EchoVaults v2.0 – Transparency Statement on Security & Encryption

Prepared by Ssu-Technology Ltd. – July 2025
Compiled by: EchoVaults Contributors

Our Philosophy: Privacy First. Always.

EchoVaults was born from a single, unwavering belief: *some memories, secrets, and instructions are too personal to trust anyone or anything else with*—not a cloud, not a third party, not even us.

Version 2.0 builds on that principle. It's not just another release; it's a result of listening to users, critics, and ethical security reviewers who all asked the same question: *How safe is safe enough for something this private?*

We've taken those concerns seriously—while staying loyal to what EchoVaults stands for:

- No online sync.
- No cloud backup.
- No external server communication.
- No hidden surveillance SDKs or trackers.
- Everything stays offline and on your device.
- If your device can't unlock, EchoVaults can't be opened.

Independent Review & Response Table

Finding	Our Response	Outcome
Basic AES encryption with low entropy	Migrated to AES-256 GCM with PBKDF2 + unique salt and high iteration count	Significantly stronger brute-force resistance
Image and file data not strongly encrypted	Implemented local-only encoding & obfuscation for media	Balanced performance with moderate passive protection
Biometric login not supported	Intentionally excluded to prevent low-friction access to vaults	Maintains strong privacy separation from phone unlocks
Brute-force if attacker has physical access	Multi-layered access: device unlock + vault password + KDF iterations	Realistically infeasible even with device in hand

Multiple Layers of Protection

Security isn't just about math—it's about the journey an attacker would need to take to compromise your data. EchoVaults provides **layered protection**, each with its own wall:

1. **Device-Level Barrier**
   Before anything, an attacker would need to unlock your phone. On iPhones and most Android devices, that alone has a >90% failure rate in real-world theft cases. EchoVaults runs atop the **native Full Disk Encryption (FDE)** built into your device: iPhones use **Apple's Secure Enclave** with AES-256 hardware encryption, while modern Android phones use **File-Based Encryption (FBE)**. These systems bind encryption keys to your passcode or biometrics, making unauthorized access virtually impossible without unlocking the phone first. In most real-world thefts, this is where attackers fail.

   EchoVaults does not run in the background, has no cloud connection, and does not sync any data online.

2. **Master Password**
   Even after unlocking your phone, access to the vault still requires a unique password created by the user. There is no recovery link. No admin override. If you don't know it, you're out. We can't help you recover it even if we are compelled to do so, since there is no account or server that collect personally identifiable information from users.

3. **Strong Encryption**
   EchoVaults uses **AES-256 GCM** for all sensitive data, along with **PBKDF2 key derivation** using high iteration counts and unique salts. This means even if someone gains access to your device and app files, they will have to brute-force the vault—something that would take years without the password.

4. **Media Handling with Consideration**
   Encrypting media fully at this time introduces performance instability on lower-end devices. That's why media files are obfuscated and encoded locally, not encrypted using heavy ciphers. This preserves usability for thousands of users while keeping your content offline, invisible to gallery apps, and unreadable without the app.

5. **No Remote Attack Surface**
   No servers. No cloud login. No syncing. EchoVaults creates no connection with the outside world. There's nothing to intercept, nothing to sniff, nothing to exploit remotely.

Why Not Encrypt Media Fully Yet?

Encrypting large media files (>50MB) with AES creates significant risk of app crashes and poor performance on mid-range or older devices. Attempting this without chunked buffering can result in out-of-memory errors.

While it's *technically* possible to implement chunked file encryption/decryption using techniques like:

- Buffered `RandomAccessFile` streaming
- Dart's `ChunkedConversionSink`
- On-disk temp file encryption

...these significantly complicate development and create longer load times for users. EchoVaults is, and will remain, a human-first app. For now, we obfuscate and encode media in a way that provides modest protection with **no performance hit**.

What We Promise

- We will **never** upload your vault to the cloud.
- We will **never** store your password or any identifying data, this is not even possible by design.
- We will **never** weaken our encryption just to make the app “easier.”
- We will **always** prioritize user experience and thoughtful security over reactionary engineering.

Is It Unbreakable?

No software encryption system is. But EchoVaults isn't trying to be a blacksite vault—it’s trying to be a reliable, humane, secure notebook for moments that matter.

Between the **offline-only model**, the **multi-layered barriers**, and the **absence of any remote threat surface**, EchoVaults is safer than most password managers, chat apps, and online vaults you use today.

The Road Ahead

In future versions, we plan to:

- Introduce **optional Media Encryption Mode** with file chunking
- Add **per-vault encryption options** for advanced users
- Offer **selective biometric fallback** (for those who want it)
- Continuously engage with the security community to refine and evolve our model

But every change will always answer one question first:

"Will this make the experience worse for someone who just wants to leave a message for someone they love?"

If yes, we won't ship it.

Summary

EchoVaults exists for a very narrow, very personal purpose. It is a digital secret drawer. We've done the hard engineering to ensure that drawer can stay locked from everyone—even us.

What you put inside is yours. What you choose to encrypt is yours. And whether you open it today, in ten years, or never... is yours.

We'll keep making it better.

Thank you for trusting EchoVaults, and collectively, we will continue to make better.

Transparency Report v.2.0

Akinola Abdulakeem
Founder EchoVaults
CEO Ssu-Technology Limited
Lagos, Nigeria.
Wed – 16th Jul 2025