

PRIVACY POLICY

Hypervault — Offline Password Manager & Air-Gapped Wallet

Effective date: July 7, 2026

1. Introduction

This Privacy Policy describes how the Hypervault mobile application (“Hypervault”, “the App”, “we”) handles your information. Hypervault is an offline password manager and air-gapped cryptocurrency wallet for Android, developed by ITS Development.

The short version: Hypervault is designed so that we cannot collect your data. The App has no user accounts, no analytics, no advertising, and — in its standard edition — no network access of any kind.

2. Data We Collect

We do not collect, transmit, sell, or share any personal data.

- No account or registration is required or possible.
- The App contains no analytics or tracking SDKs and shows no advertising.
- The standard edition of the App does not request the INTERNET permission. At the operating-system level it is technically incapable of sending any data off your device.
- We operate no servers that receive user data. Everything the App does happens locally on your device.

3. Data Stored on Your Device

All content you create in Hypervault — passwords, logins, secure notes, one-time password (TOTP) secrets, file attachments, and cryptocurrency wallet keys — is stored exclusively on your device in an encrypted vault file.

- The vault is encrypted with AES-256-GCM. The encryption key is derived from your master password and a device-held Secret Key using Argon2id and HKDF-SHA-256 (a zero-knowledge design).
- We never see, receive, or store your master password, your Secret Key, or any vault contents, and we have no technical means to access or recover them.
- If you forget your master password or lose your Secret Key, we cannot restore your data.

4. Android Permissions Used

Camera (android.permission.CAMERA). Used solely to scan QR codes — for example, TOTP setup codes, Secret Key transfer codes, and transaction-signing requests for the air-gapped wallet. Camera frames are processed locally on the device and are never stored or transmitted. The camera is optional: the App functions without it.

Biometrics (android.permission.USE_BIOMETRIC). Used to let you unlock the App with a fingerprint or face recognition instead of typing your master password. Biometric data is handled entirely by the Android operating system and its hardware-backed keystore; the App never sees, stores, or transmits your biometric data.

Network (android.permission.INTERNET). Not present in the standard edition. See Section 5 for the only exception.

5. Crash Reporting (Special Edition Only)

A separately distributed edition of the App includes crash reporting via Firebase Crashlytics (a Google service) and, for that sole purpose, requests the INTERNET permission. If — and only if — you have installed that edition:

- When the App crashes, a technical crash report is sent to Firebase Crashlytics. It may include the device model, operating system version, App version, and a stack trace of the failure.
- Crash reports never include vault contents, your master password, your Secret Key, or any other secrets.
- Crashlytics processing is governed by Google’s privacy documentation at <https://firebase.google.com/support/privacy>.

If your App build does not request network access (verifiable in Android settings under App info → Permissions), this section does not apply to you.

6. Backups and Data Transfer

The App opts out of Android’s automatic cloud backup (allowBackup is disabled), so your vault is not uploaded to Google backups. Any export, transfer, or backup of your vault happens only when you explicitly initiate it, and the exported file remains encrypted. You are in full control of where such exports are stored.

7. Data Sharing with Third Parties

We do not share any data with third parties, because no data ever reaches us. The App contains no third-party SDKs that collect data, with the single exception of Firebase Crashlytics in the special edition described in Section 5.

8. Data Retention and Deletion

All App data lives on your device and remains there for as long as you keep it. To delete all data, delete your vault inside the App, or uninstall the App and clear its storage in Android settings. Because we hold no copies, deletion on your device is complete and irreversible. The App also offers optional security features (such as automatic vault destruction after prolonged inactivity) that you configure yourself.

9. Children’s Privacy

Hypervault does not collect personal data from anyone, including children. The App is a general-audience utility and is not directed at children under 13.

10. Your Rights

Privacy regulations such as the GDPR and CCPA grant rights over personal data that an organization holds about you (access, correction, deletion, portability). We hold no personal data about you, so there is nothing for us to disclose, correct, or delete — your

data never leaves your device. You can nevertheless contact us with any privacy question at the address below.

11. Changes to This Policy

We may update this Privacy Policy from time to time, for example when new App features affect how data is handled. The current version, with its effective date, is always available at the URL published on the App's Google Play listing. Material changes will be noted in the App's release notes.

12. Contact

For any questions about this Privacy Policy or your privacy when using Hypervault:

- Email: dmitriy.palkin@itsdevelopment.ru
- Security reports: see the security policy at <https://github.com/ITSDevelopmentCore/hypervault-crypto/blob/main/SECURITY.md>

The cryptographic core of Hypervault is open source and can be independently reviewed at <https://github.com/ITSDevelopmentCore/hypervault-crypto>.