

# Acceptance Criteria

## Acceptance Criteria: {{PROJECT\_NAME}}

“ **Project:** {{PROJECT\_NAME}} **Version:** {{VERSION}} **Date:** {{DATE}}  
**Author:** {{AUTHOR}} **Status:** Draft | In Review | Approved **Reviewers:**  
{{REVIEWERS}}

## Document History

Version	Date	Author	Changes
0.1	{{DATE}}	{{AUTHOR}}	Initial draft

## 1. Purpose & Methodology

### 1.1 What Are Acceptance Criteria?

Acceptance criteria are the conditions that a system must satisfy to be accepted by a stakeholder. They answer the question: "**How will we know when this feature is done?**"

Good acceptance criteria are:

- **Testable** — Can be verified with a specific test procedure
- **Clear** — Unambiguous; no room for interpretation
- **Complete** — Cover happy path, error paths, and edge cases
- **Agreed** — Signed off by the business BEFORE development begins

# 1.2 Format: Given / When / Then (Gherkin-Style)

```
Given [an initial context / precondition that is true]
When [an action or event occurs]
Then [the expected outcome is observed]
And [additional expected outcomes, chained]
```

## Example — User Login:

```
Given a registered user with valid credentials
When the user submits the login form
Then the user is redirected to the dashboard
And a session token is created and stored in a secure cookie
And the last login timestamp is updated in the database
```

# 1.3 Categories of Acceptance Criteria

Category	Description	Example
<b>Positive (Happy Path)</b>	System works as expected with valid inputs	Successful login
<b>Negative (Sad Path)</b>	System handles invalid inputs gracefully	Wrong password error
<b>Edge Case</b>	Boundary conditions and unusual but valid scenarios	Login at exact session timeout
<b>Integration</b>	System works correctly with external services	Payment processed via Stripe
<b>Non-Functional</b>	Performance, accessibility, security criteria	Page loads in < 2 seconds
<b>Data</b>	Correct data storage, retrieval, and validation	Fields saved with correct types

# 2. Feature Acceptance Criteria

Module: {{MODULE\_1\_NAME}}

## Feature: {{FEATURE\_1\_NAME}} (FR-{{XXX}})

**Feature Description:** {{BRIEF\_DESCRIPTION}} **Business Requirement:** BR-{{XXX}} **Linked User Stories:** US-{{XXX}}, US-{{XXX}}

### Positive Scenarios:

#	Scenario	Given	When	Then
AC-001	{{SCENARIO_NAME}}	{{PRECONDITION}}	{{ACTION}}	{{EXPECTED_RESULT}}
AC-002				

### Negative Scenarios:

#	Scenario	Given	When	Then
AC-003	{{INVALID_INPUT_SCENARIO}}	{{PRECONDITION_WITH_BAD_DATA}}	{{ACTION}}	{{ERROR_MESSAGE_OR_BEHAVIOR}}
AC-004				

### Edge Cases:

#	Scenario	Given	When	Then
AC-005	{{BOUNDARY_CONDITION}}	{{EDGE_CONDITION}}	{{ACTION}}	{{EXPECTED_RESULT}}

### Non-Functional Acceptance Criteria:

#	Category	Criterion
AC-006	Performance	Feature completes in < {{X}} seconds under normal load
AC-007	Accessibility	Feature is fully operable by keyboard; ARIA labels present
AC-008	Security	{{SECURITY_CRITERION_IF_APPLICABLE}}

## Feature: User Registration (FR-020)

**Feature Description:** New users can create accounts using email and password. **Business Requirement:** BR-{{XXX}} **Linked User Stories:** US-{{XXX}}

### Positive Scenarios:

#	Scenario	Given	When	Then
---	----------	-------	------	------

AC-010	Successful registration	A user visits /register with a valid, unregistered email	User submits form with valid email, strong password, and required fields	Account is created; confirmation email sent; user redirected to email verification page
AC-011	Email verification sent	Account was just created	System processes registration	Verification email arrives within 2 minutes with unique, expiring link
AC-012	Verification link works	User receives verification email	User clicks verification link	Email verified; user redirected to login; account marked as verified

### Negative Scenarios:

#	Scenario	Given	When	Then
AC-013	Duplicate email	An account already exists with email@example.com	User submits registration with email@example.com	Error "An account with this email already exists" shown; no new account created
AC-014	Weak password	User is on registration form	User submits password "abc123"	Inline error shown: "Password must be at least 8 characters and include uppercase, number, and special character"
AC-015	Invalid email format	User is on registration form	User submits "notanemail" in email field	Inline validation error shown before form submission
AC-016	Empty required field	User is on registration form	User submits with required field empty	Inline error shown; form not submitted

### Edge Cases:

#	Scenario	Given	When	Then
AC-017	Email with plus addressing	User submits user+tag@example.com	Registration submitted	Account created; treated as valid email
AC-018	Verification link expiry	Verification link generated 25+ hours ago	User clicks expired link	Error "Verification link has expired"; option to resend verification email shown

