County IT Governance Policy

Authority, Accountability, Oversight, and County-wide Technology Standards

1. Purpose

The purpose of this policy is to establish clear authority, accountability, and governance for information technology services across the County. This policy formalizes existing practices, supports compliance requirements, improves risk management, and ensures that County technology resources are secure, reliable, sustainable, and cost-effective.

2. Scope

This policy applies to all County departments, offices, elected officials, employees, contractors, vendors, systems, networks, devices, applications, data services, and technology resources that are County-owned, County-managed, County-funded, or connected to County systems.

3. Governance Principles

County technology governance shall be based on security, operational continuity, compliance, transparency, responsible stewardship of public resources, departmental collaboration, and clear technical authority.

4. Reporting and Oversight Structure

Role	Authority / Responsibility
Commissioners Court	Retains budgetary authority, strategic policy oversight, and authority to approve major funding decisions.
County Auditor	Serves as administrative supervisor of the IT Director for coordination, accountability, escalation, documentation, and evaluation.
IT Director	Leads the IT Department and holds final technical and operational authority for County technology systems within approved budget and policy boundaries.
IT Advisory Committee	Provides advisory input, transparency, risk awareness, and cross-department coordination. It does not approve, veto, or manage IT operations.
Departments and Elected Offices	Retain ownership of business processes, official records, statutory responsibilities, and operational requirements.

5. Technical Authority of the IT Director

The IT Director holds final technical authority for County technology architecture, configuration, and operational standards, including:

- Network architecture, connectivity, segmentation, wireless, routing, switching, and firewall configuration.
- Information security standards, controls, monitoring, incident response, and technical risk mitigation.
- Identity and access management, including account provisioning, MFA, privileged access, and access lifecycle processes.
- Supported hardware, operating systems, software, endpoint configurations, cloud services, and server platforms.
- Technical requirements for vendor-managed systems and integrations.
- Backup, disaster recovery, business continuity, and system resiliency standards.
- Documentation, inventory, lifecycle planning, and configuration standards.

6. IT Advisory Committee

The County IT Advisory Committee is established to provide structured input and transparency on County-wide technology matters. The Committee is advisory only. It does not manage IT staff, direct daily operations, or override the authority of Commissioners Court, the County Auditor, or the IT Director.

7. Data Ownership and System Control

Departments and elected offices retain ownership and custodianship of their official records, business processes, and statutory responsibilities. The IT Department manages, secures, administers, and supports the underlying technology systems used to store, process, access, protect, transmit, or recover County data.

8. Technology Procurement and Review

All technology purchases, subscriptions, systems, devices, services, software, cloud platforms, vendor-managed systems, and network-connected equipment must be reviewed by IT before acquisition or deployment. IT review shall evaluate security, compatibility, supportability, licensing, lifecycle cost, compliance, vendor access, integration, data protection, and operational impact.

9. Vendor Access and Vendor-Managed Systems

- IT shall be designated as the primary technical contact for vendor-managed systems whenever feasible.
- Vendor administrative access must be approved, documented, and limited to the minimum access required.
- Vendors must coordinate technical changes through IT before making configuration, network, integration, or access changes.
- IT will maintain available technical documentation and credentials to support continuity, audit readiness, and security.

10. Standards, Exceptions, and Risk Acceptance

The IT Department shall maintain written technical standards for County-managed technology. Exceptions may be granted where justified by operational need. Exceptions must be documented and must include risk acknowledgment by the requesting Department Head or elected official and the IT Director. High-impact exceptions may be escalated to the County Auditor and, where appropriate, Commissioners Court.

11. Compliance and Audit Support

This governance structure supports compliance and audit readiness for applicable requirements including CJIS, election security assessments, cybersecurity controls, financial systems, public records, privacy obligations, and other operational risk areas. IT shall coordinate technical documentation, evidence gathering, system access controls, and remediation activities as needed.

12. Administrative Oversight Clarification

Administrative supervision of the IT Director by the County Auditor is intended to align IT with County-wide internal controls, compliance, fiscal responsibility, audit readiness, and operational risk management. This structure does not place IT under judicial operational control. Commissioners Court retains budgetary and strategic policy authority and may revise the administrative oversight structure as deemed necessary.

13. Review and Updates

This policy shall be reviewed periodically and updated as County technology needs, compliance requirements, risks, and operational priorities evolve. Material changes should be documented and communicated to affected departments.

Effective Date

This policy becomes effective upon action or acknowledgment by Commissioners Court, subject to any legal or administrative review required by the County.