OKLAHOMA COUNTY

CHANGE MANAGEMENT POLICY

Information Technology Operations

Aligned with CJIS Security Policy | NIST SP 800-53 | CIS Controls v8 | ITIL v4

Document ID:	IT-POL-CHG-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 Change Management Policy establishes a structured, consistent process for requesting, evaluating, approving, implementing, and reviewing changes to Oklahoma County information technology infrastructure and services.

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 for changes to shared infrastructure, and on MIS for all systems under MIS management.

The purpose of this policy is to:

- Minimize the risk of service disruptions, outages, and unintended consequences resulting from changes to production systems
- Ensure all changes are documented, traceable, and auditable
- Establish clear roles, responsibilities, and approval authority for changes across all infrastructure domains
- Protect the confidentiality, integrity, and availability of County systems and data — including Criminal Justice Information (CJI)
- Align change management practices with ITIL v4, NIST SP 800-53, CIS Controls v8, and the FBI CJIS Security Policy

> ***Framework Alignment:*** *NIST SP 800-53: CM-1 (Configuration Management Policy), CM-3 (Configuration Change Control) | CIS Control 4.1 | ITIL v4: Change Enablement*

2. Scope

2.1 Applicability

This policy applies to all changes made to Oklahoma County IT infrastructure, systems, and services. It is binding on all personnel who initiate, approve, implement, or review changes, including:

- All MIS department staff
- Contractors, vendors, and third-party service providers performing work on County systems
- Department staff with administrative access to County IT systems
- Any individual making configuration changes to systems managed by MIS

When a departmental IT team plans a change that could affect shared infrastructure or other County Offices, they must coordinate with MIS by submitting a Change Request through the MIS ITSM Platform or notifying the MIS Change Manager at least 5 business days before the planned change. MIS will assess the potential impact and, if necessary, schedule the change through the standard CAB review process.

Cross-Departmental Applicability: County offices with independent IT staff (County Clerk, Assessor, Sheriff's Office, Treasurer, Court Clerk) are required to follow this policy for any change that affects the County core network, shared infrastructure, or cross-departmental services managed by MIS. Changes to

department-specific systems that do not affect shared infrastructure are governed by each department's own procedures, but Offices are strongly encouraged to adopt this policy's framework for consistency.

2.2 Covered Systems

This policy covers changes to all production and pre-production systems managed by MIS, including but not limited to:

Infrastructure Domain	Examples
On-Premise Servers	Windows Server, Linux, virtualization hosts, file servers, print servers, domain controllers, etc
Network Infrastructure	Firewalls, switches, routers, wireless controllers, load balancers, VPN concentrators, etc
Cloud Services	Azure, AWS, Microsoft 365 administration, cloud-hosted applications, etc
Databases	SQL Server, Oracle, MySQL, PostgreSQL — schema changes, configuration, maintenance, etc.
Telephony & Communications	PBX systems, POTS lines, fax infrastructure, VoIP, call routing
End-User Systems	Group Policy (GPO), endpoint configuration, software deployment, imaging
Security Infrastructure	Antivirus/EDR, SIEM, firewalls (security rules), vulnerability scanners, MFA systems

2.3 Exclusions

The following are excluded from this policy but may be governed by separate procedures:

- Routine, pre-approved standard changes (defined in Section 5)
- Content changes to County websites or public-facing applications (unless infrastructure is affected)
- Individual user account provisioning and password resets performed through established SOP

Framework Alignment: *NIST SP 800-53: CM-3, CM-9 (Configuration Management Plan) | CIS Controls 4.1, 4.2*

3. Definitions

Term	Definition
Change	Any addition, modification, or removal of anything that could have an effect on IT services, infrastructure, or configurations.
Change Advisory Board (CAB)	A group of stakeholders responsible for evaluating, prioritizing, and authorizing changes. See Section 6.
Change Record	Am ITS< ticket documenting the full lifecycle of a change from request through post-implementation review.
Change Requester	The individual who initiates a change request.
Change Implementer	The individual(s) responsible for executing the approved change.
Change Approver	The individual(s) with authority to approve or reject a change request.

