Functional Requirements Document (FRD)

1. Document Purpose

This Functional Requirements Document (FRD) translates the approved Business Requirements Document (BRD) into detailed, testable system behaviors. It defines **what the User Management System (UMS) must do**, without prescribing specific implementation technologies.

This document is intended for architects, developers, QA teams, and integration partners.

---

2. System Overview

The User Management System (UMS) is a centralized platform responsible for identity, authentication, authorization, and user lifecycle management across multiple applications and services.

The system will act as a **core identity capability** and expose functionality through UI and APIs.

---

3. Actors

- **End User** – An individual accessing applications via the UMS
- **Administrator** – Manages users, roles, and access policies
- **System Administrator** – Manages system-level configuration
- **External Application** – Consumes UMS services via APIs
- **External Identity Provider** – Provides federated authentication

---

4. Functional Requirements

4.1 User Registration

FR-UR-01: The system shall allow administrators to create users manually.

FR-UR-02: The system shall support self-service user registration when enabled.

FR-UR-03: The system shall validate mandatory user attributes during registration.

FR-UR-04: The system shall send verification messages (email/SMS) during registration.

FR-UR-05: The system shall prevent duplicate user identities based on unique identifiers.

4.2 Authentication

FR-AU-01: The system shall authenticate users using credentials or federated identity.

FR-AU-02: The system shall enforce configurable password policies.

FR-AU-03: The system shall support multi-factor authentication.

FR-AU-04: The system shall issue authentication tokens upon successful login.

FR-AU-05: The system shall support session termination and logout.

4.3 Authorization

FR-AZ-01: The system shall enforce Role-Based Access Control (RBAC).

FR-AZ-02: The system shall allow assignment of one or more roles to a user.

FR-AZ-03: The system shall associate permissions with roles.

FR-AZ-04: The system shall evaluate permissions during access requests.

FR-AZ-05: The system shall support policy extensibility for attribute-based rules.

4.4 User Profile Management

FR-UP-01: The system shall allow users to view their own profiles.

FR-UP-02: The system shall allow users to update permitted profile attributes.

FR-UP-03: The system shall allow administrators to update any user profile.

FR-UP-04: The system shall store standard and custom user attributes.

4.5 User Lifecycle Management

FR-UL-01: The system shall support user activation and deactivation.

FR-UL-02: The system shall support temporary user suspension.

FR-UL-03: The system shall automatically revoke access for deactivated users.

FR-UL-04: The system shall retain historical lifecycle state changes.

4.6 Role and Permission Management

FR-RP-01: The system shall allow administrators to create and manage roles.

FR-RP-02: The system shall allow administrators to create and manage permissions.

FR-RP-03: The system shall allow mapping of permissions to roles.

FR-RP-04: The system shall support bulk role assignment operations.

4.7 Administration & Configuration

FR-AD-01: The system shall provide an administrative dashboard.

FR-AD-02: The system shall allow configuration of authentication policies.

FR-AD-03: The system shall support bulk user import and export.

4.8 Audit & Logging

FR-AL-01: The system shall log all authentication attempts.

FR-AL-02: The system shall log authorization decisions.

FR-AL-03: The system shall log all administrative actions.

FR-AL-04: The system shall provide audit reports.

4.9 Integration & APIs

FR-IN-01: The system shall expose APIs for user management operations.

FR-IN-02: The system shall expose APIs for authentication and authorization.

FR-IN-03: The system shall support standard identity protocols.

FR-IN-04: The system shall support service-to-service access validation.

---

5. Error Handling Requirements

- The system shall return standardized error codes.
- The system shall log error events for troubleshooting.
- The system shall not expose sensitive information in error responses.

---

6. Data Requirements

- User data shall be stored with versioning where applicable.
- Sensitive data shall be protected according to security policies.
- Referential integrity shall be maintained between users, roles, and permissions.

7. Assumptions and Dependencies

- External identity providers will comply with standard protocols.
- Consuming applications will enforce tokens issued by the UMS.

8. Acceptance Criteria

- All functional requirements are traceable to test cases.
- Core user flows (register, login, authorize, deactivate) execute successfully.
- Audit logs are complete and immutable.

9. Out of Scope

- UI theming and branding
- Application-specific authorization logic

10. Approval

Name	Role	Signature	Date