SearchSync Security Overview

Version 1.1 · **Effective Date:** October 7, 2026 · **Last Updated:** October 7, 2026 · Published at https://www.searchsync.com/legal/security-overview-v1.1 **Incorporated into the SearchSync Terms of Service by Section 10.1**

This document describes the safeguards SearchSync Technologies, Inc. currently operates to protect company and customer information. Items expressly identified as planned, in deployment, or as targets are stated for transparency, are not currently-operating safeguards, and are not commitments under Section 10.1 of the Terms. Recovery objectives are targets and not warranties. Availability is addressed in Section 2.4 of the Terms, which states a target rather than a service level commitment, and which a Beta Program Rider suspends where one is attached.

1. Governance

- A named Information Security Officer owns the security program.
- Written information security policy, incident response plan, and business continuity and disaster recovery plan, each reviewed at least annually and after any significant incident or material change to the business.
- All directors, founders, employees, and contractors with access to company systems or data must acknowledge the information security policy in writing.
- SearchSync is not currently SOC 2 certified. We expect to pursue SOC 2 Type I following general availability.

2. Access Control

- Access is granted on a least-privilege basis and only on approval by the Information Security Officer.
- Individual named accounts are required. Shared credentials are prohibited.
- Multi-factor authentication is required on every account that supports it, for all SearchSync personnel and contractors and for all customer users, as set out in Section 4.3 of the Terms. Where a Beta Program Rider is attached to a customer's Order Form, multi-factor authentication is available and strongly recommended for that customer's users rather than mandatory.
- Credentials are stored only in our approved password manager (1Password). Production credentials and recovery keys are held in restricted vaults and are not permitted in source code, chat, email, or personal storage.
- Access is reviewed when responsibilities change and revoked promptly on separation.
- Role-based access limits personnel access to customer data to what is required for their role.

3. Encryption

- Data in transit is encrypted using TLS.
- Data at rest is encrypted using AES-256 or stronger.
- Database connections require TLS.
- Database backups are encrypted.
- Encryption keys are managed by the underlying cloud provider.

4. Application and Infrastructure Security

- Automated vulnerability scanning of containers and open-source dependencies runs on each deployment.
- Security-focused code review is performed for new features and changes.

- Application, infrastructure, and database activity is logged, with anomaly detection for unusual access patterns.
- Infrastructure is defined as code and deployed through controlled CI/CD pipelines.
- Payment card data is collected only through Stripe-hosted payment components. Our systems do not store, transmit, or log full card numbers or card security codes.
- Session recording used for defect diagnosis is configured to mask all on-screen text and all form inputs, to exclude document and file preview components from capture, and to redact network payloads and URL identifiers. Customers may request that session recording be disabled for their organization.
- Inbound submissions received at Platform intake addresses may be filtered, quarantined, or rejected where reasonably believed to be malicious, unsolicited at volume, or unlawful, as set out in Section 6.9 of the Terms.

5. Endpoint and Personnel Security

- Devices accessing company or customer data must be supported, password-protected, and configured with full-disk encryption, automatic updates, and screen lock.
- We are deploying endpoint detection and response (CrowdStrike) to company-issued computers and to approved personal computers used to access company or customer data. Until that deployment is complete, endpoint protection relies on the device requirements described above.
- Company and customer data may be handled only through tools approved by the Information Security Officer.
- Security and phishing-awareness training is required at least annually.
- Sensitive data may not be sent through ordinary email or chat.

6. Sensitive Identifiers

- Customers may submit taxpayer identification numbers, including Social Security numbers, individual taxpayer identification numbers, and employer identification numbers, in fields the Platform designates for them and within tax documents such as Schedules K-1.
- Where the Platform stores a taxpayer identification number in a designated field, the value is encrypted and is displayed only as its last four digits.
- Tax documents uploaded by customers are stored as customer documents, encrypted at rest as described in Section 3, and subject to the access controls in Section 2.
- Access to taxpayer identification numbers is limited to personnel whose role requires it, on approval by the Information Security Officer, and is logged.
- Taxpayer identification numbers are used only to provide the Platform to the customer. They are not used for any other purpose and are excluded from de-identified data.
- Where a customer has enabled AI processing for a document that contains a taxpayer identification number, the document is transmitted to the AI provider identified in Section 8 for processing. That provider is contractually prohibited from using it to train models.
- Taxpayer identification numbers may not be sent through ordinary email or chat, and are not exported to any system other than those listed in Section 8.

7. Vendor Management

- Third-party providers receive only the information necessary to perform their services.
- We review a provider's security practices and contract terms before granting access to confidential information.
- Vendor access is limited to the minimum necessary and removed when no longer needed.

- Customers receive at least thirty (30) days' notice before a new subprocessor with access to customer data is engaged.

8. Current Subprocessors and Infrastructure

Provider	Role	Access to customer data
DigitalOcean	Application hosting, managed PostgreSQL production database, backups	Yes
Cloudflare	DNS, CDN, marketing site hosting	No
Amazon Web Services	Contingent failover infrastructure	Yes, if activated
Clerk	Authentication, identity, multi-factor authentication	Account data only
Anthropic	AI models for document processing and conversational features	Yes, at time of processing
Google Workspace	Company email; inbound investment-address email handling	Yes
Google Analytics	Marketing website analytics	No
PostHog (PostHog Cloud, US region)	Product analytics and session recording	Yes, as masked session recordings
Stripe	Payment processing	Billing data only
GitHub	Source control and CI/CD	No
1Password	Credential management	No

9. Business Continuity and Disaster Recovery

- Recovery time objective (target): one business day.
- Recovery point objective (target): up to four hours of production data loss.
- Daily automated database backups with point-in-time recovery within the available recovery window, currently seven days.
- Encrypted backups held separately from ordinary production access.
- Infrastructure rebuildable from version-controlled definitions in an alternate region or, if required, an alternate provider.
- Named primary and backup plan owners with documented activation authority.
- The plan is reviewed at least annually and after any material infrastructure change or significant outage.

10. Incident Response

- All personnel must report suspected incidents immediately by phone to the Information Security Officer, with a named backup contact.
- The Information Security Officer coordinates containment, investigation, notification, recovery, and documentation.
- We preserve evidence, maintain a written incident record, and conduct a post-incident review after any material incident.
- We engage qualified legal counsel where notification or regulatory obligations may apply.

- We maintain cyber liability and technology errors and omissions insurance with limits of not less than $1,000,000 per claim and in the aggregate, as set out in Section 10.5 of the Terms.
- Customer notification commitments are set out in Section 10.2 of the Terms: notice without undue delay and in any event within seventy-two (72) hours after we confirm a security incident affecting customer data.

11. Diligence

Once per twelve-month period, at a customer's request, we will complete one reasonable security questionnaire, make available our then-current information security policy, incident response plan, and business continuity and disaster recovery plan subject to confidentiality, and make appropriate personnel available for one diligence call.

Contact

Security questions and incident reports: info@searchsync.com SearchSync Technologies, Inc., P.O. Box 571, Mineral Springs, NC 28108, United States

Version 1.1 · © 2026 SearchSync Technologies, Inc.