County IT Written Standards

Minimum Technical Requirements for County-managed Technology

Purpose

These standards establish minimum, enforceable technical requirements for County information systems. They are intended to be lightweight, practical, and flexible enough to support diverse departmental needs while ensuring security, reliability, compliance, and supportability.

Scope

These standards apply to all County departments, offices, elected officials, employees, contractors, vendors, devices, software, services, and systems using County-owned, County-managed, County-funded, or County-connected technology.

1. Workstation and Endpoint Standards

- County workstations and laptops shall be procured through County-approved vendors or otherwise approved by IT.
- Standard workstation platforms shall be selected and maintained by IT to improve supportability and lifecycle planning.
- Unsupported or end-of-life operating systems are prohibited from connecting to County-managed networks unless a documented exception exists.
- All County endpoints must use IT-approved endpoint protection, receive security updates, and use full-disk encryption where supported and appropriate.
- Local administrator access shall be limited to operational necessity and is subject to review, removal, and documented exception handling.

2. User Accounts and Access Control

- User accounts shall be created, modified, disabled, and removed through IT-managed processes.
- Access shall be based on job role, business need, and least-privilege principles.
- Multi-factor authentication shall be required where technically feasible, especially for remote access, administrative accounts, public safety systems, CJIS-related systems, cloud services, and sensitive systems.
- Access changes must be reported promptly for terminations, transfers, role changes, and contractor/vendor changes.

3. Network Standards

- County networks shall be designed, managed, and secured by IT.
- Unauthorized routers, switches, wireless access points, modems, hotspots used as permanent infrastructure, or unmanaged network equipment are prohibited unless approved by IT.
- Networks shall be logically segmented where appropriate to support public safety, CJIS, courts, elections, finance, guest access, VoIP, servers, printers, cameras, and general County operations.
- Remote access to County systems must be approved by IT and secured using IT-approved methods.

4. Server, Cloud, and Application Standards

- Servers and cloud services supporting County operations must be reviewed and approved by IT before deployment.
- Software applications must be reviewed by IT before purchase, subscription, renewal, or deployment.
- Applications must be supported, licensed, maintained, and documented according to vendor and IT requirements.
- IT shall be the primary technical contact for vendor-managed systems whenever feasible.

5. Data Protection and Backup Standards

- Departments are responsible for identifying sensitive, regulated, or mission-critical data.
- County systems must be included in an IT-approved backup or recovery strategy where feasible.
- Backup frequency, retention, testing, and recovery priority shall be defined by IT based on risk and operational need.
- County data shall be stored only on approved systems and services. Personal or unapproved cloud storage is prohibited for County data.

6. Security Monitoring and Incident Response

- IT may monitor County systems and networks to ensure security, availability, compliance, and operational integrity.
- Suspected security incidents, lost devices, suspicious emails, unauthorized access, malware, ransomware indicators, or vendor access concerns must be reported to IT immediately.
- IT will coordinate incident response activities, including vendor coordination, law enforcement coordination, containment, recovery, communication, and documentation where required.

7. Procurement, Vendor, and Change Standards

- Technology purchases, subscriptions, services, integrations, and renewals must be reviewed by IT before acquisition or deployment.
- Vendors must coordinate technical changes with IT before making network, access, firewall, server, cloud, or application configuration changes.
- Administrative credentials and technical documentation should be documented and retained where feasible to ensure continuity and audit readiness.

8. Exceptions and Risk Acceptance

- Exceptions to these standards must be documented and approved by IT.
- Approved exceptions must include operational justification and risk acknowledgment by the requesting Department Head or elected official and the IT Director.
- High-risk exceptions may be escalated to the County Auditor and, where appropriate, Commissioners Court.

Administrative Reporting Clarification

The County IT Department remains a County department subject to the authority of Commissioners Court for budgetary and strategic policy matters. Administrative supervision of the IT Director is assigned to the County Auditor. This structure does not place IT under judicial operational control. The purpose is to align IT oversight with County-wide internal controls, compliance, documentation, audit readiness, and risk management while maintaining transparency and accountability.

Review and Updates

These standards shall be reviewed periodically and updated as technology, compliance requirements, risks, and County operations evolve.