Test Plan

1. Introduction

The purpose of this test plan is to validate the functionality of a registered user logging in from a new device, ensuring they are logged out from all other devices for enhanced account security. This includes validating user input, OTP verification, and notifications.

2. Scope

In Scope:

- User login flow from a new device.
- Input validation for phone number and password.
- OTP verification process.
- Successful login and redirection to the home page.
- Notifications (login success, SMS alerts).
- Automatic logout from all other devices.

Out of Scope:

- Multi-factor authentication settings beyond OTP.
- Account creation or password reset processes.
- Logging in from the same device.

3. Objectives

- Ensure the user can log in from a new device successfully.
- Validate that the system logs out the user from all other devices.
- Confirm the delivery of a login notification message (SMS) after successful login.
- Test proper redirection to the home page after login.

4. Test Approach

Testing Levels:

1. **Functional Testing:** Verify each step of the login process and logout mechanism.
2. **Integration Testing:** Test interactions between the UI, authentication system, and notification service.
3. **Negative Testing:** Check system behavior with invalid inputs (e.g., incorrect OTP, invalid phone number).
4. **Security Testing:** Verify secure handling of credentials and logout processes.
5. **Performance Testing:** Assess response times for OTP delivery and login success.

Testing Types:

- **Manual Testing:** For UI validations and edge cases.
- **Automation Testing:** For repetitive scenarios like input validation and notifications.

5. Test Deliverables

- Test Cases (Functional, Negative, Edge Cases).
- Test Execution Results.
- Defect Reports.
- Test Summary Report.

6. Resources

Test Environment:

- Web and Mobile Applications (Staging and Production Environments).
- Devices: iOS, Android, Windows, Mac.
- Browsers: Chrome, Safari, Firefox, Edge.

Test Data:

- User accounts (verified, unverified).
- Correct and incorrect phone numbers, passwords, and OTPs.

Tools:

- Selenium WebDriver (Automation).
- Postman (API Testing).
- JIRA (Defect Management).
- TestNG (Test Management).

7. Roles and Responsibilities

Role	Responsibility
QA Lead	Create and review test plan and cases.
Test Engineers	Execute test cases, identify defects.
Developers	Fix defects, implement changes.
DevOps	Maintain test and production environments.

8. Risks and Mitigation

Risk	Mitigation Plan
OTP not delivered to the user.	Monitor SMS gateway logs and retry mechanism for OTPs.
User not logged out from other devices.	Verify session termination across all devices.
Login fails due to high server load.	Conduct load testing to ensure system stability.
Credentials stored insecurely.	Test encryption and secure storage mechanisms.

9. Test Execution Plan

Phase 1: Functional Testing

- Validate login flow: Input validation, OTP submission, and redirection to the home page.
- Verify successful logout from other devices.

Phase 2: Negative Testing

- Test with incorrect phone numbers, passwords, and OTPs.
- Test system behavior with expired or reused OTPs.

Phase 3: Integration Testing

- Ensure the OTP service, notification system, and login flow work together seamlessly.

Phase 4: Security Testing

- Validate data encryption during login.
- Ensure secure session handling and logout mechanisms.

Phase 5: Performance Testing

- Test system response times during high traffic for login and OTP delivery.

10. Test Scenarios and Test Cases

Functional Test Cases

1. Verify the "Login" button is clickable on the login page.
2. Validate that the system accepts only valid phone numbers and passwords.
3. Check OTP delivery to the registered phone number.
4. Verify login success with a valid OTP.
5. Ensure logout occurs on all other devices after a successful login.

Negative Test Cases

1. Attempt login with an unregistered phone number.
2. Enter incorrect or expired OTP and verify error messages.
3. Verify system behavior when OTP is entered multiple times incorrectly.

Edge Cases

1. Attempt login while already logged in on another device.
2. Check for timeouts or session expiry during login flow.
3. Validate system behavior for duplicate OTP requests.

11. Test Closure

- Verify all test cases are executed, and defects are resolved.
- Confirm the system meets the acceptance criteria.
- Document results in the Test Summary Report.

