

Terms of Service

Last updated October 25, 2026 · stationclipboard.com/terms-of-service

Key points

- Station Clipboard is not an emergency service, a dispatch system, or an accountability system of record. In an emergency, call 911 and use your radio.
- Your Organization owns its data and controls who can see it. We process it to provide the Service and never sell it.
- Your Organization makes every operational, employment, inspection, investigation, and reporting decision. All output and built-in templates are advice, not decisions.
- Use your own account, keep it secure, and use the Service only as your Organization authorizes.
- Our liability is limited, disputes start with a good-faith conversation, and Texas law applies, with protections for public entities.

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

These Terms of Service ("Terms") are an agreement between you and **Station Automation Solutions LLC** ("Station Automation Solutions," "we," "us," or "our"). They govern your access to and use of Station Clipboard and everything that is part of it, described in Section 2 (together, the "Service").

Station Clipboard is a product of Station Automation Solutions LLC. The **Department Portal**, the **Command Portal**, and the **Inspection Portal** are parts of Station Clipboard, not separate companies or separate agreements. One account and these Terms cover all of them.

If you use the Service on behalf of a fire department, EMS agency, fire marshal's office, public safety organization, district, municipality, company, or other entity (an "Organization"), you confirm that you are authorized to accept these Terms on its behalf, and "you" includes that Organization.

Station Clipboard is not an emergency service. In an emergency, call 911 and use your radio. Section 10, Section 11, and Section 12 explain what the Service does and does not do on an incident. Please read them.

If you do not agree to these Terms, do not use the Service.

1. Accepting These Terms

You accept these Terms by doing any of the following:

- Selecting "I agree," "Accept," or a similar option when a Station Clipboard product asks you to
- Signing in to a Station Clipboard product that tells you that signing in means you agree to these Terms
- Signing an order form, quote, or agreement that refers to these Terms
- Using the Service

Some products ask you to accept these Terms before you use them for the first time. For example, the Command Portal asks every member to accept them the first time they open it. When you accept, we record the version, the date and time, the product, and the network address and browser or device you used.

If you are under 18, or under the age of majority where you live, you may use the Service only as your Organization authorizes, for example as a cadet, junior, or explorer member, and only with any permission the law requires from a parent or guardian.

2. Station Clipboard Products

Station Clipboard is a software platform for Fire, EMS, and public safety organizations. It includes:

- **The Department Portal** (go.stationclipboard.com): the web application where an Organization manages its people, records, and enabled modules.
- **The Command Portal** (cmd.stationclipboard.com): the full-screen incident command board that comes with the Incident Command module. It opens at its own web address, but it uses the same accounts and the same Organization data as the Department Portal, and these same Terms.
- **The Inspection Portal** (inspect.stationclipboard.com): the workspace for fire inspections, permits, code enforcement, and special events. Like the Command Portal, it uses the same accounts, data, and Terms.

- **Station Clipboard apps:** the mobile app and the Windows and Mac desktop app.
- **Kiosks and station displays:** Time Clock kiosks and Station Board screens an Organization sets up on its own devices.
- **Department websites** that an Organization publishes through Station Clipboard, on our domain or its own.
- **Public pages and links** that an Organization publishes through Station Clipboard, such as application hubs, reference requests, Information Request links, surveys, Community Alerts sign-up pages, complaint pages, event plan links, calendar links, shared tickets, Corrections links, Meet guest links, and Station Board links that people open without signing in.
- **Sparky** and the other AI-assisted features described in Section 23.
- **stationclipboard.com**, the Help Center, our support tickets and public issue board, documentation, and our communications with you.

We may add, change, rename, suspend, or remove products and features over time.

3. Modules

An Organization chooses which modules to enable. Administrators can turn modules on or off and decide who may use them. Depending on what is enabled, the Service may include:

- **Core:** personnel and member records (including medical records), roles and permissions, organization settings, announcements, department email, the calendar, notifications, Information Requests, activity logs, Workflows, department websites, and module management
- **Time and staffing:** Time Clock (including kiosk and face clock-in and clock-in areas), Scheduling, Payroll, Credits & Engagement, and Budget
- **Operations:** Incident Command and the Command Portal, Incident Reporting (NERIS), Checklists, Assets, Quartermaster, Station Board, and TIFMAS
- **Fire marshal's office:** Fire Inspections and Code Enforcement (the Inspection Portal), and Fire Investigations
- **Training and knowledge:** Training, Courses, Resources, Policies, and Drive
- **People and HR:** HR Info, Recruiting, Onboarding, Corrections, Surveys, and Elections
- **Communication:** Chat, Meet, Tickets, and Community Alerts
- **Connections:** Integrations, such as Active911, PSTrax, WhenToWork, weather and news feeds, and Google Sheets

Section 11 through Section 26 add terms for specific products and modules. They apply only when you use the product or module they describe.

4. Organizations and Administrators

Organizations are responsible for managing their own Station Clipboard account, including:

- Creating, disabling, and removing member accounts
- Assigning roles and permissions, including the Incident Command and Incident Reporting permissions
- Enabling, disabling, and configuring modules, integrations, and Workflows
- Entering and maintaining accurate records
- Managing uploaded files and published public pages and links
- Reviewing and approving records, including incident records and NERIS reports
- Deciding who may access data, including through kiosks, station displays, and shared devices
- Training members to use the Service safely and as the Organization's procedures require
- Complying with the laws, policies, and recordkeeping obligations that apply to them

Organization administrators are responsible for making sure each user only has the access their role requires.

We are not responsible for an Organization's internal decisions, including operational, incident command, employment, hiring, scheduling, payroll, discipline, certification, policy enforcement, or member status decisions made using information in the Service.

5. Accounts, Sign-In, and Security

You are responsible for keeping your passwords, kiosk PINs, verification codes, and account access confidential.

You agree to:

- Provide accurate information and keep it current
- Use only your own account, and not share your password, PIN, or verification codes
- Not access another user's account
- Sign out of shared devices, such as an apparatus tablet or a station computer, when you are done
- Tell your Organization or us promptly if you suspect unauthorized access
- Use the Service only as your Organization authorizes

Your Organization may require two-factor sign-in. When you move between Station Clipboard products, for example from the Department Portal to the Command Portal or the Help Center, we may sign you in to the second product with the same account.

Your Organization or we may limit, change, suspend, or remove your access where appropriate.

6. Privacy and Related Policies

These policies are part of these Terms:

- Our Privacy Policy, which describes how we collect, use, share, and protect information
- Our Biometric Information Policy, which applies to face clock-in
- Our Text Messaging Terms, which apply to text messages sent through the Service
- Our Data Processing Addendum, which applies to personal information we process on behalf of an Organization
- The Terms of Use for Information Requests, which apply when a member answers an Information Request

Our current service providers are described on our Subprocessors page, our security practices on our Security page, and our accessibility commitments in our Accessibility Statement.

