Software Requirements Specification

Gmail Account Login

1. Introduction

1.1 Purpose

The purpose of this document is to provide a detailed description of the software requirements for the Gmail Account Login system. This system will allow users to log in to their Gmail accounts securely.

1.2 Scope

The Gmail Account Login system covers the authentication and security aspects of user access to Gmail accounts. It does not cover the entire Gmail service.

2. System Overview

2.1 System Description

The Gmail Account Login system provides a secure and reliable authentication mechanism for users to access their Gmail accounts. Users must provide valid credentials to gain access.

3. Functional Requirements

3.1 User Authentication

3.1.1 Login

The system shall provide a login page where users can enter their email address and password.

Users must enter a valid email address and password to proceed.

Passwords must be securely hashed and stored in the database.

Passwords shall be encrypted during transmission to the server.

3.1.2 Forgot Password

Users shall have the option to reset their password if they forget it.

A password reset link will be sent to the user's registered email address.

Users can create a new password via the password reset link.

3.1.3 Multi-Factor Authentication (MFA)

Users shall have the option to enable MFA for added security.

MFA methods may include SMS, email verification codes, or authentication apps.

3.2 Session Management

3.2.1 Session Timeout

User sessions shall expire after a specified period of inactivity (e.g., 15 minutes).

Users will be prompted to re-enter their credentials after session expiration.

3.2.2 Logout

Users shall be able to log out of their Gmail account.

Logging out should terminate the user's session.

3.3 Security

3.3.1 Account Lockout

Implement account lockout mechanisms to prevent brute-force attacks.

After a specified number of unsuccessful login attempts, the account shall be locked temporarily.

3.3.2 Password Complexity

Enforce password complexity rules (e.g., minimum length, use of special characters).

Users shall be guided on creating strong passwords.

4. Non-Functional Requirements

4.1 Performance

The system shall support a large number of concurrent login requests.

Login response times shall be below 2 seconds.

4.2 Security

User passwords shall be securely stored using industry-standard encryption algorithms.

The system shall implement security best practices to protect against common web vulnerabilities (e.g., XSS, CSRF).

4.3 Availability

The system shall be available 24/7, with scheduled maintenance windows communicated in advance.

5. User Interface

The user interface shall be user-friendly, responsive, and accessible.

6. Legal and Compliance

The system shall comply with all applicable data protection and privacy laws (e.g., GDPR).

7. References

List any external documents or standards referenced in this SRS.

8. Appendices

Include any additional information or diagrams that clarify the requirements.

This SRS provides a comprehensive overview of the software requirements for the Gmail Account Login system. It should serve as a basis for the design, development, and testing of the login functionality.