User Management System - Requirements Specification

Document Information

- **Project:** User Registration and Management System
- **Version:** 1.0
- **Date:** September 22, 2025
- **Classification:** Production System Requirements

Table of Contents

1. Executive Summary

This document outlines the requirements for a secure web-based user management system that provides user registration, authentication, profile management, and administrative capabilities. The system is designed to handle user accounts with role-based access control and comprehensive security measures.

2. System Overview

2.1 Purpose

The User Management System provides a secure platform for:

- User account registration and management
- Authentication and authorization services
- User profile management
- Administrative oversight and reporting
- User search and directory services

2.2 Target Users

- **End Users:** Individuals registering and managing their accounts
- **System Administrators:** Personnel managing user accounts and system operations
- **API Consumers:** External systems integrating with user services

3. Functional Requirements

3.1 User Registration

3.1.1 Account Creation

> **REQ-001:** The system SHALL allow new users to create accounts by providing username, email, and password

> **REQ-002:** The system SHALL enforce unique usernames and email addresses across all accounts

> **REQ-003:** The system SHALL validate email addresses using RFC 5322 compliant validation

> **REQ-004:** The system SHALL require password confirmation during registration

> **REQ-005:** The system SHALL support optional profile data during registration

> **REQ-006:** The system SHALL automatically assign "user" role to new registrations

> **REQ-007:** The system SHALL send email verification for new registrations

> **REQ-008:** The system SHALL not activate accounts until email verification is completed

3.1.2 Input Validation

> **REQ-009:** Username SHALL be 3-50 characters, alphanumeric and underscore only

> **REQ-010:** Email address SHALL be validated against RFC 5322 standard

> **REQ-011:** Password SHALL meet complexity requirements (see Security Requirements)

> **REQ-012:** All user inputs SHALL be sanitized to prevent injection attacks

> **REQ-013:** Profile data SHALL be validated and size-limited (max 5KB)

3.2 Authentication

3.2.1 Login Process

> **REQ-014:** The system SHALL authenticate users using username/email and password

> **REQ-015:** The system SHALL support login using either username or email address

> **REQ-016:** The system SHALL maintain secure session management

> **REQ-017:** The system SHALL redirect authenticated users to their dashboard

> **REQ-018:** The system SHALL track last login timestamp for each user

> **REQ-019:** The system SHALL provide secure logout functionality

3.2.2 Account Security

> **REQ-020:** The system SHALL implement account lockout after 5 failed login attempts

> **REQ-021:** The system SHALL implement progressive delays for failed login attempts

> **REQ-022:** The system SHALL log all authentication events for audit purposes

> **REQ-023:** The system SHALL support account deactivation by administrators

> **REQ-024:** The system SHALL provide password reset functionality via email

3.3 User Dashboard

3.3.1 Profile Management

> **REQ-025:** The system SHALL provide a user dashboard for account management

> **REQ-026:** Users SHALL be able to view their profile information

> **REQ-027:** Users SHALL be able to update their email address

> **REQ-028:** Users SHALL be able to modify their profile data

> **REQ-029:** Users SHALL be able to change their password

> **REQ-030:** The system SHALL require current password verification for sensitive changes

3.3.2 Account Information Display

> **REQ-031:** The dashboard SHALL display user's username, email, and role

> **REQ-032:** The dashboard SHALL show account creation date

> **REQ-033:** The dashboard SHALL show last login timestamp

> **REQ-034:** The dashboard SHALL display current profile data in editable format

3.4 User Search and Directory

3.4.1 Search Functionality

> **REQ-035:** The system SHALL provide user search functionality

> **REQ-036:** Search SHALL support partial matching on usernames and email addresses

> **REQ-037:** Search results SHALL only display public profile information

> **REQ-038:** Search SHALL be available to authenticated users only

> **REQ-039:** Search queries SHALL be logged for audit purposes

3.4.2 Privacy Controls

> **REQ-040:** Users SHALL be able to control visibility of their profile in search results

> **REQ-041:** Sensitive information SHALL never be included in search results

> **REQ-042:** Search results SHALL be paginated for performance

3.5 Administrative Functions

3.5.1 User Management

> **REQ-043:** Administrators SHALL be able to view all user accounts

> **REQ-044:** Administrators SHALL be able to deactivate user accounts

> **REQ-045:** Administrators SHALL be able to reset user passwords

> **REQ-046:** Administrators SHALL be able to modify user roles

> **REQ-047:** Administrators SHALL be able to view user login history

> **REQ-048:** Administrative actions SHALL be logged with admin identity and timestamp

3.5.2 System Monitoring

> **REQ-049:** Administrators SHALL have access to system health dashboards

> **REQ-050:** The system SHALL provide user activity reports

> **REQ-051:** The system SHALL provide security incident reports

> **REQ-052:** Administrators SHALL be able to export user data for compliance purposes