Organizations are responsible for giving any notices and obtaining any consents the law requires from their members, employees, volunteers, contractors, applicants, references, residents, building contacts, and other people whose information they put in the Service.

7. Customer Data and Ownership

"Customer Data" means the information, files, records, and other content submitted to the Service by or for an Organization or its users. This includes incident records, NERIS reports, preplans, schedules, time records, personnel records, messages, and files.

As between us and the Organization, the Organization owns its Customer Data. We do not claim ownership of it, and we do not sell it.

The Organization grants us a limited license to host, process, store, transmit, display, and use Customer Data only as needed to:

- Provide the Service and the modules and integrations the Organization enables
- Send Customer Data where the Organization or its users direct, such as to NERIS, to a connected integration, or to the recipients of a message
- Provide support
- Keep the Service secure and troubleshoot problems
- Produce reports or exports that authorized users request
- Comply with law and enforce our agreements

We may use information about how the Service performs and is used, such as error reports, response times, and which features are used, to maintain and improve the Service. We do not use it to identify an Organization's members to anyone outside the Organization.

8. Uploaded Content and Files

Users and Organizations are responsible for the content and files they upload, including documents, photos, videos, course material, preplan drawings, business card photos, and attachments.

You confirm that you have the right to upload, store, share, and process anything you submit, including information about other people, such as building owners and key holders, references, and residents.

You agree not to upload content that:

- Violates any law

- Infringes another person's rights, including copyright
- Contains malicious code
- Is unlawful, abusive, threatening, or harassing
- Contains sensitive information your Organization is not authorized to store in the Service (see Section 9)
- Violates these Terms or any applicable agreement

We may remove or restrict content if we believe it violates these Terms, creates a security risk, or exposes us, users, or Organizations to legal risk.

9. Sensitive Information

Some modules are built to hold sensitive information. For example:

- Member records can hold medical records, such as immunizations, physicals, and injuries, and, if the Organization turns it on, an encrypted Social Security number field
- Payroll holds tax withholding elections, garnishments, compensation, and pay records
- HR Info holds confidential personnel records, including discipline and leave documentation
- Recruiting can collect dates of birth, driver's licenses and other identification, and background check status
- Incident Reporting holds the coded patient care, casualty, and injury information that NERIS asks for
- Fire Investigations holds information about suspects, witnesses, victims, interviews, evidence, and referrals to law enforcement
- Time Clock can hold face templates for face clock-in and the location of clock-ins (see Section 13)

Enter sensitive information only in the fields and modules built for it, and only if your Organization is authorized to store it in the Service.

Unless a separate written agreement says otherwise, do not use the Service to store:

- Patient care reports or other protected health information beyond what the Incident Reporting fields ask for. We are not a business associate under HIPAA unless we sign a business associate agreement with your Organization. If your Organization is a HIPAA covered entity, it is responsible for deciding what patient information it may enter and send.
- Criminal justice information that requires CJIS compliance. If your CAD or alerting service carries criminal justice information, filter it out before it reaches the Service.
- Payment card numbers
- Social Security numbers, bank account numbers, or full government identification numbers, except in fields built for them
- Alarm codes, lock combinations, or passwords in preplans, notes, or messages that more people can see than should know them
- Highly sensitive legal, medical, or financial records that have nothing to do with how the Service is meant to be used

Organizations are responsible for deciding whether the information they enter or upload belongs in the Service.

10. Public Safety and Emergency Use

Station Clipboard supports the administration and operations of public safety organizations. It does not replace the systems, people, and procedures those organizations rely on in an emergency.

Unless we expressly agree otherwise in writing, Station Clipboard is not:

- A 911 system, a dispatch system, or a replacement for computer-aided dispatch (CAD)
- A radio system or a replacement for radio communications
- A personnel accountability system of record, or a replacement for your accountability tags, passports, boards, or procedures
- A primary alerting or paging system
- A public warning system, such as IPAWS, Wireless Emergency Alerts, or the Emergency Alert System
- A medical charting or patient care reporting system
- A replacement for NIMS and the Incident Command System, your standard operating procedures and guidelines, or applicable NFPA standards
- A replacement for training, professional judgment, supervision, command, or compliance review

Do not rely on Station Clipboard as your only means of dispatch, emergency communication, accountability, warning the public, or making life-safety decisions. Information in the Service can be delayed, incomplete, out of date, or wrong, and the Service can be unavailable. Do not use a device in a way that distracts you while driving an apparatus or vehicle; follow your Organization's policies.

11. The Command Portal and Incident Command

The Command Portal is a tool to help incident commanders and crews organize an incident: units and assignments, crews and riding positions, personnel accountability reports (PAR), MAYDAY and other emergency declarations, checklists, benchmarks, objectives, command staff, hazards, resource requests, the incident log, the incident map, preplans, hydrants, and the closeout record. **It supports incident command. It does not run it.** When you use it, these terms apply.

Command stays with people

The incident commander and the Organization's procedures decide what happens on scene. Keep using your radios, your dispatch center, your accountability system, and NIMS and the Incident Command System.

Emergency declarations stay on the board

Declaring a MAYDAY, emergency traffic, an evacuation, or a collapse in the Command Portal records it, shows it on other screens open to the incident, and can start a PAR. It does not transmit anything over the radio, notify your dispatch center, or call for help. Declare emergencies by radio, as your procedures require.

Accountability is your Organization's responsibility

PAR rounds, PAR timers, and accounted-for marks record what people entered. The board does not know where anyone is. The PAR clock does not start on its own, and closing a round never marks anyone as accounted for. Your Organization's accountability system, and the people running it, remain responsible for accounting for every member.

It needs a working connection

The Command Portal runs in a web browser and needs an internet connection. While connected, open screens pick up each other's changes every few seconds. A device that loses its connection, or a board left in a background tab or on a sleeping screen, may stop updating. Changes entered while a device is offline are not saved. Keep a backup method, such as a paper tactical worksheet or an accountability board, for every incident.

Timers and alerts are reminders

PAR timers, benchmark prompts, checklist due times, MAYDAY banners, and notifications depend on working devices and connections. They can be late or fail to appear.

The board shows what people entered

Unit status, assignments, crew lists, riding positions, and PAR results are only as accurate as the people and systems that entered them. Crews filled in from the Time Clock or the schedule show who was clocked in or scheduled, not necessarily who responded.

Templates and checklists are starting points

Built-in incident templates, checklists, assignments, benchmarks, ICS positions, and size-up fields are examples. They are not a standard of care, and they do not replace your standard operating procedures and guidelines, NFPA standards, or training. Your Organization is responsible for reviewing them and adapting them before use.

