IT Operational Continuity and Knowledge Management Plan

Supporting Attachment to County IT Governance Packet

1. Purpose

The purpose of this plan is to ensure that essential County technology knowledge is documented, maintained, and transferable. County IT supports a broad range of department-specific systems, vendor platforms, local servers, network devices, endpoints, public safety tools, financial applications, election support systems, access control, phones, and records-related technology. This knowledge must not depend on one person, one technician, or one informal memory trail.

2. Background

The IT Department previously developed an internal orientation packet, knowledgebase, and training material for new or future IT employees. That material documented County office functions, department software, vendor contacts, support notes, hardware standards, servers, network attached storage, peripherals, phones, GPS devices, hotspots, and other recurring operational details. This plan updates that concept into a formal operational continuity practice.

3. Objectives

- Reduce single-point dependency in the IT Department.
- Improve onboarding and cross-training for IT staff.
- Preserve institutional knowledge as employees, officials, vendors, and systems change.
- Support faster troubleshooting and more consistent service delivery.
- Improve audit readiness and continuity of operations.
- Document technical dependencies for critical County functions.
- Support long-term modernization by identifying outdated systems, unsupported platforms, and fragile workflows.

4. Scope

The knowledge management program should include, at minimum, documentation for the following areas:

- County department functions and technology dependencies.
- Critical software platforms and vendor contacts.
- System ownership and support boundaries.
- Servers, network attached storage, cloud systems, and local application hosts.

- Network devices, firewalls, switches, wireless access points, and site connectivity.
- Endpoint standards, workstation/laptop specifications, printers, copiers, scanners, phones, tablets, GPS devices, and hotspots.
- Recurring troubleshooting procedures and known issues.
- Backup responsibilities, recovery notes, and disaster recovery dependencies.
- Security-sensitive workflows, including CJIS, elections, public safety, access control, and financial systems.
- Onboarding, offboarding, role change, and technician training procedures.

5. Documentation Standards

- **Controlled Location.** Documentation should be stored in an approved County-controlled system, such as a secure internal knowledgebase, SharePoint site, or other IT-approved documentation platform.
- **Searchable Format.** Documents should be organized so technicians can quickly find information by department, system, vendor, building, device type, or support issue.
- **Clear Ownership.** Each major article or section should identify who is responsible for keeping it current.
- **Sensitive Information Handling.** Documentation should not expose passwords, confidential data, CJIS-sensitive information, election-sensitive details, or security configurations to unauthorized users.
- **Version Awareness.** Major updates should show when the content was last reviewed or changed.
- **Practical Use.** Documentation should be written for actual support use, not for appearance. Steps should be clear enough for another IT employee to follow under pressure.

6. Recommended Knowledgebase Structure

Category	Examples	Purpose
Departments and Offices	County Clerk, Auditor, Sheriff, Elections, EMS, Tax Office, JP offices	Shows what each office does and which systems support that function.
Software and Vendors	LGS, NetData, AgendaQuick, TimeClock Plus, Spillman, CopSync, Votec, ES&S, PACS, ArcGIS, NinjaOne, Microsoft 365	Defines contacts, support boundaries, known issues, and setup notes.
Infrastructure	Servers, NAS devices, firewalls, switches, APs, internet circuits	Documents dependencies, locations, lifecycle status, and recovery notes.
Endpoints and Peripherals	Workstations, laptops, printers, copiers, scanners, phones, GPS, hotspots	Supports consistent troubleshooting and replacement planning.
Security and Compliance	CJIS, MFA, least privilege, EDR, backups, incident reporting	Connects daily operations to compliance and risk control.
Runbooks	Mapped drive fixes, scanner setup, printer issues, local SQL service checks, GPS setup	Turns recurring tribal knowledge into repeatable procedures.
Employee Training	Orientation, code of conduct, service	Shortens onboarding time and

	expectations, tools access	improves user service quality.

7. Service Philosophy for IT Staff

The County IT Department should maintain a service philosophy emphasizing professionalism, patience, respect, composure, adaptability, and a practical focus on making County users more efficient. Technical skill is required, but successful County IT support also depends on trust, communication, restraint, and the ability to work effectively with elected officials, department heads, staff, vendors, and public safety personnel.

8. Implementation Steps

1. Review the existing orientation packet and identify outdated, sensitive, or public-facing-inappropriate content.
2. Separate public governance concepts from internal technical details.
3. Move internal technical content into a secure County-controlled knowledgebase.
4. Create standard article templates for department profiles, vendor systems, support runbooks, infrastructure assets, and training topics.
5. Assign responsibility for reviewing and updating each major category.
6. Use the knowledgebase during new IT employee onboarding and recurring cross-training.
7. Review high-risk documentation quarterly and general documentation annually.

9. Governance Connection

This plan supports the County IT Governance Policy by improving accountability, reducing operational risk, supporting audit readiness, and making IT service delivery more consistent. It also supports the strategic roadmap by reducing single-point dependency and turning informal operational knowledge into controlled County documentation.

10. Review Cycle

This plan should be reviewed annually by the IT Director and County Auditor, with advisory input from the IT Advisory Committee when appropriate. Major system changes, staffing changes, compliance findings, or incident response lessons learned should trigger targeted updates.

Acknowledged by County Auditor: Date:

_____ _____

IT Director: Date:

_____ _____