OKLAHOMA COUNTY

INFORMATION TECHNOLOGY

Governance Charter

Establishing the Framework for County-Wide IT Policy, Standards, and Oversight

Document ID:	IT-GOV-CHARTER-001
Version:	1.0
Effective Date:	[Date of BOCC Resolution]
Last Reviewed:	[Date]
Classification:	Public
Document Owner:	Director of MIS
Adopted By:	Board of County Commissioners — Resolution No. [____]

Table of Contents

1. Purpose

Oklahoma County operates a decentralized information technology environment in which multiple elected officials' offices maintain independent IT staff and systems, all connected to a shared core infrastructure managed by the County's Management Information Systems (MIS) department.

This IT Governance Charter establishes the formal framework for County-wide information technology governance, including:

- The authority, composition, and operating procedures of the Oklahoma County IT Council (OCITC)
- The roles and responsibilities of MIS, Elected Office's IT operations, and the Director of MIS
- The process by which IT policies, standards, and guidelines are proposed, reviewed, adopted, and enforced across the County
- The delineation of shared infrastructure responsibilities versus Elected Office IT autonomy
- The compliance and accountability mechanisms that ensure consistent security and operational standards across all County IT operations

This Charter is adopted by resolution of the Board of County Commissioners and constitutes the authoritative governance framework for all Oklahoma County information technology activities.

> ***Framework Alignment:*** *NIST SP 800-53: PM-1 (Information Security Program Plan), PM-2 (Senior Information Security Officer) | CIS Control 15 (Service Provider Management) | COBIT 2019: EDM01 (Governance Framework)*

2. Scope

2.1 Organizational Scope

This Charter applies to all Oklahoma County Departments, Offices, and agencies that operate, manage, or use information technology resources, including:

Office / Department	IT Presence	Relationship to MIS
Management Information Systems (MIS)	Full IT department — County core infrastructure owner	Central IT authority for shared infrastructure and baseline standards
County Clerk's Office	Departmental IT staff	Tenant on MIS-managed core infrastructure; independent departmental systems
Assessor's Office	Departmental IT staff	Tenant on MIS-managed core infrastructure; independent departmental systems
Sheriff's Office	Departmental IT staff	Tenant on MIS-managed core infrastructure; CJIS systems owner; independent departmental systems
Treasurer's Office	Departmental IT staff	Tenant on MIS-managed core infrastructure; independent departmental systems
Court Clerk's Office	Departmental IT staff	Independent departmental systems; uses AOC resources.
BOCC Offices and Departments	Supported by MIS	Fully MIS-supported; no independent IT staff
District Attorney's Office	Supported by MIS	Fully MIS-supported; no independent IT staff

Office / Department	IT Presence	Relationship to MIS
Juvenile Bureau – Public Defender's Office	Supported by MIS	Fully MIS-supported; no independent IT staff

2.2 Technical Scope

This Charter and all policies adopted under its authority apply to:

- The County core network, internet connectivity, and shared telecommunications infrastructure managed by MIS
- All systems, devices, and services that connect to the County core network, regardless of which Department or Office owns or operates them
- All County data, regardless of where it is stored, processed, or transmitted
- All personnel who access County IT resources, including employees, contractors, vendors, and volunteers of any County Office or Department

Office and Departmental IT systems that do not connect to the County core network are encouraged but not required to comply with policies adopted under this Charter, except where federal or state law mandates compliance (e.g., CJIS Security Policy).

3. Guiding Principles

All IT governance decisions under this Charter shall be guided by the following principles:

Shared Accountability, Respect for Autonomy

Each elected official retains authority over the IT operations specific to their Office's mission. However, when those operations connect to shared County infrastructure or handle data subject to County-wide policy, shared standards apply. Governance exists to protect everyone on the shared platform, not to centralize control.

Security Is Not Optional

Baseline security standards protect all County Offices. A vulnerability in one Department or Office's systems connected to the shared network is a risk to every Office or Department. Security policies adopted under this Charter represent the minimum acceptable standard for all connected systems.

Transparency and Consensus

The IT Council operates through open deliberation and consensus. Policy recommendations are developed collaboratively, with input from all represented offices, before being forwarded to the Board of County Commissioners for adoption.

Compliance-Driven Standards

Oklahoma County is subject to federal and state compliance requirements, including the FBI CJIS Security Policy, NIST SP 800-53, HIPAA, and state data privacy laws. IT governance ensures the County meets these obligations consistently across all Offices.

