SOFTWARE & SAAS

Guide to Public Safety Software Security and Data Ownership

Public safety agencies should know where their information lives, who can access it, how it is recovered and what happens to every record when the vendor relationship ends.

13 MIN READ | AUGUST 2026

IN SHORT

Plain-language questions public safety agencies should ask about software security, access, backups, incidents, data ownership, export and contract termination.

Public safety agencies do not need to become cybersecurity firms, but they must ask vendors direct questions about the information entrusted to them.

Security conversations often become a collection of acronyms, certifications and contract language. Those items can matter, but agency leaders still need clear answers to basic questions: What information is being collected? Who controls it? Who can see it? How is it protected? Can the agency recover it? What happens when the relationship ends?

The answers should reflect the actual risk. A public website contact form, a member roster and a system containing patient or investigative information should not receive identical treatment.

Security is not one feature. It is the combination of technology, people, procedures, contracts and accountability surrounding the data throughout its life.

Identify the Data

Begin with a data inventory. The agency cannot evaluate protection without knowing what the system will collect, receive, generate and store.

Potential categories include:

- Names, contact information and emergency contacts
- Dates of birth and government identifiers
- Driver's-license, certification and credential numbers
- Personnel, disciplinary or performance records
- Protected health information
- Criminal justice or investigative information
- Incident, dispatch and operational records
- Location, schedule and availability information
- Uploaded documents, images and attachments
- Messages, acknowledgment history and audit logs
- Payment, payroll, benefit or banking information
- Device, login and usage information

For each category, identify why it is collected, who needs it, how long it must remain and what harm could result from unauthorized access, loss or alteration.

Do not collect information merely because the software provides a field for it. Data that is never collected cannot be exposed later.

Understand data flows. A record may originate in CAD, pass through an integration provider, enter the SaaS platform, appear on a dashboard and be

included in an emailed report. Every transfer and destination affects the security review.

Assign Data Classification and Responsibility

Apply the agency's classification policy, if one exists. Separate public information from internal, confidential, restricted and legally protected data.

Assign an internal owner for each major category. The software vendor protects the service, but the agency remains responsible for deciding who should have access, what should be retained and how the information may be used.

Document who approves new fields, integrations and uses. A platform selected for low-risk information should not gradually accumulate highly sensitive records without a new review.

Confirm Ownership

The agreement should state clearly that the agency retains ownership of its information.

Ownership alone is not enough. The contract must also define the vendor's rights to host, process, copy, analyze and disclose the data for the purpose of providing the service.

Ask whether the vendor may:

- Combine agency data with information from other customers
- Use content for product analytics or benchmarking
- Create de-identified or aggregated datasets
- Use agency information to train AI models

- Send information to third-party AI or analytics services
- Retain derived data after the original records are deleted
- Respond directly to legal demands without notifying the agency

Terms such as “de-identified,” “aggregated” and “service improvement” should be defined. The agency should understand which permissions survive termination.

Confirm ownership of configurations, custom forms, reports, templates and content the agency creates inside the system. Also clarify whether custom development paid for by the agency can be reused or resold by the vendor.

Understand Where Data Lives

Ask where production data, backups, logs and attachments are stored. Determine whether information remains within required geographic regions and whether customers can select or restrict hosting locations.

Identify the primary hosting provider and any separate services used for email, text messaging, file storage, analytics, customer support, monitoring, payments, integrations and AI.

The agency does not need a map of every server, but it should understand the significant organizations and jurisdictions involved in processing its information.

Control Access

Access should follow the principle of least privilege. People receive only the information and capabilities required for their responsibilities.

Evaluate both agency-user access and vendor-employee access.

For agency users, look for:

- Role-based permissions with sensible defaults
- Field-level protection for especially sensitive information
- Station, division, company or group-based access where needed
- Multifactor authentication
- Single sign-on when appropriate
- Approval for privileged roles
- Automatic or prompt deactivation when people leave
- Session controls and device management
- Audit history for administrative and sensitive actions

Avoid broad administrator access simply because permissions are difficult to configure. Not every officer, supervisor or IT employee needs to see all personnel information.

For vendor access, ask which employees can reach production data, how access is approved, whether it is time-limited and how actions are logged. Support personnel should not have unrestricted standing access merely for convenience.

Review permissions on a schedule and after promotions, transfers, leaves and terminations. A secure system can still expose information when the agency fails to remove old access.