Term	Definition
Rollback Plan	A documented procedure to reverse a change and restore the system to its pre-change state if the change fails or causes unintended impact.
Standard Change	A pre-approved, low-risk, well-documented, and repeatable change that follows an established procedure.
Normal Change	A change that must go through the full change request, assessment, approval, and review process.
Emergency Change	A change that must be implemented immediately to resolve a critical incident or prevent imminent service failure. See Section 12.
Maintenance Window	A scheduled time period during which planned changes may be implemented with reduced risk of business impact. See Section 10.
Post-Implementation Review (PIR)	A review conducted after a change is implemented to verify success, document outcomes, and capture lessons learned.
Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT service (servers, switches, applications, etc.).
Production Environment	Live systems actively used by County staff or the public to conduct business.

4. Change Classification

All changes must be classified into one of the following categories. The classification determines the approval path, lead time, and documentation requirements.

4.1 Classification Matrix

Attribute	Standard Change	Normal Change	Emergency Change
Risk Level	Low	Low to High	Varies (typically High)
Pre-Approved?	Yes — per Standard Change Catalog	No — requires CAB or manager approval	No — expedited approval required
Lead Time	None (execute per SOP)	Minimum 5 business days	Immediate
CAB Review	Not required	Required for Medium/High risk	Post-implementation review required
Documentation	SOP reference + ITSM ticket	Full change record in ITSM tool	Full change record (may be completed after implementation)
Rollback Plan	Documented in SOP	Required before approval	Required (may be verbal for P1)
PIR Required?	No (unless failure)	Yes — for all Medium/High risk	Yes — always required
Examples	Scheduled patching, user onboarding, backup rotation	Firewall rule change, server migration, GPO modification	Security incident response, critical outage remediation

4.2 Risk Assessment

Every Normal and Emergency change must include a risk assessment. Risk is determined by evaluating the following factors:

Factor	Low	Medium	High
Impact if failure occurs	Single user or non-critical system	Department, Office, or business function	County-wide or critical infrastructure
Scope of change	Single configuration item	Multiple related systems	Core infrastructure or shared services
Reversibility	Easily reversed in < 30 min	Reversible with moderate effort	Difficult or impossible to reverse
Testing completed?	Tested in non-production	Partially tested or similar precedent	Cannot be pre-tested
CJIS/Sensitive systems affected?	No	Indirect impact possible	Direct CJI system change
Users affected	< 10 users	10–100 users or one department or Office	> 100 users, multiple Offices or Departments, or County-wide

The overall risk rating is determined by the highest rating in any single factor. If any factor is rated High, the change is classified as High risk.

> ***Framework Alignment:*** *NIST SP 800-53: CM-3, CM-4 (Impact Analyses), RA-3 (Risk Assessment) | CIS Control 4.1 | ITIL v4: Change Enablement — Risk Assessment*

5. Standard Change Catalog

Standard changes are pre-approved, low-risk, well-documented changes that follow an established SOP. They do not require individual CAB review but must still be logged in the ITSM tool for audit and tracking purposes.

5.1 Criteria for Standard Changes

A change may be classified as Standard if it meets all of the following criteria:

- The change has been performed successfully multiple times with consistent results
- A documented, step-by-step SOP exists for the change
- The change is low risk with a well-understood and easily reversible impact
- The change has been formally reviewed and approved by the CAB for inclusion in the Standard Change Catalog

5.2 Initial Standard Change Catalog

The following changes are initially approved as Standard Changes. This catalog will be reviewed and updated quarterly by the CAB.

Standard Change	SOP Required	ITSM Ticket
Scheduled OS patching (per approved patching schedule)	Yes	Required
User account provisioning / onboarding	Yes	Required
User account deprovisioning / offboarding	Yes	Required
Password resets and account unlocks	Yes	Required
Scheduled backup rotation and verification	Yes	Required
Printer/peripheral deployment	Yes	Required
Pre-approved software deployment (from approved list)	Yes	Required
Certificate renewals (per documented schedule)	Yes	Required
Workstation reimaging (standard build)	Yes	Required

5.3 Adding or Removing Standard Changes

Requests to add a new Standard Change or remove an existing one must be submitted to the CAB with the following:

