OKLAHOMA COUNTY

DATA CLASSIFICATION AND HANDLING POLICY

Information Technology Operations

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

Document ID:	IT-POL-DCH-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 Data Classification and Handling Policy establishes a uniform framework for classifying, labeling, handling, storing, transmitting, and disposing of Oklahoma County information assets based on their sensitivity and the legal, regulatory, and operational requirements that govern them.

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 data classification framework introduced in the Acceptable Use Policy (IT-POL-AUP-001, Section 16) into a comprehensive, standalone policy. It applies to all County data in any form, i.e., electronic, paper, verbal, visual, etc. throughout the data's entire lifecycle, from creation through final disposition.

> ***Framework Alignment:*** *NIST SP 800-53: RA-2 (Security Categorization), MP-3 (Media Marking), SC-16 (Transmission of Security Attributes) | NIST SP 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories) | CIS Controls 3.1–3.14 | CJIS Security Policy 5.5, 5.8, 5.10*

2. Scope

2.1 Organizational Scope

This policy applies to all Oklahoma County Offices, Departments, and agencies, including those with independent IT operations. All personnel who create, access, store, process, transmit, or dispose of County data are responsible for handling it in accordance with its classification.

2.2 Data Scope

This policy covers all information owned, managed, or processed by Oklahoma County, regardless of:

- **Form - Electronic (databases, files, email, cloud), paper (printed documents, forms, records), verbal (conversations, voicemail), or visual (whiteboards, screen displays)**
- **Location - On-premises servers, cloud platforms, endpoints, mobile devices, removable media, third-party systems, off-site storage, or physical file rooms**
- **Custodian - Whether managed by MIS, departmental IT, a vendor, or an individual employee**

Data classification applies to the information itself, not to the system that stores it. A single system may contain data at multiple classification levels; the system's security posture must meet the requirements of the highest classification level of data it contains.

> ***Framework Alignment:*** *NIST SP 800-53: RA-2, MP-3 | CIS Control 3.1*

3. Definitions

Term	Definition
Data Classification	The process of assigning a sensitivity level to information based on the potential impact of its unauthorized disclosure, modification, or loss.
Data Owner	The department head or elected official ultimately responsible for data within their Department or Office's jurisdiction. The Data Owner determines the classification of their department's or Office's data and authorizes access.
Data Custodian	The individual or team (typically MIS or departmental IT) responsible for the technical storage, protection, and management of data on behalf of the Data Owner.
Data Steward	A designated individual within a department responsible for day-to-day data quality, classification decisions, and access request validation.
Sensitive Data	Any data classified as Confidential or Restricted under this policy.
Personally Identifiable Information (PII)	Information that can be used to identify, contact, or locate an individual, either alone or in combination with other information. Includes SSN, driver's license number, financial account numbers, and biometric data.
Criminal Justice Information (CJI)	Data provided by the FBI CJIS Division, including identity history, biometric data, case/incident data, and property records.
Protected Health Information (PHI)	Individually identifiable health information subject to HIPAA, including medical records, treatment information, and health insurance data.
Data Lifecycle	The complete span of a data element's existence: creation, storage, use, sharing, archival, and disposition.
Disposition	The final disposal of data through approved destruction methods, in accordance with applicable retention schedules.
Labeling	The practice of marking data (electronically or physically) with its classification level to inform handlers of the required protections.

4. Data Classification Levels

All Oklahoma County data must be assigned to one of the following four classification levels. When in doubt, data should be classified at the higher level until a formal determination is made.

4.1 Level 1: Public

Information that has been approved for unrestricted public access. Disclosure poses no risk to the County, its operations, or individuals.

Attribute	Description
Impact if Disclosed	None — information is intended for public consumption
Examples	Published meeting minutes, press releases, approved budgets, public-facing website content, County ordinances, public records responses (after review)
Default Assumption	Data is NOT Public by default. Data becomes Public only when explicitly approved for release by the Data Owner or required by law (e.g., Oklahoma Open Records Act).

4.2 Level 2: Internal Use

Information intended for use within County government. Not sensitive, but not approved for public release. This is the default classification for most day-to-day operational data.

Attribute	Description
Impact if Disclosed	Low — could cause minor inconvenience or embarrassment but no legal, financial, or safety harm
Examples	Internal memos, draft documents, organizational charts, internal policies in development, non-sensitive email, operational procedures, training materials
Default Classification	All County data that has not been explicitly classified as Public, Confidential, or Restricted defaults to Internal Use.

