**SOFTWARE REQUIREMENTS SPECIFICATION**

**for**

**PASSWORD MANAGEMENT AND SECURITY**

**PREPARED BY**

SUDARSANAA MATHAN(23CSR217)

SANTHEESH S (23CSR193)

THARANEESH RAJAN N (23CSR227)

KONGU ENGINEERING COLLEGE

27

**Table of Contents**

**Table of Contents ........................................................................................................................... ii  
Revision History ........................................................................................................................... ii**

**1. Introduction**

1.1 Purpose ............................................................................................................................. 1  
1.2 Scope ................................................................................................................................. 1  
1.3 Definitions, Acronyms, and Abbreviations ...................................................................... 1  
1.4 References ......................................................................................................................... 1  
1.5 Overview ............................................................................................................................ 1

**2. Overall Description**

2.1 Product Perspective .......................................................................................................... 2  
2.2 Product Functions ............................................................................................................ 2  
2.3 User Characteristics ......................................................................................................... 2  
2.4 Constraints ........................................................................................................................ 2

**3. Specific Requirements**

3.1 User Authentication ......................................................................................................... 3  
3.2 Password Management ........................................................................................................ 3  
3.3 Security Features .................................................................................................. 3  
3.4 Data Storage ......................................................................................................... 3

**4. System Design & Architecture**

4.1 Tech Stack ........................................................................................................................ 3  
4.2 System Architecture ........................................................................................................ 3

5. Future Enhancements …............................................................................................ 4

6.Conclusion…………………………………………………………………………………………………………………4

**1. Introduction**

**1.1 Purpose**

The Password Manager System is designed to help users securely store, manage, and retrieve their passwords. It provides a secure, user-friendly platform to manage login credentials for various websites and applications.

This document is intended for developers, project managers, stakeholders, and testers to provide a clear understanding of system requirements and design.

**1.2 Scope**

The system will offer:

* **User Authentication**: Secure login and signup
* **Password Storage**: Encrypted storage for login credentials
* **Password Retrieval**: Secure access with a master password
* **Auto-Logout**: Session expiration for enhanced security
* **Cross-Platform Access**: Accessible on web browsers.

The system will be built using modern web technologies and will be scalable for future enhancements.

**1.3 Definitions, Acronyms, and Abbreviations**

* **MFA**: Multi-Factor Authentication
* **AES**: Advanced Encryption Standard
* **JWT**: JSON Web Token (for authentication)
* **UI**: User Interface

**1.4 References**

* <https://www.lastpass.com/password-manager>
* [**https://bitwarden.com/**](https://bitwarden.com/)

**1.5 Overview**

This document is structured as follows:

* Section 2: Provides the product perspective, key features, user roles, and constraints affecting development.
* Section 3: Lists the core functional requirements
* Section 4: Describes the technology stack, encryption protocols, and system structure
* Section 5: Future enhancements and scalability options.

**2. Overall Description**

**2.1 Product Perspective**

* The system is a **web-based password manager** that securely stores user credentials **locally or in an encrypted database**.
* **Frontend**: A user-friendly web interface for users.
* **Backend**: Handles authentication, business logic, and password management.

**2.2 Product Functions**

The system will include the following functionalities:

1. **User Authentication**
   * Secure registration and login.
   * Login using master password.
2. **Password Storage and Management:**
   * Save, edit, delete passwords securely.
3. **Encryption**:
   * AES-256 encryption for password storage.
4. **Auto-Logout**:
   * Users are logged out after inactivity.
5. **Cross-Device Syncing**:
   * Passwords accessible across devices.
   * Track stock levels of medicines and medical equipment.
   * Automated alerts for low-stock items.

**2.3 User Characteristics**

* **Regular Users**: Store and manage personal passwords.
* **Administrators**: Manage user accounts

**2.4 Constraints**

* **Security Compliance**: Must adhere to **OWASP security standards**.
* **Offline Mode**: Passwords should be retrievable without an internet connection

**3. Specific Requirements**

**3.1 User Authentication**

* Users must sign up with a valid email and master password.
* Multi-Factor Authentication (MFA) can be added as an extra security layer.
* JWT-based authentication for secure login sessions.

**3.2 Password Management**

* Users can **store, edit, delete, and retrieve** passwords.
* Passwords are **automatically encrypted** before storage.
* A **password generator** provides strong, unique passwords.

**3.3 Security Features**

* AES-256 Encryption: Ensures passwords are stored securely.
* Master Password Verification: Users must enter their master password to access stored credentials.
* Auto Logout: User session expires after a defined period.

**3.4 Data Storage**

* Local Storage (Client-Side) or Database Storage (Server-Side) options available.
* Secure hashing of master password before storage**.**

**4. System Design & Architecture**

**4.1 Tech Stack**

* **Frontend:** HTML, CSS, JavaScript
* **Backend Node.js** with Express.js
* **Database (Optional):** MongoDB / IndexedDB (for encrypted storage)
* **Encryption:** AES-256 for password storage, bcrypt for authentication.

**4.2 System Architecture**

1. **Frontend UI**: User interacts with a simple web-based UI.
2. **Local Storage or Database**: Encrypted passwords are stored securely.
3. **Authentication System**: Verifies master password before granting access

**5. Future Enhancements**

* **Biometric Authentication** (Fingerprint/Face Unlock)
* **Cloud Syncing** for multi-device access
* **Dark Web Monitoring** to alert users of compromised credentials
* **Emergency Access Feature** to grant access to trusted contacts

**3.6 Conclusion**

This document provides a detailed Software Requirements Specification (SRS) for the Password Manager System, ensuring it is secure, scalable, and user-friendly.