Maps and locations can be wrong

Maps, aerial imagery, address matches, incident locations, hydrant locations and flow classes, distances, and preplans come from the Organization, its records systems, and third-party map and address services, such as Esri and the U.S. Census Bureau geocoder. A precise address match is placed on the map automatically; a less precise one waits for someone to confirm it. Distances, bearings, and measurements are straight-line estimates, not hose lays or driving routes, and directions open in a third-party map app. Any of this can be incomplete, out of date, or inaccurate. Confirm what you see on scene.

Your device's location

If you choose "Show my location" on the map, your browser asks for permission and then reads your device's location once to show where you are. The Command Portal does not track your location. Your location is not sent to us unless you start an incident at that spot, in which case the incident's location is saved.

CAD data comes from others

Calls from a CAD or alerting service, such as Active911, are only as complete, accurate, and timely as that service. CAD rules that match a call to an incident type are your Organization's rules and can match the wrong type. Check a call's details before relying on them.

Preplans, hydrants, and building contacts

Preplans can hold building details, hazards, drawings, files, and emergency contacts, such as owners and key holders. Everyone with Command Portal access in your Organization can view preplans and hydrants. Your Organization is responsible for having the right to keep this information, for keeping it current, and for not storing anything in a preplan that every Command Portal user should not see. Hydrant imports and edits are your Organization's data; we do not verify hydrant locations, flow, or service status.

Incident records

When command ends, the incident becomes a record that the Organization reviews and finalizes. A finalized record cannot be reopened or edited, so review it carefully first. Incident records belong to the Organization, which is responsible for reviewing them before relying on them and for keeping them as the law requires. A record can start a NERIS report, which is covered by Section 12.

Running your own copy

If your Organization runs the Command Portal on its own computer or local network, for example on a station computer that tablets connect to, your Organization is responsible for securing that computer and network. Connections that do not use HTTPS are not encrypted.

Accepting these Terms

The Command Portal asks each member to accept these Terms the first time they open it, and again after we publish a new version.

12. Incident Reporting and NERIS

The Incident Reporting module helps Organizations prepare, review, approve, and send incident reports to the **National Emergency Response Information System (NERIS)**. NERIS is the national fire and emergency incident reporting system of the U.S. Fire Administration (USFA), part of FEMA. It replaced the National Fire Incident Reporting System (NFIRS) and is operated by the Fire Safety Research Institute (FSRI), part of UL Research Institutes. These terms apply when your Organization uses Incident Reporting or connects it to NERIS.

We are not NERIS

Station Clipboard is an independent software vendor that connects to NERIS through its published interface. We do not operate NERIS and are not affiliated with or endorsed by USFA, FEMA, the U.S. Department of Homeland Security, FSRI, or UL Research Institutes. Any NERIS compatibility status we hold shows technical compatibility only, not endorsement.

Your Organization is the reporting entity

Your Organization is the reporting entity for its incidents and owns its incident records. It is responsible for:

- The accuracy, completeness, honesty, and timeliness of every report it sends
- Reviewing and approving each report before it is sent
- Meeting every reporting obligation that applies to it, including those of its state fire marshal, state law, local rules, and grant conditions
- Correcting reports when NERIS rejects them or asks for changes
- Managing its own NERIS account, users, and Department ID
- Following the NERIS Terms of Use and NERIS guidance for the data it sends

You authorize us to send reports for you

NERIS lets a department authorize a software vendor by enrolling the vendor's integration in the NERIS portal. When your Organization enrolls Station Clipboard and switches its NERIS connection to Production, it authorizes us, as its service provider and on its behalf, to send to NERIS the incident reports, incident analyses, and station and apparatus information that its authorized users choose to send, and to read back its NERIS department, enrollment, and report status information. Your Organization can withdraw that authorization at any time by removing Station Clipboard's enrollment in NERIS or by switching its connection out of Production.

The credentials Station Clipboard uses to connect to NERIS belong to us and are never shown to Organizations. Do not give us, or put in the Service, the username or password of anyone's personal NERIS account.

Training, Sandbox, and Production

- **Training** mode sends nothing to NERIS. New Organizations start here.
- **Sandbox** mode sends reports to the NERIS test environment. Sandbox reports are not part of the official record.
- **Production** mode sends reports to the official NERIS record. Switching to Production requires a separate permission and is recorded.

Practice in Training or Sandbox. Never send test, sample, or made-up reports to Production.

Nothing is sent without a person

Approving a report does not send it. A user with permission to send reports must send it. Sent reports go into a queue that delivers them to NERIS, retries failed attempts, and records every attempt and NERIS's response in a transmissions log. Reports started automatically from CAD calls or from a closed Command Portal incident are drafts until people complete, approve, and send them.

What is sent to NERIS

A report sends incident-level information, such as the incident address, cross streets, and coordinates; times; incident types; units and staffing counts; fire, hazard, and exposure details; coded medical, casualty, injury, and rescue information, which may include an EMS patient care report number; aid given and received; and the narrative. An incident analysis sends origin-and-cause findings. Station and apparatus information is sent only when an authorized user syncs it. Crew members' names, attachments, and fields your Organization marks as department-only are not sent.

The NERIS Terms of Use require that submitted information not contain personal information. **Do not put names, dates of birth, phone numbers, patient identifiers, or other personal information in narratives or other free-text fields** unless NERIS specifically requires it. NERIS may redact, scrub, or remove information that does not meet its requirements.

Validation is not acceptance

The Service checks reports against NERIS rules, and can ask NERIS to check a report before it is sent. These checks help find problems. They do not guarantee that NERIS will accept a report, that a report is complete or correct, or that it meets any other agency's requirements. Watch each report's status and resolve rejections.

What happens in NERIS

Once a report reaches NERIS, NERIS's own terms, policies, and the law govern it, not these Terms. Under the NERIS Terms of Use, the operator of NERIS receives a broad license to use and publish what is submitted, and NERIS publishes some approved incident information, including incident type, time, address, and location, on public dashboards. NERIS may share information with state fire marshals and others as its policies allow. We cannot remove information from NERIS except through the corrections NERIS allows.

NERIS can change or be unavailable

NERIS sets its own data standards, value sets, rules, and availability, and it can change them, limit access, or suspend vendors. We work to keep up with NERIS changes within the time NERIS requires, but we do not guarantee that the Service will support every change by a particular date, or that NERIS will be available when you need it. If the Service cannot send a report, your Organization remains responsible for reporting by another means, such as the NERIS web application.

