**Test Plan for Orange-HRM Login Page**

**1. Introduction**

This test plan outlines the testing strategy for the login functionality of the OrangeHRM system. The objective is to ensure that the login feature functions correctly, securely, and efficiently under various scenarios.

**2. Scope**

**2.1 In Scope**

* Functional testing of login functionality
* UI and usability testing
* Security testing related to authentication
* Performance testing for login response times
* Compatibility testing across different browsers and devices

**2.2 Out of Scope**

* Testing of modules beyond login (e.g., Dashboard, Employee Management)
* Database testing unless required for login validation

**3. Test Objectives**

* Verify that valid users can log in successfully
* Ensure incorrect credentials result in appropriate error messages
* Check the behaviour of forgotten password functionality
* Validate session management and timeout
* Ensure security features like account lockout after multiple failed attempts

**4. Testing Approach**

**4.1 Test Types**

**Functional Testing**

* Verify that the username and password fields accept input
* Check that valid credentials allow login
* Ensure invalid credentials show appropriate error messages
* Validate case sensitivity of username and password

**UI/Usability Testing**

* Ensure all UI elements are properly aligned and visible
* Check that placeholder texts and labels are correct
* Verify responsiveness on different screen sizes

**Security Testing**

* Attempt SQL Injection and XSS attacks on input fields
* Check for session hijacking vulnerabilities
* Verify secure password handling (e.g., no plain text storage)

**Performance Testing**

* Measure login response time under normal and peak loads
* Simulate multiple concurrent logins to assess system stability

**Compatibility Testing**

* Verify login functionality on Chrome, Firefox, Edge, Safari
* Test responsiveness on mobile and tablet devices

**5. Test Environment**

* **Browsers:** Chrome, Firefox, Edge, Safari
* **Operating Systems:** Windows, macOS, Android, iOS
* **Test Data:** Valid and invalid login credentials, edge case inputs

**6. Risks and Mitigation**

|  |  |
| --- | --- |
| **Risk** | **Mitigation Strategy** |
| System downtime during testing | Conduct tests in a staging environment |
| Security vulnerabilities | Perform thorough penetration testing |
| Compatibility issues | Test across multiple browsers and devices |

**7. Entry and Exit Criteria**

**Entry Criteria**

* Test environment is set up and accessible
* Functional specifications for login are available
* Test data is prepared

**Exit Criteria**

* All critical test cases have passed
* Major defects are resolved
* Test results are documented and reviewed

**8. Deliverables**

* Test Plan Document
* Test Execution Report
* Defect Logs

**9. Timeline**

* Test Planning: X days
* Test Execution: X days
* Bug Fixing & Retesting: X days

**10. Approval**

Team will send different types of documents for Client Approval like below:

• Test Plan

• Test Scenarios

• Test Cases

• Reports

Testing will only continue to the next steps once these approvals are done