SOFTWARE & SAAS

# Guide to Selecting a Public Safety SaaS Vendor

Features and price are only part of a software decision. This guide helps public safety agencies evaluate the complete service, infrastructure and company behind a SaaS platform.

9 MIN READ | AUGUST 2026

**IN SHORT**

A practical framework for evaluating public safety SaaS vendors across security, uptime, infrastructure, support, continuity, integrations and data ownership.

Public safety agencies depend on software for communication, staffing, records, training, reporting, recruitment and daily operations. Selecting a SaaS vendor should involve more than comparing features and prices.

The strongest product demonstration does not necessarily reveal how a vendor protects data, responds during an outage or supports customers after the sale. This guide provides a practical framework for evaluating the complete service behind the software.

This guide expands on the vendor-risk questions discussed in AI Is Creating a New Generation of Public Safety Entrepreneurs. Ask the Hard Questions. That article looks at why AI is creating exciting new opportunities while also lowering the barrier to launching software that public safety agencies may eventually depend on.

## 1 Define the Operational Problem First

Begin by documenting the problem the agency needs to solve. Identify who experiences it, how frequently it occurs and what the current process costs in time, money, duplication or risk.

Separate essential outcomes from preferred features. A long list of capabilities can distract an evaluation team from the few improvements that would create the most value.

Ask:

- Q Which workflows need to improve?
- Q Who will use the system?
- Q What information must it manage?
- Q Which existing systems must it connect with?
- Q How will the agency measure success?

## 2 Evaluate Security and Data Protection

Ask where the platform and its data are hosted, how information is encrypted and who can access production systems. Determine whether the vendor conducts vulnerability scanning, security testing and independent code or infrastructure reviews.

Ask whether development, testing and production environments are appropriately separated. Determine how administrative access is granted, reviewed and removed, and whether multifactor authentication is required for sensitive systems.

The vendor should be able to describe how it manages operating-system updates, application dependencies, security patches, malware protection, secrets and credentials. Ask how logs are protected and reviewed, how suspicious activity is detected and who receives security alerts.

Security should not depend on one person's memory or personal login. More than one authorized person should have controlled access to the hosting, databases, domains, security services, monitoring and recovery tools.

The vendor should be able to explain its backup schedule, retention practices and restoration testing. A backup that has never been tested may not provide meaningful protection.

Also ask how security incidents are identified, investigated and communicated. The contract should clearly address notification responsibilities.

---

## 3 Confirm Data Ownership and Portability

The agency should retain ownership of its information. Confirm that data can be exported in a usable format during the contract and when the relationship ends.

Ask whether exports include attachments, historical records, audit information and other related data. A spreadsheet containing only a portion of the agency's

records may not be sufficient.

Understand the vendor's deletion and retention process after termination.

---

## 4 Understand Reliability, Monitoring and Recovery

Review the vendor's uptime history and service commitment. Ask who monitors the system, who receives outage alerts and how customers are updated during an incident.

Ask the vendor to explain the infrastructure behind the uptime claim. Relevant questions may include:

- **Q** Is the platform designed to avoid a single server, database or provider becoming a point of failure?
- **Q** Are capacity, performance and database health monitored continuously?
- **Q** How does the service handle sudden spikes in traffic or usage?
- **Q** Are content delivery, firewall and denial-of-service protections in place?
- **Q** Is routine maintenance performed without taking the entire platform offline?
- **Q** Are availability reports or a public status history available?
- **Q** What events are excluded from the uptime calculation?

An uptime percentage in a contract is useful only when the agency understands how it is measured. Ask whether availability is calculated monthly or annually, what counts as an outage and what remedy applies when the commitment is missed.

The vendor should have documented plans for disaster recovery and continuity. Ask when those plans were last tested and what recovery times the vendor is prepared to support.

Clarify both the recovery-time objective and the recovery-point objective. In plain language, how long might the system remain unavailable, and how much recent data could be lost after a major failure?

Confirm that backups are encrypted, retained separately from the primary system and protected from the same account compromise or infrastructure failure. Ask when the vendor last restored a complete environment from backup.

---

## 5 Examine Support Beyond the Sales Process

Support expectations should be specific. Determine how requests are submitted, which hours are covered and how urgent operational issues are escalated.

Ask:

- **Q** Is support provided by employees or a third party?
- **Q** Are response targets documented?
- **Q** Is emergency support available?
- **Q** Who owns the issue when it involves an integration partner?
- **Q** What training and ongoing education are included?

Talk with current customers about their experience after implementation, not only during the sales process.

---

## 6 Evaluate the Vendor's Continuity

Public safety agencies should understand who is behind the product and whether the service depends on one person.

Ask who can access the source code, hosting, domains, customer records, backups, security systems, monitoring and analytics. More than one authorized person should be able to operate and recover the service.

