OKLAHOMA COUNTY

INFORMATION SECURITY POLICY

Information Technology Operations

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

Document ID:	IT-POL-ISP-001
Version:	1.0
Effective Date:	[Date of BOCC Resolution]
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 Information Security Policy establishes the overarching framework for protecting the confidentiality, integrity, and availability of Oklahoma County information assets. It defines the principles, objectives, and organizational responsibilities that govern all information security activities across the County.

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 serves as the parent document for all Oklahoma County IT security policies, standards, and guidelines. All subordinate security documents derive their authority from this policy and the IT Governance Charter.

> ***Framework Alignment:*** *NIST SP 800-53: PM-1 (Information Security Program Plan), PL-1 (Security Planning Policy) | CIS Control 15 | CJIS Security Policy 5.1*

2. Scope

2.1 Organizational Scope

This policy applies to all Oklahoma County Offices, departments, and agencies, including those with independent IT operations (County Clerk, Assessor, Sheriff's Office, Treasurer, Court Clerk), and all personnel who access, manage, or interact with County information assets. This includes employees, contractors, vendors, volunteers, elected officials, and any third party granted access to County systems.

2.2 Information Asset Scope

This policy covers all information assets owned, leased, managed, or processed by Oklahoma County, in any form:

- Electronic data stored on servers, workstations, mobile devices, cloud platforms, removable media, or backups
- Paper records containing sensitive or confidential information
- Information transmitted via email, messaging platforms, telephony, fax, or any other communication channel
- Systems and infrastructure that process, store, or transmit County information, including the County core network managed by MIS and all departmental systems connected to it

> ***Framework Alignment:*** *NIST SP 800-53: PM-1, RA-2 (Security Categorization) | CIS Controls 1, 2, 3*

3. Information Security Principles

Oklahoma County's information security program is built on the following foundational principles:

Principle	Description
Confidentiality	Information is accessible only to those authorized to have access, based on a legitimate need to know.
Integrity	Information is accurate, complete, and protected from unauthorized modification, whether accidental or intentional.
Availability	Information and systems are accessible and usable when needed by authorized users to perform their duties.
Accountability	All actions on County systems are attributable to an identified, authenticated individual. Shared and anonymous accounts are prohibited except where explicitly authorized and documented.
Least Privilege	Users and systems are granted the minimum level of access necessary to perform their authorized functions — no more, no less.
Defense in Depth	Security is implemented in multiple, overlapping layers so that the failure of any single control does not result in a complete security breach.
Compliance	The County's security posture meets or exceeds the requirements of all applicable federal, state, and local laws, regulations, and contractual obligations.

Framework Alignment: *NIST SP 800-53: Appendix A (Security Control Families) | CIS Controls v8 Overview | CJIS Security Policy 5.1*

4. Information Security Program

4.1 Program Objectives

The Oklahoma County Information Security Program is established to:

- Protect County information assets from unauthorized access, disclosure, modification, destruction, or disruption
- Ensure compliance with the FBI CJIS Security Policy, NIST SP 800-53, CIS Controls v8, HIPAA, and applicable state laws
- Establish a risk-based approach to information security investment and prioritization
- Build and maintain a security-aware workforce through training and awareness programs
- Provide a framework for incident detection, response, and recovery
- Enable the County to continue essential operations during and after a security event

4.2 Program Components

The Information Security Program consists of the following components, each supported by dedicated policies, standards, or procedures:

Component	Governing Document(s)	Status
Acceptable Use	Acceptable Use Policy (IT-POL-AUP-001)	Pending
Change Management	Change Management Policy (IT-POL-CHG-001)	Pending
Access Control & Authentication	Password and Access Management Policy (IT-POL-PAM-001)	Pending
Incident Response	Incident Response Plan (IT-POL-IRP-001)	Pending

Component	Governing Document(s)	Status
Risk Management	Risk Assessment Procedures (planned)	Planned
Vulnerability & Patch Management	Patch Management SOP (planned)	Planned
Data Classification & Handling	AUP Section 16; standalone policy planned	Partial
Business Continuity & Disaster Recovery	BC/DR Plan (planned)	Planned
Security Awareness & Training	Security Awareness Training Program	Pending
Physical Security	Physical Security Standards (planned)	Planned
Vendor & Third-Party Security	Third-Party Risk Management Standards (planned)	Planned

Framework Alignment: *NIST SP 800-53: PM-1, PM-2, PM-3, PM-9 (Risk Management Strategy) | CIS Control 15 | COBIT 2019: APO13*

