

County IT Department Charter

Mission, Responsibilities, Authority, and Guiding Principles

Mission

To provide secure, reliable, resilient, and efficient technology services that support County operations, public safety, judicial functions, financial stewardship, elections, emergency services, and public service delivery.

Vision

To operate a centralized, standards-based, transparent, and sustainable technology environment that balances departmental autonomy with County-wide security, resiliency, compliance, and fiscal responsibility.

Core Responsibilities

- Enterprise infrastructure, networking, wireless, internet connectivity, and network segmentation.
- Cybersecurity, endpoint protection, monitoring, incident response, and technical risk management.
- Identity and access management, including Entra standardization, MFA, privileged access, and account lifecycle processes.
- Endpoint, server, cloud, and application administration.
- Technology standards, lifecycle management, inventory, and asset documentation.
- Vendor technical coordination and review of technology purchases and integrations.
- Backup, disaster recovery, business continuity, and ransomware resilience planning.
- Audit support and compliance documentation for CJIS, election security, financial systems, public records, and other applicable requirements.
- Support services, ticketing workflows, onboarding/offboarding coordination, and end-user technology assistance.

Guiding Principles

- Security-first design.
- Consistency without unnecessary bureaucracy.
- Collaboration with departments and elected offices.
- Compliance with applicable regulatory and audit requirements.
- Transparency, documentation, and accountability.
- Responsible stewardship of public resources.
- Standardization where it improves reliability, security, and cost control.
- Practical flexibility where operational needs justify exceptions.

Authority

The IT Director is empowered to establish and enforce technical standards necessary to protect County systems, data, users, and technology investments. The IT Director shall coordinate with departments to meet operational needs while maintaining final technical authority over County-managed systems and networks.

Service Expectations

The IT Department should prioritize work based on risk, operational impact, public safety, legal or audit deadlines, cybersecurity exposure, service disruption, and long-term County value. Routine support should move toward structured ticketing, documented workflows, and measurable follow-up.

Review and Updates

This Charter shall be reviewed periodically and updated as County technology needs, staffing, risk, and compliance requirements evolve.