Investigations and juvenile information

Incident analyses, origin-and-cause findings, and investigation notes may relate to criminal investigations or involve minors. Your Organization is responsible for deciding what may lawfully be recorded and sent, and for coordinating with investigators before sending anything that could affect an investigation.

Records and exports

We keep a copy of each report, what was sent, and NERIS's responses as part of your Customer Data. Printed and exported reports, including the redacted "public" PDF, are conveniences. Your Organization must review them before releasing them, including in response to a public records request. NERIS is not your Organization's system of record, and the Service does not file NFIRS or state reports for you.

NERIS data we receive

We use information we receive from NERIS only to provide the Service to your Organization, and we do not sell or republish it.

13. Time Clock, Clock-In Areas, and Face Clock-In

Time Clock lets members clock in and out from the portal, the mobile app, or a kiosk using a username and password, a PIN, or, if the Organization enables it, face clock-in (shown as "Face ID" in the portal; it is not Apple's Face ID).

Clock-in areas and device details

If an Organization turns on clock-in areas, the portal and the mobile app read the device's location once when a member clocks in, and refuse a clock-in from outside the Organization's areas. Every clock-in and clock-out from the portal or the mobile app also records the device and network it came from. Before using these features, the Organization is responsible for:

- Telling members, in writing where the law requires, that clock-ins record location and device details, and getting any acknowledgment the law requires, including under electronic monitoring notice laws
- Offering another way to record time, such as a station kiosk or an officer entering the shift, to members who cannot or do not share their location
- Setting areas accurately; location readings can be imprecise indoors or on some devices

Face clock-in

Face clock-in turns a camera image into a face template, a set of numbers, on the device. We store the template encrypted and use it only to confirm who is clocking in. We do not store face photos for clock-in, and we never sell biometric information or use it for advertising. Our Biometric Information Policy explains how templates are collected, protected, kept, and destroyed, and is part of these Terms.

Before a member enrolls, the Organization is responsible for:

- Giving the member the written notice the law requires, including the purpose of collection and how long the template will be kept
- Obtaining the member's written or electronic consent where the law requires it, including for enrollment started through Onboarding and for a minor, from a parent or guardian where required
- Offering another way to clock in, such as a PIN or a username and password, where the law or Organization policy requires it
- Resetting a member's face clock-in enrollment, which deletes the template, when the member leaves or no longer needs it, as the Biometric Information Policy describes
- Placing and securing kiosks and approved devices
- Complying with applicable biometric privacy laws

Our fillable Face Clock-In Notice and Consent form is a starting point for the notice and consent; have it reviewed for your state.

Time entries are only as accurate as the people, devices, and corrections that produce them.

14. Scheduling, Payroll, Credits, and Budget

- **Scheduling** builds schedules and suggests assignments from the rules, requirements, and availability the Organization enters. The Organization decides who works and remains responsible for staffing levels, hour limits, and labor rules.
- **Payroll** calculates pay, overtime (including under an FLSA §7(k) work period), and deductions from the settings, pay codes, tax profiles, and time the Organization enters, and produces pay records and export files. We do not move money, pay employees, withhold or deposit taxes, or file tax returns or wage reports. The Organization or its payroll provider does. The Organization must review every payroll before paying it.
- **Credits & Engagement** tracks the credits and rewards the Organization defines. The Organization decides what members earn and is responsible for any benefit it offers.
- **Budget** keeps the figures people enter. It is not accounting software, and it does not track receipts or replace an audit.

The Service does not give legal, tax, accounting, or employment advice. Check calculations and settings with a qualified professional where the law or your policies require it.

15. Member Records, HR Info, Recruiting, Onboarding, and Corrections

- The Organization makes every hiring, onboarding, disciplinary, leave, and employment decision, and is responsible for complying with employment, anti-discrimination, civil service, background check, public records, and privacy laws when it does.
- Recruiting's eligibility rules and scoring are advisory. If an Organization turns on Sparky for an application hub, Sparky can read applications and give each a summary, concerns, and a score (see Section 23). These tools do not make decisions, and they can be wrong. A person at the Organization must review every applicant and make every decision.

- An Organization that uses AI to evaluate applicants is responsible for any notice, consent, bias audit, or alternative process the law requires, including under laws on automated employment decision tools, and for telling applicants how their applications are reviewed.
- **Information Requests** let an officer ask members to update their records. Members answer under the Terms of Use for Information Requests. The Organization is responsible for asking only for information it is entitled to collect.
- **Medical records** on a member's record are confidential. Give access only to people who need it, and keep them only as the law allows.
- Recruiting can record background check consent and status, but we do not run background checks. If the Organization uses a background check provider, it is responsible for complying with the Fair Credit Reporting Act and similar laws.
- Application hubs can be set up for minors, such as cadet, junior, and explorer programs. The Organization is responsible for age limits and for any parent or guardian consent the law requires.
- Applicants, references, and people answering a Corrections link without signing in use the Service through the Organization. The Organization is responsible for the notices and information it gives them.
- Onboarding can store logins for outside services that the Organization issues to new members. Store only logins the Organization is allowed to share, and change them when someone leaves.
- HR Info records are confidential. Only give access to people who need it.

16. Training, Courses, Resources, Drive, and Electronic Signatures

- **Training and Courses** keep the training records, attendance, scores, and completions the Service records. They do not replace the records of a state certification body or any other agency, and the Organization is responsible for checking that its records meet the requirements that apply to it.
- **Courses** track how much of a video was actually watched and record attempts to skip ahead. Do not try to get around that tracking.
- **Resources and Drive** store and share documents, policies, and files. The Organization is responsible for what it shares and with whom.
- **Electronic signatures and acknowledgments.** When you sign, acknowledge, or accept something in the Service, such as a policy, an HR record, an announcement, an ICS 214, or these Terms, you agree that your electronic action has the same effect as a handwritten signature, to the extent the law allows. We record the time, and may record the network address and browser you used. The Organization is responsible for deciding whether an electronic signature meets its own legal requirements.

17. Checklists, Assets, and Quartermaster

- Checklists, inspections, and asset records help Organizations track apparatus, equipment, and gear. They do not replace manufacturer instructions, NFPA standards, or regulatory inspection requirements.
- Failed-item and expiration alerts can be late or fail to arrive. Take equipment out of service according to your Organization's procedures, whether or not the Service shows an alert.
- Checklists can be filled in on a device that is offline and saved when it reconnects. Until then, other people cannot see those results.
- Quartermaster tracks the inventory and requests the Organization enters. The Organization is responsible for issuing gear, and for its fit, condition, and safety.

18. TIFMAS

The TIFMAS module helps Organizations record deployments under the Texas Intrastate Fire Mutual Aid System and prepare the paperwork those deployments require, such as ICS 214 activity logs and reimbursement packets. The Service does not submit anything to the state for you.