Risk-Based Testing (RBT) Approach

1. Identifying Risks

The primary risks associated with this user story include:

- **Critical Risks:**
  - Users unable to log in due to input validation or OTP issues.
  - Sessions not being logged out on other devices, leading to potential security risks.
  - SMS notifications not being sent, leading to unawareness of unauthorized access.
  - Login redirection failure.
- **Moderate Risks:**
  - Delays in SMS notifications.
  - UI/UX issues affecting user flow.
  - Multiple failed login attempts blocking the user (lockout scenarios).
- **Low Risks:**
  - Minor typos in error messages.
  - Performance issues under load (e.g., OTP delays, session termination delays).

2. Prioritizing Risks

Based on severity and likelihood:

- High Priority: Critical risks (security, functionality).
- Medium Priority: Moderate risks (usability, performance).
- Low Priority: Cosmetic or minor issues.

Test Cases for Each User Story (Acceptance and Edge Cases)

Test Suite 1: Login Functionality

Acceptance Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC01	Login with valid phone number, password, and OTP	High	User logs in successfully, SMS notification is sent, and other devices are logged out.
TC02	Attempt login with incorrect phone number	High	Error: "Invalid phone number."
TC03	Attempt login with incorrect password	High	Error: "Incorrect password."
TC04	Login with expired OTP	High	Error: "OTP has expired."
TC05	Successful redirection after login	High	User is redirected to the home page.

Edge Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC06	Login attempt with multiple failed OTPs	Medium	Account temporarily locked after a defined number of failed attempts.
TC07	Login without entering phone number or password	Medium	Error: "Phone number and password are required."
TC08	Session timeout during login	Medium	Error: "Session expired. Please try again."
TC09	Simultaneous login attempts from two devices	High	Only one device is logged in, and other device receives a "Session Expired" message.
TC10	Login when the SMS gateway is unavailable	High	Fallback mechanism triggers or appropriate error message is displayed.

Test Suite 2: OTP Functionality

Acceptance Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC11	Receive OTP after entering valid phone number	High	OTP is sent to the registered number.
TC12	Validate incorrect OTP entry	High	Error: "Invalid OTP. Please try again."
TC13	Validate OTP expiry	High	Error: "OTP has expired."

Edge Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC14	Resend OTP functionality	Medium	New OTP is sent, and previously sent OTP is invalidated.
TC15	Attempt to use the same OTP multiple times	High	Error: "OTP already used."

Test Suite 3: Logout from All Other Devices

Acceptance Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC16	Verify session termination on previously logged-in devices	High	All active sessions are terminated except for the new device.

Edge Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC17	Verify old session behavior after successful login on new device	High	"Session Expired" message is displayed on old devices.
TC18	Login simultaneously from multiple locations	High	Only one device is logged in; others are logged out automatically.

Test Suite 4: Notifications

Acceptance Test Cases:

Test ID	Test Case Description	Priority	Expected Result
TC19	Verify SMS notification for successful login	High	SMS notification is sent after successful login on the new device.

Edge Test Cases

Test ID	Test Case Description	Priority	Expected Result
TC20	SMS delay or failure due to gateway issue	High	Error message is displayed, and retry is attempted.

Test Runs

Test Run 1: Happy Path

- Objective: Verify that a user can log in successfully with valid credentials, log out from all other devices, and receive notifications.
- Test Cases: TC01, TC11, TC19.

Test Run 2: Input Validation

- Objective: Test the robustness of input validation for phone number, password, and OTP.
- Test Cases: TC02, TC03, TC05, TC07, TC12, TC14.

Test Run 3: Edge Case Testing

- Objective: Test uncommon or edge scenarios, such as SMS gateway failures, session timeouts, and multiple failed login attempts.
- Test Cases: TC08, TC09, TC10, TC14, TC20.

Test Run 4: Security Testing

- Objective: Verify session termination and security measures to ensure account access from only one device.
- Test Cases: TC16, TC17, TC18.