Progress Over Perfection

Oklahoma County is building its IT governance program from the ground up. This Charter establishes the framework; policies, standards, and procedures will be developed iteratively over time. The goal is steady, measurable improvement.

4. Governance Structure

4.1 Overview

Oklahoma County IT governance operates through a three-tier structure:

Tier	Body	Role	Authority
1 — Adoption	Board of County Commissioners	Formally adopts County-wide IT policies by resolution	Final policy approval; binding on all County offices
2 — Deliberation	Oklahoma County IT Council	Reviews, deliberates, and recommends IT policies and standards; resolves cross-departmental IT issues	Recommends policies to BOCC; sets technical standards; mediates disputes
3 — Execution	MIS Department + Departmental IT	Develops, implements, and operationalizes IT policies and standards within their respective domains	MIS: shared infrastructure and baseline policy drafting. Departments: departmental systems and operations

4.2 Policy Adoption Flow

The following process governs the adoption of County-wide IT policies:

1. MIS (or any IT Council member) drafts a proposed policy and submits it to the IT Council for review
2. The IT Council reviews the proposed policy, requests modifications if needed, and deliberates until consensus is reached or a vote is called
3. The IT Council forwards the approved recommendation to the Board of County Commissioners with a supporting memorandum
4. The Board of County Commissioners considers the recommendation and, if approved, adopts the policy by resolution
5. Upon adoption, the policy is binding on all County offices and departments within its defined scope
6. MIS publishes the adopted policy and coordinates implementation across all affected offices

Policies recommended by the IT Council but not yet adopted by the BOCC do not have binding authority. However, MIS may implement recommended policies on MIS-managed infrastructure as operational standards pending BOCC adoption.

Framework Alignment: *COBIT 2019: EDM01 (Governance Framework Setting and Maintenance) | NIST SP 800-53: PM-1, PM-3 (Information Security Resources)*

5. Oklahoma County IT Council

5.1 Composition

The IT Council is composed of the following members:

Seat	Represented Office	Voting Status
1	County Clerk	Voting
2	Assessor	Voting
3	Sheriff	Voting
4	Treasurer	Voting
5	Court Clerk	Voting
6	County Commissioner — District 1	Voting
7	County Commissioner — District 2	Voting
8	County Commissioner — District 3	Voting
Chair	Director of MIS	Non-Voting

Each elected official designates their representative to the IT Council. Representatives may be the elected official themselves, their chief of staff, their IT Director, or another designee with authority to represent the office on IT matters. Designations must be submitted in writing to the Director of MIS.

5.2 Chairperson

The Director of MIS serves as the non-voting Chairperson of the OCITC. The Chairperson is responsible for:

- Setting the agenda for each IT Council meeting
- Facilitating discussion and maintaining order during meetings
- Ensuring that policy proposals are properly prepared, reviewed, and documented before Council deliberation
- Presenting IT Council recommendations to the Board of County Commissioners
- Reporting on the status of IT initiatives, policy compliance, and security posture to the Council
- Breaking tie votes only when a quorum is present and a tie persists after discussion

5.3 Voting and Quorum

The IT Council operates under the following rules:

- **Five (5) of eight (8) voting members must be present (in person or via approved teleconference) to conduct official business.**
- **The Council shall attempt to reach consensus on all matters. When consensus cannot be achieved, a formal vote is called.**
- **Each voting member has one vote. A simple majority of voting members present is required to approve a recommendation, provided a quorum is met.**
- **In the event of a tie, the Chairperson (Director of IT) casts the deciding vote.**

- **Voting members may designate a proxy in writing to the Chairperson. Proxy designations are valid for a single meeting unless otherwise specified.**

5.4 Meeting Cadence

- **The IT Council shall meet at a minimum quarterly. The Chairperson shall establish a recurring schedule at the beginning of each calendar year.**
- **The Chairperson or any three (3) voting members may call a special meeting with at least five (5) business days' notice.**
- **The Chairperson may call an emergency meeting with 24 hours' notice when an urgent IT security, compliance, or operational matter requires immediate Council attention.**