Protect Storage and Transmission

Require encryption during transmission and at rest for sensitive information. Ask how encryption keys, API tokens, database credentials and other secrets are stored and rotated.

Encryption does not replace access control. An authorized account can often view decrypted information, which is why multifactor authentication, least privilege and monitoring remain essential.

Ask how the vendor separates:

- One customer from another
- Development, testing and production environments
- Application services from databases and backups
- Ordinary administrative access from highly privileged access

Determine whether real customer data is copied into development or testing. If it is, the same protection and retention requirements should follow it.

Uploaded files need protection too. A secure database does not help if attachments are stored publicly or shared through permanent unprotected links.

Review Secure Development and Maintenance

Software security changes over time. New vulnerabilities are discovered, dependencies age and integrations evolve.

Ask how the vendor handles:

- Code review and testing
- Dependency and vulnerability scanning
- Operating-system and application patching
- Penetration testing
- Security findings and remediation deadlines
- Open-source components
- Emergency updates
- Separation of developer and production privileges
- AI-generated code review

Independent audits and certifications can provide useful evidence, but understand their scope. A report covering the hosting environment may not evaluate every application feature, integration or operational process.

Ask for the date and scope of the most recent assessment, not simply whether one has ever occurred.

Review Monitoring and Incidents

The vendor should monitor availability, performance, administrative actions and signs of misuse or compromise.

Ask:

- **Q** Which events generate alerts?
- **Q** Who receives and investigates them?
- **Q** Is monitoring continuous or limited to business hours?
- **Q** How are failed logins, unusual exports and permission changes detected?
- **Q** How long are security and audit logs retained?
- **Q** Can the agency obtain relevant logs during an investigation?

Review the incident-response plan. It should define investigation, containment, recovery, evidence preservation, customer communication and required notifications.

The contract should specify when the vendor must notify the agency after discovering an incident. Avoid language that delays notice until the vendor completes its entire investigation or decides that harm is likely.

Confirm the notification contacts and update them regularly. A well-written notice sent to a former employee does not help the agency respond.

Ask whether the vendor has experienced previous material incidents and what changes resulted. The existence of an incident is not automatically disqualifying. The response, transparency and improvements matter.

Test Backups and Recovery

Backups protect against hardware failure, accidental deletion, bad releases, ransomware and other destructive events.

Ask about:

- Backup frequency
- Retention periods
- Encryption
- Geographic or account separation
- Protection against deletion or alteration
- Restoration testing
- Recovery priorities
- Customer-specific recovery

Define the recovery-point objective and recovery-time objective. In plain language, how much recent information might be lost, and how long could the service remain unavailable?

A vendor saying “we back up every day” does not answer whether it can restore a complete working system. Ask when restoration was last tested and whether the test included databases, attachments, configuration, permissions and integrations.

Understand whether the agency can request restoration of accidentally deleted records and what that service costs.

Evaluate Availability and Operational Resilience

Security includes keeping authorized users able to access the service.

Review uptime history, monitoring, redundancy, capacity planning and maintenance. Ask how the platform handles provider failures, expired certificates, denial-of-service attacks and sudden traffic increases.

Read the uptime definition carefully. Determine what counts as unavailable, which events are excluded, how the percentage is calculated and what remedy applies.

The agency should also maintain an operational fallback. Even a well-designed service can become unavailable. Document how critical work continues during an outage and how information is reconciled afterward.

Demand Useful Export

The agency should be able to retrieve its information during the contract, not only after announcing termination.

A complete export may need to include:

- Core records and relationships
- Member-created and administrator-created content
- Attachments and images
- Historical values and status changes
- Messages and acknowledgments
- Audit logs
- Form submissions and signatures
- Report definitions and custom fields
- Identifiers needed to reconnect related records

Ask for a sample export during evaluation. Open the files and determine whether ordinary technical staff can understand them. A proprietary file or undocumented database dump may satisfy a narrow contract clause without providing practical portability.

Clarify export frequency, size limits, fees and delivery time. Determine whether the agency can automate exports or maintain an independent archive for especially important records.

Test the export periodically. Waiting until a contract dispute or vendor failure is the worst time to discover that key attachments or history are missing.

Define Retention and Deletion

Retention must reflect operational, legal, public-record and privacy requirements.

Define how long the system keeps active records, deleted items, logs, messages, attachments and backups. Determine whether different categories can follow different schedules.