- A documented SOP for the proposed standard change
- Evidence of at least three (3) successful prior implementations
- A risk assessment confirming low risk and easy reversibility
- The CAB will review and vote on the request at the next scheduled meeting

Framework Alignment: *NIST SP 800-53: CM-3, CM-7 (Least Functionality) | ITIL v4: Standard Change Model*

6. Change Advisory Board (CAB)

6.1 CAB Purpose

The Change Advisory Board is a standing body responsible for reviewing, evaluating, and authorizing Normal and post-reviewing Emergency changes. The CAB ensures that changes are properly assessed for risk, resource requirements, scheduling conflicts, and business impact before implementation.

6.2 CAB Membership

Role	CAB Responsibility	Standing / Ad Hoc
IT Operations Manager	CAB Chair — convenes meetings, facilitates discussion, holds final authority on disputes	Standing
Senior Security Analyst	Reviews all changes for security impact, CJIS compliance, and risk posture	Standing
Systems Engineer III (rotating)	Provides technical assessment of proposed changes within their area of ownership	Standing (1 of 3, rotating weekly)
Change Requester	Presents the change request, answers technical questions, and defends the risk assessment	Ad Hoc (for their change only)

Role	CAB Responsibility	Standing / Ad Hoc
Department Representative	Provides business impact perspective when the change affects a specific department	Ad Hoc (as needed)
Vendor/Contractor	Provides technical input when vendor-managed systems are affected	Ad Hoc (as needed)

Departmental IT Liaison: When a proposed change affects systems or services used by a specific County office with independent IT staff, the Change Manager shall invite that department's IT representative to participate in the CAB review as an ad hoc member. Departmental liaisons provide impact assessment from their office's perspective and may raise concerns or request scheduling adjustments. This ensures cross-departmental changes are evaluated with full stakeholder input.

6.3 CAB Meeting Cadence

- **Regular Meetings:** The CAB will meet weekly at a consistent, scheduled time
- **Special Sessions:** Any CAB member may request a special session for urgent (but non-emergency) changes with at least 24 hours notice
- **Quorum:** A quorum of the IT Operations Manager plus the Senior Security Analyst plus one SE III must be present for any approval
- **Documentation:** All CAB decisions, approvals, rejections, and deferrals will be documented in the associated ITSM change record

6.4 CAB Decision Options

Decision	Meaning	Next Step
Approved	Change may proceed as planned	Schedule implementation within approved window
Approved with Conditions	Change may proceed after specified conditions are met	Meet conditions, update ticket, proceed
Deferred	Change is not rejected but requires more information or a different timing	Resubmit with additional detail at next CAB
Rejected	Change is not approved due to unacceptable risk, poor planning, or lack of justification	Requester may revise and resubmit

Framework Alignment: *NIST SP 800-53: CM-3 (Configuration Change Control) | ITIL v4: Change Enablement — Change Authority*

7. Change Request Process

7.1 Process Overview

All changes (except Standard Changes) must follow this process. Emergency changes follow an expedited version detailed in Section 12.

Step	Action	Responsible Party	Tool
1	Submit Change Request in ITSM tool with all required fields (see Section 8)	Change Requester	ITSM Tool
2	MIS Manager performs initial triage: validates classification, completeness, and assigns to CAB agenda	MIS Operations Manager	ITSM Tool
3	CAB reviews change: risk assessment, implementation plan, rollback plan, scheduling	CAB	CAB Meeting
4	CAB renders decision (Approve / Approve w/ Conditions / Defer / Reject)	CAB	ITSM Tool
5	If approved: schedule implementation within approved maintenance window	Change Implementer	ITSM Tool
6	Notify affected users/departments per communication plan	Change Requester	Email / Teams
7	Implement change per approved implementation plan	Change Implementer	As needed
8	Validate change: confirm success, test functionality, verify no unintended impact	Change Implementer	As needed
9	If failed: execute rollback plan, document failure, escalate as needed	Change Implementer	ITSM Tool
10	Complete Post-Implementation Review and close change record	Change Requester	ITSM Tool

7.2 Lead Time Requirements

- **Normal Changes:** Normal changes must be submitted a minimum of 5 business days before the planned implementation date to allow for CAB review
- **High-Risk Changes:** Changes with County-wide impact or affecting critical infrastructure must be submitted a minimum of 10 business days in advance
- **Emergency Changes:** See Section 12 for the expedited emergency change process

Framework Alignment: *NIST SP 800-53: CM-3 | CIS Control 4.1 | ITIL v4: Change Enablement — Change Flow*

8. Change Request Requirements

Every change request submitted in the ITSM Tool must include the following information. Incomplete requests will be returned to the requester.

