Version <1.0>

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| <dd/mmm/yy> | <x.x> | <details> | Lâm Quang Duy |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

1. Brief Description 4

2. Basic Flow of Events 4

3. Alternative Flows 4

4. Subflows 4

4.1 Subflow Nhập tên đăng nhập hoặc địa chỉ email: 4

4.2 Subflow Kiểm tra địa chỉ email: 4

4.3 Subflow Nhập mã xác minh: 5

4.4 Subflow Đặt lại mật khẩu: 5

4.5 Subflow Thông báo đặt lại mật khẩu thành công: 5

4.6 Subflow Yêu cầu trợ giúp từ bộ phận hỗ trợ: 5

5. Key Scenarios 5

5.1 Người dùng quên mật khẩu: 5

5.2 Tin nhắn email không đến 5

5.3 Mã xác thực không hợp lệ 5

5.4 Đặt lại mật khẩu không thành công 5

5.5 Sự cố với Cơ sở dữ liệu 5

6. Preconditions 5

7. Postconditions 5

8. Extension Points 6

9. Special Requirements 6

10. Additional Information 6

# Brief Description

Chức năng "Quên mật khẩu" là tính năng trong hệ thống cho phép người dùng khôi phục lại mật khẩu của mình nếu họ quên mật khẩu hoặc không thể đăng nhập vào tài khoản của mình. Chức năng này cung cấp cho người dùng một số lựa chọn để xác minh danh tính và khôi phục lại mật khẩu của mình, bao gồm gửi mã xác minh qua email hoặc số điện thoại, trả lời câu hỏi bảo mật hoặc yêu cầu quản trị viên cấp lại mật khẩu mới. Sau khi xác minh danh tính, người dùng có thể đặt lại mật khẩu mới và truy cập lại tài khoản của mình.

# Basic Flow of Events

* Người dùng đăng nhập vào tài khoản của mình trong ứng dụng.
* Người dùng được thông báo là mật khẩu không chính xác.
* Người dùng vào liên kết “Quên mật khẩu”.
* Hệ thống yêu cầu người dùng cung cấp địa chỉ email hoặc số điện thoại đã đăng ký với tài khoản của họ.
* Người dùng cung cấp thông tin địa chỉ email hoặc số điện thoại và nhấn vào nút "Gửi mã xác minh".
* Hệ thống gửi một mã xác minh đến địa chỉ email của người dùng.
* Người dùng nhập mã xác minh được gửi đến và nhấn vào nút "Tiếp tục".
* Hệ thống xác minh mã xác minh được cung cấp và hiển thị trang đặt lại mật khẩu mới.
* Người dùng đặt lại mật khẩu mới và xác nhận mật khẩu.
* Hệ thống cập nhật mật khẩu mới của người dùng và hiển thị thông báo thành công đến người dùng.
* Người dùng đăng nhập lại bằng tài khoản và mật khẩu mới của mình.

# Alternative Flows

1. Nếu người dùng nhập sai địa chỉ email hoặc số điện thoại đã đăng ký, hệ thống hiển thị thông báo lỗi và yêu cầu người dùng nhập lại địa chỉ email hoặc số điện thoại chính xác.
2. Trong lúc đăng nhập, người dùng sai ngay từ bước nhập địa chỉ email, lúc này hệ thống sẽ báo lỗi địa chỉ email của người dùng có tồn tại trước khi kiểm tra mật khẩu có chính xác hay không.
3. Nếu người dùng không nhận được mã xác minh sau khi yêu cầu, họ có thể yêu cầu gửi lại mã xác minh hoặc liên hệ với bộ phận hỗ trợ để được hỗ trợ.
4. Trường hợp người dùng đã vào liên kết Quên mật khẩu để tạo lại mật khẩu từ địa chỉ email đã đăng kí ứng dụng. Hệ thống sẽ gửi lại mã OTP để người dùng xác nhận danh tính của họ. Tuy nhiên có một số lần là người dùng không thể nhận được mã OTP trong khoảng thời gian quy định. VIệc này có thể được khắc phục khi người dùng có thể dùng tới nút gửi lại mã xác nhận để hệ thống thêm 1 lần nữa gửi lại mã OTP.
5. Nếu người dùng không thể đặt lại mật khẩu mới bằng cách sử dụng phương pháp khôi phục, họ có thể liên hệ với bộ phận hỗ trợ để được hỗ trợ.
6. Nếu người dùng không thể sử dụng chức năng lấy mã OTP để xác nhận danh tính (do nguyên nhân không thể đăng nhập vào email đã đăng kí với ứng dụng). Việc này sẽ tùy theo mức độ nghiêm trọng để xử lí, đặc biệt là với các tải khoản của người chủ quán ăn khi có thông tin quán và các dữ liệu liên quan khác. Lúc này tìm đến bộ phận hỗ trợ ứng dụng có thể được coi là biện pháp duy nhất. Lúc này bộ phận hỗ trợ sẽ xác nhận danh tính của người dùng theo hướng xác nhận qua số điện thoại, hoặc số CCCD đã đăng kí với ứng dụng trong lúc hình thành quán ăn trên ứng dụng.

