# Non‑Functional Requirements Document: ERP/IMS for PineCone Pro Supplies

**Document Version:** 1.0  
**Prepared By:** [Your Name]  
**Date:** 27 September 2025

## 1 Purpose and Scope

This document defines the non‑functional requirements (NFRs) for the Enterprise Resource Planning and Inventory Management System (ERP/IMS) being implemented at PineCone Pro Supplies (PCS). While the Product Requirements Document specifies functional capabilities, this NFR document outlines the quality attributes—performance, availability, scalability, security and compliance—that the system must meet to support business objectives. The goal is to ensure that as PCS transitions from disparate spreadsheets to a unified ERP/IMS, the system is reliable, resilient and capable of supporting future growth.

## 2 Related Documents

* **Primary Feature List:** Describes the key functional capabilities required for the ERP/IMS【66184561068235†L0-L8】.
* **Product Requirements (MVP & Phase 2):** Provides functional requirements and initial non‑functional targets such as concurrent user load, latency, and uptime【91221083353783†L25-L33】【91221083353783†L14-L17】.

## 3 Performance Requirements

### 3.1 Concurrency and Throughput

The system must support up to **200 concurrent users** performing a mix of activities including order entry, inventory transactions, purchasing, reporting and administration【91221083353783†L25-L33】. Concurrency levels should scale linearly as new warehouses or sales channels are added. The system should handle at least **100 new sales orders per minute** without performance degradation during peak periods, reflecting the multi‑channel order volumes noted in the business scenario【91221083353783†L14-L17】.

### 3.2 Response Time and Latency

* **Order Processing:** The system shall process and commit each sales order (from validation through payment authorisation and stock reservation) in **≤ 2 seconds** on average【91221083353783†L25-L33】. Even during peak loads, the 95th percentile response time for order creation must not exceed **3 seconds**.
* **Inventory Updates:** Inventory transactions (receipts, transfers, picks, cycle counts, returns) must reflect in the system within **1 minute** of completion【91221083353783†L25-L33】. This ensures accurate available‑to‑promise and prevents oversells.
* **User Interactions:** Navigation between screens, saving master data records and running standard queries (e.g., product lookups) should respond in **≤ 1 second** for 90 % of interactions. Heavy analytics dashboards may take up to **3 seconds** but should display progressive loading indicators.
* **Reports & Batch Processes:** Batch jobs such as nightly inventory reconciliations, tax report generation or data exports must complete within **2 hours** to avoid impacting daily operations. User‑initiated reports should generate within **30 seconds** or provide asynchronous notification upon completion.

### 3.3 Scalability

The system must scale to support growth in SKUs, warehouses and channels. Currently PCS manages more than **12 000 SKUs** across multiple locations【91221083353783†L4-L8】; architecture must accommodate at least **50 000 SKUs** without major re‑engineering. Horizontal scaling (e.g., adding application nodes) should allow throughput to increase proportionally. Database design should partition data by company or warehouse to distribute load, and cloud resources should scale automatically based on CPU and memory utilisation. The modular architecture must support integration of Phase 2 modules (demand forecasting, promotion engine, light manufacturing) without downtime【91221083353783†L48-L52】.

### 3.4 Efficiency & Resource Utilisation

System components must optimise resource usage to minimise infrastructure costs while ensuring responsiveness. Memory utilisation should remain below **70 %** on average to allow for overhead and spikes. CPU utilisation should not exceed **80 %** during normal operations. Database queries must be indexed and optimised; expensive reports should be pre‑aggregated or executed off‑peak. Use caching for read‑heavy endpoints such as product catalog queries and price lookups. Client‑side applications should minimise network chatter by using batch APIs and local caching.

## 4 Availability & Service‑Level Objectives (SLOs)

### 4.1 Uptime Targets

PCS operates continuous e‑commerce, requiring high system availability. The ERP/IMS must achieve **99.9 % uptime** overall, equating to no more than **8.76 hours** of unplanned downtime per year【91221083353783†L25-L33】. Critical functions (order entry, inventory updates, purchasing, tax calculation) should be designed for **high availability (HA)** through load balancing, clustering and automated failover.

### 4.2 Business Continuity

* **Recovery Time Objective (RTO):** In the event of a system outage, recovery of core ERP/IMS functionality must occur within **1 hour** to ensure service‑level targets (e.g., shipping 95 % of orders within 24 hours) are maintained【91221083353783†L14-L17】.
* **Recovery Point Objective (RPO):** The system must restore data without more than **5 minutes** of data loss. Transactional data (orders, receipts, payments) must be replicated to a secondary site in real‑time.
* **Backup and Disaster Recovery:** Full backups must be taken nightly with point‑in‑time recovery enabled. Hot standby or multi‑region database replication should be employed to meet RTO/RPO. Disaster recovery plans must be tested twice annually.

### 4.3 Maintenance Windows

Planned maintenance should be scheduled outside peak business hours (e.g., weekends at 2 a.m. ET) and limited to **≤ 4 hours** per month. Where possible, updates should be performed in a rolling manner to avoid downtime. Users must be notified 48 hours in advance of scheduled maintenance.

