

Secure Passwords Terms of Service

Version 1.2 — Effective October 5, 2026

These Terms of Service ("Terms") are a binding agreement between you and Secure Passwords LLC, a Wyoming limited liability company ("Secure Passwords," "we," "us," or "our") governing your use of the Secure Passwords password manager, including our website and web vault, mobile applications, browser extensions, autofill and passkey services, sharing features, automation API, AI assistance features, and any related services (together, the "Service").

By creating an account, clicking "I agree," or using the Service, you accept these Terms, our Acceptable Use Policy (<https://app.securepasswords.com/acceptable-use>), and our Privacy Policy (<https://app.securepasswords.com/privacy>). If you do not agree, do not use the Service.

1. Who May Use the Service

- You must be at least 13 years old (or 16 where required by local law) to use the Service. If you are under 18, you may use the Service only with the consent of a parent or legal guardian who agrees to these Terms on your behalf.
- If you use the Service through an organization (for example, a Teams plan seat), you may also be subject to your organization's own policies. Where your organization's agreement with us conflicts with these Terms, the organization's agreement controls for your use of that organization's resources.
- You may not use the Service if you are barred from doing so under applicable law, including export control and sanctions laws described in Section 17.

2. Your Account, Master Password, and Recovery

- You are responsible for maintaining accurate account information and for everything that happens under your account.
- **Your master password is never transmitted to or stored by us in any usable form.** Encryption keys are derived from it on your device. We cannot see it, reset it, or recover it.
- **If you lose your master password and have not set up an account recovery key, your encrypted vault data is permanently unrecoverable.** This is a deliberate security property of the Service, not a defect, and you accept this risk by using the Service.
- You are responsible for safeguarding your master password, recovery key, multi-factor authentication devices and recovery codes, hardware security keys, and any device on which the Service is installed or unlocked.

- You must notify us promptly at security@securepasswords.com if you believe your account has been compromised.

3. The Service

The Service provides encrypted storage and management of credentials and related items (passwords, secure notes, payment cards, bank accounts, crypto wallet details, personal information, and file attachments), plus features including autofill, password generation, password health analysis, breach monitoring, two-factor authentication code storage, passkeys, hardware security key support, secure item sharing, folders, Teams organizations, security recommendations, an automation API, and AI-assisted help.

We may add, change, or remove features over time as described in Section 18.

4. Zero-Knowledge Architecture and Your Vault Data

- Vault contents are encrypted and decrypted on your devices. Our servers store only ciphertext they cannot decrypt ("Vault Data").
- **You retain all rights to your Vault Data.** You grant us a limited, non-exclusive license to store, transmit, back up, and otherwise process your encrypted Vault Data solely to provide and protect the Service.
- Certain limited data is necessarily processed outside the encrypted vault so that the Service can function — for example your name, username, and email address, billing status, device and session metadata, and security settings. Our Privacy Policy (<https://app.securepasswords.com/privacy>) describes this in detail.
- We do not and cannot review Vault Data. You are solely responsible for what you store, and for maintaining independent copies of anything irreplaceable (for example, cryptocurrency wallet recovery phrases). Export tools are provided in the app.

5. Plans, Subscriptions, and Billing

- The Service offers a free plan and paid subscription plans (including individual premium plans and Teams seat packs). Current features and pricing are described in the app and on our website.
- **Auto-renewal.** Paid subscriptions renew automatically at the end of each billing period at the then-current price unless you cancel before the renewal date. We will notify you in advance of material price increases, and they take effect no earlier than your next renewal.
- **Cancellation.** You can cancel at any time in the app's billing settings (or, for purchases made through an app store, in that store's subscription settings). Cancellation stops future renewals; your plan remains active through the end of the paid period.
- **Refunds.** Except where required by law or expressly stated otherwise, payments are non-refundable and there are no credits for partial periods. Purchases made through the Apple App Store or Google Play

are subject to that store's refund policies, and refund requests for those purchases must be directed to the store.

- **Payment processing** for direct purchases is handled by Stripe; we do not store full payment card numbers.
- **Downgrades.** If a paid plan lapses, your account reverts to the free plan. Your Vault Data is retained, but features exceeding free-plan limits may become read-only or unavailable until you re-subscribe.
- **Teams seats.** Teams plans are sold in seat packs billed annually. The purchasing account owner is responsible for all charges for the seat quantity purchased, whether or not seats are assigned.

