Software Requirements Specification (SRS) Document

July 24, 2025

Contents

1 Executive Summary

This Software Requirements Specification (SRS) document outlines the requirements for the development of a comprehensive inventory system. The system aims to provide a secure, scalable, and reliable solution for managing user accounts, roles, and access control. This document serves as a contract between the stakeholders and the development team, ensuring that the system meets the required standards and functionality.

2 Introduction

2.1 Purpose

The purpose of this SRS document is to provide a detailed description of the requirements for the development of the inventory system.

2.2 Scope

The scope of this project includes the development of a web-based inventory system that provides user authentication, role-based access control, and data encryption.

2.3 Definitions

- **System**: The inventory system to be developed.
- **User**: An individual who interacts with the system.
- **Administrator**: A user with elevated privileges to manage the system.

2.4 References

- Stakeholder Interview Notes
- Security Best Practices
- Data Quality Requirements

2.5 Overview

The system will be built using a web-based architecture and hosted on a cloud-based infrastructure. The system will provide a user interface to manage user accounts and roles, as well as a mechanism for users to reset their passwords.

3 Overall Description

3.1 Product Perspective

The system will be a web-based application that interacts with a centralized identity management system.

3.2 Product Functions

The system will provide the following functions:

- User authentication
- Role-based access control
- Data encryption
- Error handling and logging
- Data backup and disaster recovery

3.3 User Characteristics

The users of the system will be administrators and end-users. Administrators will have elevated privileges to manage the system, while end-users will have limited access.

3.4 Constraints

The system will be built using a web-based architecture and hosted on a cloud-based infrastructure.

3.5 Assumptions

- The system will be built using a web-based architecture.
- The system will be hosted on a cloud-based infrastructure.

4 Specific Requirements

4.1 Functional Requirements

4.1.1 REQ-001: User Authentication

The system shall authenticate user credentials against a centralized identity management system.

- **Description**: The system will verify user credentials against a centralized identity management system.
- **Inputs**: User credentials (username and password)
- **Outputs**: Authentication result (success or failure)
- **Processing Logic**: The system will use a secure authentication protocol to verify user credentials.
- **Business Rules**: The system will enforce a password policy that requires passwords to be changed every 90 days.
- **Exception Handling**: The system will display an error message if authentication fails.
- **Acceptance Criteria**: The system shall authenticate user credentials successfully.

4.1.2 REQ-002: Single Sign-On (SSO)

The system shall provide a single sign-on (SSO) capability for all authorized users.

- **Description**: The system will provide a single sign-on capability for all authorized users.
- **Inputs**: User credentials (username and password)
- **Outputs**: SSO token
- **Processing Logic**: The system will use a secure authentication protocol to generate an SSO token.
- **Business Rules**: The system will enforce a session timeout policy.
- **Exception Handling**: The system will display an error message if SSO fails.
- **Acceptance Criteria**: The system shall provide a single sign-on capability successfully.

4.1.3 REQ-003: Input Data Validation

The system shall validate user input data to prevent SQL injection attacks.

- **Description**: The system will validate user input data to prevent SQL injection attacks.
- **Inputs**: User input data
- **Outputs**: Validation result (success or failure)
- **Processing Logic**: The system will use a secure validation protocol to verify user input data.
- **Business Rules**: The system will enforce data validation rules.
- **Exception Handling**: The system will display an error message if validation fails.
- **Acceptance Criteria**: The system shall validate user input data successfully.

4.2 Non-Functional Requirements

4.2.1 NFR-001: Performance

The system shall respond to user requests within 2 seconds.

- **Description**: The system will respond to user requests within 2 seconds.
- **Measurable Criteria**: The system shall respond to user requests within 2 seconds.

4.2.2 NFR-002: Security

The system shall ensure that all data transmitted between the client and server is encrypted using TLS 1.2 or later.

- **Description**: The system will ensure that all data transmitted between the client and server is encrypted using TLS 1.2 or later.
- **Measurable Criteria**: The system shall ensure that all data transmitted between the client and server is encrypted using TLS 1.2 or later.

4.3 Interface Requirements

4.3.1 REQ-INT-001: User Interface

The system shall provide a user interface to manage user accounts and roles.

- **Description**: The system will provide a user interface to manage user accounts and roles.
- **Inputs**: User input (username, password, role)
- **Outputs**: User account and role information
- **Processing Logic**: The system will use a secure authentication protocol to manage user accounts and roles.
- **Business Rules**: The system will enforce a role-based access control policy.
- **Exception Handling**: The system will display an error message if user account or role management fails.
- **Acceptance Criteria**: The system shall provide a user interface to manage user accounts and roles successfully.

5 Appendices

5.1 Data Dictionary

- **User**: An individual who interacts with the system.
- **Administrator**: A user with elevated privileges to manage the system.
- **Role**: A set of privileges assigned to a user.

5.2 Traceability Matrix

REQ-ID	Source/Justification
REQ-001	Stakeholder Interview Notes, Section 3.1
REQ-002	Stakeholder Interview Notes, Section 3.2
REQ-003	Security Best Practices
...	...

5.3 Risk Analysis

The following risks have been identified:

- **Risk 1**: The system may not meet performance requirements.
- **Risk 2**: The system may not ensure data security.

5.4 Assumptions and Constraints

- **Assumptions**: + The system will be built using a web-based architecture. + The system will be hosted on a cloud-based infrastructure.
- **Constraints**: + The system shall be developed within 6 months. + The system shall be deployed on a cloud-based infrastructure.

6 Approval Signature Blocks

This SRS document has been approved by the following stakeholders:

- **Project Manager**: [Name]
- **Business Analyst**: [Name]
- **Technical Lead**: [Name]

7 Version Control Information

This SRS document is version 1.0 and was last updated on July 24, 2025.