4.3 Level 3: Confidential

Information that is protected by law, regulation, contract, or County policy. Unauthorized disclosure could cause significant harm to individuals, the County, or third parties.

Attribute	Description
Impact if Disclosed	Significant — could result in legal liability, financial loss, regulatory penalties, identity theft, reputational damage, or harm to individuals
Legal / Regulatory Basis	Oklahoma Open Records Act exemptions, HIPAA, state privacy laws, contractual confidentiality obligations, attorney-client privilege, personnel records statutes
Examples	See Section 5 (Sensitive Data Inventory)

4.4 Level 4: Restricted

The highest sensitivity level. Information whose unauthorized disclosure, modification, or loss could cause severe harm to public safety, law enforcement operations, individuals, or County operations. Requires the most stringent protections.

Attribute	Description
Impact if Disclosed	Severe — could endanger public safety, compromise law enforcement operations, result in criminal liability, cause irreversible harm to individuals, or trigger mandatory breach notification
Legal / Regulatory Basis	FBI CJIS Security Policy, federal law enforcement statutes, juvenile records protections, court-sealed records, security configurations, active investigation confidentiality
Examples	See Section 5 (Sensitive Data Inventory)

> ***Framework Alignment:*** *NIST SP 800-60: Volume I (Guide for Mapping Types of Information) | NIST SP 800-53: RA-2 | FIPS 199 (Standards for Security Categorization)*

5. Sensitive Data Inventory

The following table provides a non-exhaustive inventory of sensitive data types handled by Oklahoma County, their classification, the primary governing regulation, and the County Office or Department most likely to be the Data Owner. This inventory should be reviewed annually and expanded as new data types are identified.

Data Type	Classification	Primary Regulation / Basis	Primary Data Owner(s)
Criminal Justice Information (CJI)	Restricted	FBI CJIS Security Policy	Sheriff's Office; District Attorney's Office
Active law enforcement case files	Restricted	State law; investigative confidentiality	Sheriff's Office; District Attorney's Office
Juvenile records	Restricted	Oklahoma Juvenile Code; federal JJDPA	Court Clerk; Sheriff's Office; Juvenile Bureau; District Attorney's Office
Court-sealed records	Restricted	Court order	Court Clerk
Social Security numbers	Restricted	Oklahoma Identity Theft Prevention Act; federal law	All offices (varies)
Biometric data (fingerprints, facial recognition)	Restricted	CJIS Security Policy; state privacy law	Sheriff's Office
Protected Health Information (PHI)	Confidential / Restricted	HIPAA; Oklahoma health privacy statutes	County Pharmacy; HR (employee records)
Financial account numbers (bank, credit card)	Confidential	PCI DSS (if applicable); state law	Treasurer
Tax records and assessment data (non-public)	Confidential	Oklahoma tax confidentiality statutes	Assessor; Treasurer
Payroll and employee compensation data	Confidential	Personnel records statutes	HR; County Clerk
Personnel / HR records (disciplinary, medical, performance)	Confidential	Personnel records statutes; ADA; FMLA	HR; each office for their employees
Attorney-client privileged communications	Confidential	Attorney-client privilege	County legal counsel; all offices
Election data (voter registration PII, ballot data)	Confidential	Oklahoma Election Code; HAVA	Election Board (note: separate from County IT, but may touch County systems)
IT security configurations and vulnerability data	Confidential	Operational security	MIS; Departmental IT
Vendor contracts with confidentiality clauses	Confidential	Contractual obligation	Procuring office
Passwords, credentials, encryption keys	Restricted	Operational security; CJIS	MIS; Departmental IT
Audit logs and security monitoring data	Confidential	Operational security; CJIS 5.4	MIS; Departmental IT
Backup media and disaster recovery data	Per source classification	Inherits classification of source data	MIS; Departmental IT

This inventory is a starting point, not a complete catalog. Each Data Owner is responsible for identifying and classifying data within their office's jurisdiction. MIS provides guidance and support for classification decisions.

6. Data Handling Requirements by Classification

The following matrix defines the minimum handling requirements for each classification level. Where a specific regulation (CJIS, HIPAA) imposes a stricter requirement, the stricter requirement applies.

