SecureVault – Zero■Knowledge Password & Data Vault Complete Project Specification

1. Project Overview

SecureVault is a production■grade, zero■knowledge password and sensitive data vault designed to securely store user secrets such as passwords, notes, cards, API keys, and files. All encryption and decryption occur strictly on the client side, ensuring the server never has access to plaintext data or encryption keys.

2. Architecture & Security Model

SecureVault follows a Zero■Knowledge Architecture: • Client■side encryption using AES■256■GCM • Key derivation via PBKDF2 or Argon2 • Unique salt and IV per user and per vault item • Master password never stored or transmitted • Server stores encrypted blobs only

3. Core Features

Authentication: • Email & password login/signup • Password strength meter • Brute■force protection • Auto■lock & session timeout Vault: • Add, edit, delete vault items • Categories & tags • Search & filtering • Clipboard auto■wipe • Password generator • Password health analysis

4. Encryption Workflow

1. User enters master password 2. Client derives encryption key using PBKDF2/Argon2 3. Vault data encrypted locally 4. Encrypted data sent to backend 5. Backend stores ciphertext only 6. Decryption happens locally on access

5. Database (Supabase PostgreSQL)

Tables: users(id, email, password_hash, created_at) vault_items(id, user_id, item_type, encrypted_data, iv, created_at, updated_at) files(id, user_id, encrypted_blob, iv, metadata)

6. API Design

Auth: POST /api/auth/register POST /api/auth/login POST /api/auth/logout Vault: GET /api/vault POST /api/vault PUT /api/vault/:id DELETE /api/vault/:id

7. Browser Extension Support

• Chrome/Firefox extension • Secure password autofill • Encrypted vault sync • Uses same zero■knowledge crypto layer • Clipboard protection & domain matching

8. Mobile App (React Native)

• Cross■platform (Android & iOS) • Biometric unlock (Face ID / Fingerprint) • Secure local storage (Keychain / Keystore) • Offline access with encrypted cache

9. Biometric Unlock

• WebAuthn for browsers • Device biometrics on mobile • Unlocks locally stored encryption key • Never replaces master password

10. Encrypted File Storage

• Client■side encrypted file uploads • AES■256 encryption per file • Metadata encrypted • Secure downloads with local decryption

11. Deployment

Frontend: Vercel Backend: Render/Railway Database: Supabase HTTPS enforced Secrets via environment variables only

12. Conclusion

SecureVault is a full■scale, industry■grade security project suitable for production use, portfolio demonstration, and academic submission. It demonstrates strong knowledge of cryptography, web security, system design, and modern full■stack development.