# 1. Overview

Title: 1. Overview

Content:

This document outlines the design and architecture of the Salesforce solution to be developed. It covers key components including:

* Case Management: Implementation of Salesforce Service Cloud to manage case workflows and track progress through Case and Task objects.
* Business Rules: Utilization of Salesforce Flow and Process Builder to automate business processes and enforce rules within the Salesforce platform.
* User Interface: Design of user-friendly interfaces using Salesforce Lightning Components and Salesforce Lightning App Builder for seamless user interaction.
* Integration: Connecting various data sources and services using Salesforce Connect and APIs, along with AppExchange connectors for enhanced integration capabilities.
* Security: Implementation of role-based access control and data security measures within Salesforce using Profiles, Permission Sets, and Field-Level Security.
* Deployment: Strategies for deploying solutions using Salesforce Change Sets, Metadata API, and managing application lifecycle with Salesforce DevOps tools.

# 2. User Authentication

# User Authentication in Salesforce

## 1. Login

Authentication Method: Users will log in using their enterprise LDAP credentials integrated through Salesforce Identity or Single Sign-On (SSO) capabilities, leveraging Azure Active Directory (AAD) for seamless authentication.

## 2. Password Policy

Requirements:

* Minimum length: 8 characters
* Must include:
* At least one uppercase letter
* At least one lowercase letter
* At least one digit
* At least one special character

Implementation: This can be enforced by configuring the Salesforce password policies within the Setup menu under "Password Policies" to ensure that all user passwords meet these criteria.

## 3. Multi-Factor Authentication (MFA)

Verification Method: A One-Time Password (OTP) will be sent via email or SMS for additional verification.

Implementation: Configure Salesforce's built-in Multi-Factor Authentication settings to enable OTP delivery through both email and SMS. This can be set up within the "MFA" settings in the Setup menu.

## 4. Session Timeout

Configuration: Implement a session timeout of 15 minutes after inactivity.

Implementation: Use Salesforce's session settings to configure the timeout period for user sessions under "Session Settings" in the Setup menu, ensuring users are automatically logged out after the specified period of inactivity.

## 5. Account Lockout

Policy: User accounts will be locked after 5 failed login attempts.

Implementation: Implement this policy using Salesforce's built-in security settings to define the threshold for account lockout, which can be configured under "Login Access Policies" in the Setup menu to track login attempts and trigger account lockout after reaching the threshold.