Handling Control	Public	Internal Use	Confidential	Restricted
Storage — electronic	No restrictions	County systems only (no personal devices without approval)	County-approved systems with access controls; encrypted at rest	County-approved systems only; AES-256 or FIPS 140-3 encrypted at rest; access logged
Storage — paper	No restrictions	Secure office environment	Locked cabinet, drawer, or room when unattended	Locked container in a secured area; access restricted and logged
Transmission — email	No restrictions	County email	County email with encryption (TLS enforced); no personal email	Encrypted (TLS + message encryption or approved secure transfer); never via personal email or unapproved platforms
Transmission — file transfer	No restrictions	County-approved platforms	Approved encrypted file transfer only (SFTP, approved cloud with encryption)	FIPS 140-3 validated encryption in transit; approved platforms only; logged
Access control	None required	County employees and authorized contractors	Role-based access; need-to-know validated by Data Owner or Steward	Strictly need-to-know; Data Owner approval; MFA enforced; access reviewed quarterly
Removable media	Allowed	Allowed with MIS awareness	Encrypted removable media only; MIS approval required	FIPS 140-3 encrypted media only; LASO approval for CJI; logged
Printing	No restrictions	Standard County printers	Retrieve immediately; do not leave unattended at printer	Supervised printing only; retrieve immediately; shred misprints
Screen visibility	No restrictions	Standard office precautions	Privacy screens recommended in public areas	Privacy screens required; screens not visible to unauthorized individuals
Cloud storage	County-approved platforms	County-approved platforms (OneDrive, SharePoint)	Approved platforms with DLP and access controls; no personal cloud	Approved platforms only with FIPS encryption, DLP, access logging; no personal cloud; LASO approval for CJI
Mobile devices	No restrictions	County or BYOD (enrolled)	County-managed or MDM-enrolled BYOD; encrypted; remote wipe enabled	County-managed devices only; FIPS encryption; no BYOD for Restricted data without exception
Verbal discussion	No restrictions	Normal discretion	Private setting; not in public areas	Private, controlled setting; no speakerphone in shared spaces
Sharing with third parties	Permitted	With business justification	Data Owner approval; NDA or contractual confidentiality required	Data Owner approval; NDA; security assessment of recipient;

Handling Control	Public	Internal Use	Confidential	Restricted
				CJIS Security Addendum for CJI
Disposition — electronic	Standard deletion	Standard deletion	Secure deletion (overwrite or crypto-erase)	NIST SP 800-88 media sanitization; CJIS-approved methods for CJI; documented
Disposition — paper	Standard recycling	Standard recycling	Cross-cut shredding	Cross-cut shredding or incineration; documented

Framework Alignment: *NIST SP 800-53: AC-3, AC-4, MP-2, MP-3, MP-5, MP-6, SC-8, SC-13, SC-28 | CIS Controls 3.1–3.14 | CJIS Security Policy 5.5, 5.8, 5.10*

7. Data Labeling

7.1 Labeling Requirements

Data labeling communicates classification to anyone who encounters the data. The following labeling standards apply:

Classification	Electronic Labeling	Physical Labeling
Public	No label required (absence of a label does NOT imply Public)	No label required
Internal Use	Recommended but not required; use “Internal Use” label where practical	Recommended for cover pages of printed documents
Confidential	Required. Apply M365 Sensitivity Label “Confidential” (when deployed); include “CONFIDENTIAL” on document headers/footers	Required. Stamp or print “CONFIDENTIAL” on cover page and each page where practical
Restricted	Required. Apply M365 Sensitivity Label “Restricted” (when deployed); include “RESTRICTED” on document headers/footers; DLP policies enforced	Required. Stamp or print “RESTRICTED” on every page; sealed envelope for physical transport

7.2 M365 Sensitivity Labels

MIS will implement Microsoft 365 Sensitivity Labels to automate classification and enforcement for electronic data. The implementation plan includes:

1. Phase 1: Deploy labels for manual application by users (Confidential and Restricted)
2. Phase 2: Enable recommended labeling via M365 DLP policy suggestions based on content detection (e.g., SSN patterns, CJI keywords)
3. Phase 3: Enable automatic labeling for clearly identifiable sensitive data patterns with DLP enforcement

Until M365 Sensitivity Labels are fully deployed, users are responsible for manually labeling documents and emails per the requirements above.