When the contract ends, document:

1. The deadline for requesting or downloading an export
2. How long production copies remain available
3. When ordinary copies are deleted
4. How long information persists in backups
5. Whether the vendor provides written confirmation of deletion
6. How legal holds or open investigations affect deletion

Immediate deletion is not always desirable. The agency needs enough time to verify its export and transition. Indefinite retention is not acceptable either.

Public-record obligations remain with the agency even when a vendor hosts the information. Confirm how searches, preservation and exports support those duties.

Evaluate Third Parties

Most SaaS companies rely on other providers. These may include cloud hosting, email, text messaging, payment processing, support platforms, analytics, monitoring, AI and integration partners.

Request a current list of significant subprocessors and the function each performs. Determine whether the vendor evaluates their security and contracts.

Ask how the agency is notified before a new subprocessor begins handling information and whether the agency has any right to object when the change creates a meaningful compliance or security concern.

Third-party risk also includes integrations selected by the agency. Understand which vendor owns each connection, where credentials are stored and who responds when data stops moving.

Address AI Use Directly

AI features can summarize records, answer questions, generate reports and assist users. They can also send information to additional services or produce conclusions that users trust without verification.

Ask:

> **Q** Which data is sent to an AI model or provider?

- Q Is agency data retained by that provider?
- Q Can it be used to train models?
- Q Can the agency disable AI features?
- Q Are prompts and outputs logged?
- Q Which users may invoke AI against sensitive information?
- Q How are incorrect or biased outputs handled?
- Q Is a human review required before consequential action?

AI should follow the same permissions as the underlying system. A user should not be able to ask an AI assistant to reveal information they cannot otherwise access.

Put Security Commitments in the Contract

Sales explanations and security questionnaires are useful, but important commitments should appear in the contract or incorporated security addendum.

Address:

- Data ownership and processing rights
- Required security controls
- Incident notification
- Subprocessors
- Insurance
- Audit or assessment evidence
- Data location
- Availability commitments
- Backup and recovery
- Export and transition assistance
- Retention and deletion
- Responsibilities after termination

Avoid contract language allowing the vendor to reduce security obligations unilaterally through a website policy that can change without notice.

Define responsibility when an incident results from agency configuration, compromised user credentials, a vendor failure or an integration partner. Security is shared, but shared responsibility should not mean unclear responsibility.

Create an Ongoing Review Process

Security review should not end at purchase.

At least annually, and after significant changes, review:

- Current data and integrations
- User and administrator access
- Security assessment evidence
- Subprocessor changes
- Incidents and outages
- Backup and recovery testing
- Export capability
- Insurance and contract requirements
- New AI or analytics features
- Changes in law, policy or agency risk

Assign ownership for the review and document decisions. A vendor approved five years ago should not remain trusted solely because nobody reopened the file.

CHECKLIST

Public Safety Software Security

Before approval or renewal, confirm:

- [ ] The agency understands the data collected and where it flows.
- [ ] Vendor processing, analytics and AI rights are defined.
- [ ] Sensitive actions are logged and reviewable.
- [ ] Development, testing and production are separated.
- [ ] The contract states that the agency owns its information.
- [ ] Access follows least privilege and supports multifactor authentication.
- [ ] Data and attachments are encrypted appropriately.
- [ ] Vulnerabilities and patches are managed on defined timelines.

- [ ] Monitoring and incident response operate beyond one person's availability.
- [ ] Backups are protected and restoration has been tested.
- [ ] Complete, usable exports have been demonstrated.
- [ ] Significant subprocessors are disclosed.
- [ ] Security evidence is reviewed regularly, not only during the initial sale.
- [ ] Incident-notification requirements are documented.
- [ ] Uptime, recovery and fallback expectations are understood.
- [ ] Retention and deletion cover production, logs and backups.
- [ ] AI use is transparent and permission-aware.

Frequently asked questions

Who owns data stored in SaaS software?

The contract should state that the agency owns its information and define the vendor's limited processing rights.

Is encryption enough?

No. Security also requires access control, monitoring, patching, backups, incident response and secure operations.

What should a data export contain?

It should include usable records, attachments, history and audit information needed to continue operations.

What happens after termination?

The agreement should define export timing, retention, deletion and handling of backup copies.

Should agencies ask about AI use?

Yes. Determine whether agency data is sent to AI services or used for model training and require appropriate controls.

For the complete vendor decision framework, read the Guide to Selecting a Public Safety SaaS Vendor.

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.

Davelannone.com | LinkedIn | Contact | Schedule a Meeting