**New Password**

| State # | User | Settings | Encryptor |
| --- | --- | --- | --- |
| 1 | User enters a password |  |  |
| 2 |  |  | Validate the password |
| 3 |  |  | Argon 2id Hash Password |
|  |  |  | Generate PBKDF2 key from password |
| 4 |  |  | Generate Encryption Key |
| 5 |  |  | Generate Encryption IV |
| 6 |  |  | Encrypt Key & IV with PBKDF2 key |
| 7 |  |  | Secure Erase Password, PBKDF2 Key |
| 8 |  | Save Password Hashes & Encrypted key & iv |  |
| 9 |  |  | Generate 5 word recovery phrase |
| 10 |  |  | Argon2id Hash the phrase |
| 11 |  |  | PBKDF2 generate key from phrase |
| 12 |  |  | Encrypt KEy & IV with PBKDF2 key |
| 13 |  | Save Phrase Hash & Encrypted Key & IV |  |

**Password Reset**

| State # | User | Dashboard | Encryptor |
| --- | --- | --- | --- |
| 1 | User selects ‘Reset Password’ |  |  |
| 2 |  | Request Recovery Phrase |  |
| 3 |  |  | Argon 2id hash from input |
| 4 |  |  | Compare to saved phrase hash |
| 5 |  |  | PBKDF2 key from phrase |
| 6 |  |  | Use key to decrypt Encryption Key & IV |
| 7 |  |  | Decrypt Database |
| 8 |  |  | Secure Erase Hashes, Old Cipher Key & IV |
| 9 |  | Prompt new Password |  |
| 10 | User supplies new password |  |  |
| 11 |  |  | Proceed from step 2 of #New Password |

**Encryption of files**

| State # | User | Encryptor | Database |
| --- | --- | --- | --- |
| 1 | Generates Journal Entries |  |  |
| 2 | Selects Save |  |  |
| 3 |  | Create cipher text using Key and IV from memory. |  |
| 4 |  |  | Store cipher text in appropriate collumn |