# Subflows

## Subflow Nhập tên đăng nhập hoặc địa chỉ email:

Người dùng nhập tên đăng nhập hoặc địa chỉ email đã đăng ký với tài khoản của họ. Nếu tài khoản không tồn tại hoặc thông tin không chính xác, hệ thống sẽ hiển thị thông báo lỗi và yêu cầu người dùng nhập lại thông tin.

## Subflow Kiểm tra địa chỉ email:

Hệ thống sẽ kiểm tra xem địa chỉ email được nhập vào có tồn tại trong hệ thống hay không. Nếu không tồn tại, hệ thống sẽ hiển thị thông báo lỗi và yêu cầu người dùng nhập lại thông tin. Nếu địa chỉ email hợp lệ, hệ thống sẽ tiếp tục gửi một liên kết đặt lại mật khẩu đến địa chỉ email đó.

## Subflow Nhập mã xác minh:

Người dùng sẽ nhập mã xác minh được gửi đến địa chỉ email hoặc số điện thoại của họ để xác minh danh tính của mình. Nếu mã xác minh không chính xác, hệ thống sẽ hiển thị thông báo lỗi và yêu cầu người dùng nhập lại.

## Subflow Đặt lại mật khẩu:

Sau khi xác minh danh tính, người dùng sẽ được chuyển đến trang đặt lại mật khẩu, nơi họ có thể nhập mật khẩu mới của mình. Hệ thống sẽ yêu cầu người dùng nhập mật khẩu mới và xác nhận lại mật khẩu mới để đảm bảo tính chính xác của mật khẩu.

## Subflow Thông báo đặt lại mật khẩu thành công:

Hệ thống sẽ hiển thị thông báo đặt lại mật khẩu thành công và yêu cầu người dùng đăng nhập lại với mật khẩu mới.

## Subflow Yêu cầu trợ giúp từ bộ phận hỗ trợ:

Nếu người dùng không thể đặt lại mật khẩu bằng các Subflows trên, họ có thể yêu cầu trợ giúp đỡ để lấy lại tài khoản.

# Key Scenarios

## Người dùng quên mật khẩu:

Mô tả: người dùng không thể đăng nhập vào tài khoản của mình vì quên mật khẩu. Người dùng cần sử dụng tính năng quên mật khẩu để lấy lại quyền truy cập vào tài khoản.

## Tin nhắn email không đến

Mô tả: người dùng sử dụng tính năng quên mật khẩu để yêu cầu một liên kết đặt lại mật khẩu qua email. Tuy nhiên, email với liên kết đặt lại mật khẩu không được gửi hoặc không đến đúng hộp thư của người dùng.

## Mã xác thực không hợp lệ

Mô tả: Trong trường hợp này, sau khi người dùng đã yêu cầu đặt lại mật khẩu qua email, họ sẽ nhận được một mã xác thực để xác nhận danh tính của mình. Nếu mã xác thực không hợp lệ hoặc đã hết hạn, người dùng sẽ không thể tiếp tục quá trình đặt lại mật khẩu.

## Đặt lại mật khẩu không thành công

Mô tả: người dùng đã tiến hành đặt lại mật khẩu bằng liên kết đặt lại được gửi qua email và mã xác thực. Tuy nhiên, người dùng gặp sự cố khi đặt lại mật khẩu và không thể đăng nhập vào tài khoản của mình.

## Sự cố với Cơ sở dữ liệu

Mô tả: Trong trường hợp này, có thể xảy ra sự cố với cơ sở dữ liệu trong quá trình đặt lại mật khẩu, dẫn đến việc người dùng không thể thực hiện yêu cầu đặt lại mật khẩu.

