

Secure Passwords Privacy Policy

Version 1.3 — Effective October 11, 2026

This Privacy Policy explains what information Secure Passwords LLC, a Wyoming limited liability company ("Secure Passwords," "we," "us"), collects when you use the Secure Passwords password manager — our website and web vault, mobile apps, browser extensions, automation API, and AI features (the "Service") — how we use it, and the choices and rights you have.

The short version: **your vault is end-to-end encrypted and we cannot read it.** We collect the minimum account and operational data needed to run a security product, we do not sell personal information, and we do not show ads.

1. Information We Cannot Access

- **Your master password** never leaves your device. Authentication uses a derived hash that is itself re-hashed on our servers; neither form can be reversed into your password.
- **Your vault contents** — passwords, secure notes, payment cards, bank accounts, crypto wallet details, personal information items, file attachments and their filenames, folder names, TOTP secrets, and shared item contents — are encrypted on your device with keys derived from your master password. Our servers store only ciphertext. We cannot decrypt, view, or recover it.
- If you lose your master password and any recovery key you created, we cannot restore your vault. That is a designed property of the system.

2. Information We Collect

Account information. Name, username, email address, and optional profile details you add (display name, avatar image, time zone, language, date/time format). Avatar images are stored so they can be displayed without unlocking your vault.

Encrypted vault data and its minimal metadata. Alongside the ciphertext itself we store the item type (e.g., "password" vs. "note"), timestamps, and — for attachments — file size, extension, and declared file type, which we need for storage quotas and safety limits. We never see decrypted contents.

Authentication and security data. Salted, hashed authentication verifiers; key-derivation parameters; MFA status and encrypted TOTP seed; hashed recovery codes; hardware security key public keys and metadata (never private keys); passkey-related public material; and your security settings (for example Location Access rules).

Devices and sessions. When you sign in we record device identifiers generated by the app, device type, operating system and browser, IP address, approximate location derived from IP (city/region/country), sign-in time and method, and which client you used (web, extension, or mobile). This powers the session list, trusted devices, new-device alerts, and your Location Access rules.

Security event history. An audit trail of security-relevant actions on your account (sign-ins, MFA changes, sharing events, API token use, and similar), including IP address and timestamps. This is the data behind the Session History and security notification features.

Billing information. Plan, subscription status, and Stripe customer and subscription identifiers. Payments are processed by Stripe (or by Apple/Google for app-store purchases); we never store full card numbers.

Free trial and trial-abuse prevention. If you start a free Premium trial, we store when it started and ends and which reminder emails we have sent. No payment details are collected for the trial. So that each person can have one trial, we also keep two one-way keyed hashes (HMACs): one of your email address after removing cosmetic variations (such as "+" tags and, for Gmail, dots), and one of the IP address you started the trial from. We cannot turn these back into your email address or IP address, and they are not used to identify your device or to build a profile of you. We also check your email domain against a list of disposable-email services. These records exist only to prevent repeated trials and to block mass sign-ups.

Organization data. If you own or join a Teams organization: organization name, member names, email addresses, roles, statuses, invitations, and seat usage.

Support and AI conversations. If you contact support or use the AI assistant, we process the messages you send. Support cases are stored with your account. Do not include vault secrets in support or AI conversations — they are not needed.

Optional, off-by-default data. Some features collect data only if you turn them on: login and autofill history ("Track History"), anonymous error reporting ("Help Improve"), and anonymous usage analytics ("App Attribution"). Each can be switched off at any time in Security settings.

Breach checking. Password breach checks use k-anonymity: only the first five characters of a one-way hash of a password ever leave your device, which is not enough for us or Have I Been Pwned to learn the password. Your email address is used for account-level breach notifications only as described in the feature.

3. What We Do Not Do

- We do not sell or rent personal information, and we have not done so.
- We do not show advertising and do not share your data with ad networks or data brokers.
- We do not use your vault data for analytics, advertising, or training AI models — we could not, because we cannot decrypt it.

4. How We Use Information

We use the data above to: provide and secure the Service (authentication, sync, autofill, sharing, MFA, breach and health checks); detect and prevent abuse, fraud, and unauthorized access; provide security alerts and notifications you have enabled; process subscriptions and payments; run free trials, send trial reminders, and prevent trial abuse; provide support and AI-assisted help; understand aggregate product usage where you have opted in; and comply with legal obligations.

Where GDPR or similar law applies, our legal bases are: performance of our contract with you (core service delivery), legitimate interests (service security, abuse prevention, product improvement), consent (optional features such as history tracking, analytics, and marketing emails — withdrawable at any time), and legal obligation.

