



Security

Last updated October 25, 2026 · stationclipboard.com/security

Key points

- All traffic is encrypted, and the most sensitive data, such as face templates, Social Security numbers, and sign-in secrets, is also encrypted at rest with AES-256-GCM.
- Each Organization's data is kept separate, and its own roles and permissions decide who sees what.
- Our staff's access to customer accounts is limited and permanently logged.
- We notify Organizations of a confirmed security incident within 72 hours.
- Security researchers acting in good faith under our disclosure policy are welcome and protected.

This summary is for convenience. The full text below is what governs.

Fire departments, EMS agencies, and fire marshal's offices use Station Clipboard for personnel records, incident reports, investigations, and more. This page describes the safeguards **Station Automation Solutions LLC** uses to protect that information. Our Data Processing Addendum makes these safeguards a commitment to every Organization.

1. Infrastructure

- The Service runs in U.S. data centers operated by major cloud providers that maintain recognized security programs. Customer data is stored in the United States.
- Production databases are backed up regularly by our infrastructure provider.
- Our service providers are described on our Subprocessors page, and each may use information only to provide its service to us.

2. Encryption

- **In transit.** Every connection to the Service uses HTTPS, and our sites send HTTP Strict Transport Security so browsers never fall back to an unencrypted connection.
- **At rest.** In addition to the encryption our infrastructure applies to stored data, we encrypt the most sensitive fields ourselves with AES-256-GCM: face templates, Social Security numbers, two-factor authenticator secrets, election ballots, Google account tokens, text messaging credentials, and logins Organizations store for new members.
- **Hashing.** Passwords and kiosk PINs are stored only as one-way hashes. Links we email, such as Information Request links, and phone upload links are stored only as one-way hashes, so a copy of our database does not reveal them.

3. Access Control and Sign-In

- Each Organization's data is logically separated. Members of one Organization cannot see another's data, and requests that name another Organization are refused.
- Roles and permissions are set by the Organization, action by action and module by module. Modules an Organization has turned off cannot be reached.
- Two-factor sign-in is available to every Organization.
- Failed sign-ins are recorded and repeated attempts are throttled. Sessions end after a week without use.
- Sensitive fields, such as Social Security numbers, are shown masked, and each full view is logged.
- Links for people without accounts, such as Information Requests, event plans, and phone photo uploads, do one thing, expire, and can be withdrawn.

4. Our Staff's Access

- Only a small number of authorized staff can access customer accounts, and only to provide support, fix problems, move data at an Organization's request, keep the Service secure, or comply with the law.
- Staff permissions are granted capability by capability, so each person gets only the tools their job needs.
- Database administration tools require two-factor sign-in, hide passwords, tokens, and other secrets, and record every change and query.
- Entering an Organization's account and viewing the Service as a user are recorded in a permanent audit log.
- Staff are bound by confidentiality obligations.

5. Application Safeguards

- Our API accepts browser requests only from our own sites.
- Public pages and sign-in are rate limited, and public complaint forms have bot checks.
- Department websites are served without cookies, scripts, or forms, under a strict content security policy.
- Uploaded files are private by default and served only to people allowed to see them.
- Integration keys and tokens are kept on our servers and never shown again after they are saved.
- Errors are captured automatically so that we can find and fix problems quickly.

6. Logging and Accountability

- Every Organization has an activity log of significant actions. Security and permission changes are kept for the life of the account.
- Sign-ins, failed attempts, password resets, and two-factor events are kept for 180 days, with the network address and device.
- Payroll, HR, elections, onboarding, NERIS, and medical record views have their own audit trails.
- Administrators who view the Service as a member are recorded in the Organization's activity log.

7. AI Safeguards

- Sparky is off until it is turned on for an Organization, which chooses the roles that may use it and the areas it can reach.
- Sparky acts with the permissions of the member using it, never more, and changes records only after the member confirms.
- Passwords, PINs, tokens, face templates, Social Security numbers, and members' medical records are blocked from AI requests.
- We do not use Customer Data to train AI models of our own. Our Privacy Policy lists every AI feature and what it sends.

8. Incident Response

If we confirm a security incident affecting Customer Personal Data, we notify affected Organizations within 72 hours, tell them what we know, contain and investigate it, and help them meet their own notification obligations, as our Data Processing Addendum describes.

9. Reliability and Continuity

We work to keep the Service available and recoverable, with regular backups and monitoring. Station Clipboard supports emergency operations but does not replace radios, dispatch, or your accountability system, and every Organization should keep a backup method for incidents, as our Terms of Service explain.

10. Your Organization's Part

- Turn on two-factor sign-in, at least for administrators.
- Give each person only the permissions their role needs, and review roles regularly.
- Disable accounts promptly when people leave, and change any shared logins.
- Secure kiosks, station displays, and shared devices, and sign out of shared devices.
- Report suspected unauthorized access to us right away.

11. Vulnerability Disclosure Policy

We welcome reports from security researchers. If you believe you have found a vulnerability in Station Clipboard, email hello@stationclipboard.com with the subject line "Security" and include the steps to reproduce it, its likely impact, and how to reach you.

In scope

stationclipboard.com, go.stationclipboard.com, cmd.stationclipboard.com, inspect.stationclipboard.com, department websites we host, and the Station Clipboard mobile and desktop apps.

Please

- Test only with accounts you own or are authorized to use, and access only the minimum data needed to show the problem
- Stop and tell us right away if you reach personal information, and do not keep, share, or use it
- Do not run denial-of-service tests, spam, social engineering, or physical tests, and do not test third-party services we use
- Do not change or delete data, or degrade the Service for others; remember that public safety agencies rely on it
- Give us a reasonable time to fix the problem before telling anyone else about it

Our commitments

- We will acknowledge your report within three business days and keep you informed as we work on it.
- If you follow this policy in good faith, we consider your research authorized, will not pursue legal action against you for it, and will support you if someone else does.
- We will credit you when we fix the issue, if you would like.

We do not currently offer payment for reports. Our machine-readable contact details are at </.well-known/security.txt>.

12. Security Reviews and Questionnaires

Organizations reviewing Station Clipboard for procurement, insurance, or an IT review can ask us to complete a security questionnaire, sign our Data Processing Addendum, or meet with us. Email hello@stationclipboard.com with the subject line "Security Review."

Security · Last updated October 25, 2026

Questions about this document: hello@stationclipboard.com or (979) 341-9333. Every legal document and fillable form is in the Legal Center.