Use | Information intended for County employees only; not sensitive | Internal memos, org charts, general procedures |
| Confidential | Information requiring protection under law, regulation, or policy | PII, personnel records, financial account data, legal correspondence |
| Restricted | Highest sensitivity: significant harm if disclosed | CJI, law enforcement case files, HIPAA data, security configurations |

### 15.2 Data Handling Requirements

- Users must not transmit Confidential or Restricted data via unencrypted channels
- Confidential and Restricted data must not be stored on unauthorized cloud services, personal email, or personal storage devices
- Users must not access data beyond what is required for their role (principle of least privilege)
- Data leaving the County network (e.g., via email, cloud, removable media) must be protected according to its classification
- Users must follow all applicable records retention and disposition requirements

***Framework Alignment:*** *NIST SP 800-53: RA-2 (Security Categorization), MP-3 (Media Marking) | CIS Controls 3.2, 3.7, 3.10*

## 16. Prohibited Activities

The following activities are expressly prohibited on County IT resources. This list is not exhaustive; any activity that violates the spirit of this policy or applicable law is prohibited.

### 16.1 Security Violations

- Attempting to gain unauthorized access to any system, account, data, or network — regardless of whether the attempt is successful
- Performing network scanning, port scanning, vulnerability scanning, or penetration testing unless authorized by MIS in writing
- Capturing, intercepting, or monitoring network traffic (sniffing) without explicit authorization
- Introducing malware, ransomware, viruses, worms, keyloggers, or other malicious code
- Disabling, circumventing, or tampering with security controls, logging, antivirus, firewalls, or endpoint protection

### 16.2 Unauthorized Use

- Using County resources for personal financial gain, private business operations, or unauthorized commercial purposes
- Political campaigning, lobbying, or fundraising using County systems
- Gambling, cryptocurrency mining, or participation in illegal activities
- Harassment, discrimination, bullying, or threatening behavior through any County system
- Accessing, storing, or distributing pornographic, sexually explicit, or obscene material (law enforcement investigative use excepted, with documented authorization)

### 16.3 Data and System Integrity

- Unauthorized modification, deletion, or destruction of County data or records
- Exfiltrating, copying, or transmitting County data to unauthorized parties

- Concealing, falsifying, or tampering with audit logs or monitoring data
- Using anonymizing tools or proxies to disguise the origin or nature of network activity

***Framework Alignment:*** *NIST SP 800-53: AC-2, AU-9 (Protection of Audit Information), SI-4 | CIS Controls 8.1, 13.1*

# 17. Enforcement and Violations

## 17.1 Violation Consequences

Violations of this policy may result in one or more of the following actions, depending on the severity and nature of the violation:

| Severity | Examples | Potential Consequences |
|---|---|---|
| Minor | Incidental excessive personal use; first-time failure to lock workstation | Verbal warning; written documentation; mandatory retraining |
| Moderate | Unauthorized software installation; sharing credentials; repeated minor violations | Written reprimand; temporary access suspension; mandatory retraining |
| Serious | Unauthorized access to data; BYOD policy violation involving sensitive data; social media disclosure of confidential info | Suspension of access; formal disciplinary action; referral to HR |
| Critical | Intentional data exfiltration; introduction of malware; CJI security violation; illegal activity | Immediate access revocation; termination; referral to law enforcement; civil/criminal prosecution |

## 17.2 Investigation Authority

MIS, in coordination with County management, HR, and legal counsel, reserves the right to:

- Immediately suspend or revoke system access in response to a suspected or confirmed security incident
- Inspect any County-owned device, system, or account without prior notice
- Request forensic analysis of County devices as part of an investigation
- Refer matters to law enforcement when criminal activity is suspected

All investigations will be conducted in accordance with applicable County policies, labor agreements, and state and federal law.

**CJIS** CJIS Security Policy violations are reportable events. The LASO must notify the CSO/SIB of any CJIS policy violations, and affected access may be suspended pending investigation.

