# 1. Overview

Title: 1. Overview

Content:

This document outlines the design and architecture of the CustomTech solution to be developed. It encompasses key modules including incident management, business rules, user interface, integration, security, and deployment.

The design will leverage CustomTech's capabilities in IT Service Management (ITSM) to ensure efficient handling of incidents and requests, alongside implementing business rules for automation and decision-making. The user interface will be crafted to be intuitive and user-friendly, utilizing CustomTech's UI frameworks and design principles. Integration with external systems will be facilitated through CustomTech's Integration Hub and APIs, ensuring seamless data exchange. Security measures will adhere to best practices to protect sensitive information and comply with regulatory standards. Finally, deployment strategies will be discussed to ensure a smooth transition to the production environment.

# 2. User Authentication

Title: 2. User Authentication

Login: Users will authenticate using enterprise LDAP credentials integrated with CustomTech's LDAP authentication mechanism.

Password Policy: The password must have a minimum length of 8 characters and include at least one uppercase letter, one lowercase letter, one digit, and one special character. This policy will be enforced through CustomTech's security configuration settings.

Multi-Factor Authentication: Implement Multi-Factor Authentication (MFA) by utilizing CustomTech’s built-in capabilities to send One-Time Passwords (OTP) via email or SMS, providing an additional layer of verification during the login process.

Session Timeout: Configure a session timeout of 15 minutes of inactivity within the CustomTech security settings to enhance security.

Account Lockout: Establish account lockout policies to automatically lock the user account after 5 failed login attempts, configured through CustomTech’s security options.