Project Design Phase-II

Solution Requirements

Date	2-10-2025
Team ID	NM2025TMID07413
Project Name	Optimizing User, Group, and Role Management with Access Control and Workflows
Marks	4 Mark

Functional Requirements

1. User Account Management

The system should allow creating, updating, and deleting user accounts.

The system should automatically import or sync user data from the HR system.

2. Group Management

The system should enable grouping users based on department, project, or role.

Admins should be able to assign and modify group memberships easily.

3. Role Management

The system should define roles with specific access permissions.

Users should automatically receive roles based on job title or department.

4. Access Control

The system should implement Role-Based Access Control (RBAC).

It should restrict unauthorized users from accessing sensitive resources.

5. Workflow Automation

The system should route access requests through predefined approval workflows.

Admins or managers should receive notifications for pending approvals.

Approved requests should trigger automatic provisioning of access rights.

6. Audit and Reporting

The system should maintain an audit log of all access-related actions.

Reports should be generated for compliance and review purposes.

7. Authentication and Authorization

The system should support secure login mechanisms (e.g., SSO, MFA).

It should verify user identity before granting system access.

8. Self-Service Portal

Users should be able to request access or revoke access through a self-service interface.

The portal should display the status of access requests.

9. Notification System

The system should send email or dashboard alerts for approvals, denials, and access changes.

10. Integration Capabilities

The system should integrate with existing HR, IT, and application systems for seamless data flow.

Non-Functional Requirements

1. Performance

The system should process user access requests within 3 seconds.

It should support at least 1,000 concurrent users without performance degradation.

2. Scalability

The system should scale easily to accommodate growth in the number of users, roles, and applications.

It should support integration with new systems without major architectural changes.

3. Security

The system must use encryption (SSL/TLS) for all data transmissions.

It should support Multi-Factor Authentication (MFA) for user login.

Access to sensitive modules should be limited to authorized personnel only.

4. Availability

The system should maintain 99.9% uptime to ensure continuous access control operations.

It must have backup and disaster recovery mechanisms in place.

5. Usability

The user interface should be simple, intuitive, and easy to navigate for both users and admins.

Users should be able to complete common tasks (like access requests) without training.

6. Reliability

The system should ensure accurate and consistent access control operations.

No data loss should occur during workflow or integration processes.

7. Maintainability

The system should allow administrators to easily update workflows, roles, and permissions.

Regular system maintenance should not disrupt operations.

8. Auditability

All access and workflow activities must be logged and traceable for compliance audits.

Logs should be tamper-proof and retained for a defined retention period.

9. Interoperability

The system should support API-based integration with HR, ERP, and third-party applications.

It should be compatible with multiple operating systems and authentication protocols (e.g., LDAP, SAML).

10. Compliance

The system should comply with organizational policies and data protection laws such as GDPR or ISO 27001 standards.