For non-compliance involving departmental IT operations, enforcement follows the escalation process defined in the IT Governance Charter (Section 9): notification, remediation period, IT Council deliberation, and Board

of County Commissioners action if necessary. MIS retains emergency disconnect authority for systems posing imminent risk to the County core network.

***Framework Alignment:*** *NIST SP 800-53: PL-4, IR-1 (Incident Response Policy), AU-6 | CIS Controls 17.1*

# 18. Policy Administration

## 18.1 Policy Review

This policy shall be reviewed and updated at a minimum annually, or more frequently in response to:

Policy reviews are coordinated by the Director of Information Technology and presented to the Oklahoma County IT Council for deliberation. Amendments to this policy follow the policy development process defined in the IT Governance Charter (Section 8) and require Board of County Commissioners approval by resolution.

- Significant changes in the County's IT environment or security posture
- Changes to applicable laws, regulations, or compliance frameworks (including CJIS Security Policy updates)
- Findings from security incidents, audits, or risk assessments
- Changes to organizational structure or staffing

## 18.2 Exception Requests

Requests for exceptions to any provision of this policy must be submitted in writing to the MIS Director and must include:

- The specific policy section for which an exception is requested
- A business justification explaining why the exception is necessary
- An assessment of the risk created by the exception
- Proposed compensating controls to mitigate that risk
- A defined expiration date for the exception

Exceptions must be approved by the MIS Director and, for exceptions affecting Restricted or CJI data, by the CJIS LASO. Approved exceptions must be documented and reviewed at each policy review cycle.

***Framework Alignment:*** *NIST SP 800-53: PL-1 (Security Planning Policy), PM-1 | CIS Control 15.1*

# 19. Related Policies and Standards

This Acceptable Use Policy operates in conjunction with the following documents (existing or planned):

| Document | Status | Relationship |
|---|---|---|
| IT Governance Charter | Pending | Authorizing framework for all County-wide IT policies; defines IT Council, |

| Document | Status | Relationship |
|---|---|---|
| | | policy adoption process, and enforcement authority |
| Information Security Policy | Pending | Parent policy establishing the County's security program |
| Change Management Policy | Pending | Governs changes to County IT systems |
| Incident Response Plan | Pending | Defines incident handling procedures |
| Password and Access Management Policy | Pending | Detailed authentication and access standards |
| Data Classification and Handling Policy | Planned | Expanded data classification framework |
| BYOD Policy | Planned | Detailed BYOD enrollment and management procedures |
| Records Retention Schedule | Existing | County records retention requirements |
| Oklahoma County Employee Handbook | Existing | County HR policies and disciplinary procedures |
| CJIS Security Policy (FBI) | External | Federal requirements for CJI handling |
| NIST SP 800-53 Rev. 5 | External | Federal security and privacy controls |
| CIS Controls v8 | External | Consensus security best practices |

## Acknowledgment of Acceptable Use Policy

By signing below, I acknowledge that I have received, read, and understand the Oklahoma County Acceptable Use Policy. I agree to comply with all provisions of this policy and understand that violations may result in disciplinary action, up to and including termination of employment or contract, and may result in civil or criminal penalties.

I understand that Oklahoma County reserves the right to monitor all use of County IT resources, and that I have no expectation of privacy when using County systems or when accessing County resources from personal devices.

I understand that this policy may be updated periodically and that I am responsible for reviewing and complying with the most current version.

**Printed Name:** _____ **Department:** _____

**Signature:** _____ **Date:** _____

**FOR CJIS-AUTHORIZED PERSONNEL ONLY:**

I further acknowledge that I have been briefed on the FBI CJIS Security Policy, understand the additional requirements for handling Criminal Justice Information (CJI), and agree to comply with all CJIS security provisions in addition to the requirements of this Acceptable Use Policy.

CJIS Acknowledgment Signature: _____ Date: _____