5.5 Meeting Procedures

- The Chairperson distributes the agenda and all supporting materials at least five (5) business days before each regular meeting
- Meeting minutes are recorded and distributed to all Council members within five (5) business days of each meeting
- Minutes shall document attendance, agenda items, discussion summaries, decisions, and action items with assigned owners and due dates
- Minutes are retained as official County records per the applicable records retention schedule

5.6 IT Council Responsibilities

The IT Council is responsible for the following:

Responsibility	Description
Policy Review and Recommendation	Review proposed IT policies and standards developed by MIS or member Offices; recommend adoption, modification, or rejection to the Board of County Commissioners
Standards Alignment	Ensure consistency of IT security and operational standards across all County Offices connected to shared infrastructure
Shared Infrastructure Decisions	Deliberate on matters affecting the County core network, shared services, and cross-departmental IT dependencies
Compliance Oversight	Monitor County-wide compliance with adopted IT policies and applicable federal/state requirements (CJIS, NIST, HIPAA)
Dispute Resolution	Mediate disputes between County offices related to IT policy, shared infrastructure, or resource allocation
Budget Input	Provide input on IT budget priorities that affect shared infrastructure and cross-departmental initiatives
Annual Review	Conduct an annual review of this Charter, all adopted IT policies, and the County's IT security posture

Framework Alignment: *COBIT 2019: EDM01, EDM05 (Stakeholder Engagement) | NIST SP 800-53: PM-1, PM-2 | ITIL v4: Governance*

6. Roles and Responsibilities

6.1 Board of County Commissioners

- Adopts County-wide IT policies by resolution upon recommendation of the IT Council
- Allocates resources for shared IT infrastructure and County-wide IT initiatives
- Receives annual reports from the Director of IT on the state of County IT operations and security

6.2 County Manager

- Provides executive oversight of the Director of MIS and the MIS department
- Ensures IT governance recommendations are considered in County-wide administrative decisions
- Supports enforcement of adopted IT policies across County Offices

6.3 Director of MIS

- Chairs the IT Council (non-voting)
- Oversees the MIS department and the County's shared IT infrastructure
- Responsible for drafting, maintaining, and operationalizing County-wide IT policies and standards
- Presents IT Council recommendations and annual reports to the Board of County Commissioners
- Serves as the County's primary point of accountability for IT security and compliance
- Coordinates with Elected Official IT leadership on cross-departmental initiatives, incident response, and compliance matters
- Reports to the County Manager

6.4 MIS Department

The Management Information Systems (MIS) department is responsible for:

- **Design, deployment, operation, and security of the County core network, internet connectivity, shared servers, core telecommunications, and enterprise services (email, directory services, ERP, etc.)**
- **Drafting IT policies, standards, and guidelines for IT Council review and BOCC adoption**
- **Establishing and enforcing minimum security standards for all systems connected to the County core network**
- **Serving as the coordinating body for IT security incidents that affect shared infrastructure or multiple County Offices**
- **Supporting Departmental IT offices in meeting CJIS, NIST, and other compliance requirements as they relate to shared infrastructure**
- **Publishing technical standards and configuration baselines for systems connecting to the County network**

6.5 Departmental IT Operations

IT staff and operations within individual elected officials' offices (County Clerk, Assessor, Sheriff, Treasurer, Court Clerk) are responsible for:

- Managing IT systems, applications, and infrastructure specific to their Office's mission and operations
- Complying with all County-wide IT policies adopted by the Board of County Commissioners under this Charter
- Complying with MIS-published technical standards and security baselines for any system connected to the County core network
- Participating in the IT Council through their designated representative
- Coordinating with MIS on changes that affect shared infrastructure, cross-departmental services, or network connectivity
- Reporting IT security incidents that affect or could affect shared infrastructure or other County Offices to MIS within the timeframes defined in the applicable Incident Response Plan
- Maintaining compliance with federal and state requirements applicable to their office (e.g., the Sheriff's Office with CJIS; the Treasurer with tax data protection, etc.)

Elected autonomy is preserved for Office-specific systems and operations. This Charter does not transfer management authority over departmental systems to MIS. However, all systems connected to the shared County network must meet the minimum security and operational standards established through the governance process defined herein.