3.5.3 Database Administration

> **REQ-053:** Administrators SHALL have controlled access to database reporting functions

> **REQ-054:** Database queries SHALL be limited to read-only operations for reporting

> **REQ-055:** All database access SHALL be logged and monitored

> **REQ-056:** Administrative database access SHALL require additional authentication

4. Security Requirements

4.1 Password Security

> **SEC-001:** Passwords SHALL be a minimum of 12 characters

> **SEC-002:** Passwords SHALL require at least one uppercase letter, lowercase letter, number, and special character

> **SEC-003:** Passwords SHALL be hashed using bcrypt with minimum cost factor of 12

> **SEC-004:** The system SHALL prevent use of common/breached passwords

> **SEC-005:** Password history SHALL prevent reuse of last 12 passwords

4.2 Session Management

> **SEC-006:** Sessions SHALL use cryptographically secure random session IDs

> **SEC-007:** Session cookies SHALL be httpOnly and secure

> **SEC-008:** Sessions SHALL expire after 8 hours of inactivity

> **SEC-009:** Sessions SHALL expire after 24 hours regardless of activity

> **SEC-010:** The system SHALL invalidate all sessions on password change

4.3 Input Security

> **SEC-011:** All database interactions SHALL use parameterized queries

> **SEC-012:** All user inputs SHALL be validated and sanitized

> **SEC-013:** The system SHALL implement CSRF protection

> **SEC-014:** The system SHALL implement XSS protection headers

SEC-015: File uploads SHALL be restricted and scanned

4.4 Access Control

SEC-016: The system SHALL implement role-based access control

SEC-017: Administrative functions SHALL require "admin" role

SEC-018: API endpoints SHALL validate user permissions

SEC-019: The system SHALL implement principle of least privilege

SEC-020: Administrative role assignment SHALL require dual approval

4.5 Data Protection

SEC-021: Personal data SHALL be encrypted at rest

SEC-022: All communications SHALL use TLS 1.3 or higher

SEC-023: The system SHALL implement data retention policies

SEC-024: The system SHALL support GDPR data deletion requests

SEC-025: Audit logs SHALL be immutable and encrypted

5. Performance Requirements

5.1 Response Times

PERF-001: Login operations SHALL complete within 2 seconds

PERF-002: Registration operations SHALL complete within 3 seconds

PERF-003: Profile updates SHALL complete within 2 seconds

PERF-004: Search operations SHALL return results within 1 second

PERF-005: Administrative reports SHALL generate within 10 seconds

5.2 Scalability

PERF-006: The system SHALL support 10,000 concurrent users

PERF-007: The system SHALL support 1 million registered users

PERF-008: Database operations SHALL be optimized for high concurrency

PERF-009: The system SHALL implement connection pooling

PERF-010: Static resources SHALL be served via CDN

5.3 Availability

PERF-011: The system SHALL maintain 99.9% uptime

PERF-012: The system SHALL implement graceful degradation

PERF-013: Maintenance windows SHALL not exceed 4 hours

PERF-014: The system SHALL implement health checks

PERF-015: Critical failures SHALL trigger automated alerts

6. Data Requirements

6.1 User Data Model

> **DATA-001:** User records SHALL include: id, username, email, password_hash, role, created_at, is_active, last_login

> **DATA-002:** Profile data SHALL be stored as structured JSON with size limits

> **DATA-003:** Authentication events SHALL be logged with timestamp, user_id, ip_address, success/failure

> **DATA-004:** Session data SHALL include: session_id, user_id, expires_at, created_at

> **DATA-005:** All timestamps SHALL use UTC timezone

6.2 Data Integrity

> **DATA-006:** The system SHALL enforce referential integrity constraints

> **DATA-007:** User emails and usernames SHALL have unique constraints

> **DATA-008:** Database transactions SHALL be ACID compliant

> **DATA-009:** Data validation SHALL occur at both application and database levels

> **DATA-010:** The system SHALL implement data backup and recovery procedures

6.3 Data Privacy

> **DATA-011:** Personal data SHALL be classified and handled per privacy policies