- The Organization is responsible for the accuracy of what it submits and for meeting every deadline and requirement of the agencies involved.
- We do not guarantee that any deployment will be reimbursed, or that any form will be accepted.
- Station Clipboard is not affiliated with or endorsed by the Texas A&M Forest Service, the Texas Division of Emergency Management, or any other agency that administers TIFMAS or reimbursement.

19. Fire Inspections, Code Enforcement, and Fire Investigations

These modules support a fire marshal's office. The Organization is the authority having jurisdiction, and it makes every inspection, enforcement, and investigative decision.

Inspections, permits, and code enforcement

- Built-in checklists, code references, violation text, occupancy and risk classes, inspection intervals, and fee settings are starting points. Codes, amendments, and local ordinances differ by jurisdiction and change over time. The Organization is responsible for using the codes it has adopted, and for the accuracy of every inspection, violation, permit, notice, and fee.
- Notices, permits, and reports produced by the Service are drafts the Organization reviews, signs, and serves. Recording that a notice was sent or a citation issued does not deliver it. The Organization is responsible for service, deadlines, appeals, and due process.
- Fees are recorded, not collected. We do not process payments for inspections or permits.
- Business owners and representatives who sign on a device sign the Organization's record, not an agreement with us.

Public complaints

- The Organization decides whether to accept public complaints, whether reporters must identify themselves, and how it responds. A complaint page is not an emergency line; the Organization should say so on it and point to 911.
- The Service hides a reporter's contact details from staff who don't manage complaints and from printed notices. Whether a reporter's identity must be disclosed, for example in response to a public records request, is the Organization's decision under its laws.

Fire investigations

- The Service is a case management and documentation tool. It is not a law enforcement records system, a criminal justice information system, or an evidence storage facility, and it is not designed to meet CJIS requirements. Do not enter criminal history or other criminal justice information obtained from law enforcement systems.
- Chain of custody records, evidence labels, interview records, rights advisements, and reports show what investigators entered. The Organization is responsible for evidence handling, the legal basis for each search and interview, recording laws and consent, the rights of suspects and juveniles, discovery and disclosure obligations, and coordination with prosecutors and law enforcement.
- Photo files keep their original metadata, including location. Remove it before sharing a file outside the Organization if it should not be shared.
- Built-in scene steps, prompts, and report templates are not a standard of care and do not replace NFPA 921, NFPA 1033, or the Organization's procedures.
- Assistance features suggest how to sort notes and describe photos. An investigator must review every suggestion; nothing is saved until they accept it.

20. Messages, Chat, Meet, Calendar, and Notifications

- Announcements, department email, Chat, Tickets, and push, desktop, and email notifications can be delayed, filtered, or not delivered, for example because of device settings, Do Not Disturb, network problems, or a provider's spam filtering. Do not rely on them for emergency communication.
- The Organization controls who can read and post in its channels and is responsible for keeping messages as public records and retention laws require. Direct messages are part of the Organization's Customer Data.
- Meet connects participants' browsers directly to each other. Station Clipboard does not record Meet video or audio, but it keeps meeting chat and attendance. Participants must not record a meeting without the consent the law requires.
- Calendar feed links and shared event links work without signing in. Anyone who has the link can see what it shows, so share them carefully.
- Ticket share links let people outside the Organization read and reply to a ticket. Share them only with people who should see the ticket.

21. Community Alerts

Community Alerts lets an Organization send email and text message alerts to residents who subscribe.

- **The Organization is the sender.** Text messages are sent through the Organization's own text messaging account, such as a Twilio account and its registered messaging campaign. The Organization is responsible for its alerts' content, for its messaging account and registrations, and for complying with the laws on consent, text messaging, and email that apply to it, including the Telephone Consumer Protection Act and the CAN-SPAM Act.
- The Organization is responsible for the wording residents agree to when they subscribe, for adding people only with their consent, and for honoring opt-outs. The Service records each subscriber's consent and handles STOP replies, but the Organization must keep its messaging account set up to send replies to the Service.
- Our Text Messaging Terms describe text alerts to residents. The Organization may link to them and to our Privacy Policy from its sign-up page, along with its own privacy policy.
- Community Alerts is not a public warning system and does not replace IPAWS, Wireless Emergency Alerts, the Emergency Alert System, sirens, or official emergency notifications.
- Delivery is not guaranteed. Carriers, email providers, and devices can delay, filter, or block messages.

- Subscribers may be charged message and data rates by their carrier. Text messaging charges are between the Organization and its messaging provider.

22. Surveys, Elections, Station Board, Websites, and Public Pages

- **Department websites** are published under the Organization's name. The Organization is responsible for their content, including text, photos, and links; for having the rights to what it publishes; for keeping emergency and contact information current; and for any domain it connects, including its registration and DNS. We may take down content that violates these Terms or the law. If the Organization's account ends, its website stops being served.
- **Elections** are designed so that no one, including us and the Organization's administrators, can see how an individual member voted. The Organization is responsible for its election rules, eligibility, bylaws, and for certifying results. We do not guarantee that an election meets any legal or bylaw requirement.
- **Surveys** can be answered by members or the public, by name or anonymously. Anonymous public responses are stored without a user ID or network address. The Organization is responsible for what it asks and how it uses the answers.
- **Station Board** screens and **public pages and links** show whatever the Organization chooses to display, sometimes to the public. Do not show sensitive or confidential information on a screen or page that people without access can see.
- Public pages and websites are published under the Organization's name. The Organization is responsible for their content and for making them accessible as the law requires, including the web accessibility rules that apply to state and local governments under Title II of the Americans with Disabilities Act. Our Accessibility Statement describes what we do on our side.

23. Sparky and Other AI Features

Sparky, our AI assistant, and the other AI-assisted features use a third-party AI service provider that we select, currently Google (Gemini) or OpenAI, as listed on our Subprocessors page. Our Privacy Policy lists each feature, when it runs, and what the provider receives. They include Sparky's assistant and web search, Recruiting application reviews, inspection overviews, fire investigation assistance, reading paper Information Requests, business card scanning, and summaries of issue reports.

Sparky is off until it is turned on for an Organization, and the Organization decides which roles may use it, which areas of the Service it can reach, and which application hubs and inspection features use it.