5. Roles and Responsibilities

5.1 Board of County Commissioners

- Adopts County-wide IT security policies by resolution upon IT Council recommendation
- Allocates resources to support the information security program
- Receives annual security posture reports from the Director of IT

5.2 IT Council

- Reviews and recommends information security policies and standards
- Provides cross-departmental perspective on security priorities and resource allocation
- Monitors compliance posture across all County offices

5.3 Director of MIS

- Provides oversight is accountable for the overall security program
- Chairs the IT Council and presents security recommendations to the BOCC
- Ensures adequate resources are allocated to security operations
- Reports on the County’s security posture at least annually to the BOCC

5.4 MIS Operations Manager

- Manages day-to-day security operations within MIS
- Oversees implementation of security policies, standards, and controls on MIS-managed infrastructure
- Coordinates security incident response for shared infrastructure
- Manages the security team

5.5 Senior Security Analyst

- Serves as the primary subject matter expert for security architecture, policy, and compliance
- Conducts security assessments, vulnerability management, and compliance monitoring
- Reviews changes to security-relevant systems (firewalls, EDR, SIEM, access controls)
- Leads security incident investigation and forensic analysis
- Supports CJIS compliance activities in coordination with the LASO

5.6 CJIS Local Agency Security Officer (LASO)

- Designated by the Sheriff's Office as the County's point of contact for CJIS security compliance
- Ensures all personnel accessing CJI meet CJIS background check and training requirements
- Reports CJIS security incidents to the State CJIS Systems Agency
- Has authority to suspend CJI access on non-compliant systems

5.7 Departmental IT Leadership

- Responsible for implementing and enforcing County-wide security policies within their respective Offices
- Ensures departmental systems connected to the County core network meet minimum security baselines
- Reports security incidents affecting their systems to MIS for coordination
- Participates in security assessments and compliance reviews

5.8 All Users

- Comply with all adopted IT security policies, including the Acceptable Use Policy
- Complete required security awareness training within established timeframes
- Report suspected security incidents, policy violations, or suspicious activity to MIS immediately
- Protect the confidentiality of information they access in the course of their duties

Framework Alignment: *NIST SP 800-53: PM-2 (Senior Information Security Officer), AT-1 (Security Awareness Training Policy) | CIS Controls 14, 17*

6. Risk Management

6.1 Risk Management Approach

Oklahoma County adopts a risk-based approach to information security. Security investments, controls, and priorities are driven by an assessment of the threats, vulnerabilities, and impacts relevant to County operations.

6.2 Risk Assessment

- MIS shall conduct a formal risk assessment of County IT infrastructure and information assets at least annually

- Risk assessments shall be aligned with NIST SP 800-30 (Guide for Conducting Risk Assessments) and shall consider threats to confidentiality, integrity, and availability
- Risk assessments shall identify, prioritize, and document risks, including the likelihood and potential impact of each identified risk
- High-priority risks shall be tracked in a risk register maintained by the MIS Operations Manager and reviewed quarterly

6.3 Risk Treatment

For each identified risk, the County shall select one of the following treatment strategies:

- **Implement controls to reduce the likelihood or impact of the risk to an acceptable level**
- **Transfer the risk to a third party (e.g., through cyber liability insurance or contractual provisions)**
- **Formally accept the risk when the cost of mitigation exceeds the potential impact, documented with IT Operations Manager and Director of IT approval**
- **Eliminate the risk by discontinuing the activity or system that creates it**

Risk acceptance decisions for risks rated High or Critical require Director of MIS approval and must be documented in the risk register with a justification and review date.

> ***Framework Alignment:*** *NIST SP 800-53: RA-1, RA-3 (Risk Assessment), PM-9 (Risk Management Strategy) | CIS Control 7 (Continuous Vulnerability Management)*

7. Access Control

Access to County information systems and data shall be controlled based on the principles of least privilege and need-to-know. Detailed access control requirements are defined in the Password and Access Management Policy (IT-POL-PAM-001). The following high-level requirements apply:

- All access to County systems requires unique, individual credentials assigned to a single person
- Shared, generic, or anonymous accounts are prohibited except where technically required and formally documented with compensating controls
- Multi-factor authentication (MFA) is required for remote access (VPN), privileged accounts, cloud administration, and access to CJI systems
- Access rights are granted based on job function and approved by the user's supervisor and system owner
- Access rights are reviewed at least quarterly for privileged accounts and annually for standard accounts
- Access is revoked within 24 hours of an employee's separation, transfer, or role change that no longer requires the access
- Privileged access (administrator, root, domain admin) is restricted to the minimum number of personnel required and is subject to enhanced monitoring

> ***Framework Alignment:*** *NIST SP 800-53: AC-1 through AC-25 | CIS Controls 5, 6 | CJIS Security Policy 5.5*

CJIS	CJIS Security Policy 5.5 (Access Control): Access to CJI is limited to authorized personnel with a validated need and right to know. Advanced authentication (MFA) is mandatory for all CJI access regardless of location.