7.3 Labeling Exceptions

Certain data types carry an inherent classification that does not require individual labeling:

- CJI is always Restricted by definition — systems processing CJI are labeled as CJI systems, and all data within those systems is treated as Restricted
- Email marked attorney-client privileged is always Confidential or Restricted
- Personnel files in HR systems are always Confidential

Framework Alignment: *NIST SP 800-53: MP-3 (Media Marking) | CIS Control 3.7*

8. Roles and Responsibilities

Role	Data Classification Responsibilities
Data Owner (Department Head / Elected Official)	Determines the classification of data within their office's jurisdiction. Authorizes access to Confidential and Restricted data. Approves sharing with third parties. Responsible for ensuring their office complies with handling requirements. May delegate day-to-day decisions to a Data Steward.
Data Steward (Departmental Designee)	Acts on behalf of the Data Owner for day-to-day classification decisions, access request validation, and data quality management. Must be formally designated in writing by the Data Owner.
Data Custodian (MIS / Departmental IT)	Implements the technical controls required by the data's classification: encryption, access controls, backup, logging, and disposition. Does not determine classification — that is the Data Owner's responsibility.
All Users	Handle data in accordance with its classification. Label Confidential and Restricted data per Section 7. Report suspected data breaches or mishandling immediately. Complete data handling training.
MIS / Senior Security Analyst	Publishes and maintains DLP rules, encryption standards, and labeling tools. Monitors for data handling violations via DLP and SIEM. Provides guidance on classification decisions when requested by Data Owners. Investigates suspected data breaches.
IT Council	Reviews and recommends updates to this policy. Provides cross-departmental perspective on data classification disputes. Receives quarterly compliance reports.

Records Management Governance: Oklahoma County has an established Records Retention Policy and Records Management Program, governed by the Oklahoma County Information Technology Council. The IT Council has general program management responsibility for records management, including reviewing policies, approving disposal of eligible records, and establishing recordkeeping standards. The County Clerk manages historical records. MIS is responsible for electronic records management, secure deletion procedures, and ensuring the accessibility and preservation of electronic records per the Records Management Program. All records retention and disposition activities under this Data Classification and Handling Policy are subject to the Oklahoma County Records Retention Policy and the Oklahoma County Records Retention Schedule.

9. Data Lifecycle Management

9.1 Creation and Collection

- Data is classified at the point of creation or collection — not retroactively
- When creating new documents, databases, or data stores, the creator applies the appropriate classification based on the content
- Systems that collect data from the public (online forms, portals) must be designed with classification in mind — sensitive fields are identified during system design
- Data collected from external sources (vendors, other agencies, courts) inherits the classification required by the source's governing regulation or the County's own classification, whichever is more restrictive

9.2 Storage and Processing

- Data must be stored on systems that meet the technical requirements for its classification level (Section 6)
- A system that stores data at multiple classification levels must meet the requirements of the highest level present
- Data Custodians (MIS / departmental IT) are responsible for ensuring storage systems meet the required controls
- Data must not be copied to less-secure systems, personal devices, or unapproved cloud platforms

9.3 Sharing and Transmission

- Data sharing within the County requires need-to-know justification appropriate to the classification level
- Sharing Confidential or Restricted data externally requires Data Owner approval and appropriate protections (NDA, encryption, secure transfer method)
- Sharing CJI externally requires LASO approval and compliance with CJIS Security Policy data sharing provisions
- All external data sharing agreements involving Confidential or Restricted data should be documented

9.4 Archival

- Data that is no longer actively used but must be retained per retention schedules is archived to approved, classified storage
- Archived data retains its original classification — archival does not reduce the required protections
- Archived data must remain accessible for legal discovery, audit, and compliance purposes

9.5 Disposition

- Data is disposed of only after the applicable retention period defined in the Oklahoma County Records Retention Schedule has expired AND there are no active legal holds, pending litigation, or audit requirements. Premature disposal of official records is expressly prohibited per the Records Retention Policy and may result in disciplinary action and civil or criminal liability.
- Disposition methods must match the classification level (see Section 6 handling matrix) and must use Oklahoma County approved destruction methods: shredding for paper records (the County-approved

method per the Records Retention Policy), and secure erasure, reformatting, or overwriting for electronic records per MIS guidelines. A Certificate of Final Disposition must be obtained upon completion of destruction by a vendor.