- To answer a request, we send the AI provider the information that request needs. Depending on the request and your permissions, this can include your conversation, files you attach, the page you are on, member names and email addresses, and records you are allowed to see. Passwords, PINs, face templates, Social Security numbers, and members' medical records are never sent.
- We do not use Customer Data to train AI models of our own.
- AI output can be inaccurate, incomplete, biased, or out of date, and it can describe things that are not true. Review it before relying on it, especially for anything involving safety, pay, discipline, hiring, inspections, investigations, or legal obligations.
- Sparky cannot change records on its own. It proposes an action and acts only after you confirm. You are responsible for what you confirm and for files you ask it to create.
- Application reviews, scores, overviews, and investigation suggestions are advice. Do not base an employment, enforcement, or investigative decision on AI output without your own review. If your Organization uses AI in employment decisions, it is responsible for any notice, audit, or alternative the law requires.
- Sparky's web search sends a short query to the AI provider's search service. Results come from public websites we do not control.
- Do not enter information into an AI feature that your Organization has not authorized you to share, and do not use AI features to identify people from photos.

The Scheduling auto-builder is a rules-based tool and does not use an AI service.

24. Integrations, Workflows, and Third-Party Services

The Service relies on and connects to third-party services, including hosting, storage, email, push notifications, maps and address lookup, weather and news, AI providers, CAD and alerting services, scheduling and apparatus-check services, calendar and spreadsheet services, and NERIS.

When an Organization connects an integration, such as Active911, PSTrax, WhenToWork, a weather service, Google Sheets, or a text messaging account, or builds a Workflow that sends data to another system, it directs us to exchange Customer Data with that system using the Organization's own account and credentials. The Organization is responsible for having the right to connect those accounts. The other service's own terms and privacy policy apply to what it does with that data. We keep integration keys and tokens on our servers and do not show them again after they are saved.

We are not responsible for third-party services, their content, their accuracy, their outages, or changes they make.

25. Mobile and Desktop Apps

Station Clipboard offers a mobile app, distributed through the Apple App Store and any other app store we choose, and a desktop app for Windows and Mac. The apps open the Department Portal and give access to an Organization's account, enabled modules, and authorized records. The Command Portal opens in your web browser.

Subject to these Terms and the Organization's agreement, we grant authorized users a limited, revocable, non-exclusive, non-transferable license to install and use the apps on devices they own or control, for authorized Organization purposes.

- An active Organization account, a compatible device, a supported operating system, internet access, and a current app version may be required.
- The desktop app does not update itself. Download new versions from stationclipboard.com. Older versions may stop working when that is necessary for security, compatibility, or reliability.
- The desktop app starts when you sign in to your computer and keeps running in the tray or menu bar unless you change those settings. It allows the portal to use notifications, your camera and microphone, and your location when a feature asks for them.
- Some features need device permissions, such as notifications, camera, or photo library access. Denying a permission may stop that feature from working.
- The apps are not an emergency dispatch, emergency alerting, life-safety, or guaranteed real-time communication service.
- Installing or removing an app does not create, cancel, or change an Organization's subscription, account, or agreement with us.

Additional terms for apps from the Apple App Store. These Terms are between you and us, not Apple. Apple is not responsible for the app or its content, and has no obligation to provide maintenance or support for it. If the app fails to meet an applicable warranty, you may notify Apple, and Apple may refund any purchase price you paid for the app; to the extent the law allows, Apple has no other warranty obligation for it. We, not Apple, are responsible for addressing any claims about the app, including product liability claims, claims that it fails to meet a legal or regulatory requirement, consumer protection claims, and claims that it infringes someone's intellectual property. You confirm that you are not located in a country subject to a U.S. government embargo and are not on any U.S. government list of prohibited or restricted parties. You must also follow the App Store's own terms. Apple and its subsidiaries are third-party beneficiaries of these Terms as they apply to the app, and may enforce them against you.

Other app stores. If you get an app from another store, such as Google Play, that store's terms also apply, and that store is not responsible for the app.

26. Support, Issue Reports, and Access by Our Staff

Access by our staff. Our authorized staff may access an Organization's account, including by viewing the Service as a particular user, and may use administrative tools that reach stored data directly. We use this access to provide support the Organization or a user asks for, to investigate problems, to set up or move data at the Organization's request, to keep the Service secure, and to comply with the law. We limit it to staff who need it, and we record it in our own audit logs. Our staff's access may not appear in the Organization's activity log.

Staff viewing the Service as a user cannot accept these Terms for that user. Organization administrators who view the Service as a member are recorded in the Organization's activity log.

Support tickets and issue reports. When you open a support ticket or report an issue, we receive what you write, a screenshot of your screen unless you remove it, and the technical details our Privacy Policy describes. Issue reports go to our support team, not your Organization, and an AI provider writes a short summary and title for each one. The title, category, priority, and status of an issue you report, and any public update we write, may appear on our public issue board. Your name, your description, and your screenshot are never shown there. Remove the screenshot if your screen shows information that should not leave your Organization.

Error reports. The Service may automatically capture technical details when something goes wrong, such as the error, the page, and the browser. These are not shown publicly.

27. Organization Compliance Responsibilities

Organizations are responsible for making sure their use of the Service complies with the laws, regulations, contracts, and policies that apply to them. These may include:

- Employment, civil service, anti-discrimination, and background check laws
- Volunteer service rules
- Payroll, wage, and tax laws
- Public records and records retention laws
- Fire service, EMS, and incident reporting requirements, including NERIS and state reporting rules
- Training and certification requirements

- Privacy, biometric privacy, health information, employee monitoring, text messaging, and email laws
- Accessibility requirements for public pages they publish
- Department policies and bylaws
- Municipal, county, district, state, and federal requirements

We provide tools, templates, records, exports, and reports. The Organization remains responsible for checking that they are accurate and compliant.

28. Acceptable Use

You agree not to:

- Use the Service for unlawful purposes
- Access data you are not authorized to access, or try to bypass permissions or security controls
- Share credentials or use another person's account
- Upload malicious code or interfere with the Service
- Probe, scan, or test the Service for vulnerabilities without our written permission
- Reverse engineer, decompile, or try to extract source code, except where the law allows
- Scrape the Service, or access it by automated means other than the integrations, Workflows, and interfaces we provide
- Resell or sublicense the Service without our written permission
- Harass, threaten, abuse, or harm others
- Misrepresent records, attendance, PAR results, certifications, time entries, course progress, reports, votes, or approvals
- Declare a false MAYDAY or other emergency, or enter false accountability information
- Send test, sample, or made-up reports to NERIS Production, or put personal information in NERIS free-text fields
- Try to identify how an individual voted in an Elections ballot or who gave an anonymous survey answer
- Use Community Alerts for marketing, fundraising, or anything other than the Organization's public safety and community information
- Send spam or messages to people who have not consented to receive them
- Submit false, harassing, or retaliatory complaints, or use a public page to impersonate someone
- Use the Service to surveil, stalk, or track people, or to look up information about people for reasons unrelated to the Organization's work
- Publish content on a department website or public page that is unlawful, misleading, or infringes someone else's rights
- Get around rate limits, link expirations, or other technical limits, or share a personal link meant for someone else
- Use the Service in a way that could harm us, other users, Organizations, or the public

To report a security vulnerability, follow our vulnerability disclosure policy. Testing done in good faith under that policy is authorized.

