# 1. Overview

#### Content:

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

* Case Management: Implementation of workflows in Power Automate to manage case processes and track progress.
* Business Rules: Utilization of Power Automate to automate business processes and enforce rules using triggers and actions.
* User Interface: While Power Automate does not directly manage user interfaces, it complements Power Apps by automating backend processes that enhance user interactions.
* Integration: Connecting various data sources and services using Power Automate connectors, enabling data flow across applications and services.
* Security: Implementation of role-based access control and data security measures within Power Automate, ensuring that only authorized users can execute flows and access data.
* Deployment: Strategies for deploying automated workflows using Microsoft Dataverse, along with managing the application lifecycle using ALM tools specific to Power Automate.

# 2. User Authentication

# Microsoft Power Automate Design: User Authentication

## 1. Login

Authentication Method:

* Users will authenticate using their enterprise LDAP credentials integrated with Azure Active Directory (AAD) for seamless authentication. This will be achieved by creating a flow that interacts with the Azure AD connector to validate user credentials.

## 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:

* Utilize Power Automate’s HTTP request trigger to receive registration data and apply validation logic within the flow to enforce the password policy before allowing user registration.

## 3. Multi-Factor Authentication (MFA)

Verification Method:

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

Implementation:

* Configure Azure Multi-Factor Authentication (MFA) settings in Azure AD and create a flow in Power Automate to send the OTP via email or SMS using connectors for Outlook and Twilio (or another SMS service).

## 4. Session Timeout

Configuration:

* Implement a session timeout of 15 minutes after inactivity.

Implementation:

* Although session management is primarily handled in Power Apps, you can create a flow in Power Automate that tracks user activity logs and triggers a logout process by invoking an API or updating a database record after the specified period of inactivity.

## 5. Account Lockout

Policy:

* User accounts will be locked after 5 failed login attempts.

Implementation:

* Create a Power Automate flow that monitors login attempts. Use a SharePoint list or a SQL database to track each user's failed attempts. When the count reaches 5, the flow will trigger an action to lock the account (e.g., updating a user status in the database or sending a notification to an admin).