7. Shared Infrastructure and Network Governance

7.1 MIS-Managed Infrastructure

The following infrastructure components are owned and managed by MIS and are designated as shared County infrastructure:

- County core network (backbone, distribution, and access layers)
- Internet connectivity and perimeter security (firewalls, IDS/IPS, web filtering)
- Core switching, routing, and wireless infrastructure
- Shared telecommunications infrastructure (PBX, POTS lines, SIP trunks, VoIP)
- Enterprise directory services (Active Directory / LDAP / Entra)
- Enterprise email and collaboration platforms
- Enterprise Resource Planning (ERP) Software (i.e., Munis)
- Geographic Information System (GIS) Software (i.e., ESRI)
- County-wide backup and disaster recovery infrastructure
- County data center(s) and server room physical infrastructure

7.2 Network Connection Requirements

Any system, device, or service connected to the County core network — regardless of which department owns it — must meet the following minimum requirements:

- Comply with all County-wide IT policies adopted under this Charter
- Meet the minimum security configuration baselines published by MIS (hardening standards, patching requirements, endpoint protection)
- Be registered in the County asset inventory maintained by MIS

- Not introduce unauthorized network services (DHCP, DNS, wireless access points, VPN tunnels) without MIS approval
- Submit to MIS vulnerability scanning and security monitoring for any component connected to the shared network

MIS reserves the right to disconnect any device or system from the County core network that poses an imminent security risk, regardless of which department owns it. Disconnection actions will be documented, and the owning department will be notified immediately with an explanation and remediation requirements.

> ***Framework Alignment:*** *NIST SP 800-53: CA-3 (System Interconnections), SC-7 (Boundary Protection), CM-8 (Information System Component Inventory) | CIS Controls 1.1, 1.2, 12.1*

7.3 Change Coordination

Changes to shared infrastructure are governed by the Oklahoma County Change Management Policy (IT-POL-CHG-001). Additionally:

- Departmental IT operations must notify MIS of any change to departmental systems that could affect the County core network, shared services, or other Offices and Departments
- MIS must notify affected Offices and Departments of planned changes to shared infrastructure that could impact their operations, per the notification schedules in the Change Management Policy
- Disputes regarding change scheduling or impact are escalated to the IT Council for resolution

8. IT Policy Framework

8.1 Policy Hierarchy

IT governance documents adopted under this Charter are organized in the following hierarchy:

Document Type	Purpose	Approval Authority	Binding Scope
Governance Charter	Establishes the governance framework, roles, and authority structure	Board of County Commissioners (Resolution)	All County Offices
Policies	Define mandatory requirements, rules, and expectations for IT activities across the County	Board of County Commissioners (Resolution), upon IT Council recommendation	All County offices (as defined in each policy's scope)
Standards	Define specific technical or procedural requirements that implement a policy (e.g., minimum password length, encryption requirements)	IT Council approval; published by MIS	All systems connected to County core network
Guidelines	Provide recommended (non-mandatory) practices that support policies and standards	Published by MIS; informational	Advisory — not binding

Document Type	Purpose	Approval Authority	Binding Scope
Standard Operating Procedures (SOPs)	Define step-by-step instructions for executing specific tasks	MIS (for MIS operations) or department IT lead (for departmental operations)	Department-specific unless adopted County-wide

8.2 Policy Development Process

Any County Office or IT Council member may propose a new policy or amendment. The standard development process is:

7. Proposal: The sponsoring office submits a policy proposal to the Director of MIS, including the problem statement, proposed scope, and draft language (if available)
8. Drafting: MIS (or the sponsoring Office, in collaboration with MIS) develops a formal draft policy aligned with applicable frameworks (NIST, CIS, CJIS)
9. Review Period: The draft is distributed to all IT Council members for a minimum 15-business-day review and comment period
10. Revision: MIS incorporates feedback and produces a revised draft. Substantial changes may require an additional review cycle.
11. IT Council Deliberation: The IT Council discusses the revised draft at a regular or special meeting. The Council votes to recommend adoption, request further revision, or reject the proposal.
12. BOCC Adoption: Recommended policies are forwarded to the Board of County Commissioners with a memorandum summarizing the policy, the Council's recommendation, and any dissenting views.
13. Publication and Implementation: Upon BOCC adoption, MIS publishes the policy and coordinates implementation, training, and awareness across all affected offices.