8. Data Protection

8.1 Data Classification

All County information shall be classified and handled according to the data classification framework defined in the Acceptable Use Policy (IT-POL-AUP-001, Section 16):

Classification	Protection Level
Public	No special protection required; approved for unrestricted release
Internal Use	Standard protection; accessible to County employees; not for public release
Confidential	Enhanced protection required; access restricted by law, regulation, or policy (PII, personnel records, financial data)
Restricted	Highest protection; significant harm if disclosed (CJI, HIPAA data, law enforcement case files, security configurations)

8.2 Encryption

- Data classified as Confidential or Restricted must be encrypted in transit using TLS 1.2 or higher
- Data classified as Restricted must be encrypted at rest using AES-256 or equivalent
- CJI must be encrypted using FIPS 140-3 validated cryptographic modules, both in transit and at rest
- Full-disk encryption is required on all County laptops and mobile devices
- Removable media containing Confidential or Restricted data must be encrypted

8.3 Data Loss Prevention

Oklahoma County employs Data Loss Prevention (DLP) tools to detect and prevent unauthorized transmission of sensitive data. DLP controls:

- Monitor email, web uploads, and removable media for patterns matching Confidential and Restricted data
- Block or quarantine transmissions that violate data handling rules, with alerts sent to the security team
- Are configured and maintained by the Senior Security Analyst

Framework Alignment: *NIST SP 800-53: SC-8, SC-13 (Cryptographic Protection), SC-28 (Protection of Information at Rest), MP-5 (Media Transport) | CIS Controls 3.6, 3.9, 3.10*

9. Network Security

9.1 Boundary Protection

- The County core network perimeter is protected by enterprise firewalls managed by MIS
- All inbound and outbound traffic is filtered, logged, and monitored
- Network segmentation is implemented to isolate sensitive environments (CJI systems, financial systems, guest networks) from the general County network
- Web content filtering is enforced on all County internet traffic
- Intrusion detection/prevention systems (IDS/IPS) monitor network traffic for malicious activity

9.2 Internal Network Security

- All network devices (switches, routers, wireless controllers) are hardened per CIS Benchmarks or manufacturer security guidelines
- Unauthorized network devices (personal routers, switches, wireless access points) are prohibited on the County network
- Network access control mechanisms are used to validate device compliance before granting network access
- Administrative access to network infrastructure requires MFA and is logged

9.3 Wireless Security

- County wireless networks use WPA3 or WPA2-Enterprise with RADIUS authentication
- Guest wireless is isolated from the County production network with no access to internal resources
- Rogue wireless access point detection is enabled

Framework Alignment: *NIST SP 800-53: SC-7 (Boundary Protection), SC-8, SI-3 (Malicious Code Protection), SI-4 | CIS Controls 9, 12, 13*

10. Endpoint Security

- All County endpoints (desktops, laptops, servers) must have approved Endpoint Detection and Response (EDR) software installed and active
- EDR agents must not be disabled, tampered with, or uninstalled by users
- Endpoint configurations must comply with CIS Benchmarks or equivalent hardening standards
- Operating systems and applications must be patched per the timelines defined in the Patch Management SOP
- Local administrator rights are restricted to authorized personnel only
- Removable media (USB drives, external hard drives) are restricted by policy; access requires MIS approval
- Screen lock must activate after no more than 15 minutes of inactivity (10 minutes for CJI systems)

Framework Alignment: *NIST SP 800-53: SI-3, CM-6 (Configuration Settings), CM-7 (Least Functionality) | CIS Controls 4, 10*

11. Vulnerability and Patch Management

11.1 Vulnerability Management

- MIS conducts vulnerability scans of all County-managed systems at least monthly and after any significant infrastructure change
- Critical vulnerabilities (CVSS 9.0+) must be remediated or mitigated within 15 calendar days of discovery
- High vulnerabilities (CVSS 7.0–8.9) must be remediated within 30 calendar days
- Medium and low vulnerabilities are tracked and remediated according to the risk-based prioritization in the risk register
- Vulnerability scan results are reviewed by the Senior Security Analyst and reported to the MIS Operations Manager monthly

