🔎 DocLockBox — Secure Document Vault: Product and Security Overview

Version: 1.0
Date: April 2025

---

1. Product Vision

DocLockBox is a next-generation secure vault designed to protect your most sensitive documents. Built with multiple layers of advanced encryption and a local-first storage philosophy, DocLockBox ensures that your data stays private, protected, and accessible only by you.

DocLockBox isn't just about storing files — it's about empowering users with the freedom to control, organize, and selectively share their digital life, while maintaining uncompromised security.

Tagline: *Your Documents. Your Control.*

---

2. Core Features

🔒 Multi-Layered Encryption Architecture

- **AES-256 Encryption Per File**: Every document is encrypted individually with AES-256, the gold standard for securing classified data.
- **Per-File Unique Keys**: Each file is protected by its own randomly generated encryption key, eliminating the risk of key reuse or cascading breaches.
- **Passphrase-Based Master Key**: Users create a personal passphrase that is hardened using PBKDF2 (Password-Based Key Derivation Function 2) with a high iteration count to resist brute-force attacks.
- **Key Wrapping**: Each file's unique encryption key is itself encrypted by a master key derived from the user's passphrase, adding an extra layer of protection.

- **On-Demand Passphrase Change and Key Rotation**: Users can change their passphrase at any time, triggering a secure rotation of all associated encryption keys without exposing original document contents.

🔍 Intelligent Local Search

- **Secure Keyword Indexing**: When uploading a document, users must select one or more keywords associated with the file. This enables efficient local search based on file metadata.
- **Encrypted Metadata Storage**: Keywords and filenames are encrypted separately, ensuring privacy.
- **On-Device Search Engine**: All search operations are performed locally. No keyword, document name, or content ever leaves the device.

📲 Local-First Storage Philosophy

- All documents and metadata are stored encrypted on the user's device.
- DocLockBox does **not sync or upload files** to any cloud service by default, maintaining absolute user sovereignty over their data.

🔄 Future-Ready Secure Sharing (Coming Soon)

- **Secure Device Sync**: Users will be able to export and import their entire DocLockBox to trusted devices securely, using encrypted transfer protocols.
- **Time-Limited Document Sharing**: Users will be able to grant **temporary, encrypted access** to specific documents to selected recipients identified via email.
- **Granular Access Control**: Share access with expiration times, revocation capability, and view-only options.
- **AI-based Question and Answer on the stored documents**

---

3. Security Architecture Details

🌍 Encryption Workflow

1. **Upload Document**:
    - User selects a document.
    - User must assign one or more keywords for searchability.
2. **Key Generation**:

    - A new **random 256-bit AES key** is generated for this document.
    - User's master key (derived from their passphrase via PBKDF2) encrypts this AES key (key wrapping).
3. **Storage**:
    - The document is encrypted with the AES key.
    - Keywords and filenames are encrypted separately.
    - All encrypted blobs are stored locally.
4. **Search**:
    - User's local device decrypts the encrypted keyword index and matches against query terms.
    - Files matching keywords or filenames are surfaced securely and efficiently.

---

4. Privacy Policy Commitments

- DocLockBox **does not collect** user documents, keywords, passphrases, or any personal content.
- DocLockBox **operates entirely offline** by default.
- No telemetry, no analytics, no hidden data collection.
- Future optional sharing features will be **opt-in**, **end-to-end encrypted**, and **user-controlled**.

---

5. User Experience

Seamless and Secure

- Clean, intuitive interface designed with Flutter for cross-platform elegance.
- Minimalist design focusing on security, ease of use, and accessibility.

Fail-Safe Mechanisms

- **Auto-Lock** after inactivity.
- **Biometric Unlock Toggle**: Users can enable or disable biometric authentication (Touch ID, Face ID) for unlocking DocLockBox at any time from within the app settings.

- **On-Demand Passphrase Update**: Users can change their passphrase securely with automatic re-encryption of all keys.
- **Auto-Expire Temporary Files**: Decrypted temporary files are automatically cleaned up after a session.

---

6. Why DocLockBox Matters

In an era where data privacy is increasingly under threat, DocLockBox offers a new standard of trust and sovereignty. We believe your documents belong to you — and no one else.

No compromise. No shortcuts. Just true security.

Welcome to DocLockBox.

📜 Document Metadata

- **App Name**: DocLockBox
- **Platform**: macOS, iOS
- **Encryption**: AES-256 (per-file), PBKDF2 hardened passphrase, key wrapping, on-demand key rotation
- **Storage**: Local-only (default), optional secure sharing in future
- **Core Technologies**: Dart, Flutter, SQLite (encrypted), platform native secure storage

---

✨ End of Document