LEADERSHIP

Guide to Preserving Institutional Knowledge in a Fire/EMS Department

Departments lose critical knowledge when responsibilities, accounts and recurring processes live with one person. Preserve what the organization needs before a departure creates an emergency.

9 MIN READ | AUGUST 2026

IN SHORT

A practical guide to documenting responsibilities, sharing access, cross-training members and protecting operational and administrative continuity in fire and EMS departments.

Every fire and EMS department depends on knowledge that does not appear in an SOP, roster or job description.

Someone knows how the annual state filing is prepared, which vendor services the generator, why a training requirement was configured a certain way and how to recover the department's website. Someone remembers the history behind a policy, the county contact who can solve a problem and the manual step required when an integration fails.

That knowledge often becomes visible only when the person who holds it is unavailable.

Institutional knowledge includes operational, administrative, technical, financial and relationship information the department needs to function over time.

Preserving it does not mean documenting every thought or eliminating personal judgment. It means ensuring critical responsibilities can continue when people retire, transfer, are promoted, take leave or depart unexpectedly.

Identify Critical Responsibilities

Begin with the work the department must perform, not the people currently performing it.

Create an inventory covering areas such as:

- Membership and personnel records
- Recruitment and onboarding
- Training and certifications
- Scheduling and staffing
- Incident reporting
- LOSAP, benefits and incentives
- Payroll and finance
- Apparatus and equipment
- Facilities and utilities
- Purchasing and vendors
- Grants and compliance
- Websites and social media
- Software administration and integrations
- Public records and governance
- Events, fundraising and hall rentals

For each responsibility, identify the primary owner, backup, frequency, deadline, systems used, outside contacts and consequence if missed.

Focus first on work that affects safety, compliance, money, access or uninterrupted operations.

Find the Single-Person Dependencies

Ask what stops when one specific person is unavailable.

Warning signs include:

- Only one person has administrator access.
- A recurring report depends on a private spreadsheet.
- No one else knows the renewal date or contract terms.
- Vendor relationships live in a personal phone.
- A process is described as “ask Joe” or “Mary handles that.”
- Instructions exist only in old emails.
- Another person has never completed the task.
- The department cannot recover an account without the owner.

Not every responsibility needs several people performing it daily. Every critical responsibility needs a documented backup and a practical transfer path.

Build a Responsibility Register

A responsibility register is a simple index of recurring and critical work.

Useful fields include:

- Responsibility name
- Purpose
- Primary owner
- Backup owner
- Schedule or trigger
- Systems and accounts
- Required inputs
- Outside contacts
- Expected output
- Approval authority
- Documentation location
- Last review date

The register does not replace detailed procedures. It helps leadership see what exists, where the instructions live and which areas have no backup.

Review it quarterly and during every leadership or administrative transition.

Document the Process at the Right Level

Documentation should allow a reasonably qualified person to understand and complete the work.

Include:

1. Why the process exists
2. When it occurs
3. Who initiates and approves it
4. Required information
5. Step-by-step actions
6. Common exceptions
7. Final output or confirmation
8. Records that must be retained
9. Where to get help

Use screenshots or short video demonstrations when they add clarity, but do not rely on video alone. Searchable written steps are easier to update and use during an urgent problem.

Record the reason behind important choices. A future administrator needs to know not only which setting was selected, but what operational or policy need it serves.

Create a Recurring Operations Calendar

Many knowledge failures involve work that happens monthly, quarterly or annually.

Maintain a shared calendar for:

- License and certification renewals
- Insurance
- Contracts and subscriptions
- Government filings
- Budget preparation
- Grant reports
- LOSAP and benefit deadlines
- Apparatus and facility inspections
- Preventive maintenance
- Elections and appointments
- Required training
- Website and domain renewals
- Access and security reviews

Each event should identify an owner, backup, preparation window and documentation link. Use reminders early enough for the department to act before a deadline becomes urgent.

Protect Accounts and Access

Critical accounts should belong to the department, not a person's private email address.

This includes:

- Domain registration
- Website hosting
- Social media
- Banking and payments
- Member-management systems
- Records and reporting platforms
- Cloud storage
- Email administration
- Analytics and monitoring
- Vendors and utilities

Use department-controlled email addresses, individual user accounts, multifactor authentication and an approved password manager. Maintain more than one authorized administrator.

Document recovery methods and test them. A backup administrator who cannot complete account recovery is not a reliable backup.

Remove access promptly when a person leaves or changes responsibility. Preserve audit history and necessary records.

Cross-Train Through Real Work

Reading a procedure is not the same as completing it.

Backups should observe the task, perform it under supervision and eventually complete it independently. Rotate appropriate recurring responsibilities so knowledge remains active.

Use three stages:

1. **Show:** The current owner explains and performs the process.
2. **Do together:** The backup performs it with the owner available.
3. **Verify:** The backup completes the work independently and the result is reviewed.

Schedule periodic refreshers for work that happens infrequently. A person trained two years ago may not remember the process or know what changed.

Capture Decisions and Their Context

Departments often preserve the final policy while losing the reason behind it.

Maintain a decision log for significant administrative and technical choices. Record the date, participants, decision, alternatives considered, reason and future review point.