# Preconditions

* Người dùng đã tải ứng dụng “Tìm kiếm quán ăn” trên thiết bị di động.
* Hệ thống ứng dụng "Tìm kiếm quán ăn" đã được kích hoạt và sẵn sàng hoạt động.
* Hệ thống máy chủ và cơ sở dữ liệu của ứng dụng đã được kết nối và hoạt động đúng cách.
* Thiết bị của người dùng đã kết nối thành công với internet và có kết nối ổn định để đảm bảo quá trình đăng nhập diễn ra thành công.
* Người dùng phải đăng nhập, xác thực thông tin là của mình.

# Postconditions

* Hệ thống đã gửi email đến người dùng để cung cấp hướng dẫn để khôi phục mật khẩu.
* Người dùng đã xác nhận thông tin tài khoản của mình và nhận được các hướng dẫn để khôi phục mật khẩu.
* Người dùng đã đặt lại mật khẩu của mình và có thể đăng nhập vào ứng dụng bằng mật khẩu mới của họ.
* Hệ thống đã bảo mật thông tin người dùng và không lưu trữ mật khẩu trong văn bản thô.

# Extension Points

* Hỗ trợ nhiều phương thức khôi phục mật khẩu khác nhau, chẳng hạn như thông qua điện thoại di động hoặc ứng dụng xác thực bổ sung.
* Cung cấp tùy chọn để xác minh danh tính người dùng, chẳng hạn như thông qua câu hỏi bảo mật hoặc mã xác thực hai yếu tố, để đảm bảo rằng chỉ có người dùng chính xác mới có thể đặt lại mật khẩu.
* Cung cấp tính năng tự động khôi phục mật khẩu, mà không cần tương tác của người dùng, ví dụ như bằng cách sử dụng thông tin xác thực bổ sung để đánh giá danh tính của người dùng.
* Đề xuất các giải pháp bảo mật tài khoản khác cho người dùng, chẳng hạn như sử dụng mã xác thực hai yếu tố hoặc thay đổi mật khẩu định kỳ để bảo vệ tài khoản của họ.

# Special Requirements

* Bảo mật thông tin người dùng: Đảm bảo rằng các thông tin đăng nhập, thông tin xác thực, mã xác thực, và mật khẩu được bảo mật và chỉ được truy cập bởi người dùng chính xác.
* Kiểm tra tính hợp lệ của email hoặc số điện thoại: Đảm bảo rằng email hoặc số điện thoại được nhập đúng và hợp lệ để có thể gửi liên kết hoặc mã xác thực đến người dùng.
* Thực hiện giới hạn số lần khôi phục mật khẩu: Để tránh việc tấn công từ hacker, giới hạn số lần khôi phục mật khẩu hoặc cung cấp các giải pháp xác thực bổ sung để đảm bảo rằng chỉ có người dùng chính xác mới có thể khôi phục mật khẩu.
* Cập nhật mật khẩu mới một cách an toàn: Đảm bảo rằng việc cập nhật mật khẩu mới được thực hiện một cách an toàn, thông qua việc mã hóa hoặc sử dụng các giải pháp bảo mật khác để bảo vệ thông tin người dùng.
* Hỗ trợ nhiều ngôn ngữ: Đối với các ứng dụng được sử dụng trên toàn cầu, hỗ trợ nhiều ngôn ngữ sẽ giúp người dùng dễ dàng sử dụng ứng dụng để khôi phục mật khẩu của mình.

# Additional Information

Chức năng quên mật khẩu là một tính năng quan trọng trong hệ thống đăng nhập và bảo mật thông tin người dùng. Để đảm bảo tính bảo mật của thông tin, hệ thống cần phải sử dụng các thuật toán mã hóa mạnh và cơ chế xác thực người dùng trước khi cho phép đặt lại mật khẩu. Ngoài ra, hệ thống cần cung cấp cho người dùng các lời khuyên về mật khẩu mạnh và cách giữ an toàn thông tin cá nhân. Đồng thời, hệ thống cần ghi lại các hoạt động của người dùng trong quá trình thực hiện chức năng quên mật khẩu để phục vụ cho việc phát hiện và giải quyết các vấn đề liên quan đến bảo mật thông tin.