**Business Requirement Document (BRD) cho Hệ thống Đăng nhập**

**I. Tổng quan về dự án**

* **Tên dự án**: Hệ thống quản lý đăng nhập người dùng
* **Mô tả**: Hệ thống đăng nhập sẽ cho phép người dùng truy cập vào hệ thống bằng tên đăng nhập và mật khẩu, đồng thời cung cấp xác thực bảo mật để bảo vệ tài khoản.
* **Mục tiêu**: Đảm bảo rằng chỉ những người dùng được xác thực mới có quyền truy cập vào hệ thống.

**II. Phạm vi của dự án**

* Xây dựng hệ thống đăng nhập bảo mật bao gồm các tính năng:
  + Đăng nhập.
  + Đăng ký tài khoản mới.
  + Khôi phục mật khẩu.
  + Đăng xuất.

**III. Các bên liên quan**

* **Người dùng cuối**: Người dùng hệ thống.
* **Quản trị viên hệ thống**: Người quản lý cơ sở dữ liệu người dùng và điều chỉnh quyền truy cập.

**IV. Yêu cầu nghiệp vụ**

1. **Đăng nhập**:
   * Người dùng cần nhập tên đăng nhập và mật khẩu hợp lệ để đăng nhập vào hệ thống.
2. **Khôi phục mật khẩu**:
   * Người dùng có thể yêu cầu hệ thống gửi email để đặt lại mật khẩu khi quên.
3. **Đăng ký**:
   * Người dùng có thể đăng ký tài khoản mới nếu chưa có.
4. **Đăng xuất**:
   * Người dùng có thể đăng xuất khỏi hệ thống sau khi hoàn tất phiên làm việc.
5. **Xác thực đa yếu tố (MFA)** (Yêu cầu mở rộng):
   * Hệ thống cần hỗ trợ xác thực hai lớp để đảm bảo tính bảo mật.

**V. Giả định và Rủi ro**

* **Giả định**: Người dùng phải có một địa chỉ email hợp lệ để khôi phục mật khẩu.
* **Rủi ro**: Các cuộc tấn công bảo mật như brute force, SQL injection có thể xảy ra nếu không thực hiện các biện pháp bảo mật thích hợp.

**2. Software Requirement Specification (SRS) cho Hệ thống Đăng nhập**

**I. Tổng quan hệ thống**

* **Mục tiêu**: Phát triển hệ thống đăng nhập bảo mật cho phép người dùng đăng nhập, đăng xuất, đăng ký và khôi phục mật khẩu.
* **Phạm vi**: Ứng dụng web hỗ trợ tính năng đăng nhập cho nhiều người dùng với các vai trò khác nhau.

**II. Yêu cầu chức năng**

1. **Use Case 1: Đăng nhập**
   * **Mô tả**: Người dùng nhập tên đăng nhập và mật khẩu để truy cập hệ thống.
   * **Actors**: Người dùng.
   * **Dòng sự kiện chính**:
     1. Người dùng nhập tên đăng nhập và mật khẩu.
     2. Hệ thống kiểm tra thông tin.
     3. Nếu thông tin hợp lệ, người dùng được chuyển đến trang chính.
   * **Dòng sự kiện thay thế**:
     1. Nếu thông tin không hợp lệ, hệ thống hiển thị thông báo lỗi.
2. **Use Case 2: Đăng ký tài khoản**
   * **Mô tả**: Người dùng có thể tạo tài khoản mới.
   * **Actors**: Người dùng.
   * **Dòng sự kiện chính**:
     1. Người dùng nhấp vào liên kết "Đăng ký".
     2. Người dùng nhập thông tin (tên, email, mật khẩu).
     3. Hệ thống lưu thông tin người dùng và gửi email xác nhận.
   * **Dòng sự kiện thay thế**:
     1. Nếu email đã tồn tại, hệ thống thông báo lỗi.
3. **Use Case 3: Khôi phục mật khẩu**
   * **Mô tả**: Người dùng có thể yêu cầu đặt lại mật khẩu nếu quên.
   * **Actors**: Người dùng.
   * **Dòng sự kiện chính**:
     1. Người dùng nhấp vào liên kết "Quên mật khẩu".
     2. Người dùng nhập địa chỉ email đã đăng ký.
     3. Hệ thống gửi liên kết đặt lại mật khẩu qua email.
   * **Dòng sự kiện thay thế**:
     1. Nếu email không tồn tại, hệ thống thông báo lỗi.
4. **Use Case 4: Đăng xuất**
   * **Mô tả**: Người dùng có thể thoát khỏi hệ thống sau khi hoàn thành công việc.
   * **Actors**: Người dùng.
   * **Dòng sự kiện chính**:
     1. Người dùng nhấp vào nút "Đăng xuất".
     2. Hệ thống kết thúc phiên làm việc của người dùng và quay lại trang đăng nhập.

**III. Yêu cầu phi chức năng**

* **Bảo mật**:
  + Hệ thống phải hỗ trợ xác thực hai lớp (2FA) để tăng cường bảo mật.
* **Hiệu năng**:
  + Hệ thống phải có khả năng xử lý tối thiểu 500 người dùng đồng thời.
* **Khả năng sử dụng**:
  + Giao diện người dùng phải thân thiện, dễ sử dụng, và có khả năng tương thích trên nhiều thiết bị (máy tính, điện thoại di động).

**IV. Giả định**

* Người dùng cần có kết nối Internet để truy cập vào hệ thống.
* Mật khẩu người dùng sẽ được mã hóa trước khi lưu vào cơ sở dữ liệu.