29. Subscriptions, Trials, Fees, and Payment

Access to Station Clipboard may be provided under a subscription, trial, order form, quote, invoice, written agreement, or other approved arrangement.

Fees, billing frequency, included modules and products, usage limits (such as storage), renewal terms, and payment requirements are set out in the Organization's agreement.

Unless otherwise stated in writing:

- Fees are non-refundable, except where the law requires a refund
- Payment is due according to the invoice or agreement
- Late or failed payment may lead to suspension or termination
- Pricing may change at renewal with reasonable notice
- Taxes, if any, are the Organization's responsibility, except where the Organization is exempt
- When a trial ends, access may stop until a subscription begins

If a governmental Organization's governing body does not appropriate funds for a renewal term, the Organization may end its subscription at the end of the term already paid for by giving us written notice.

We do not store payment card numbers. If payments are processed by a third-party provider, that provider's terms apply to the payment.

30. Service Availability and Maintenance

We work to keep Station Clipboard reliable and available, but we do not guarantee uninterrupted, error-free, or delay-free operation, including during an incident.

The Service may be unavailable because of maintenance, updates, security actions, infrastructure problems, third-party outages (including those of hosting providers, CAD and alerting services, map services, NERIS, and carriers), internet or cellular disruptions, emergency repairs, or events outside our control.

We may modify, suspend, limit, or discontinue parts of the Service where needed for security, reliability, legal compliance, or product quality.

31. Beta, Trial, and Preview Features

Some features may be released as beta, trial, preview, experimental, or early-access features. They may be incomplete or unstable, and they may change, be limited, or be removed at any time.

They are provided for testing and feedback. Do not rely on them for critical operations unless we approve it in writing.

32. Reports, Exports, and Record Accuracy

The Service produces reports, exports, dashboards, logs, summaries, and records from data entered by users, Organizations, and connected systems.

Organizations are responsible for reviewing records before relying on them for payroll, compliance, training, certification, discipline, public records, incident reporting, reimbursement, legal, or operational purposes.

We do not guarantee that any report or export satisfies a particular legal, regulatory, payroll, employment, fire service, EMS, or public records requirement.

33. Public Records and Legal Requests

Customer Data held for a governmental Organization may be a public record under the laws that apply to it. The Organization is the custodian of its records and decides how to respond to public records requests. If we receive a public records request for an Organization's Customer Data, we will refer the requester to the Organization.

If we receive a subpoena, warrant, or other legal demand for an Organization's Customer Data, we will tell the Organization before we respond, unless the law prohibits it, so that it can seek to protect the data. We will give the Organization reasonable help to export records it needs to respond to a request.

34. Intellectual Property

Station Clipboard, the Department Portal, the Command Portal, the apps, the software, designs, logos, branding, layouts, features, workflows, built-in templates and checklists, documentation, and related materials are owned by Station Automation Solutions LLC or its licensors.

These Terms give you a limited, non-exclusive, non-transferable, revocable right to use the Service while your access is authorized. No other rights are granted. Your Organization may copy and adapt our built-in templates and checklists for its own internal use.

You may not copy, reproduce, modify, distribute, sell, lease, sublicense, or create derivative works from the Service unless we permit it in writing.

NERIS, NFIRS, NFPA, TIFMAS, and other names of agencies, standards, and products belong to their owners. We use them only to describe what the Service works with; their use does not mean those owners endorse us.

35. Copyright Complaints

We respect intellectual property rights and expect users to do the same. If you believe content in the Service, including a department website or public page, infringes your copyright, send a notice to hello@stationclipboard.com with the subject line "Copyright Notice" that includes:

- Your name, address, telephone number, and email address, and your physical or electronic signature
- The copyrighted work you believe is infringed
- The web address or other information that lets us find the material
- A statement that you have a good-faith belief that the use is not authorized by the copyright owner, its agent, or the law
- A statement, under penalty of perjury, that the information in your notice is accurate and that you are the copyright owner or authorized to act for the owner

We may remove or disable access to the material and will tell the Organization that published it, which may send a counter-notice with the information the law requires. We may end the access of users who repeatedly infringe.

36. Feedback

If you send us ideas, suggestions, bug reports, feature requests, or other feedback, you allow us to use it without restriction or payment.

37. Confidentiality

Through the Service you may see non-public information, such as personnel files, incident details, preplans, building contacts, and operational information.

You agree to protect it, and to access, use, or disclose it only as your Organization, these Terms, the law, and any applicable agreement allow.

Organizations are responsible for training and supervising their users in handling confidential and sensitive information.

38. Suspension and Termination

We may suspend or end access if:

- Fees are not paid
- A user or Organization violates these Terms
- Access creates a security or legal risk
- The Service is misused
- The law requires it
- An agreement expires or ends
- Continued access could harm us, users, Organizations, or the public

Where it is practical and lawful, we will give the Organization notice and a chance to fix the problem before suspending its account. We may suspend access immediately, without notice, when needed to stop a security threat, an emergency, or serious harm, and we will restore it once the problem is resolved.

Organizations may cancel according to their agreement, or by sending us our Account Closure and Data Export Request. When access ends, the right to use the Service ends. Before then, the Organization should export the records it needs; we will give reasonable help. When an account is scheduled for deletion, it goes offline and can be restored for 7 days, including to complete a final export. After that, its data is deleted as our Privacy Policy and Data Processing Addendum describe, unless the Organization's agreement or the law requires otherwise.

39. Disclaimers

The Service is provided "as is" and "as available."

To the fullest extent the law allows, we disclaim all warranties, express or implied, including warranties of merchantability, fitness for a particular purpose, title, non-infringement, availability, accuracy, and reliability.

We do not warrant that:

- The Service will be uninterrupted, available during an incident, or error-free
- The Service will meet every Organization requirement
- Timers, alerts, notifications, PAR prompts, or messages will be delivered on time or at all
- Maps, locations, addresses, hydrant data, preplans, or data from CAD and other integrations will be accurate
- Calculations, AI output, or data entered by users will be accurate
- NERIS or any other agency will accept a report
- Records will satisfy every legal or regulatory requirement
- Third-party services, including NERIS, will remain available
- Reports or exports will be accepted by any agency, court, auditor, employer, regulator, or authority

40. Limitation of Liability

To the fullest extent the law allows, neither Station Automation Solutions LLC nor Station Clipboard will be liable for indirect, incidental, special, consequential, exemplary, or punitive damages, including lost profits, lost revenue, lost data, business interruption, reputational harm, or loss of goodwill.