Ask what happens if an owner or critical employee dies, becomes ill, retires, leaves the company or is terminated. The vendor should have documentation, access controls and a realistic succession plan.

Also consider a hostile departure. If the person who built or manages the platform is fired and unhappy, could that individual delete code, infrastructure, customer data or backups? Access should be role-based, logged and removable immediately. Critical resources should be owned by the company, not attached to an individual's personal account.

---

## 7 Determine Whether the Business Is Sustainable

Low pricing can be attractive, but the vendor must generate enough revenue to support hosting, security, development, customer service, insurance and long-term

maintenance.

Ask what is included, what costs extra and how pricing may change as the agency adds users, locations, data, integrations or features.

Pricing alone does not establish quality. It should, however, support the level of service being promised.

---

## 8 Review Integrations and APIs

Do not accept a general claim that the product integrates with other platforms. Identify the exact data exchanged, the direction of the connection, the update frequency and which party supports it.

Ask whether the integration uses an official API, file exchange, email parsing, browser automation or another method. Determine what happens if the connected vendor changes its system or pricing.

---

## 9 Address Compliance and Accessibility

Requirements vary according to the agency, jurisdiction, users and information involved. Potential considerations include PII, HIPAA, criminal justice information, public records, retention, audit logs, cyber insurance and independent standards such as SOC 2.

Accessibility should also be discussed. Ask how the product supports users with disabilities and whether the vendor has documented its current accessibility status and improvement process.

---

## 10 Request a Demonstration Based on Real Workflows

Provide vendors with several realistic scenarios instead of allowing every demonstration to follow a polished standard script.

Ask the vendor to show how an administrator completes a common task, how a regular user experiences it and what happens when something goes wrong. Include reporting, permission management, data export and support workflows.

---

## 11 Check References Carefully

Speak with agencies that resemble yours in size, structure and use case. Ask what implementation required, what surprised them and how responsive the vendor has been.

Useful reference questions include:

- **Q** Would you select the vendor again?
- **Q** What took longer than expected?
- **Q** Which promised capabilities were not ready?
- **Q** How does the vendor handle problems?

**Q** Has pricing remained predictable?

## 12 Review the Contract as an Operational Document

The agreement should clearly address pricing, renewal, termination, data ownership, exports, security incidents, service commitments, support and responsibilities shared with third parties.

Legal review is important, but operational leaders should also read the contract. They are often best positioned to identify a promise that does not match the actual workflow.

CHECKLIST

### Public Safety SaaS Vendor

Before making a final selection, confirm that the agency can answer yes to the following:

- [ ] We defined the operational problem and success measures.
- [ ] We retain ownership of our data and can export it in a usable format.
- [ ] Support expectations and escalation paths are documented.
- [ ] The vendor's pricing and business model appear sustainable.
- [ ] Compliance and accessibility requirements have been addressed.
- [ ] We understand where our data is stored and how it is protected.
- [ ] We reviewed backups, monitoring, uptime and disaster recovery.
- [ ] The service does not depend entirely on one person.
- [ ] Required integrations have been demonstrated and explained.
- [ ] References confirmed the vendor's performance after the sale.

- [ ] The contract reflects the operational and security commitments discussed.

## Frequently asked questions

**What is the most important factor when selecting a public safety SaaS vendor?**

The most important factor is whether the complete service can reliably support the agency's operational need. Features matter, but so do security, uptime, support, data ownership, infrastructure and the vendor's ability to continue operating over time.

**Who should participate in evaluating public safety software?**

Include operational users, administrators, IT or security personnel, leadership, procurement and legal reviewers when appropriate. The people who will use and support the system should help define requirements and evaluate realistic workflows.

**What security questions should an agency ask a SaaS vendor?**

Ask where data is hosted, how it is encrypted, how administrative access is controlled, how vulnerabilities and patches are managed, how activity is monitored and how the vendor responds to a security incident. Also confirm that critical systems are not controlled through one person's login.

**How should an agency evaluate a vendor's uptime commitment?**

Review the actual uptime history, measurement period, exclusions and remedies. Ask how the infrastructure avoids single points of failure, how outages are detected and communicated, and whether backups and disaster-recovery plans have been tested.

**What happens to agency data when the contract ends?**

The contract should confirm that the agency owns its data and can export it in a usable format. Clarify whether the export includes attachments, historical records and audit information, as well as when remaining copies will be deleted.

Choosing public safety software is ultimately an exercise in trust. Features matter, but agencies are also selecting the people, processes and business that will stand behind those features when they are needed.

For a broader perspective on AI-enabled public safety innovation and the risks agencies should evaluate, read AI Is Creating a New Generation of Public Safety Entrepreneurs. Ask the Hard Questions..

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