Requirements Document

Introduction

This document specifies the requirements for a user authentication system that provides secure login, logout, and password reset functionality. The system enables users to securely access protected resources while maintaining account security through proper credential management and recovery mechanisms.

Glossary

- **Authentication System**: The software component responsible for verifying user identity and managing access credentials
- **User**: An individual who has registered an account and seeks to access protected system resources
- **Session**: A temporary authenticated state that persists user login status across requests
- **Credentials**: Username/email and password combination used for user identification and verification
- **Password Reset Token**: A temporary, unique identifier used to authorize password changes during recovery
- **Protected Resource**: Any system functionality that requires user authentication to access

Requirements

Requirement 1

User Story: As a new user, I want to register for an account with email and password, so that I can access protected system features.

Acceptance Criteria

1. WHEN a user provides a valid email address and secure password THEN the Authentication System SHALL create a new user account and store encrypted credentials
2. WHEN a user attempts registration with an already registered email THEN the Authentication System SHALL prevent duplicate account creation and notify the user
3. WHEN a user provides an invalid email format THEN the Authentication System SHALL reject the registration and display appropriate validation messages
4. WHEN a user provides a password that does not meet security requirements THEN the Authentication System SHALL reject the registration and specify password criteria
5. WHEN account creation succeeds THEN the Authentication System SHALL send a confirmation email to verify the email address

Requirement 2

User Story: As a registered user, I want to log into my account using my credentials, so that I can access my personalized content and features.

Acceptance Criteria

1. WHEN a user provides valid credentials THEN the Authentication System SHALL create an authenticated session and grant access to protected resources
2. WHEN a user provides invalid credentials THEN the Authentication System SHALL deny access and display an appropriate error message
3. WHEN a user attempts login with an unverified email THEN the Authentication System SHALL prevent login and prompt for email verification
4. WHEN a successful login occurs THEN the Authentication System SHALL record the login timestamp and update last access information
5. WHEN multiple failed login attempts occur from the same account THEN the Authentication System SHALL temporarily lock the account to prevent brute force attacks

Requirement 3

User Story: As an authenticated user, I want to log out of my account, so that I can secure my session when finished using the system.

Acceptance Criteria

1. WHEN a user initiates logout THEN the Authentication System SHALL invalidate the current session and remove authentication tokens
2. WHEN logout completes THEN the Authentication System SHALL redirect the user to a public page and clear all session data
3. WHEN a user attempts to access protected resources after logout THEN the Authentication System SHALL deny access and prompt for re-authentication
4. WHEN logout occurs THEN the Authentication System SHALL record the logout timestamp for security auditing

Requirement 4

User Story: As a user who forgot my password, I want to reset my password using my email address, so that I can regain access to my account.

Acceptance Criteria

1. WHEN a user requests password reset with a registered email THEN the Authentication System SHALL generate a secure reset token and send it via email
2. WHEN a user requests password reset with an unregistered email THEN the Authentication System SHALL not reveal whether the email exists but SHALL complete the process silently
3. WHEN a user clicks a valid reset link THEN the Authentication System SHALL present a secure form to enter a new password
4. WHEN a user submits a new password via reset token THEN the Authentication System SHALL update the password and invalidate the reset token
5. WHEN a reset token expires or is used THEN the Authentication System SHALL reject subsequent attempts to use the same token

Requirement 5

User Story: As a system administrator, I want user passwords to be securely stored and managed, so that user credentials remain protected even if data is compromised.

Acceptance Criteria

1. WHEN storing user passwords THEN the Authentication System SHALL hash passwords using a cryptographically secure algorithm with salt
2. WHEN comparing passwords during login THEN the Authentication System SHALL use secure comparison methods to prevent timing attacks
3. WHEN generating reset tokens THEN the Authentication System SHALL create cryptographically random tokens with sufficient entropy
4. WHEN handling sensitive operations THEN the Authentication System SHALL implement rate limiting to prevent abuse
5. WHEN processing authentication requests THEN the Authentication System SHALL log security events for monitoring and auditing

Requirement 6

User Story: As a user, I want my session to remain active while I'm using the system, so that I don't have to repeatedly log in during normal usage.

Acceptance Criteria

1. WHEN a user performs actions within the session timeout period THEN the Authentication System SHALL extend the session automatically
2. WHEN a session expires due to inactivity THEN the Authentication System SHALL require re-authentication for protected resources
3. WHEN a user closes their browser THEN the Authentication System SHALL maintain session state if "remember me" was selected
4. WHEN detecting suspicious session activity THEN the Authentication System SHALL invalidate the session and require re-authentication
5. WHEN a user logs in from a new device THEN the Authentication System SHALL optionally notify the user via email for security awareness