- All disposition of Confidential and Restricted data must be documented with: what was destroyed, the method used, the date, and the individual who performed or supervised the destruction
- Disposition of CJI must follow CJIS Security Policy media sanitization requirements and be reported to the LASO

Framework Alignment: *NIST SP 800-53: MP-6 (Media Sanitization), SI-12 (Information Management and Retention) | NIST SP 800-88 (Guidelines for Media Sanitization) | CIS Controls 3.1, 3.14*

10. Records Retention

10.1 Retention Framework

Oklahoma County data retention is governed by the Oklahoma County Records Retention Policy and the Oklahoma County Records Retention Schedule, which is the only retention policy authorized for use. The Records Retention Schedule identifies what records are being managed and defines how long they must be retained based on business, legal, compliance, and operational requirements. The following sources inform the retention schedule:

- Oklahoma state records retention statutes and the Oklahoma Department of Libraries retention schedules
- Federal requirements applicable to specific data types (CJIS, HIPAA, IRS)
- Department-specific retention schedules where they exist
- Legal hold obligations arising from pending or anticipated litigation

All retention and disposition of County records must comply with the Oklahoma County Records Retention Schedule. If an elected official or department head believes a record scheduled for destruction needs to be preserved longer, a notification of intent to retain must be submitted to the IT Council per the Records Retention Policy (Section 5.2.1). No more than two extensions by notice are permitted, and additional retention beyond seven years requires a policy amendment. The following minimum retention periods apply specifically to IT-managed data types not explicitly covered in the Records Retention Schedule:

Data Category	Minimum Retention	Basis
IT security logs (general systems)	90 days minimum	Operational security; County standard
IT security logs (CJI systems)	1 year minimum	CJIS Security Policy 5.4
Email and electronic communications	Per Oklahoma County Records Retention Schedule (based on content classification)	Records Retention Policy; varies by content
Backup media (tapes, disk)	Per Records Retention Policy Section 6: for disaster recovery only; recycled when superseded	Records Retention Policy

Legal holds override all retention schedules. Per the Oklahoma County Records Retention Policy (Section 5.2.2), the Oklahoma County District Attorney's Office and Treasurer's Office are the only offices with the

authority to issue or release a legal hold order that suspends the retention and disposal requirements for records. When a legal hold is issued, all records potentially relevant to the matter must be preserved regardless of retention schedules, until the hold is formally released. Custodians must acknowledge receipt of hold orders within seven days.

10.2 Retention Responsibilities

- Data Owners are responsible for knowing and applying the retention schedules applicable to their data
- Data Custodians (MIS / departmental IT) implement technical retention controls (archival, automated deletion where configured) at the direction of Data Owners
- MIS does not independently delete data — disposition requires Data Owner authorization
- The IT Council reviews the Records Retention Schedule annually for statutory changes that impact record retention and destruction, per the Records Retention Policy (Section 3.1)

Framework Alignment: *Oklahoma Records Management Act (67 O.S. § 201 et seq.) | NIST SP 800-53: SI-12 | CIS Control 3.1*

11. Data Loss Prevention (DLP)

11.1 DLP Program

Oklahoma County operates Data Loss Prevention tools to detect and prevent unauthorized transmission of sensitive data. The DLP program is managed by the MIS Senior Security Analyst and operates across the following channels:

- Email (outbound content scanning)
- Web uploads and cloud sharing
- Removable media and endpoint data transfers
- Microsoft 365 (SharePoint, OneDrive, Teams) content policies

11.2 DLP Detection Rules

DLP rules are configured to detect the following sensitive data patterns at minimum:

- Social Security numbers (SSN pattern matching)
- Financial account numbers (credit card, bank account patterns)
- CJI identifiers and keywords (where technically feasible without excessive false positives)
- Health information keywords and patterns (HIPAA)
- Documents labeled Confidential or Restricted (via M365 Sensitivity Labels when deployed)

11.3 DLP Actions

Classification Detected	DLP Action	Notification
Confidential — internal transfer	Allow with logging	None (logged for audit)

Classification Detected	DLP Action	Notification
Confidential — external transfer	Warn user; require justification or manager override	User notification; logged; weekly review by security team
Restricted — any external transfer	Block transmission; quarantine content	User notification; immediate alert to Senior Security Analyst
Restricted — unauthorized internal transfer	Warn user; log event	Alert to Senior Security Analyst; follow-up investigation if pattern detected

DLP rules are tuned regularly to balance detection effectiveness with false positive rates. The Senior Security Analyst reviews DLP alert logs weekly and adjusts rules as needed.

