# 1. Overview

\*\*Title: 1. Overview\*\*

\*\*Content:\*\*

This document outlines the design and architecture of the ServiceNow solution to be developed. It covers key modules including incident management, business rules, user interface, integration, security, and deployment. The focus will be on leveraging ServiceNow's capabilities to deliver efficient workflows, automate processes, and ensure a seamless user experience.

# 2. User Authentication

### Title: 2. User Authentication

#### Content:

\*\*Login:\*\*

Users authenticate using enterprise LDAP credentials integrated via ServiceNow's LDAP authentication feature.

\*\*Password Policy:\*\*

- 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

This can be enforced in ServiceNow by configuring the password policy under the "Password Policy" settings in the System Security module.

\*\*Multi-Factor Authentication:\*\*

Multi-factor authentication can be enabled in ServiceNow using the Multi-Factor Authentication (MFA) feature. An One-Time Password (OTP) will be sent via email or SMS for additional verification, which can be configured to work with an external provider or through ServiceNow’s native capabilities.

\*\*Session Timeout:\*\*

Set a session timeout of 15 minutes of inactivity by configuring the "Session Timeout" settings in the System Properties.

\*\*Account Lockout:\*\*

To implement an account lockout policy, ServiceNow can be configured to lock accounts after 5 failed login attempts. This can be managed through the security settings in the System Security module.

---

This design section provides a clear mapping of Pega's user authentication features to ServiceNow's capabilities, ensuring compliance with security standards and enhancing user security.