# Business Requirements Document (BRD)

## 1. Document Overview

### 1.1 Purpose

This document defines the business requirements for a **User Management System (UMS)**. The system will manage user identities, access, roles, and lifecycle events across applications in a secure, scalable, and auditable manner. The BRD serves as a shared understanding between business stakeholders, product owners, architects, and development teams.

### 1.2 Scope

The User Management System will provide centralized capabilities for: - User registration and onboarding - Authentication and authorization - Role and permission management - User profile and lifecycle management - Security, compliance, and auditing

The system may integrate with internal applications, third-party systems, and external identity providers.

### 1.3 Stakeholders

- Business Owners
- Product Management
- Security & Compliance Team
- IT Operations
- Application Development Teams
- End Users (Admins and Standard Users)

---

## 2. Business Objectives

- Establish a single source of truth for user identities
- Reduce security risks through standardized access control
- Improve user onboarding and access provisioning efficiency
- Enable compliance with regulatory and audit requirements
- Support scalability for future applications and users

---

## 3. Current State (As-Is)

- User accounts managed separately across multiple applications
- Inconsistent authentication and authorization mechanisms
- Manual user provisioning and deprovisioning
- Limited auditability and visibility into access changes
- Higher operational overhead and security risk

---

# 4. Target State (To-Be)

- Centralized User Management System
- Standard authentication protocols (e.g., OAuth 2.0, OpenID Connect)
- Role-based and attribute-based access control
- Automated user lifecycle management
- Centralized logging, auditing, and reporting

---

# 5. Business Requirements

## 5.1 User Registration & Onboarding

- The system shall allow users to be created manually by administrators.
- The system shall support self-service user registration (configurable).
- The system shall validate user identity information.
- The system shall support email and/or SMS verification.

## 5.2 Authentication

- The system shall support secure user login.
- The system shall support multi-factor authentication (MFA).
- The system shall support integration with external identity providers (e.g., LDAP, SSO providers).
- The system shall manage password policies (complexity, rotation, expiry).

## 5.3 Authorization

- The system shall support Role-Based Access Control (RBAC).
- The system shall allow assignment of multiple roles per user.
- The system shall support permission mapping to application resources.
- The system shall support attribute-based access rules (future extensibility).

## 5.4 User Profile Management

- The system shall allow users to view and update their profiles (based on permissions).
- The system shall store user attributes (name, email, status, roles, etc.).
- The system shall support custom attributes.

## 5.5 User Lifecycle Management

- The system shall support user activation and deactivation.
- The system shall support temporary suspension of users.
- The system shall support automated deprovisioning upon exit events.
- The system shall maintain historical user state changes.

## 5.6 Administration

- The system shall provide an administrative dashboard.
- The system shall allow administrators to manage users, roles, and permissions.
- The system shall support bulk user operations (import/export).

### 5.7 Audit & Compliance

- The system shall log all authentication and authorization events.
- The system shall log administrative actions.
- The system shall provide audit reports for compliance purposes.
- The system shall retain logs based on configurable retention policies.

### 5.8 Integration

- The system shall expose APIs for user and access management.
- The system shall integrate with internal applications.
- The system shall support standard identity protocols.

---

## 6. Non-Functional Requirements

### 6.1 Security

- Data shall be encrypted at rest and in transit.
- The system shall follow industry security best practices.
- The system shall protect against common threats (OWASP Top 10).

### 6.2 Performance

- The system shall support concurrent user authentication requests.
- Authentication response time shall meet defined SLAs.

### 6.3 Scalability

- The system shall scale horizontally to support growth in users and applications.

### 6.4 Availability

- The system shall support high availability.
- The system shall support disaster recovery mechanisms.

### 6.5 Usability

- The system shall provide a user-friendly interface for administrators and users.

---

## 7. Assumptions

- Users will access the system via web or integrated applications.
- Identity standards will be preferred over proprietary mechanisms.
- Security requirements will evolve over time.

---

## 8. Constraints

- Compliance with organizational security policies

- Budget and timeline limitations
- Integration dependencies with existing systems

---

## 9. Risks

- Integration complexity with legacy systems
- User adoption challenges
- Evolving regulatory requirements

---

## 10. Success Metrics

- Reduction in time to onboard/offboard users
- Decrease in access-related incidents
- Improved audit compliance scores
- Increased reuse across applications

---

## 11. Out of Scope

- Application-specific business logic
- Non-identity-related data management

---

## 12. Approval

| Name | Role | Signature | Date |
| --- | --- | --- | --- |
| | | | |