# Lex Assist Role-Based Access and AI Feature Testing Plan

## Overview

This document outlines the testing strategy for validating role-based access control and AI features in the Lex Assist application. The tests cover authentication flows, authorization checks, and AI functionality across different user roles and subscription tiers.

## 1. Authentication Testing

### 1.1 User Registration

* **Test ID**: AUTH-REG-001
* **Description**: Verify new user registration with email and password
* **Steps**:
  1. Submit registration form with valid email, password, and full name
  2. Verify user record is created in database
  3. Verify default 'user' role is assigned
  4. Verify 'free' subscription tier is assigned
* **Expected Result**: User successfully registered with correct role and tier

### 1.2 Email Login

* **Test ID**: AUTH-LOGIN-001
* **Description**: Verify user login with email and password
* **Steps**:
  1. Submit login form with valid credentials
  2. Verify JWT token is issued with correct claims
  3. Verify user profile is loaded
* **Expected Result**: User successfully authenticated with correct profile data

### 1.3 OTP Login

* **Test ID**: AUTH-LOGIN-002
* **Description**: Verify user login with mobile OTP
* **Steps**:
  1. Request OTP for registered mobile number
  2. Submit OTP verification form
  3. Verify JWT token is issued with correct claims
* **Expected Result**: User successfully authenticated via OTP

### 1.4 Token Refresh

* **Test ID**: AUTH-TOKEN-001
* **Description**: Verify token refresh functionality
* **Steps**:
  1. Login with valid credentials
  2. Wait until token is near expiry
  3. Attempt token refresh
* **Expected Result**: New valid token issued without requiring re-login

### 1.5 Logout

* **Test ID**: AUTH-LOGOUT-001
* **Description**: Verify user logout functionality
* **Steps**:
  1. Login with valid credentials
  2. Perform logout
  3. Attempt to access protected resources
* **Expected Result**: Session terminated, protected resources inaccessible

## 2. Role-Based Access Testing

### 2.1 Super Admin Access

* **Test ID**: RBAC-ADMIN-001
* **Description**: Verify Super Admin access to all features
* **Steps**:
  1. Login as Super Admin
  2. Attempt to access all system features and settings
  3. Attempt to modify subscription tiers
  4. Attempt to change user roles
* **Expected Result**: Full access to all features and administrative functions

### 2.2 Admin Access

* **Test ID**: RBAC-ADMIN-002
* **Description**: Verify Admin access limitations
* **Steps**:
  1. Login as Admin
  2. Attempt to access all app features
  3. Attempt to access system settings
  4. Attempt to modify subscription tiers
* **Expected Result**: Access to all app features but not system settings or tier configuration

### 2.3 Free Tier User Access

* **Test ID**: RBAC-USER-001
* **Description**: Verify Free tier user access limitations
* **Steps**:
  1. Login as Free tier user
  2. Attempt to access basic features (case briefs, law sections, case histories)
  3. Attempt to access premium features (AI analysis, case drafting)
* **Expected Result**: Access only to basic features, premium features blocked

### 2.4 Pro Tier User Access

* **Test ID**: RBAC-USER-002
* **Description**: Verify Pro tier user access limitations
* **Steps**:
  1. Login as Pro tier user
  2. Attempt to access basic features
  3. Attempt to access AI analysis
  4. Attempt to access Enterprise-only features (case drafting)
* **Expected Result**: Access to basic features and AI analysis, but not case drafting

### 2.5 Enterprise Tier User Access

* **Test ID**: RBAC-USER-003
* **Description**: Verify Enterprise tier user access
* **Steps**:
  1. Login as Enterprise tier user
  2. Attempt to access all user features
* **Expected Result**: Access to all user features including case drafting

### 2.6 Role Modification

* **Test ID**: RBAC-ADMIN-003
* **Description**: Verify role modification restrictions
* **Steps**:
  1. Login as different user roles
  2. Attempt to modify user roles
* **Expected Result**: Only Super Admin can modify roles

## 3. AI Feature Testing

### 3.1 Law Section Extraction

* **Test ID**: AI-FEATURE-001
* **Description**: Verify law section extraction functionality
* **Steps**:
  1. Login as user with appropriate tier
  2. Submit case brief for analysis
  3. Verify law sections are extracted correctly
* **Expected Result**: Relevant law sections extracted with proper formatting

### 3.2 Case History Retrieval

* **Test ID**: AI-FEATURE-002
* **Description**: Verify case history retrieval functionality
* **Steps**:
  1. Login as user with appropriate tier
  2. Submit case brief for analysis
  3. Verify case histories are retrieved correctly
* **Expected Result**: Relevant case histories retrieved with proper formatting

### 3.3 Legal Analysis

* **Test ID**: AI-FEATURE-003
* **Description**: Verify legal analysis functionality
* **Steps**:
  1. Login as Pro or Enterprise tier user
  2. Submit case brief for analysis
  3. Verify legal analysis is generated correctly
* **Expected Result**: Comprehensive legal analysis with key issues and recommendations

