INTRODUCTION

1. Project Objective

The main objective of this project is to create a secure and efficient system for managing users, groups, and roles with proper access control and automated workflows.

- To make user onboarding and offboarding simple and fast.
- To ensure only the right people get the right access (security).
- To automate workflows like access requests and approvals.
- To reduce manual work and chances of errors.
- To maintain compliance with organizational and legal standards.

2. Functional Requirements

The system should be able to do the following:

1. **User Management**
    - Add, update, and remove users.
    - Provide self-service options (like password reset).
2. **Group Management**

    - Create groups (e.g., department or project-based).
    - Assign permissions to groups.

3. **Role Management**
    - Define roles (Admin, Manager, User, Guest).
    - Assign permissions based on roles.
4. **Access Control**
    - Enforce authentication (username, password, MFA).
    - Ensure least-privilege access (only what is required).
5. **Workflow Automation**
    - Automate access requests (user requests → manager approval → access granted).
    - Auto-remove access when a user leaves or changes role.
6. **Security & Compliance**
    - Maintain audit logs of access changes.
    - Support periodic access reviews.

3. Technology Stack

- **Identity Management** → Azure Active Directory / Okta / Keycloak
- **Workflow Automation** → ServiceNow / Camunda / custom workflow engine
- **Programming Language** → Python / Java / JavaScript (for integration/customization)
- **Database** → MySQL / PostgreSQL / MongoDB (to store user and role data)
- **Authentication** → MFA, SSO (using OAuth 2.0, SAML, OpenID Connect)
- **Monitoring & Security** → SIEM tools like Splunk / ELK Stack for logging and auditing
- **Deployment** → Cloud-based (Azure / AWS) or On-premises