11.2 Patch Management

- Critical security patches must be evaluated and deployed within 72 hours of release for internet-facing systems and within 14 days for internal systems
- Routine patches are deployed per the Patch Management SOP on the approved patch schedule
- Emergency out-of-band patches follow the Emergency Change process defined in the Change Management Policy
- Patch compliance rates are tracked as a KPI and reported monthly

Framework Alignment: *NIST SP 800-53: RA-5 (Vulnerability Scanning), SI-2 (Flaw Remediation) | CIS Controls 7.1–7.7*

12. Security Logging and Monitoring

12.1 Logging Requirements

The following events must be logged on all County systems:

- Successful and failed authentication attempts
- Privileged account usage and administrative actions
- Access to Confidential and Restricted data
- System configuration changes
- Security tool alerts (EDR, IDS/IPS, DLP, firewall)
- Account creation, modification, deletion, and privilege escalation
- Network connection and disconnection events for remote access

12.2 SIEM and Monitoring

- Security logs from all critical systems are forwarded to the County SIEM platform for centralized analysis and correlation
- The SIEM is monitored by the security team during business hours, with automated alerting for critical events 24/7

- Alert triage and response follow the procedures defined in the Incident Response Plan
- Log retention periods are defined by data classification and compliance requirements: minimum 1 year for CJI system logs, minimum 90 days for general systems

Framework Alignment: *NIST SP 800-53: AU-2, AU-3, AU-6, AU-12, SI-4 | CIS Controls 8.1–8.12 | CJIS Security Policy 5.4*

CJIS CJIS Security Policy 5.4 (Auditing and Accountability): CJI system logs must capture sufficient detail to reconstruct security-relevant events and must be reviewed at minimum weekly.

13. Incident Response

Oklahoma County maintains an Incident Response Plan (IT-POL-IRP-001) that defines detailed procedures for detecting, containing, eradicating, and recovering from security incidents. This section establishes the high-level incident response framework.

13.1 Incident Response Principles

- All personnel are required to report suspected security incidents immediately to MIS
- MIS serves as the coordinating body for all security incidents affecting shared infrastructure or multiple County offices
- The Senior Security Analyst leads technical incident investigation and forensics
- The Director of MIS authorizes external communications and escalation to law enforcement or legal counsel
- The County's cyber liability insurance carrier should be notified per policy terms for incidents that may result in a claim

13.2 Incident Severity Classification

Severity	Description	Response Time	Examples
Critical (P1)	Imminent or active compromise; County operations severely impacted; CJI or PII breach confirmed	Immediate — all-hands response	Ransomware, active intrusion, confirmed CJI breach
High (P2)	Significant security event; potential for data exposure; major system degradation	Within 1 hour	Malware outbreak, suspected data exfiltration, compromised privileged account
Medium (P3)	Contained security event; limited scope; no confirmed data exposure	Within 4 hours	Phishing compromise (single account), unauthorized access attempt, policy violation
Low (P4)	Minor event; informational; no immediate threat	Within 1 business day	Failed login anomalies, low-severity vulnerability discovery, policy clarification

Framework Alignment: *NIST SP 800-53: IR-1 through IR-10 | CIS Controls 17 | CJIS Security Policy 5.3*

14. Business Continuity and Disaster Recovery

14.1 Backup Requirements

- All critical County systems and data must be backed up according to a documented backup schedule
- Backups must be stored in a secure location separate from the primary data center
- Backup integrity must be verified through regular test restores (at least quarterly for critical systems)
- Backup encryption is required for Confidential and Restricted data

14.2 Disaster Recovery

- MIS shall maintain a Disaster Recovery Plan that defines recovery procedures, priorities, and timelines for critical systems
- Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) shall be defined for each critical system in coordination with business stakeholders
- The DR Plan shall be tested at least annually through tabletop exercises or functional recovery tests

Framework Alignment: *NIST SP 800-53: CP-1 through CP-13 (Contingency Planning) | CIS Controls 11.1–11.5*

15. Security Awareness and Training

15.1 Training Requirements

- All County employees and contractors must complete security awareness training within 30 days of onboarding and annually thereafter
- Personnel with access to CJI must complete CJIS Security Awareness Training within six months of initial access and biennially thereafter
- Phishing simulation exercises are conducted at least quarterly to measure and improve user resilience
- Role-based training is required for personnel with elevated security responsibilities (IT staff, administrators, security analysts)