### 3.4 Case File Drafting

* **Test ID**: AI-FEATURE-004
* **Description**: Verify case file drafting functionality
* **Steps**:
  1. Login as Enterprise tier user
  2. Submit case brief for analysis
  3. Request case file drafting
* **Expected Result**: Complete case file draft generated

### 3.5 Tier-Based Feature Limitations

* **Test ID**: AI-FEATURE-005
* **Description**: Verify tier-based feature limitations
* **Steps**:
  1. Login as users with different tiers
  2. Attempt to access AI features
* **Expected Result**: Access granted or denied based on subscription tier

## 4. API Security Testing

### 4.1 Authentication Headers

* **Test ID**: API-SEC-001
* **Description**: Verify API requires authentication headers
* **Steps**:
  1. Attempt to access protected endpoints without authentication
  2. Attempt to access protected endpoints with invalid token
* **Expected Result**: Access denied with appropriate error messages

### 4.2 CORS Configuration

* **Test ID**: API-SEC-002
* **Description**: Verify CORS configuration
* **Steps**:
  1. Attempt to access API from allowed origins
  2. Attempt to access API from disallowed origins
* **Expected Result**: Access allowed only from configured origins

### 4.3 Rate Limiting

* **Test ID**: API-SEC-003
* **Description**: Verify rate limiting functionality
* **Steps**:
  1. Make multiple rapid requests to API endpoints
* **Expected Result**: Requests throttled after exceeding limit

## 5. Integration Testing

### 5.1 End-to-End Authentication Flow

* **Test ID**: INT-AUTH-001
* **Description**: Verify complete authentication flow
* **Steps**:
  1. Register new user
  2. Verify email
  3. Login
  4. Access features
  5. Logout
* **Expected Result**: Seamless flow through all authentication steps

### 5.2 End-to-End Analysis Flow

* **Test ID**: INT-ANALYSIS-001
* **Description**: Verify complete case analysis flow
* **Steps**:
  1. Login as appropriate tier user
  2. Submit case brief
  3. View law sections
  4. View case histories
  5. View legal analysis
  6. Download/share results
* **Expected Result**: Complete analysis workflow functions correctly

### 5.3 Subscription Upgrade Flow

* **Test ID**: INT-SUB-001
* **Description**: Verify subscription upgrade process
* **Steps**:
  1. Login as Free tier user
  2. Initiate upgrade to Pro tier
  3. Complete payment process
  4. Verify access to Pro features
* **Expected Result**: Successful tier upgrade with immediate feature access

## 6. Performance Testing

### 6.1 AI Response Time

* **Test ID**: PERF-AI-001
* **Description**: Verify AI analysis response time
* **Steps**:
  1. Submit case briefs of varying lengths
  2. Measure response time
* **Expected Result**: Response time within acceptable limits (< 10 seconds for typical briefs)

### 6.2 Concurrent User Load

* **Test ID**: PERF-LOAD-001
* **Description**: Verify system performance under load
* **Steps**:
  1. Simulate multiple concurrent users
  2. Measure response times and system stability
* **Expected Result**: System remains responsive under expected load

## 7. Test Environment Setup

### 7.1 Test Database

* Separate Supabase project for testing
* Pre-populated with test users of different roles and tiers
* Test data for law sections and case histories

### 7.2 Test Credentials

* Super Admin: [superadmin@lexassist.com](mailto:superadmin@lexassist.com) / password123
* Admin: [admin@lexassist.com](mailto:admin@lexassist.com) / password123
* Free User: [free@lexassist.com](mailto:free@lexassist.com) / password123
* Pro User: [pro@lexassist.com](mailto:pro@lexassist.com) / password123
* Enterprise User: [enterprise@lexassist.com](mailto:enterprise@lexassist.com) / password123

### 7.3 Test Environment Variables

SUPABASE\_URL=https://test-project-url.supabase.co

SUPABASE\_KEY=test-anon-key

API\_BASE\_URL=http://localhost:8000

## 8. Test Execution Plan

1. Set up test environment with test database and users
2. Execute authentication tests (Section 1)
3. Execute role-based access tests (Section 2)
4. Execute AI feature tests (Section 3)
5. Execute API security tests (Section 4)
6. Execute integration tests (Section 5)
7. Execute performance tests (Section 6)
8. Document test results and issues
9. Address critical issues before deployment

## 9. Test Reporting

Test results will be documented in a structured report including:

* Test case ID
* Pass/Fail status
* Actual results
* Issues identified
* Screenshots or logs where applicable
* Recommendations for fixes

## 10. Acceptance Criteria

The testing phase will be considered complete when:

* All critical test cases pass
* No high-severity security issues remain
* Role-based access controls function correctly for all user types
* AI features perform correctly within acceptable time limits
* Frontend-backend integration is seamless