Functional Requirements Document (FRD)

E-Insurance Application: User Login and Policy Management

1. Feature Overview

Description: The e-insurance application allows users to securely log in, manage their insurance policies, file claims, and view policy details. Users can access their existing policies, purchase new policies, and track claim status within the platform.

Context: This feature provides a secure authentication mechanism for users and also serves as the core of the application, ensuring users can safely access and manage their insurance details.

Purpose: To enable users to log into their accounts securely and interact with their insurance details. The system ensures only authorized access to sensitive information like insurance policy details, claim status, and personal data.

2. Accessing the Feature

Steps to Access the Feature:
1. Open the e-insurance application on the web or mobile.
2. On the homepage, click on the Login button at the top-right corner.
3. The Login Screen will be displayed where users can enter their username/email and password.
4. After successful login, users will be redirected to the Dashboard where they can view their active policies, manage claims, and perform other actions.

3. User Interfaces

Login Screen Elements:

Element	Label	Placeholder	Field Type	Width	Mandatory
Username/Email Field	Username/Email	Enter your username or email address	Text	300px	Yes

Password Field	Password	Enter your password	Password	300px	Yes
Login Button	Login		Button		Yes
Forgot Password Link	Forgot Password?		Link		No
Sign Up Link	New User? Sign up.		Link		No

4. User Journey

Scenario 1:

Successful Login:
1. The user navigates to the login page.
2. Enters valid username/email and password.
3. The system verifies credentials.
4. Upon successful verification, the user is redirected to the Dashboard where they can view their policies.

Scenario 2:

Incorrect Login Credentials:
1. The user enters an incorrect username/email or password.
2. The system displays an error message: "Invalid username/email or password."
3. The user corrects the input and retries logging in.

Scenario 3:

Forgotten Password:
1. The user clicks on Forgot Password?
2. The user is prompted to enter their registered email.
3. The system sends a password reset link to the user's email.

5. Role-Based Access Restrictions

User Roles and Permissions:

1. Admin: Full access to all policies and claims, including the ability to modify and approve claims.
2. Policyholder (User): Can view their own policies, file claims, and track claim status. Cannot view or modify policies of other users.
3. Guest: Can view public insurance details and sign-up for the platform, but cannot access their own policy details without registration/login.

6. Error Handling

Error Scenarios and Messages:

1. Invalid Credentials: Message - "Invalid username/email or password. Please try again."
2. Empty Fields: Message - "Please enter both username/email and password."
3. Account Locked: Message - "Your account has been locked due to multiple failed login attempts. Please try again later or contact support."
4. Server Error: Message - "Oops! Something went wrong. Please try again later."
5. Forgot Password: Message - "A password reset link has been sent to your email."

7. Default Configurations

Default Settings for New Record (New User):

1. Account Status: Active
2. Role: Policyholder (User)
3. Login Attempts: 0
4. Password Expiry: 180 days (password should be updated after 6 months)
5. Default Session Timeout: 15 minutes of inactivity

8. Acceptance Criteria

Given the user has a valid account, when they enter correct login credentials (username/email and password), then they are successfully logged in and redirected to the dashboard.

Given the user enters incorrect login credentials, when they attempt to login, then an error message is displayed indicating that the credentials are invalid.

Given the user is logged out, when they attempt to access a restricted page, then they are redirected to the login page.

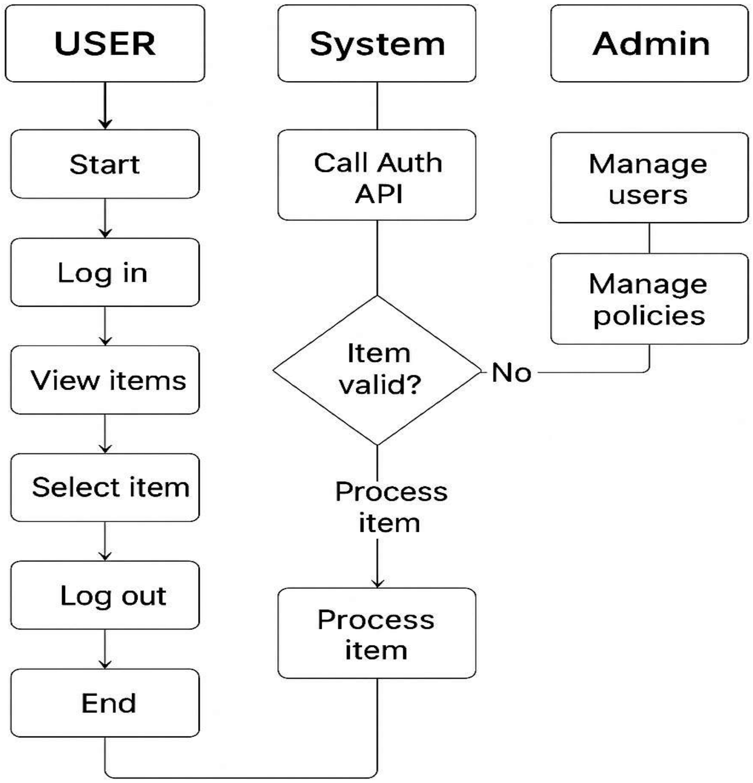
Given the user forgot their password, when they click the "Forgot Password" link and enter their registered email, then they receive a password reset link via email.

9. Functional Workflow :

This flowchart explains the flow between the User, System, and Admin roles:

- The **User** starts the app, logs in, views available items, selects an item, logs out, and ends the session.
- Once an item is selected, the **System** calls the Authentication (Auth) API to check if the item is valid.

- If the item is **valid**, the system processes the item.
- If the item is **not valid**, the **Admin** is involved to manage users or update the policies.
- After processing, the flow returns to the user to continue or end the session.


USER
System
Admin
Start
Call Auth API
Manage users
Log in
Manage policies
Item valid?
No
View items
Select item
Process item
Log out
Process item
End