8.1 Required Fields

Field	Description	Required For
Change Title	Clear, concise description of the change	All
Change Requester	Name and role of the person requesting the change	All
Change Implementer(s)	Name(s) of the person(s) who will execute the change	All
Change Classification	Standard, Normal, or Emergency	All

Field	Description	Required For
Risk Rating	Low, Medium, or High (per Section 4.2 matrix)	Normal, Emergency
Business Justification	Why is this change needed? What problem does it solve?	Normal, Emergency
Description of Change	Detailed technical description of what will be changed	All
Systems/CIs Affected	List of all servers, devices, services, or applications impacted	All
CJIS Systems Affected?	Yes/No — if Yes, CJIS review by Senior Security Analyst is mandatory	All
Implementation Plan	Step-by-step procedure for executing the change	Normal, Emergency
Rollback Plan	Step-by-step procedure to reverse the change if it fails	Normal, Emergency
Testing Plan	How the change will be validated after implementation	Normal, Emergency
Planned Start Date/Time	Scheduled date and time for implementation	Normal
Planned End Date/Time	Expected completion time	Normal
Maintenance Window?	Is this within the approved maintenance window? If not, justification required	Normal
Communication Plan	Who needs to be notified before, during, and after the change?	Normal (Medium/High risk)
Dependencies	Other changes, vendor availability, or conditions this change depends on	Normal

Framework Alignment: *NIST SP 800-53: CM-3 | ITIL v4: Change Enablement — Change Record*

9. Approval Authority

The approval authority for a change is determined by its classification and risk rating:

Change Type	Risk Level	Approval Authority
Standard Change	Low (pre-approved)	No individual approval required — follow SOP, log in ITSM Tool
Normal Change	Low	IT Operations Manager (may approve without full CAB)
Normal Change	Medium	CAB approval required
Normal Change	High	CAB approval required + IT Operations Manager sign-off
Normal Change (CJIS)	Any	CAB approval required + Senior Security Analyst sign-off
Emergency Change	Any	IT Operations Manager verbal/written approval (see Section 12)

9.1 Delegation of Authority

In the absence of the MIS Operations Manager, the Director of MIS may approve any changes. Otherwise, the following applies:

- The Senior Security Analyst may approve Low-risk Normal changes
- Medium and High-risk Normal changes must be deferred until the IT Operations Manager is available, unless the delay creates unacceptable operational risk — in which case, the Senior Security Analyst may approve with full documentation
- Emergency change authority cannot be delegated below the Senior Security Analyst level

Framework Alignment: *NIST SP 800-53: CM-3 (Change Control), AC-5 (Separation of Duties) | ITIL v4: Change Authority*

10. Maintenance Windows

10.1 Defined Maintenance Windows

Oklahoma County establishes the following maintenance windows to minimize business impact from planned changes:

Window	Schedule	Permitted Change Types
Primary Maintenance Window	Monday 6:00 PM – Tuesday 6:00 AM	All change types including high-risk and infrastructure-wide
Secondary Maintenance Window	Wednesday 6:00 PM – Thursday 5:00 AM	Low and Medium-risk changes only
Tertiary Maintenance Window	Sunday 8:00 AM – Sunday 12:00 PM	All change types including high-risk affecting the Sheriff's Office
Patch Window	Every Tuesday of each month, 8:00 PM – Wednesday 5:00 AM	Scheduled OS and application patching

10.2 Out-of-Window Changes

Changes implemented outside of a defined maintenance window require:

- Documented business justification explaining why the maintenance window cannot be used
- Explicit approval from the MIS Operations Manager (or delegate per Section 9)
- Notification to all affected departments and Offices at least 24 hours in advance (when possible)
- Enhanced monitoring during and after implementation

Changes during business hours (Monday–Friday, 7:00 AM–6:00 PM) are strongly discouraged for any change rated Medium or High risk. Out-of-window changes during business hours require MIS Operations Manager approval regardless of risk level.