#	Scenario	Given	When	Then
AC-019	Double registration attempt	User submits form; due to slow network submits twice	Two identical POST requests sent	Only one account created; second request returns appropriate error

## Feature: User Login (FR-021)

### Positive Scenarios:

#	Scenario	Given	When	Then
AC-020	Successful login	A verified user with valid credentials	User submits login form	Authenticated; redirected to dashboard; session created
AC-021	Remember me	A verified user checks "Remember Me"	User submits login form	Session persists for 30 days; user stays logged in after browser close

### Negative Scenarios:

#	Scenario	Given	When	Then
AC-022	Wrong password	A registered user exists	User submits incorrect password	Generic error "Invalid email or password" (no enumeration); login not granted
AC-023	Non-existent email	No account for this email	User submits login	Same generic error "Invalid email or password" (prevent user enumeration)
AC-024	Account locked	User has made 5 failed attempts	User attempts login again	Message: "Account temporarily locked. Try again in 15 minutes."

### Edge Cases:

#	Scenario	Given	When	Then
AC-025	Session expiry	User has been idle for 31 minutes	User attempts to navigate	Redirected to login; session cleared; unsaved work warning shown

#	Scenario	Given	When	Then
AC-026	Login on unverified account	Account created but email not verified	User attempts to log in	Error "Please verify your email before logging in" with option to resend

## Feature: {{NEXT\_FEATURE\_NAME}} (FR-{{XXX}})

### Positive Scenarios:

#	Scenario	Given	When	Then
AC-{{NEXT}}				

### Negative Scenarios:

#	Scenario	Given	When	Then
AC-{{NEXT}}				

### Edge Cases:

#	Scenario	Given	When	Then
AC-{{NEXT}}				

## 3. Integration Scenarios

#	Integration	Scenario	Expected Behavior	Test Environment
INT-001	{{EXTERNAL_SERVICE}}	{{SCENARIO}}	{{EXPECTED}}	Sandbox / Mock
INT-002	Email provider	Transactional email delivery	Email received within 2 minutes	Mailtrap / staging
INT-003	{{PAYMENT_PROVIDER}}	Successful payment	Transaction recorded; confirmation shown; webhook received	Stripe test mode
INT-004	{{PAYMENT_PROVIDER}}	Payment declined	User sees friendly error; no order created; no double-charge	Stripe test mode
INT-005	{{THIRD_PARTY_API}}	API timeout	System shows user-friendly error; request logged; no data corruption	Mocked timeout

#	Integration	Scenario	Expected Behavior	Test Environment
INT-006	{{THIRD_PARTY_API}}	API unavailable	System degrades gracefully; non-dependent features still work	Service unavailable mock

## 4. Non-Functional Acceptance Criteria

### 4.1 Performance

#	Criterion	Target	Test Method
NF-AC-001	All pages load within target time	< 3s initial, < 1.5s subsequent	Lighthouse on staging
NF-AC-002	All API endpoints respond within target	< 500ms at p95 under normal load	k6 load test
NF-AC-003	Core Web Vitals pass	LCP < 2.5s, CLS < 0.1, FCP < 1.8s	Lighthouse

### 4.2 Accessibility

#	Criterion	Target	Test Method
NF-AC-010	No critical accessibility violations	0 critical violations	axe-core automated scan
NF-AC-011	Keyboard navigation complete	All features operable without mouse	Manual test
NF-AC-012	Color contrast compliant	≥ 4.5:1 text/background	Contrast checker

### 4.3 Security

#	Criterion	Target	Test Method
NF-AC-020	No OWASP Top 10 vulnerabilities	0 critical/high findings	OWASP ZAP scan
NF-AC-021	All user inputs sanitized	No XSS/injection vulnerabilities	SAST + manual testing
NF-AC-022	No sensitive data in client-side code	No API keys, tokens in browser	Code review + browser DevTools

# 5. UAT Scenario Mapping

AC ID	AC Description	UAT Scenario ID	UAT Tester	Status
AC-010	Successful registration	UAT-001	{{TESTER}}	Not Started
AC-011	Email verification sent	UAT-002		
AC-020	Successful login	UAT-003		
INT-003	Payment success	UAT-010		
NF-AC-001	Page load performance	UAT-P01		

# 6. Traceability to Requirements

AC ID	Acceptance Criterion	FR Reference	BR Reference	US Reference
AC-001	{{CRITERION}}	FR-{{XXX}}	BR-{{XXX}}	US-{{XXX}}
AC-010	Successful registration	FR-020	BR-{{XXX}}	US-{{XXX}}

“ Full traceability: [requirements-traceability-matrix.md](requirements-traceability-matrix.md)

# Approval

Role	Name	Date	Signature
Author			
Reviewer			
Business Analyst			
Product Owner			
QA Engineer			
AI Director (John)			
Client Representative			

---

Revision #8

Created 2026-02-24 14:52:18 UTC by John

Updated 2026-05-25 07:31:39 UTC by John