ETERNAKEYS LEGAL

Terms of Service

Version 1.1 · Effective 2026-04-14

Open PDF | Download PDF | Preview in page

1. Acceptance of Terms
By creating an account or using the EternaKeys service ("Service"), you agree to be bound by these Terms of Service ("Terms"). If you do not agree, do not use the Service.
2. Service Description
EternaKeys provides a zero-knowledge encrypted digital legacy vault. Vault content is encrypted on your device before transmission to our servers. We store only ciphertext and operational metadata necessary for the service to function (such as item types, sizes, timestamps, and account information).
3. User Responsibilities
You are solely responsible for maintaining the security of your authentication credentials (passkeys and/or hardware keys) and vault passphrase.
You must provide accurate account information.
You are responsible for all activity under your account.
You must not use the Service for any unlawful purpose or in violation of the Acceptable Use Policy.
4. Zero-Knowledge Architecture and Credential Risk
EternaKeys is designed such that encryption credentials are controlled by you, not the platform.
Account access depends on your registered passkeys (hardware keys or platform authenticators). If all registered passkeys are lost and no backup passkey is available, account access cannot be restored.
Vault data access depends on your vault passphrase, which never leaves your device. **If your vault passphrase is lost, encrypted vault data is permanently and irreversibly inaccessible** — no one, including EternaKeys, can decrypt it.
Heir access is governed by the Authorized Access Trigger (AAT) workflow and does not bypass vault encryption. Heirs must independently possess the vault passphrase to decrypt

released content.

5. Heirs Access and Authorized Access Triggers

The Service provides an Authorized Access Trigger (AAT) workflow through which designated heirs may request access to vault contents. This process includes identity verification, notification to the account owner, a configurable veto window, and administrative review. EternaKeys does not guarantee that heirs will successfully complete this process.

6. Payment and Subscription

Paid plans are billed annually. You may cancel at any time. Upon cancellation, access continues through the end of the billing period. After the retention window, encrypted data is permanently deleted. Since only you hold decryption keys, server-side deletion is final.

7. Intellectual Property

The Service, including its design, features, and technology, is owned by EternaKeys Inc. You retain all rights to your encrypted content. We claim no ownership over your data.

8. Limitation of Liability

To the maximum extent permitted by law, EternaKeys shall not be liable for any indirect, incidental, special, consequential, or punitive damages, including loss of data resulting from credential loss. No security system can guarantee absolute protection.

9. Disclaimer of Warranties

The Service is provided "as is" without warranties of any kind, express or implied. We do not warrant uninterrupted or error-free operation.

10. Changes to Terms

We may update these Terms from time to time. Material changes will be communicated via email or in-app notice. Continued use after changes constitutes acceptance.

11. Governing Law

These Terms shall be governed by and construed in accordance with the laws of the State of Delaware, without regard to conflict of law principles.

12. Contact

For questions about these Terms, contact us at legal@eternakeys.com.