10.3 Blackout Periods

No non-emergency changes may NOT be implemented during the following blackout periods:

- Fiscal year-end close (last 5 business days of the fiscal year and first 3 business days of the new fiscal year)
- Election periods (3 business days before through 1 business day after any County election)

- Any period designated by the MIS Operations Manager due to active incidents, audits, or special operational conditions

Emergency changes are exempt from blackout restrictions but require heightened scrutiny and documentation.

> ***Framework Alignment:*** *NIST SP 800-53: CM-3, MA-2 (Controlled Maintenance) | CIS Control 4.1 | ITIL v4: Change Schedule*

11. Implementation and Rollback

11.1 Implementation Requirements

All change implementers must adhere to the following requirements during change execution:

- Verify that the change record is in "Approved" status before beginning implementation
- Confirm that all pre-implementation backups, snapshots, or recovery points have been completed
- Follow the approved implementation plan step by step — deviations from the plan require immediate notification to the MIS Operations Manager
- Document actual start time, each major step completed, and any issues encountered in the ITSM change record
- Perform all validation and testing steps defined in the change record before declaring the change successful
- Notify affected users and the MIS Operations Manager upon completion

11.2 Rollback Criteria

A change must be rolled back if any of the following conditions are met:

- The change causes an unplanned service outage or degradation
- The change produces results that differ materially from what was expected
- The change cannot be completed within the approved maintenance window
- Post-implementation testing reveals functional failures or data integrity issues
- The Director of MIS, MIS Operations Manager, or Senior Security Analyst directs a rollback

The rollback plan must be executable by someone other than the change implementer. If the primary implementer is unavailable during an issue, a qualified team member must be able to execute the rollback from the documented plan alone.

11.3 Post-Implementation Validation

After every change, the implementer must verify:

- The system or service is functioning as expected
- Dependent systems and services are unaffected
- Monitoring and alerting are active and showing normal status

- End users can access the system or service (where applicable)
- The ITSM change record is updated with the actual outcome

Framework Alignment: *NIST SP 800-53: CM-3, CM-5 (Access Restrictions for Change), CP-10 (System Recovery and Reconstitution) | CIS Controls 4.1, 11.4*

12. Emergency Changes

12.1 Definition

An Emergency Change is a change that must be implemented immediately to:

- Resolve a Priority 1 (P1) or Priority 2 (P2) incident causing active service disruption
- Address an actively exploited or imminent security vulnerability
- Prevent imminent data loss, system failure, or safety hazard
- Comply with a time-sensitive legal, regulatory, or law enforcement directive

Emergency changes are not a mechanism to bypass the change process for convenience. Using the emergency change process for non-emergency changes is a policy violation.

12.2 Emergency Change Process

Step	Action	Timeline
1	Change implementer contacts the MIS Operations Manager (or Director of MIS or Senior Security Analyst if unavailable) to request emergency change authorization	Immediately
2	Verbal or written approval is granted (phone, text, email, or Teams message)	Within 15 minutes
3	Create an ITSM change record marked as "Emergency" with as much detail as available	Before or during implementation
4	Implement the change, documenting actions taken in real time	As needed
5	Complete post-implementation validation	Immediately after
6	Complete the full ITSM change record within 24 hours of implementation	Within 24 hours
7	Mandatory Post-Implementation Review at next CAB meeting	Next scheduled CAB

12.3 Emergency Change Documentation

The emergency change record must be completed within 24 hours of implementation and must include:

- The incident or condition that triggered the emergency
- Who authorized the emergency change and how (verbal, email, etc.)
- What was changed — detailed technical description
- What rollback plan was available (even if not executed)
- Post-implementation validation results
- Root cause analysis (if applicable) and recommendations to prevent recurrence

NOTE	All emergency changes will be reviewed at the next CAB meeting regardless of outcome. The CAB will assess whether the emergency classification was warranted, whether the change was properly executed, and whether a permanent fix or follow-up change is needed.

