

Privacy Policy

Version 1.1 · Effective 2026-04-14

[Open PDF](#)[Download PDF](#)[Preview in page](#)

1. Overview

EternaKeys ("we", "us", "our") is committed to protecting your privacy. This Privacy Policy explains what data we collect, how we use it, and your rights regarding that data.

2. Zero-Knowledge Architecture

Your vault content is encrypted on your device before transmission using AES-256-GCM with keys derived from your passphrase via Argon2id. We never receive, store, or have access to your plaintext vault content or vault passphrase.

3. Data We Collect

3.1 Account Information

Email address (for authentication and notifications)

Legal name (optional, for heir documentation)

Passkey credential identifiers (WebAuthn public keys, for authentication)

Hashed account password (stored only for administrative accounts, not standard user accounts)

3.2 Operational Metadata

To provide the service, we store operational metadata including:

Vault item types, sizes, and timestamps

Heir designation records

Session and authentication data (IP addresses, user agents)

Audit log entries (event types, timestamps — never vault content)

Assent records (legal acknowledgments with timestamps)

3.3 Encrypted Data

We store encrypted vault data (ciphertext) that we cannot decrypt. This includes encrypted item content, encrypted titles, and encrypted file attachments.

4. How We Use Your Data

To provide, maintain, and improve the Service

To authenticate your identity



EternaKeys

Sign in

Get started

To integrate the Authorized Access Trigger workflow for designated help

To send transactional notifications (security alerts, heir access requests)

To comply with legal obligations

5. Data Sharing

We do not sell your personal data. We may share data with:

Infrastructure providers (hosting, email delivery) under data processing agreements

Law enforcement when required by valid legal process (note: we can only provide ciphertext and metadata, not plaintext vault content)

6. Data Retention

Active account data is retained while your account is active. Upon cancellation, encrypted data is retained for 30 days before permanent deletion. Audit logs may be retained longer for security and compliance purposes.

7. Your Rights

You may:

Access your account information

Export your encrypted vault data at any time

Request account deletion

Update your account information

8. Cookies

We use essential cookies for authentication (session tokens). We do not use tracking cookies or third-party analytics cookies. See our cookie consent notice for details.

9. Security

We employ industry-standard security measures including TLS encryption in transit, server-side rate limiting, CSRF protection, and strict Content Security Policy headers. Vault content is protected by client-side encryption that we cannot bypass.

10. Children's Privacy

The Service is not directed to individuals under 18. We do not knowingly collect personal information from children.

11. Changes to This Policy

We may update this Privacy Policy from time to time. Material changes will be communicated via email or in-app notice.

12. Contact

For privacy inquiries, contact us at privacy@eternakeys.com.