Examples include:

- Selecting a software platform
- Changing a participation rule
- Configuring a permission model
- Adopting a new vendor
- Altering an incentive plan
- Creating a data-retention practice

Context helps future leaders distinguish a deliberate requirement from an outdated habit.

Organize Vendor and Partner Knowledge

Maintain a shared vendor register containing:

- Company and service
- Contract owner
- Account number
- Primary and escalation contacts
- Contract dates
- Pricing and renewal terms
- Support process
- Credentials location
- Integration dependencies
- Data export or termination terms

Document important government, association and mutual-aid contacts as well. Personal relationships matter, but the department should know the role and purpose of the connection.

Do not wait until a problem to discover that the only contact left the vendor six months earlier.

Preserve Knowledge During Projects

New software, apparatus, construction, grants and major events create decisions that may affect the department for years.

Store project plans, contracts, configurations, approvals, training and final lessons in a common location. Include a closeout summary explaining what was completed, what remains and who owns the result.

Require vendors and contractors to provide usable documentation. Do not accept a system that only the original developer can maintain.

Build Knowledge Transfer Into Role Changes

Use a transition checklist whenever someone changes a leadership or administrative role.

Include:

- Responsibilities being transferred
- Open issues and upcoming deadlines
- Accounts and access
- Vendors and contacts
- Reports and recurring meetings
- Physical keys, files and equipment
- Decisions awaiting action
- Training required by the successor

The outgoing person and successor should review the list together when possible. Leadership should verify completion instead of assuming the handoff happened informally.

Plan for an Unplanned Departure

Not every transition provides notice or cooperation.

Prepare for illness, suspension, termination, conflict or another sudden loss of access. Leadership should be able to disable accounts, recover systems, locate records, contact vendors and identify immediate deadlines without relying on the departing person.

No one should be able to delete the website, disable software, move money or remove the department's access because the organization allowed one personal account to control everything.

Use audit logs, backups, shared control and prompt offboarding. Test recovery while relationships are healthy.

Decide Where Knowledge Lives

Use a central, searchable location with role-based access.

Organize information by responsibility rather than by the name of the person who created it. Use consistent titles, dates and version control.

Sensitive personnel, financial and security information requires restricted access. A central system does not mean every member can see every document.

Avoid scattering current procedures across email, personal drives and private devices. Link the responsibility register and calendar directly to the authoritative documentation.

Review and Maintain the Knowledge System

Documentation becomes dangerous when people assume it is current and it is not.

Assign review cadences based on risk:

- Critical access and recovery: quarterly
- Contracts and renewals: before each renewal cycle
- Annual responsibilities: after each completion
- Operational procedures: when policy or systems change
- Vendor contacts: twice a year
- Responsibility register: quarterly
- Full continuity review: annually

Include a last-reviewed date and owner on important procedures. Encourage users to report unclear or outdated steps.

CHECKLIST

Institutional Knowledge

Confirm that the department has:

- [ ] Inventoried critical responsibilities
- [ ] Named primary and backup owners
- [ ] Documented recurring deadlines
- [ ] Created usable procedures
- [ ] Established department-owned accounts
- [ ] Protected credentials and recovery
- [ ] Cross-trained backups through real work
- [ ] Recorded significant decisions and reasons
- [ ] Organized vendor and partner information
- [ ] Built transition and offboarding checklists
- [ ] Prepared for sudden departures
- [ ] Centralized documentation with permissions
- [ ] Scheduled recurring reviews

Frequently asked questions

What is institutional knowledge in a fire or EMS department?

It is the operational, administrative, technical and relationship knowledge the department needs to function over time, including recurring processes, system access, decisions, contacts and practical experience.

What should a department document first?

Begin with responsibilities affecting safety, compliance, money, critical access and uninterrupted operations, especially those controlled by one person.

How many people should know each critical process?

At least one primary and one capable backup should exist for critical work. Higher-risk responsibilities may require additional separation of duties or leadership oversight.

Should passwords be included in procedure documents?

No. Store credentials in an approved password manager and reference the appropriate account or vault in the procedure.

How often should procedures be reviewed?

Review them whenever the workflow, system or policy changes. High-risk procedures should also have a scheduled quarterly or annual review.

How can a volunteer department maintain documentation with limited time?

Start with the highest-risk responsibilities, use simple templates and update documentation immediately after the task is performed. A short accurate procedure is more useful than an ambitious manual that never gets finished.

What is the difference between institutional knowledge and succession planning?

Institutional knowledge focuses on preserving how the organization operates. Succession planning focuses on preparing people to assume future leadership and key roles. Departments need both.

For the leadership-development side of continuity, read the Guide to Succession Planning for Volunteer Fire and EMS Leadership.

Last reviewed August 2026

Dave Iannone

FOUNDER & CHIEF PRODUCT OFFICER, FIRST ARRIVING

He co-founded Firehouse.com and now leads First Arriving, a public safety SaaS company. A fire service veteran and former journalist, he writes on technology, marketing, recruitment and leadership in and around public safety.

DaveIannone.com | LinkedIn | Contact | Schedule a Meeting