2. SOFTWARE SPECIFICATION

This chapter outlines the system specifications, detailing user, and system requirements with a focus on the roles of warehouse manager, system administrator, and sales staff. The essential features are shown below.

2.1 User requirement		
2.1.1 Functional requirements	***2.1.1.1Warehouse Manager***	(1) View Inventory (2) Update Inventory
	2.1.1.2 System Administrator	(1) User Management (2) Data Integrity and Reconciliation
	2.1.1.3 Sales staff	(1) In-store Stock Inspection (2) Update Sales
2.1.2 Non-functional requirements	***2.1.2.1 Performance***	(1) Response Time (2) Scalability (3) Reliability
	2.1.2.2 Security	(1) Data Security (2) Authentication and Authorization (3) Data Encryption
	2.1.2.3 Reliability	(1) Backup and Recovery (2) Fault Tolerance
	2.1.2.4 Compliance	(1) Regulatory Compliance

2.2 System requirement		
2.2.1 Functional requirements	***2.2.1.1 Software Requirements***	(1) Operating System (2) Web Server (3) Database (4) Programming Languages (5) Frameworks and Libraries
	2.2.1.2 Network Requirements	(1) Internet Connection (2) Firewall (3) Data Encryption
	2.2.1.3 Security Requirements	(1) User Authentication (2) Role-Based Access Control (3) Data Backup (4) Security Updates
2.2.2 Non-functional requirements	***2.2.2.1 Performance***	(1) Response Time (2) Scalability (3) Reliability
	2.2.2.2 Security	(1) Data Security (2) Authentication and Authorization (3) Data Encryption
	2.2.2.3 Usability	(1) User Interface Design (2) Accessibility (3) Training and Support
	2.2.2.4 Maintainability	(1) Modular (2) Documentation (3) Version control

2.1 User requirement

2.1.1 Functional requirements

2.1.1.1 Warehouse Manager

(1) View Inventory

Warehouse manager shall be able to see the current inventory of furniture items.

(2) Update Inventory

Warehouse manager shall enable to add new inventory items, update quantities.

2.1.1.2 System Administrator

(1) User Management

The administrator shall have the access to add, remove, and manage user accounts within the system.

(2) Data Integrity and Reconciliation

The system shall ensure the accuracy and consistency of data by performing regular checks and

reconciliations.

2.1.1.3 Sales staff

(1) In-store Stock Inspection

Sales staff shall be able to check the availability of furniture items in the store.

(2) Update Sales

Sales staff shall able to record new sales transactions and update customer purchase records.

2.1.2 Non-functional requirements

2.1.2.1 Performance

(1) Response Time

The system should respond quickly to user interactions, especially for critical functions like inventory updates and sales transactions.

(2) Scalability

The system should be designed to handle an increasing number of users, data, and transactions without a significant drop in performance.

(3) Reliability

The system should be reliable, with minimal downtime and robust error handling mechanisms in place.

2.1.2.2 Security

(1) Data Security

The system should ensure that user data, inventory information, and sales records are
stored securely and avoid from unauthorized access.

(2) Authentication and Authorization

The system should implement strong authentication mechanisms to verify user identities and control access to different system functionalities based on user roles.

(3) Data Encryption

The system should encrypt sensitive data in transit and prevent data breaches during rest time.

2.1.2.3 Reliability

(1) Backup and Recovery

The system should implement regular data backups and has a robust recovery plan to prevent data loss in case of system failures.

(2) Fault Tolerance

The system should continue functioning even in the presence of hardware or software failures.

2.1.2.4 Compliance

(1) Regulatory Compliance

The system should comply with relevant data protection regulations and industry standards.

2.2 System requirement

2.2.1 Functional requirements

2.2.1.1 Software Requirements

(1) Operating System

The system should be compatible server such as Linux or Windows Server.

(2) Web Server

The system shall have web server software like Apache or Nginx to host the web application.

(3) Database

The system should have relational database management system (RDBMS) like MySQL, PostgreSQL,or SQL Server to store and manage data.

(4) Programming Languages

The system shall have programming languages like HTML, CSS, JavaScript for front-end development and languages like Python, PHP,or Java for back-end development.

(5) Frameworks and Libraries

The system should use of web development frameworks and libraries such as React, Angular,or Vuejs for front-end development and frameworks like Django or Nodejs for back-end development.

2.2.1.2 Network Requirements

(1) Internet Connection

The system shall be stable and high-speed internet connection for users to access the system.

(2) Firewall

The system should implement a firewall to protect the system from unauthorized access and cyber threats.

(3) Data Encryption

The system shall use encryption protocols such as HTTPS to secure data transmission over the network.

2.2.1.3 Security Requirements

(1) User Authentication

The system shall implement secure user authentication mechanisms such as password hashing, multi-factor authentication.

(2) Role-Based Access Control

The system shall assign specific access rights to users based on their roles to ensure data security and privacy.

(3) Data Backup

The system shall regularly back up data to prevent data loss in case of system failures or cyber attacks.

(4) Security Updates

The system shall keep software and system components up to date with the latest security patches to solve vulnerabilities.

2.2.2 Non-functional requirements

2.2.2.1 Performance

(1) Response Time

The system should respond to user interactions within an acceptable time frame to ensure a seamless

user experience.

(2) Scalability

The system should be able to handle an increasing number of users, transactions, and data without a significant decrease in performance.

(3) Reliability

The system should be reliable, with minimal downtime and robust error handling mechanisms in place.

2.2.2.2 Security

(1) Data Security

The system should ensure that user data, inventory information, and transaction records are securely stored and protected from unauthorized access.

(2) Authentication and Authorization.

Implement strong authentication mechanisms to verify user identities and control access to system functionalities based on user roles.

(3) Data Encryption

The system should encrypt sensitive data in transit and prevent data breaches during rest time.

2.2.2.3 Usability

(1) User Interface Design

The system should design an intuitive and user-friendly interface for easy navigation and efficient task completion.

(2) Accessibility

The system should ensure that users are accessible to the system.

(3) Training and Support

The system should provide manual and support resources to help users understand and use the system effectively.

2.2.2.4 Maintainability

(1) Modular

The system should design in a modular way to facilitate easier maintenance and future updates.

(2) Documentation

The system should provide comprehensive documentation for system administrators and users to understand system functionalities and configurations.

(3) Version control

The system should implement version control for the system code and configuration to track changes and facilitate rollback if needed.