6. Teams and Organizations

- The owner and administrators of a Teams organization can manage membership, suspend or remove members, and view organization metadata (member names, email addresses, roles, statuses, and seat usage). **Joining an organization does not give the organization access to your personal vault contents.**
- Organization owners are responsible for having the right to invite the people they invite, and for their organization's compliance with these Terms.

7. Acceptable Use

Your use of the Service must comply with our Acceptable Use Policy (<https://app.securepasswords.com/acceptable-use>), which is part of these Terms. We may suspend or terminate accounts that violate it as described in Section 14.

8. Automation API and Access Tokens

- Personal access tokens and other API credentials you create are your responsibility. Anyone holding a token with a vault-unwrapping capability can decrypt the Vault Data it grants access to; treat tokens like passwords, scope them narrowly, set expirations, and revoke them when no longer needed.
- API access is subject to published rate limits and scopes. We may throttle, suspend, or revoke API access that degrades the Service or violates these Terms.

9. AI Features

- AI-assisted features (such as in-app help and support drafting) generate content automatically. **AI output may be inaccurate or incomplete and is provided for convenience only** — it is not professional, legal, or security advice, and you should verify anything important.
- AI features never receive your decrypted Vault Data unless you explicitly provide it in a conversation. Do not paste secrets into AI conversations; the assistant does not need them.

- AI features may be powered by third-party model providers acting as our processors, as described in the Privacy Policy.

10. Third-Party Services

The Service interoperates with third-party services — for example Stripe for payments, Have I Been Pwned for k-anonymity breach checks, platform autofill and passkey frameworks, and app stores for distribution and in-app purchases. Your use of a third-party service is governed by that third party's terms, and we are not responsible for third-party services.

11. Apple App Store Additional Terms

If you obtained the app from the Apple App Store, the following additional terms apply:

- These Terms are between you and Secure Passwords only, not with Apple Inc. ("Apple"). Apple is not responsible for the app or its content.
- The license granted to you is a non-transferable license to use the app on Apple-branded products that you own or control, as permitted by the Usage Rules in the Apple Media Services Terms and Conditions (except that the app may be accessed by other accounts via Family Sharing or volume purchasing where enabled).
- Apple has no obligation to furnish maintenance or support for the app.
- In the event of any failure of the app to conform to an applicable warranty, you may notify Apple, and Apple will refund the purchase price you paid for the app (if any); to the maximum extent permitted by law, Apple has no other warranty obligation with respect to the app.
- Apple is not responsible for addressing any claims by you or a third party relating to the app, including product liability claims, claims that the app fails to conform to legal or regulatory requirements, and claims under consumer protection or similar legislation.
- In the event of a third-party claim that the app or your possession and use of it infringes intellectual property rights, Secure Passwords, not Apple, is responsible for the investigation, defense, settlement, and discharge of the claim.
- You represent that you are not located in a country subject to a U.S. Government embargo or designated a "terrorist supporting" country, and that you are not on any U.S. Government list of prohibited or restricted parties.
- Questions, complaints, and claims regarding the app should be directed to support@securepasswords.com.
- You must comply with applicable third-party terms of agreement when using the app (for example, your wireless data agreement).
- Apple and its subsidiaries are third-party beneficiaries of these Terms, and upon your acceptance, Apple has the right (and is deemed to have accepted the right) to enforce these Terms against you as a third-party beneficiary.

12. Google Play Additional Terms

If you obtained the app from Google Play, your download and use of the app are also subject to the Google Play Terms of Service, and in-app purchases made through Google Play are processed and refunded under Google Play's payment and refund policies.

13. Intellectual Property; Feedback

- The Service, including its software, design, and branding, is owned by Secure Passwords and its licensors and is protected by intellectual property laws. Except for the limited rights expressly granted here, no rights are transferred to you.
- We grant you a personal, limited, non-exclusive, non-transferable, revocable license to install and use the apps and extensions we make available, for your own use of the Service in accordance with these Terms.
- If you send us feedback or suggestions, you grant us a perpetual, irrevocable, royalty-free license to use them without restriction or compensation.

14. Suspension and Termination

- **By you.** You may stop using the Service at any time and may delete your account in the app (Settings → Account). Account deletion is subject to a short grace period during which you can cancel it; after the grace period, your account and all associated data — including your encrypted Vault Data — are permanently purged and cannot be restored. Export your data first.
- **By us.** We may suspend or terminate your access (with notice where practicable) if you materially breach these Terms or the Acceptable Use Policy, if required by law, or if your use poses a security or operational risk to the Service or other users. Where practicable, we will provide an opportunity to export Vault Data before an account is closed, unless legally prohibited or the data itself is the subject of the violation.
- Sections that by their nature should survive termination (including Sections 4, 13, 15, 16, 18, 19, and 20) survive.

