# Test Plan - VWO Login Page

## 1. Introduction

This test plan outlines the strategy, scope, objectives, and schedule for testing the VWO Login Page (https://app.vwo.com/#/login). The purpose of this test plan is to ensure that the login functionality works as expected and meets business requirements.

## 2. Test Plan Details

|  |  |
| --- | --- |
| Project Name | VWO Login Page Testing |
| Module Name | Login Functionality |
| Prepared By | [Enter Author] |
| Reviewed By | [Enter Reviewer] |
| Date | [Enter Date] |
| Version | 1.0 |

## 3. Scope

This test plan covers the testing of the login functionality of the VWO application. It includes valid login scenarios, invalid login attempts, UI/UX validation, security testing, and performance testing.

## 4. Testing Approach

The testing will follow a manual and automated approach. Functional testing, boundary value analysis, equivalence partitioning, and negative testing techniques will be applied.

## 5. Test Items

The following aspects of the login page will be tested:  
- Valid and invalid username/password combinations  
- Forgot password functionality  
- UI/UX consistency  
- Session management  
- Security (SQL injection, XSS, brute force attacks)

## 6. Test Environment

The tests will be conducted in the following environments:  
- Browsers: Chrome, Firefox, Edge, Safari  
- Devices: Desktop, Mobile, Tablet  
- Operating Systems: Windows, macOS, Android, iOS  
- Test Tools: Selenium, Postman, JMeter (for performance testing)

## 7. Test Schedule

Testing will be conducted as per the following timeline:  
- Test Planning: [Start Date] - [End Date]  
- Test Case Preparation: [Start Date] - [End Date]  
- Test Execution: [Start Date] - [End Date]  
- Defect Fixing & Retesting: [Start Date] - [End Date]  
- Test Closure: [Start Date]

## 8. Test Deliverables

The following deliverables will be provided:  
- Test Plan Document  
- Test Cases  
- Test Execution Reports  
- Defect Reports  
- Final Test Summary Report

## 9. Risks & Mitigation Plan

Potential risks include delayed development changes, test environment instability, and unexpected bugs. Mitigation strategies include early communication with developers, backup test environments, and continuous monitoring.

## 10. Entry & Exit Criteria

\*\*Entry Criteria:\*\*  
- Login page is developed and stable  
- Test data is available  
- Test environment is ready  
  
\*\*Exit Criteria:\*\*  
- All high and critical defects are fixed  
- Test execution is completed with acceptable pass percentage  
- Test summary report is prepared and shared

## 11. Approval

[Mention the stakeholders who will approve the test plan]