8.3 Policy Review Cycle

All policies adopted under this Charter are subject to periodic review:

- **All adopted policies are reviewed at least once per calendar year by MIS and the IT Council to ensure continued relevance, accuracy, and compliance alignment.**
- **A policy must be reviewed outside the annual cycle when: a significant security incident occurs; a referenced compliance framework is updated (e.g., CJIS Security Policy revision); organizational or infrastructure changes materially affect the policy's scope.**
- **Any policy that has not been reviewed within 24 months of its last review date is flagged for mandatory review at the next IT Council meeting.**

Framework Alignment: *NIST SP 800-53: PM-1 (Information Security Program Plan) | CIS Control 15.1 | COBIT 2019: APO01 (Management Framework)*

9. Compliance and Enforcement

9.1 Compliance Expectations

All County Offices are expected to comply with IT policies adopted by the Board of County Commissioners under this Charter. Compliance is monitored through the following mechanisms:

- Periodic compliance assessments conducted by MIS (or a designated third party) to evaluate adherence to adopted policies and standards
- IT Council review of compliance status at regular meetings
- Annual reports from the Director of MIS to the BOCC on County-wide IT compliance posture
- CJIS audits and other external compliance reviews, the results of which are shared with the IT Council

9.2 Non-Compliance

When a compliance gap or policy violation is identified:

14. Notification: MIS notifies the affected Office's IT leadership and IT Council representative of the finding in writing, including the specific policy provision, the nature of the gap, and the risk it creates.
15. Remediation Period: The affected department has 30 calendar days (or 10 days for critical security findings) to submit a remediation plan to MIS.
16. Remediation Execution: The Office or Department implements the remediation plan within the agreed timeline. MIS is available to provide technical assistance.
17. Escalation: If remediation is not completed within the agreed timeline and no extension has been granted, the matter is escalated to the IT Council for deliberation.
18. IT Council Action: The IT Council may recommend corrective actions, including resource allocation, timeline adjustments, or — in cases of persistent non-compliance creating material risk — escalation to the Board of County Commissioners.
19. BOCC Action: The Board of County Commissioners may take any action within its authority to address persistent non-compliance, including directing compliance, conditioning resource allocation, or other measures consistent with applicable law.

9.3 Emergency Security Actions

Notwithstanding the escalation process above, MIS retains the authority to take immediate protective action when a connected system poses an imminent threat to the County core network or other Offices and Departments:

- MIS may disconnect systems, block network traffic, or disable accounts to contain a security threat
- MIS must notify the affected department and the Director of MIS within one (1) hour of taking emergency action
- The IT Council must be briefed on any emergency security action at the next scheduled meeting or via emergency session if warranted
- Emergency actions are temporary containment measures; they do not constitute disciplinary action and must be lifted as soon as the threat is remediated

CJIS	CJIS Security Policy compliance is a federal requirement, not a discretionary policy choice. Non-compliance with CJIS requirements on systems processing CJI may result in loss of access to FBI CJIS systems, affecting the Sheriff's Office and any other Office with CJIS access. CJIS compliance gaps are treated as critical findings with expedited remediation timelines.

Framework Alignment: *NIST SP 800-53: CA-2 (Security Assessments), CA-7 (Continuous Monitoring), PM-14 (Testing, Training, and Monitoring) | CIS Control 4.1*

10. Security Governance

10.1 County-Wide Security Baseline

MIS is responsible for establishing and maintaining a County-wide security baseline that applies to all systems connected to the County core network. This baseline addresses:

- Endpoint protection requirements (antivirus, EDR, host-based firewall)
- Patching and vulnerability management standards
- Authentication and access control requirements (password policy, MFA)
- Encryption requirements for data in transit and at rest
- Logging and audit requirements
- Network segmentation and boundary protection standards

The security baseline is published by MIS as a Technical Standard under the policy hierarchy defined in Section 8. It does not require BOCC resolution but must be approved by the IT Council.

10.2 CJIS Compliance Coordination

The Sheriff's Office is the primary Criminal Justice Agency (CJA) for Oklahoma County CJIS operations. CJIS compliance coordination is structured as follows:

- The Sheriff's Office designates the County CJIS Local Agency Security Officer (LASO)
- MIS supports CJIS compliance for shared infrastructure components that carry or support CJI traffic
- Any County Office or system that accesses, processes, or supports CJI must comply with the FBI CJIS Security Policy, regardless of whether the system is managed by MIS or by departmental IT
- CJIS audit findings related to shared infrastructure are jointly owned by MIS and the Sheriff's Office for remediation
- The LASO has authority to suspend CJI access on any County system that is found to be non-compliant with CJIS requirements