> ***Framework Alignment:*** *NIST SP 800-53: SC-7 (Boundary Protection), SI-4 (Information System Monitoring), AC-4 (Information Flow Enforcement) | CIS Controls 3.13, 3.14*

12. Data Breach Response

When a suspected or confirmed data breach involving Confidential or Restricted data is identified, the following steps are taken in coordination with the Incident Response Plan (IT-POL-IRP-001):

1. The individual discovering the breach reports it immediately to MIS and their supervisor
2. MIS activates the Incident Response Team per the IRP severity classification
3. The Senior Security Analyst assesses what data was accessed, the classification level, the number of records/individuals affected, and the likely cause
4. The Director of MIS engages County legal counsel to determine notification obligations under Oklahoma's Security Breach Notification Act (24 O.S. § 163) and any other applicable laws (HIPAA, CJIS)
5. The cyber insurance carrier is notified per policy terms
6. For CJI breaches, the LASO reports to the State CJIS Systems Agency per CJIS requirements
7. For HIPAA breaches, notification follows HIPAA Breach Notification Rule requirements (45 CFR §§ 164.400–414)
8. Affected individuals are notified per legal counsel's guidance and applicable law
9. A Post-Incident Review is conducted per the IRP to identify root cause and prevent recurrence

Time is critical. Oklahoma law requires notification without unreasonable delay. HIPAA requires notification within 60 days of discovery for breaches affecting 500+ individuals. CJIS incident reporting timelines are defined by the State CSA. Legal counsel determines the specific obligations for each incident.

> ***Framework Alignment:*** *Oklahoma Security Breach Notification Act (24 O.S. § 163) | HIPAA Breach Notification Rule (45 CFR § 164.400–414) | CJIS Security Policy 5.3 | NIST SP 800-53: IR-6*

13. Training and Awareness

- All County employees must receive data classification and handling training as part of their security awareness training (within 30 days of onboarding and annually thereafter)
- Training must cover: the four classification levels, how to determine classification, labeling requirements, handling requirements by level, and how to report suspected data breaches
- Personnel who regularly handle Confidential or Restricted data should receive enhanced training specific to the regulations governing that data (e.g., CJIS training for CJI handlers, HIPAA training for PHI handlers)
- Data Owners and Data Stewards should receive additional guidance on their classification and access authorization responsibilities
- Training completion is tracked and reported as part of the security awareness training metrics

Framework Alignment: *NIST SP 800-53: AT-2 (Security Awareness Training) | CIS Control 14 | CJIS Security Policy 5.2*

14. Enforcement

Violations of this policy are subject to the enforcement provisions of the Acceptable Use Policy (IT-POL-AUP-001). The severity of enforcement action corresponds to the classification level of the data involved:

- **Public / Internal Use mishandling - Verbal or written warning; retraining**
- **Confidential data mishandling - Written reprimand; access suspension; mandatory retraining; potential HR referral**
- **Restricted data mishandling - Immediate access suspension; formal disciplinary action; potential law enforcement referral; CJIS violation reporting (if CJI involved)**

For departmental IT operations, enforcement follows the IT Governance Charter escalation process (Section 9).

15. Policy Administration

15.1 Review Cycle

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

15.2 Sensitive Data Inventory Updates

The Sensitive Data Inventory (Section 5) is reviewed semi-annually by MIS and updated when new data types are identified, when regulations change, or when new systems are deployed. Data Owners are responsible for notifying MIS of new sensitive data types within their jurisdiction.

16. Related Policies and Documents

Document	ID	Relationship
IT Governance Charter	IT-GOV-CHARTER-001	Authorizing framework
Oklahoma County Records Retention Policy and Records Retention Schedule	County Records Management Program	Authoritative records retention and disposition framework; governs all retention schedules and legal holds
Acceptable Use Policy	IT-POL-AUP-001	Contains original four-tier classification framework; this policy supersedes and expands Section 16
Information Security Policy	IT-POL-ISP-001	Parent security policy; references data classification
Incident Response Plan	IT-POL-IRP-001	Defines breach investigation and notification procedures
Password & Access Management Policy	IT-POL-PAM-001	Governs access control enforcement referenced in handling matrix
IT Security Baseline Standard	IT-STD-SEC-001	Technical controls that implement classification protections
Change Management Policy	IT-POL-CHG-001	Governs changes to DLP rules and labeling infrastructure
BC/DR Plan	IT-POL-BCDR-001	Backup and recovery requirements align with data classification
Oklahoma Open Records Act	51 O.S. § 24A.1 et seq.	Governs public access to County records
Oklahoma Security Breach Notification Act	24 O.S. § 163	Breach notification requirements
Oklahoma Records Management Act	67 O.S. § 201 et seq.	State statute; implemented by the County Records Retention Policy
HIPAA Privacy and Security Rules	45 CFR Parts 160, 164	PHI handling requirements
FBI CJIS Security Policy	External	CJI handling and protection requirements
NIST SP 800-60	External	Guide for mapping information types to security categories
NIST SP 800-88	External	Guidelines for media sanitization