15.2 Awareness Program

- MIS publishes regular security awareness communications (alerts, tips, policy reminders) to all County staff
- Security awareness metrics (training completion rates, phishing simulation results) are tracked and reported to the IT Council annually

Framework Alignment: *NIST SP 800-53: AT-1, AT-2, AT-3, AT-4 | CIS Controls 14.1–14.9 | CJIS Security Policy 5.2*

16. Third-Party and Vendor Security

- All third-party vendors with access to County systems or data must be subject to a security risk assessment prior to engagement
- Vendor contracts must include security requirements, data protection obligations, breach notification provisions, and right-to-audit clauses
- Vendors accessing CJI must execute a CJIS Security Addendum and comply with all CJIS personnel security requirements
- Vendor remote access must use County-approved methods with MFA and logging enabled
- Vendor access is reviewed at least annually and revoked within 24 hours of contract termination

Framework Alignment: *NIST SP 800-53: SA-4, SA-9 (External System Services), PS-7 (Third-Party Personnel Security) | CIS Controls 15.1–15.7*

17. Physical Security

- Server rooms, data centers, and network closets must have controlled access limited to authorized personnel
- Physical access to secure areas must be logged and reviewed periodically
- Visitors to secure areas must be escorted by authorized personnel at all times
- Environmental controls (fire suppression, temperature monitoring, water detection) must be maintained in server rooms and data centers
- Workstations used to access Restricted or CJI data must be in physically secure areas not accessible to the general public

Framework Alignment: *NIST SP 800-53: PE-1 through PE-20 (Physical and Environmental Protection) | CIS Controls 1.1 | CJIS Security Policy 5.9*

18. Compliance and Audit

18.1 Compliance Framework

Oklahoma County's information security program is aligned with the following frameworks and regulations:

- **Mandatory for all systems handling Criminal Justice Information** - FBI CJIS Security Policy
- **Primary control framework for the County's security program** - NIST SP 800-53 Rev. 5
- **Prioritized security best practices for implementation guidance** - CIS Controls v8
- **Where applicable to County health-related data** - HIPAA
- **Governs breach reporting obligations** - Security Breach Notification Act

18.2 Audit and Assessment

- MIS shall facilitate internal security assessments at least annually
- External penetration testing shall be conducted at least annually by a qualified third party
- CJIS audits are conducted per the State CJIS Systems Agency schedule; findings are shared with the IT Council

- Audit findings are tracked in the risk register with assigned remediation owners and deadlines
- The Director of MIS reports compliance status to the BOCC at least annually

Framework Alignment: *NIST SP 800-53: CA-1, CA-2, CA-7 (Continuous Monitoring), CA-8 (Penetration Testing) | CIS Control 18*

19. Enforcement

Violations of this policy are subject to the enforcement provisions of the Oklahoma County Acceptable Use Policy (IT-POL-AUP-001). For departmental IT operations, enforcement follows the escalation process defined in the IT Governance Charter (Section 9): notification, remediation, IT Council deliberation, and Board of County Commissioners action.

Security violations involving CJI are reportable to the LASO and the State CJIS Systems Agency, and may result in suspension of CJI access.

20. Policy Administration

20.1 Review Cycle

This policy shall be reviewed at least annually by MIS and the IT Council. Reviews are coordinated by the Director of IT. Amendments require Board of County Commissioners approval per the IT Governance Charter.

20.2 Exception Process

Exceptions to this policy must be submitted in writing to the IT Operations Manager with a business justification, risk assessment, proposed compensating controls, and expiration date. Exceptions affecting Restricted or CJI data require Director of IT and LASO approval.

21. Related Policies and Documents

Document	ID	Status
IT Governance Charter	IT-GOV-CHARTER-001	Pending
Acceptable Use Policy	IT-POL-AUP-001	Pending
Change Management Policy	IT-POL-CHG-001	Pending
Password and Access Management Policy	IT-POL-PAM-001	Pending
Incident Response Plan	IT-POL-IRP-001	Pending
Patch Management SOP	IT-SOP-PATCH-001	Planned
Business Continuity / Disaster Recovery Plan	IT-POL-BCDR-001	Planned
FBI CJIS Security Policy	External	Current Version

Document	ID	Status
NIST SP 800-53 Rev. 5	External	Current Version
CIS Controls v8	External	Current Version