15. Disclaimers

THE SERVICE IS PROVIDED "AS IS" AND "AS AVAILABLE." TO THE MAXIMUM EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, WE DO NOT WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, ERROR-FREE, OR IMMUNE TO COMPROMISE; THAT BREACH MONITORING WILL DETECT EVERY BREACH; THAT PASSWORD HEALTH OR SECURITY RECOMMENDATIONS WILL IDENTIFY EVERY RISK; OR THAT AUTOFILL WILL BEHAVE CORRECTLY ON EVERY WEBSITE

OR APP. NOTHING IN THIS SECTION LIMITS RIGHTS YOU HAVE UNDER MANDATORY CONSUMER PROTECTION LAW.

16. Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY LAW: (A) NEITHER PARTY IS LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, OR FOR LOST PROFITS, REVENUES, DATA, OR GOODWILL; (B) WE ARE NOT LIABLE FOR LOSS OF VAULT DATA RESULTING FROM A LOST MASTER PASSWORD OR RECOVERY KEY, FROM YOUR DEVICES OR CREDENTIALS BEING COMPROMISED, OR FROM YOUR FAILURE TO MAINTAIN EXPORTS OR BACKUPS; AND (C) OUR TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THE SERVICE IS LIMITED TO THE GREATER OF FIFTY U.S. DOLLARS (US \$50) OR THE AMOUNTS YOU PAID US FOR THE SERVICE IN THE TWELVE (12) MONTHS BEFORE THE EVENT GIVING RISE TO LIABILITY. SOME JURISDICTIONS DO NOT ALLOW CERTAIN LIMITATIONS, SO PARTS OF THIS SECTION MAY NOT APPLY TO YOU.

17. Export Controls and Sanctions

The Service includes encryption software subject to export control laws. You may not use, export, or re-export the Service in violation of U.S. export control and sanctions laws or any other applicable jurisdiction's laws, and you may not use the Service if you are located in an embargoed territory or listed on a restricted-party list.

18. Changes to the Service and to These Terms

- We may modify the Service, and we may modify these Terms, the Acceptable Use Policy, and the Privacy Policy. For material changes we will give you reasonable advance notice (for example, by email, in-app notice, or a re-acceptance prompt) before the changes take effect.
- Continued use of the Service after the effective date of updated Terms constitutes acceptance. If you do not agree to updated Terms, stop using the Service and, if you wish, export your data and delete your account.

19. Governing Law and Dispute Resolution

- These Terms are governed by the laws of the State of Wyoming, USA, excluding its conflict-of-laws rules, except where the mandatory consumer protection law of your country of residence applies.
- **Informal resolution first.** Before filing a claim, you agree to contact us at legal@securepasswords.com and give us 30 days to attempt to resolve the dispute informally.
- **Arbitration.** Except for disputes qualifying for small-claims court or seeking injunctive relief for intellectual property or unauthorized access, any dispute arising out of these Terms or the Service will be resolved by binding individual arbitration administered by the American Arbitration Association

under its Consumer Arbitration Rules. **You and Secure Passwords each waive the right to a jury trial and to participate in a class action.**

- **Opt-out.** You may opt out of this arbitration agreement by emailing legal@securepasswords.com within 30 days of first accepting these Terms, with your account email and a statement that you opt out of arbitration.
- If you reside in the EU/EEA or UK, nothing in this Section deprives you of the protection of mandatory provisions of your local law or your right to bring proceedings in your local courts.

20. Miscellaneous

- **Copyright complaints.** Notices of claimed copyright infringement may be sent to legal@securepasswords.com and should include the information required by 17 U.S.C. § 512(c)(3).
- These Terms, together with the Acceptable Use Policy and Privacy Policy, are the entire agreement between you and us regarding the Service.
- If any provision is found unenforceable, the remainder stays in effect. Our failure to enforce a provision is not a waiver.
- You may not assign these Terms without our consent; we may assign them in connection with a merger, acquisition, or sale of assets with notice to you.
- Notices to you may be provided by email to your account address or in-app.

21. Contact

Secure Passwords LLC (Secure Passwords) — support@securepasswords.com (support) · legal@securepasswords.com (legal) · security@securepasswords.com (security reports) · privacy@securepasswords.com (privacy)