5. How We Share Information

We share personal data only with service providers ("subprocessors") acting on our instructions to run the Service, and in the limited situations below:

- **Stripe** — payment processing for direct purchases.
- **Amazon Web Services (Amazon SES)** — transactional email delivery (verification, security alerts, invitations, free-trial reminders).
- **Microsoft 365** — hosts our support and privacy mailboxes, so messages you send to us there are processed by Microsoft.
- **Cloud infrastructure providers** — hosting of our servers, database, and encrypted file storage.
- **Have I Been Pwned** — k-anonymity breach lookups (hash prefixes only, as described above).
- **AI model providers** — processing of AI assistant conversations to generate responses; conversations are not used by us to train models.
- **Apple and Google** — if you purchase through their app stores, they process the transaction under their own policies.
- **Legal requirements.** We may disclose data we hold if required by valid legal process. Because vault data is end-to-end encrypted, we could produce only ciphertext and the metadata described in Section 2. Where lawful, we will notify you of demands for your data.
- **Business transfers.** If we are involved in a merger, acquisition, or asset sale, data may transfer as part of that transaction; this Policy will continue to apply, and we will notify you of any change in control.
- **With your direction** — for example when you share a vault item with another user (encrypted so only the recipient can read it) or join an organization.

6. Data Retention and Deletion

- Account and vault data are retained while your account is active.
- **You can delete your account in the app** (Settings → Account → Delete Account) on every platform. Deletion takes effect after a short grace period during which you can change your mind; after it, your account and all associated data — vault items, attachments, folders, sessions, devices, security keys, shares, API tokens, organization memberships you own, and your audit trail — are permanently purged from our systems.
- Backups containing purged data expire on a rolling basis within a bounded period after deletion.
- We retain limited billing records where required by tax and accounting law.
- **Trial-abuse records survive account deletion.** The one-way hashes described in Section 2 (free trial and trial-abuse prevention) are kept after you delete your account, because deleting an account must not reset the one-trial limit. They contain no readable personal data. The hash of an IP address is kept only as long as needed to apply the per-IP limit (30 days) and the hash of an email address is kept for as long as we offer free trials. You can ask us to review or remove them at privacy@securepasswords.com, but if we remove the email hash we cannot prevent that address from receiving another trial.

7. Security

Security is the product. Measures include: end-to-end AES-GCM encryption of vault data with keys derived on-device via Argon2id; server-side re-hashing of authentication verifiers; encrypted storage of server-held secrets; TLS for all transport; session revocation and refresh-token reuse detection; optional MFA including TOTP and phishing-resistant hardware security keys; rate limiting and lockouts; scoped, hashed API tokens; and an append-only audit trail. No system is perfectly secure, and Section 1's design means the most important key — your master password — is in your hands.

8. Your Rights and Choices

- **Access and portability.** You can view your data in the app and export your vault at any time using the built-in export tools.
- **Correction.** You can edit account and profile information in Settings.
- **Deletion.** In-app account deletion is described in Section 6.
- **Preferences.** Notification, marketing, analytics, and history-tracking choices are in Settings; marketing email is off by default and every marketing message includes an unsubscribe link. Security-critical notices (for example, sign-in alerts required to protect your account) cannot be disabled.
- Depending on where you live (for example the EU/EEA, UK, or California), you may have additional statutory rights — to access, correct, delete, restrict, or object to processing, to data portability, to withdraw consent, to opt out of "sale" or "sharing" (we do neither), to non-discrimination for exercising your rights, and to complain to a supervisory authority. To exercise any right, use the in-app tools or

contact privacy@securepasswords.com; we will verify your request and respond within the legally required time.

9. International Transfers

We are based in the United States and process data there. Where we transfer personal data from the EU/EEA, UK, or Switzerland, we rely on appropriate safeguards such as Standard Contractual Clauses with our subprocessors.

10. Children

The Service is not directed to children under 13 (or the higher minimum age in your jurisdiction), and we do not knowingly collect personal data from them. If you believe a child has created an account, contact privacy@securepasswords.com and we will delete it.

11. Cookies and Similar Technologies

The web app uses only strictly necessary cookies and local storage: session tokens, a page-access cookie, and your interface preferences (such as theme). We do not use advertising or cross-site tracking cookies, and we honor the spirit of Global Privacy Control by not selling or sharing data in the first place.

12. Changes to This Policy

We will notify you of material changes in advance — by email, in-app notice, or a re-acceptance prompt — and update the version and effective date above. Earlier versions are available on request.

13. Contact

Privacy questions and requests: privacy@securepasswords.com. General support: support@securepasswords.com. If you are in the EU/EEA or UK, you may also lodge a complaint with your local data protection authority.