## Functional Requirements

### Save Different Login Details

Users should have the ability to save different login details aside from the traditional email and password. They should have the ability to store dates, pins and more for ease of access.

### Account Types

This feature allows users to create different account types within the password manager, such as personal and family accounts. With a family account, members can share saved passwords among authorized family members***.***

### Search and Filter

Users should have the ability to search for specific login details or apply filters to quickly locate desired accounts among their saved information.

## Non-Functional Requirements

### Secure/Lock Passwords

The password manager should provide mechanisms to securely store and lock passwords, preventing unauthorized access to sensitive information.

### 256-AES Encryption

Utilizing 256-bit Advanced Encryption Standard (AES) encryption ensures that stored data is highly secure and protected against unauthorized access or data breaches.

### Secure Login

This feature addresses the inadequacies of the previous login system by enhancing security measures. The goal is to significantly improve upon the previous login system, ensuring that user authentication processes are robust, resilient, and capable of effectively safeguarding sensitive information from unauthorized access.

### Move MasterVault Online

Transitioning the MasterVaultonline ensures accessibility from anywhere with an internet connection, improving convenience for users.

### Paraphrase Generator

This feature generates complex and unique paraphrases based on a keyword provided by the user, which can be used as strong passwords for their accounts, enhancing security by creating passwords that are difficult to guess or crack through brute-force attacks.