The Service is a support tool for people who make operational decisions. To the fullest extent the law allows, we are not liable for injury, death, or property damage that results from operational, incident command, or life-safety decisions made by an Organization or its members, including decisions made while relying on information in the Service.

To the fullest extent the law allows, our total liability arising out of or related to the Service or these Terms, for all claims together, will not exceed the greater of the amount the Organization paid us for the Service in the twelve months before the event that gave rise to the claim, or one hundred U.S. dollars.

These limits apply to every theory of liability, including contract, tort (including negligence), strict liability, and statute, even if we were told the damages were possible, and even if a remedy fails of its essential purpose. They reflect the price of the Service and how risk is shared between us, and they are an essential part of our agreement.

These limits do not apply to liability that the law does not allow to be limited, such as liability for gross negligence or willful misconduct where the law provides so. Some jurisdictions do not allow certain limitations, so some of these may not apply to you.

41. Indemnification

To the fullest extent the law allows, you and your Organization agree to defend, indemnify, and hold harmless Station Automation Solutions LLC, Station Clipboard, and their owners, officers, employees, contractors, agents, and service providers from claims, damages, losses, liabilities, costs, and expenses arising from:

- Misuse of the Service
- Violation of these Terms, the NERIS Terms of Use, the law, or third-party rights
- Customer Data or uploaded content, including reports sent to NERIS
- Messages the Organization sends, including Community Alerts
- Failure to obtain a required notice or consent, including for biometric enrollment
- Unauthorized access caused by user or Organization conduct
- The Organization's own decisions, including operational, incident command, employment, payroll, discipline, inspection, enforcement, investigation, compliance, and public records decisions
- Content the Organization publishes on a department website or public page

We will tell you promptly about a claim covered by this section, let you control its defense and settlement with counsel reasonably acceptable to us, and give reasonable help at your expense. You may not settle a claim in a way that admits fault for us or binds us to do anything without our written consent. We may take part in the defense with our own counsel at our own expense.

42. Public Entities

If your Organization is a governmental entity:

- The indemnification, limitation of liability, governing law, and venue provisions of these Terms apply only to the extent the laws that govern it allow. Where those laws prohibit the Organization from agreeing to indemnify, the indemnification provision does not apply to the Organization, and each party is responsible for its own acts to the extent the law provides.
- Nothing in these Terms waives any immunity, defense, or limit on liability the Organization has under law.
- Nothing in these Terms requires the Organization to keep confidential anything that public records laws require it to disclose.
- A change to these Terms does not bind the Organization to anything its laws require its governing body to approve until the Organization approves it, but it does apply to its users' use of the Service.

43. Governing Law, Venue, and Disputes

These Terms are governed by the laws of the State of Texas, without regard to conflict-of-law rules.

Talk to us first. Before starting a lawsuit or other proceeding, the party with a dispute will send the other a written description of it, and both will try in good faith to resolve it for at least 30 days. Disputes about the Service can usually be fixed this way. Either party may ask a court for an injunction at any time to protect its data, intellectual property, or confidential information.

Where disputes are decided. Unless the law or a separate written agreement requires otherwise, disputes arising from or related to these Terms or the Service will be decided in the state or federal courts located in Harris County, Texas, and both parties consent to those courts' jurisdiction.

Individual claims, without a jury. To the extent the law allows, each party brings claims only in its individual capacity, not as a plaintiff or class member in a class, collective, or representative proceeding, and each party waives the right to a jury trial.

Time limit. To the extent the law allows, a claim arising from these Terms or the Service must be brought within one year after it arises, or it is permanently barred.

If your Organization is a governmental entity whose laws require its own state's law or courts, or do not allow any part of this section, those laws apply instead, to that extent.

44. Changes to These Terms

We may update these Terms from time to time. When we do, we will change the "Last updated" date above and tell you about material changes through the Service, the website, email, or another reasonable method. Unless a change is needed sooner for legal, security, or safety reasons, or only adds a new feature, material changes take effect 15 days after we publish them.

When we publish a new version, Station Clipboard products may ask you to accept it before you continue. Continuing to use the Service after updated Terms take effect also means you accept them. If you do not agree to a change, stop using the Service, and your Organization may cancel under its agreement.

45. Separate Agreements

An Organization may have a separate written agreement with Station Automation Solutions LLC that adds to or differs from these Terms. If a signed written agreement directly conflicts with these Terms, the signed agreement controls for that Organization, to the extent of the conflict. If the Data Processing Addendum conflicts with these Terms about personal information, the Data Processing Addendum controls.

46. General

- **Electronic communications.** You agree that we may send you notices and other communications electronically, through the Service or by email, and that they satisfy any requirement that communications be in writing. Emails from Station Clipboard may come from a stationautomations.com or stationclipboard.com address.
- **Assignment.** You may not transfer these Terms without our written consent. We may transfer them in connection with a merger, acquisition, or sale of assets, or to an affiliate.
- **Severability.** If any part of these Terms cannot be enforced, the rest remains in effect.
- **No waiver.** Not enforcing a provision is not a waiver of our right to enforce it later.
- **Events beyond our control.** We are not responsible for delays or failures caused by events outside our reasonable control, such as natural disasters, utility or internet failures, third-party outages, or acts of government.
- **Export.** You may not use or export the Service in violation of U.S. export laws and sanctions.
- **U.S. government users.** The Service is "commercial computer software" and "commercial computer software documentation," and U.S. government users receive only the rights described in these Terms.
- **Notices to us.** Send legal notices to hello@stationclipboard.com with the subject line "Legal Notice." A notice is received when we confirm receipt.
- **Independent parties.** We and the Organization are independent contractors. These Terms do not create a partnership, joint venture, agency, or employment relationship.
- **No third-party beneficiaries.** Except as Section 25 says about Apple, no one other than you and us has rights under these Terms. Members and residents keep the rights the law gives them.
- **Survival.** Provisions that by their nature should continue after these Terms end, including those on Customer Data, confidentiality, fees owed, disclaimers, limitation of liability, indemnification, and disputes, continue.
- **Interpretation.** "Including" means "including without limitation." Headings, the key points at the top, and summaries are for convenience only and do not change the meaning of these Terms.
- **Entire agreement.** These Terms, the policies listed in Section 6, and any signed agreement with your Organization are the entire agreement about the Service, and replace earlier versions of these Terms.

47. Contact Us

Questions about these Terms may be sent to:

Station Automation Solutions LLC, owner and operator of Station Clipboard
Houston, Texas
Email: hello@stationclipboard.com
Phone: (979) 341-9333

Every Station Clipboard legal document is listed in our Legal Center.

Terms of Service · 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.