Framework Alignment: *NIST SP 800-53: CM-3, IR-4 (Incident Handling) | CIS Control 4.1 | ITIL v4: Emergency Change Process*

13. Post-Implementation Review (PIR)

13.1 When PIR is Required

A Post-Implementation Review must be completed for:

- All Normal changes rated Medium or High risk
- All Emergency changes (regardless of risk level)
- Any change that resulted in a rollback, failure, or unintended impact
- Any change to CJIS systems
- Any change specifically flagged for PIR by the CAB

13.2 PIR Content

The PIR must address the following questions and be documented in the ITSM change record:

- **Success Assessment:** Was the change implemented as planned?
- **Timeliness:** Was the change completed within the approved window?
- **Issues Encountered:** Were there any unplanned outages, errors, or deviations?
- **Rollback:** Was the rollback plan needed? If so, was it effective?
- **Communication:** Were users/departments properly notified?
- **Lessons Learned:** What could be improved for similar changes in the future?
- **Follow-Up Actions:** Are follow-up actions, additional changes, or documentation updates needed?

Framework Alignment: *NIST SP 800-53: CM-3, CA-7 (Continuous Monitoring) | ITIL v4: Post-Implementation Review*

14. CJIS-Specific Change Requirements

Changes to systems that process, store, or transmit Criminal Justice Information (CJI) are subject to additional requirements under the FBI CJIS Security Policy. These requirements supplement the general change management process.

14.1 CJIS Change Identification

Any change request that may affect a CJIS system must be flagged in the ITSM change record. CJIS systems include:

- CJIS-connected terminals and workstations
- Servers hosting or processing CJI data

- Network segments carrying CJI traffic
- Firewalls, VPN concentrators, and encryption devices protecting CJI
- Authentication and access control systems for CJI environments
- Audit logging systems that capture CJI access events

14.2 CJIS Change Approval

- All changes to CJIS systems require review and sign-off by the Senior Security Analyst, regardless of risk level
- Medium and High-risk changes to CJIS systems must be communicated to the County CJIS Local Agency Security Officer (LASO) prior to implementation
- Changes that alter the security architecture, encryption, or access control mechanisms of CJIS systems must be approved by the MIS Operations Manager and the LASO

14.3 CJIS Change Documentation

- All changes to CJIS systems must be retained for a minimum period consistent with CJIS audit requirements
- Change records must be available for review during CJIS audits
- The change record must document whether CJIS data was at any point exposed, at risk, or potentially affected during the change

CJIS	CJIS Security Policy 5.4 (Auditing and Accountability) and 5.10 (System and Communications Protection) require that changes to CJI systems be documented, authorized, and auditable. Unauthorized changes to CJIS systems are reportable security events.

Framework Alignment: *CJIS Security Policy v5.9.5: Sections 5.4, 5.5, 5.10 | NIST SP 800-53: CM-3, CM-5, AU-12*

15. Metrics and Reporting

15.1 Key Performance Indicators

The MIS Operations Manager will track the following change management metrics on a monthly basis:

Metric	Target	Measurement Source
Change Success Rate	≥ 95% of changes implemented without rollback or incident	ITSM Tool
Unauthorized Change Rate	0 unauthorized changes per month	ITSM Tool + audit logs
Emergency Change Percentage	≤ 10% of total changes classified as Emergency	ITSM Tool
CAB Compliance Rate	100% of required changes reviewed by CAB	CAB meeting minutes
PIR Completion Rate	100% of required PIRs completed within 5 business days	ITSM Tool

Metric	Target	Measurement Source
Mean Lead Time (Normal)	≤ 7 business days from request to implementation	ITSM Tool
Change-Related Incidents	≤ 2 incidents caused by changes per month	ITSM Tool
CJIS Change Compliance	100% of CJIS changes reviewed by Senior Security Analyst	ITSM Tool

15.2 Reporting

- Change management metrics will be included in the monthly MIS Operations report
- Trend analysis will be conducted quarterly to identify systemic issues or process improvement opportunities
- The CAB will review metrics at the first meeting of each month

Framework Alignment: *NIST SP 800-53: CM-3, CA-7, PM-6 (Measures of Performance) | ITIL v4: Continual Improvement*

16. Enforcement and Violations

16.1 Unauthorized Changes

An unauthorized change is any modification to a production system that was not approved through the processes defined in this policy. Unauthorized changes include changes made without a change record, changes made outside the approved scope or window, and changes made without required approvals.

