

Secure Passwords Acceptable Use Policy

Version 1.1 — Effective October 5, 2026

This Acceptable Use Policy ("AUP") is part of the Secure Passwords Terms of Service (<https://app.securepasswords.com/terms>) and applies to every use of the Service — the web vault, mobile apps, browser extensions, autofill, sharing, Teams organizations, the automation API, and AI features. Because Secure Passwords is zero-knowledge, we cannot see what you store; this policy governs how you use the Service, and we enforce it based on observable activity, service metadata, and reports.

1. Lawful Use Only

You may not use the Service to:

- Violate any applicable law or regulation, or induce or assist anyone else to do so.
- Store, share, or manage credentials, keys, or data that you obtained unlawfully or are not authorized to hold — including stolen credentials, credential dumps, or access tokens for accounts and systems that are not yours or that you are not authorized to access.
- Store or share material that is illegal for you to possess or distribute, including child sexual abuse material, in any form (including as attachments or encrypted content).
- Infringe others' intellectual property, privacy, or publicity rights.
- Evade a sanctions program or export control restriction.

2. No Attacks on the Service

You may not:

- Probe, scan, or test the vulnerability of the Service, or breach or circumvent its authentication or security controls, except through our coordinated disclosure process (Section 6).
- Access or attempt to access another user's account, vault, session, or organization without their authorization.
- Interfere with the Service's operation — including denial-of-service attacks, resource flooding, rate-limit evasion, or introducing malware into the Service.
- Circumvent plan limits, seat limits, billing controls, or client-side enforcement (for example, tampering with entitlement checks).
- Reverse engineer, decompile, or disassemble the Service except to the extent a law expressly permits it despite this restriction.

- Resell, rent, sublicense, or operate the Service for third parties as a service bureau without a written agreement with us.

3. No Abuse of Sharing, Invitations, or Messaging

You may not use item sharing, organization invitations, emails generated by the Service, or any other Service-generated communication to:

- Send spam or unsolicited bulk invitations.
- Conduct phishing, social engineering, or impersonation (including impersonating Secure Passwords staff).
- Distribute malware, malicious links, or fraudulent content.

4. Automation API and Client Rules

- Use the automation API only with tokens issued for your own account, within your granted scopes and published rate limits.
- Do not share personal access tokens, embed them in public code or client-side applications, or use automation to harvest data or degrade the Service for others.
- Automated traffic that materially degrades the Service may be throttled or blocked without notice.

5. AI Features

You may not use AI-assisted features to generate or attempt to generate content for phishing, malware, harassment, or other unlawful or abusive purposes, or attempt to extract other users' data, system prompts, or service credentials from the AI assistant. Do not submit other people's personal data to the AI assistant without a lawful basis.

6. Security Research and Coordinated Disclosure

We welcome good-faith security research. If you believe you have found a vulnerability:

- Report it to security@securepasswords.com and give us a reasonable opportunity to remediate before public disclosure.
- Do not access, modify, or destroy other users' data; use only accounts you own for testing; and do not degrade the Service.

Good-faith research conducted within these rules is authorized and is not a violation of this AUP.

7. Enforcement

- We may investigate suspected violations using service metadata, logs, and reports (we cannot and do not inspect encrypted vault contents), and may throttle, suspend, or terminate accounts, tokens, organizations, or sharing capabilities involved in violations, as described in the Terms of Service.
- Where practicable and lawful, we will notify you and give you a chance to remedy a violation before suspension or termination. Serious violations — including attacks on the Service, unlawful content, or fraud — may result in immediate action and, where appropriate, referral to law enforcement.
- We may update this AUP as described in the Terms of Service.

8. Reporting Abuse

To report a violation of this policy, contact abuse@securepasswords.com. To report a security vulnerability, contact security@securepasswords.com.