OPTIMIZING USER,GROUP AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS

Project Documentation format

1. Document Overview

This section introduces the purpose and scope of the document. It explains that the FSD defines the functional behavior of the centralized access management system, including user management, role-based access control, group handling, workflow automation, and audit monitoring. It also identifies the intended audience such as developers, testers, project managers, and system administrators.

2. System Overview

This section provides a high-level description of the system. The proposed platform is a web-based centralized access governance solution that manages the complete user lifecycle and enforces secure authorization through RBAC and automated workflows. The system aims to reduce manual effort, improve security, and ensure compliance through audit tracking.

3. Functional Modules

The system is divided into the following major functional modules:

User Management Module handles user registration, profile updates, activation, deactivation, and search operations. It ensures that user lifecycle events are properly controlled and recorded.

Role and Group Management Module allows administrators to create roles, define permissions, create groups, and map users to groups. It supports permission inheritance to simplify large-scale administration.

Access Control Module enforces authentication and authorization. It validates user credentials, generates secure sessions, and checks permissions before granting access to protected resources.

Workflow Management Module automates the access request process. It routes requests to appropriate approvers, supports multi-level approvals, sends notifications, and maintains approval history.

Audit and Monitoring Module records all critical activities including logins, role changes, approvals, and permission updates. It provides reporting capabilities for compliance and security review.

4. Functional Requirements Description

Each function of the system is described with inputs, processing logic, and outputs. For example, when a user submits an access request, the system validates the request, determines the appropriate approver, routes the request through the workflow engine, updates the database, and notifies the user of the status. Similar detailed flows are defined for login, role assignment, and group management.

5. User Interface Requirements

This section defines how users interact with the system. The interface must be responsive, user-friendly, and role-aware. Administrators should have dashboards for managing users and roles, managers should have approval panels, and end users should have simple access request screens. Proper validation messages and navigation clarity must be maintained.

6. Security Requirements

The system must implement strong authentication, encrypted communication, secure session handling, and strict role-based authorization checks. Passwords must be stored securely, and all sensitive operations must be logged. The design must prevent unauthorized access and privilege escalation.

7. Reporting Requirements

The system should generate reports such as user access reports, role assignment reports, audit trails, and workflow history. Reports should be viewable on screen and downloadable for compliance purposes.

8. Assumptions and Dependencies

This section lists assumptions such as availability of network connectivity, trained administrators, and supported web browsers. Dependencies may include database servers, authentication services, and hosting infrastructure.

9. Acceptance Criteria

The system will be accepted when all functional modules operate correctly, workflows execute as expected, security controls are validated, and performance meets the defined thresholds. Successful completion of functional and security testing marks final acceptance.