Project Document

S.no	Name	Email
1	CHOKKA VENKATESWARLU	chokkavenkateswarlu5@gmail.com
2	KOLLI LAKSHMI GAYATHRI	kolligayathri33@gmail.com
3	PULIBANDLA MALLIKARJUNA RAO	pulibandlamallikarjunarao@gmail.com
4	BONUMUKKALA SRINIVASAREDDY	sr8119799@gmail.com

Project Title

1. Project Overview

This project focuses on implementing access control for the **Project Table** within the ServiceNow platform to streamline operations for employees with the **"Employee Management"** role. The objective is to restrict access to specific fields, ensuring these employees focus solely on relevant fields. This customization will enhance **data security, operational focus, and usability** within the platform, aligning with the long-term organizational goal of improving **employee efficiency and data governance**.

2. Objectives

Business Goals

- Improve data governance by limiting access to sensitive fields.
- Enhance employee productivity by minimizing distractions from irrelevant information.
- Ensure compliance with organizational access control policies.

Specific Outcomes

- Hide predefined fields from employees with the **"Employee Management"** role.

- Implement granular access control through ServiceNow ACLs (Access Control Lists).
- Provide a user-friendly interface that reflects these access restrictions.

3. Key Features and Concepts Utilized

ServiceNow Table Customization: Customizing the **Project Table** to meet specific access control requirements.

Form Design: Ensuring a clean and accessible form interface for restricted users.

Access Control Lists (ACL): Configuring ACLs to enforce field-level security and limit access based on roles.

Data Models: Defining and associating the correct fields with the required roles.

Modules and Applications: Leveraging ServiceNow modules for streamlined access and navigation.

4. Detailed Steps to Solution Design

Step 1: Requirements Gathering

- Identify fields to be hidden.

- Define the roles affected by these restrictions.

Step 2: Data Model Configuration

- Map the **Project Table** data structure and identify sensitive fields requiring restriction.

Step 3: Access Control List (ACL) Configuration

- Navigate to **System Security > Access Control (ACL)**.
- Create new ACL rules for the **Project Table** fields:
    - Specify conditions to check for the **"Employee Management"** role.
    - Set access privileges to "read-only" or "hidden" for restricted fields.

5. Testing and Validation

Unit Testing

- Verify that ACL rules correctly enforce access restrictions for individual fields.

User Interface Testing

- Test the form interface to ensure fields are hidden as expected.
- Gather feedback from users under the restricted role to identify potential usability issues.

6. Key Scenarios Addressed by ServiceNow in the Implementation Project

- **Scenario 1**: An "Employee Management" user logs in and sees a customized Project table with restricted fields.
- **Scenario 2**: A manager logs in and accesses all fields without restriction.
- **Scenario 3**: Unauthorized users attempting to access hidden fields are denied.

7. Conclusion

This project successfully implemented access control for the **Project Table** using ServiceNow's customization capabilities and ACL rules. By restricting sensitive fields for the **"Employee Management"** role, the solution enhances security, ensures compliance, and supports organizational efficiency. Comprehensive testing validated the functionality and usability of the implemented solution.