> **DATA-012:** User consent SHALL be tracked for data processing activities

> **DATA-013:** Data retention periods SHALL be enforced automatically

> **DATA-014:** Data anonymization SHALL be implemented for analytics

> **DATA-015:** Cross-border data transfers SHALL comply with applicable laws

7. Integration Requirements

7.1 API Specifications

INT-001: The system SHALL provide RESTful API endpoints

INT-002: API responses SHALL use JSON format

INT-003: API authentication SHALL use JWT tokens

INT-004: API versioning SHALL be implemented in URLs

INT-005: Rate limiting SHALL be implemented for all API endpoints

7.2 External Services

INT-006: Email services SHALL be integrated for notifications

INT-007: The system SHALL integrate with CAPTCHA services

INT-008: LDAP/Active Directory integration SHALL be supported

INT-009: Single Sign-On (SSO) SHALL be supported via SAML/OAuth

INT-010: Audit logging SHALL integrate with SIEM systems

8. Compliance and Audit Requirements

8.1 Regulatory Compliance

COMP-001: The system SHALL comply with GDPR requirements

COMP-002: The system SHALL comply with CCPA requirements

COMP-003: SOC 2 compliance SHALL be maintained

COMP-004: Regular security assessments SHALL be conducted

COMP-005: Vulnerability scanning SHALL be performed monthly

8.2 Audit and Logging

COMP-006: All user actions SHALL be logged with sufficient detail

COMP-007: Security events SHALL be logged to immutable storage

COMP-008: Audit logs SHALL be retained for minimum 7 years

COMP-009: Log integrity SHALL be cryptographically verified

COMP-010: Audit reports SHALL be generated quarterly

9. Technical Specifications

9.1 Technology Stack

TECH-001: Backend SHALL use Node.js with Express framework

TECH-002: Database SHALL use PostgreSQL for production deployment

TECH-003: Session storage SHALL use Redis for scalability

TECH-004: Frontend SHALL use modern web standards (HTML5, CSS3, ES6+)

TECH-005: SSL/TLS certificates SHALL be managed automatically

9.2 Infrastructure Requirements

TECH-006: The system SHALL be deployable in container environments

TECH-007: Infrastructure SHALL support horizontal scaling

TECH-008: Load balancing SHALL distribute traffic across instances

TECH-009: Database replication SHALL be implemented for high availability

TECH-010: Monitoring and alerting SHALL cover all system components

10. User Experience Requirements

10.1 Interface Design

UX-001: The interface SHALL be responsive and mobile-friendly

UX-002: The system SHALL comply with WCAG 2.1 AA accessibility standards

UX-003: Form validation SHALL provide real-time feedback

UX-004: Error messages SHALL be user-friendly and actionable

UX-005: The interface SHALL support internationalization

10.2 Usability

UX-006: New user onboarding SHALL be intuitive and guided

UX-007: Password strength indicators SHALL be provided

UX-008: The system SHALL remember user preferences

UX-009: Help documentation SHALL be context-sensitive

UX-010: User feedback mechanisms SHALL be integrated

11. Testing Requirements

11.1 Security Testing

TEST-001: Penetration testing SHALL be conducted quarterly

TEST-002: Automated security scanning SHALL run with each deployment

TEST-003: SQL injection testing SHALL cover all database interactions

TEST-004: XSS testing SHALL cover all user input fields

TEST-005: Authentication bypass testing SHALL be performed

11.2 Performance Testing

TEST-006: Load testing SHALL simulate expected user volumes

TEST-007: Stress testing SHALL identify system breaking points

TEST-008: Endurance testing SHALL verify long-term stability

TEST-009: Database performance SHALL be tested under load

TEST-010: API response times SHALL be continuously monitored

11.3 Functional Testing

TEST-011: Unit tests SHALL achieve minimum 90% code coverage

TEST-012: Integration tests SHALL cover all API endpoints

TEST-013: End-to-end tests SHALL cover critical user workflows

TEST-014: Regression testing SHALL be automated

TEST-015: User acceptance testing SHALL validate requirements

12. Deployment and Maintenance

12.1 Deployment Requirements

DEPLOY-001: Blue-green deployment strategy SHALL minimize downtime

DEPLOY-002: Database migrations SHALL be reversible

DEPLOY-003: Configuration management SHALL support multiple environments

DEPLOY-004: Automated deployment pipelines SHALL include all testing phases

DEPLOY-005: Rollback procedures SHALL be tested and documented

12.2 Maintenance and Support

DEPLOY-006: 24/7 system monitoring SHALL be implemented

DEPLOY-007: Incident response procedures SHALL be documented

DEPLOY-008: Regular security updates SHALL be applied

DEPLOY-009: Performance optimization SHALL be ongoing

DEPLOY-010: Documentation SHALL be maintained current with system changes

13. Success Criteria

13.1 Acceptance Criteria

- All functional requirements SHALL be implemented and tested
- Security requirements SHALL pass independent security audit
- Performance requirements SHALL be verified under simulated load
- Compliance requirements SHALL be certified by qualified assessors
- User acceptance testing SHALL achieve 95% satisfaction rating

13.2 Go-Live Criteria

- Production infrastructure SHALL be fully operational
- All integration points SHALL be tested and functional
- Staff training SHALL be completed for all user roles
- Incident response procedures SHALL be activated
- Backup and recovery procedures SHALL be verified

Document Control

- **Author:** System Analyst
- **Reviewed By:** Security Team, Architecture Team
- **Approved By:** Project Sponsor
- **Next Review Date:** Annual or upon significant system changes

Change History

Version	Date	Author	Description
1.0	2025-09-22	System Analyst	Initial requirements specification