10.3 Incident Response Coordination

IT security incidents that affect shared infrastructure or cross departmental boundaries are coordinated through MIS:

- MIS serves as the incident response coordinator for multi-department and shared infrastructure incidents
- Individual departments are responsible for incident response on their own systems but must notify MIS immediately when an incident affects or could affect shared infrastructure or other offices
- The Incident Response Plan (when adopted) will define specific roles, escalation procedures, and communication protocols for County-wide incidents
- All CJIS security incidents are reported through the LASO per CJIS Security Policy requirements

Framework Alignment: *NIST SP 800-53: IR-1 (Incident Response Policy), IR-6 (Incident Reporting), SI-4 (System Monitoring) | CJIS Security Policy 5.3 (Incident Response)*

11. Dispute Resolution

Disagreements between County Offices regarding IT policy interpretation, shared infrastructure decisions, change management conflicts, or compliance requirements are resolved through the following escalation path:

1. Direct Resolution: The affected parties (Office IT leadership and MIS) attempt to resolve the matter directly through discussion and negotiation.
2. Director of IT Mediation: If direct resolution fails, either party may request mediation by the Director of IT, who will facilitate a resolution meeting within 10 business days.
3. IT Council Deliberation: If mediation fails, the matter is placed on the next IT Council meeting agenda. The Council hears both parties and issues a recommendation by majority vote.
4. County Manager Review: If the IT Council's recommendation is not accepted by the affected parties, the matter may be escalated to the County Manager for a binding administrative decision.
5. Board of County Commissioners: Matters of policy-level significance that cannot be resolved administratively may be brought before the BOCC by the County Manager or any affected elected official.

The dispute resolution process is intended to be collaborative, not adversarial. Most IT disputes should be resolved at Stages 1 or 2.

12. Charter Administration

12.1 Amendments

This Charter may be amended through the following process:

- Any IT Council member or the Director of IT may propose an amendment
- Proposed amendments follow the same review and approval process as new policies (Section 8.2)
- Amendments require approval by the Board of County Commissioners by resolution
- Minor administrative corrections (formatting, typographical errors, title updates) may be made by the Director of IT without BOCC action, provided no substantive change to policy language occurs

12.2 Annual Review

The Director of IT shall coordinate an annual review of this Charter with the IT Council. The annual review shall assess:

- Whether the governance structure is functioning as intended
- Whether roles and responsibilities require adjustment
- Whether the policy development and adoption process is effective
- Whether new compliance requirements or organizational changes necessitate Charter amendments
- The overall state of County IT security and operational maturity

The results of the annual review shall be presented to the Board of County Commissioners by the Director of IT.

12.3 Effective Date

This Charter takes effect upon adoption by the Board of County Commissioners by resolution.

13. Related Policies and Documents

Document	ID	Status
IT Governance Charter (this document)	IT-GOV-CHARTER-001	Draft Complete
Acceptable Use Policy	IT-POL-AUP-001	Draft Complete
Change Management Policy	IT-POL-CHG-001	Draft Complete
Information Security Policy	IT-POL-ISP-001	Draft Complete
Incident Response Plan	IT-POL-IRP-001	Draft Complete
Password and Access Management Policy	IT-POL-PAM-001	Draft Complete
County IT Security Baseline (Technical Standard)	IT-STD-SEC-001	To be created
FBI CJIS Security Policy	External	Current Version
NIST SP 800-53 Rev. 5	External	Current Version
CIS Controls v8	External	Current Version

Adoption and Signatures

This Information Technology Governance Charter is hereby adopted by the Board of County Commissioners of Oklahoma County, Oklahoma, by Resolution No. [_____], on this _____ day of _____, 20___.

County Commissioner — District 1

Signature Date

County Commissioner — District 2

Signature Date

County Commissioner — District 3

Signature Date

Attest:

County Clerk

Signature Date

Acknowledgment by IT Council

We, the undersigned representatives of the Oklahoma County IT Council, acknowledge that we have reviewed this IT Governance Charter and support its adoption by the Board of County Commissioners.

County Clerk Representative	**Date:**
County Assessor Representative	**Date:**
Sheriff's Office Representative	**Date:**
County Treasurer Representative	**Date:**
Court Clerk Representative	**Date:**
Director of Information Technology (Chairperson)	**Date:**