Unauthorized changes will be treated as policy violations and may result in:

- Mandatory rollback of the unauthorized change
- Formal documentation of the violation in the employee's record
- Temporary or permanent revocation of system access privileges
- Disciplinary action in accordance with County personnel policies
- For CJIS systems: reporting to the LASO and potential CJIS access suspension

16.2 Repeated Non-Compliance

Patterns of non-compliance with the change management process — including incomplete documentation, skipped approvals, or failure to complete PIRs — will be addressed through:

- Retraining on change management procedures
- Increased oversight and additional approval requirements for the individual
- Escalation to County management if non-compliance continues

Framework Alignment: *NIST SP 800-53: CM-3, PL-4 (Rules of Behavior) | CIS Control 4.1*

For unauthorized changes originating from departmental IT operations outside of MIS, enforcement follows the escalation process defined in the IT Governance Charter (Section 9): written notification to the department, remediation period, IT Council deliberation, and Board of County Commissioners action if necessary. MIS retains the authority to block or reverse unauthorized changes to shared infrastructure immediately to protect County operations.

17. Policy Administration

17.1 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 MIS Operations Manager and the Director of MIS, and presented to the Oklahoma County IT Council for deliberation. Amendments follow the policy development process defined in the IT Governance Charter (Section 8) and require Board of County Commissioners approval by resolution.

- Significant changes to the County's IT environment, infrastructure, or team structure
- Changes to applicable compliance frameworks (CJIS Security Policy, NIST, CIS Controls)
- Findings from security incidents, audits, or post-implementation reviews
- Feedback from the CAB or operational teams indicating process gaps

17.2 Standard Change Catalog Review

The Standard Change Catalog (Section 5) will be reviewed quarterly by the CAB to:

- Validate that existing Standard Changes still meet the criteria for pre-approval
- Add new Standard Changes based on operational need and demonstrated success
- Remove or reclassify Standard Changes that have experienced failures or increased risk

17.3 Exception Requests

Requests for exceptions to any provision of this policy must follow the exception request process defined in the Acceptable Use Policy (IT-POL-AUP-001, Section 19.2).

Framework Alignment: *NIST SP 800-53: CM-1, PL-1, PM-1 | CIS Control 15.1*

18. Related Policies and Standards

This Change Management Policy operates in conjunction with the following documents:

Document	ID	Relationship
IT Governance Charter	IT-GOV-CHARTER-001	Parent usage policy; references change management requirements

Document	ID	Relationship
Acceptable Use Policy	IT-POL-AUP-001	Parent usage policy; references change management requirements
Information Security Policy	IT-POL-ISP-001	Planned — overarching security program policy
Incident Response Plan	IT-POL-IRP-001	Planned — emergency changes often triggered by incidents
Password and Access Management Policy	IT-POL-PAM-001	Planned — access control changes governed by this policy
System SOPs	Various	Standard change procedures and runbooks
CJIS Security Policy (FBI)	v5.9.5	Federal requirements for CJI system changes
NIST SP 800-53 Rev. 5	External	Federal security and privacy controls
CIS Controls v8	External	Consensus security best practices
ITIL v4 Foundation	External	Service management framework — Change Enablement practice

Acknowledgment

By signing below, I acknowledge that I have received, read, and understand the Oklahoma County Change Management Policy. I agree to comply with all provisions of this policy when initiating, approving, implementing, or reviewing changes to County IT systems.

I understand that unauthorized changes to County systems are a policy violation and may result in disciplinary action, access revocation, and — for CJIS systems — reporting to the appropriate authorities.

Printed Name: _____ **Role / Title:** _____

Signature: _____ **Date:** _____