### 4.4 Monitoring and Alerts

The system must provide real‑time monitoring of application health, database performance, message queues and integration points. Key metrics (CPU, memory, disk I/O, response times, error rates) must be collected and visualised. Alerts shall be configured for threshold breaches (e.g., response time > 2 seconds, database replication lag > 1 minute). On‑call engineers should receive notifications via email/SMS/Slack. Root‑cause analysis must be performed for any incidents impacting SLOs, and corrective actions documented.

## 5 Security and Compliance Requirements

Although the focus of this document is performance and availability, security and compliance are closely related to system reliability. PCS handles hazardous products and multi‑state taxes; thus compliance and data protection are vital.

### 5.1 Role‑Based Access Control (RBAC)

All modules must implement RBAC with fine‑grained permissions for functions such as product management, purchasing, order processing and financial reporting【91221083353783†L25-L33】. Users should be assigned roles (e.g., warehouse associate, CSR, purchasing lead, accountant, admin) with least‑privilege access. Changes to roles and permissions must be logged.

### 5.2 Data Privacy & Protection

Sensitive data (payment information, customer details, vendor terms) must be encrypted in transit (TLS 1.2+) and at rest (AES‑256). Passwords must be stored using salted hashing algorithms (e.g., Argon2). Access to production data should be restricted, and environment segregation (dev/test/prod) enforced. Audit trails must track user activity, including record creation, updates and deletions.

### 5.3 Regulatory Compliance

* **Hazardous Materials:** The system must support OSHA and DOT regulations for handling and shipping hazardous chemicals, including Material Safety Data Sheet (MSDS) tracking and hazmat documentation【91221083353783†L29-L31】. Rules regarding permitted carriers, quantity limits and placarding must be enforced.
* **Tax & Audit:** Sales tax must be calculated and filed correctly for North Carolina and prepared for additional states (Virginia, South Carolina)【91221083353783†L36-L38】. Audit logs must be retained for at least **7 years** to satisfy regulatory requirements.
* **Data Retention:** Customer and transaction data must be retained according to legal requirements (minimum **7 years** for financial records). Data disposal processes must be implemented.

## 6 Reliability and Integrity

### 6.1 Data Accuracy

Inventory accuracy must be maintained at or above **98 %** as measured by cycle counts and reconciliations【91221083353783†L25-L33】. The system shall implement validation rules, double‑entry transactions and exception handling to prevent data corruption. Concurrency controls (optimistic locking, versioning) must ensure consistent updates when multiple users edit the same records.

### 6.2 Error Handling and Graceful Degradation

The system must handle external failures (e.g., payment gateway downtime, carrier API errors) gracefully, providing clear messages to users and retrying operations where appropriate. In the event of partial failures, the system should degrade functionality while preserving core capabilities (e.g., allow order entry even if tax service is temporarily unavailable, with tax recalculated later).

### 6.3 Testing and Quality Assurance

Non‑functional requirements must be validated through load testing, failover testing and security penetration tests. Performance tests should simulate peak loads with realistic data volumes. Continuous integration/continuous deployment (CI/CD) pipelines should include automated regression tests and environment configuration checks.

## 7 Maintainability and Support

### 7.1 Modularity and Configurability

The ERP/IMS should follow a modular architecture with well‑defined interfaces for each module (PIM, inventory, order management, purchasing, finance). Business rules (e.g., reorder point thresholds, tax rates, promotions) must be configurable without code changes. Clear documentation should describe configuration options and extension points. Source code should follow industry standards with sufficient comments to aid maintenance.

### 7.2 Observability and Logging

Comprehensive logging is essential for troubleshooting and auditability. Logs must capture user actions, API requests/responses and system events with timestamps. Log levels (info, warn, error) should be configurable. Logs must be centralised and searchable; sensitive data should be redacted.

### 7.3 Support and Incident Management

An incident management process should be established with defined severity levels, escalation paths and communication channels. Post‑incident reviews must include root‑cause analysis and action items. Support teams must have access to monitoring dashboards, logs and runbooks. A knowledge base should provide answers to common issues and troubleshooting steps.

## 8 Environmental and Operational Constraints

* **Integration Dependencies:** The ERP/IMS integrates with external systems such as e‑commerce platforms, Amazon marketplace, POS, payment gateways and carriers. Availability of these third‑party services may affect overall performance and must be monitored. The system should implement retries and fallbacks when external APIs are unavailable.
* **Hardware/Infrastructure:** Deployment will be cloud‑based to leverage auto‑scaling and HA features. Data centres must meet Tier III standards and maintain redundant power, networking and cooling. Network bandwidth must be sufficient to support data replication and API calls.
* **User Environment:** The system must support modern browsers (Chrome, Firefox, Edge, Safari) and responsive UI design for tablets and desktop. RF scanners used in warehouses must integrate seamlessly and continue operating offline with local caching, synchronising when connectivity is restored.

## 9 Compliance with Service‑Level Agreements

To ensure that the ERP/IMS meets contractual commitments, service‑level agreements (SLAs) and service‑level objectives (SLOs) must be defined, monitored and enforced. Key SLAs include:

| Metric | Target | Rationale | Reference |
| --- | --- | --- | --- |
| **Order shipping SLA** | 95 % of orders shipped within 24 h (business days) | Aligns with the functional requirement to fulfil orders quickly【91221083353783†L14-L17】 | Service‑level target |
| **Inventory accuracy** | ≥ 98 % | Reduces oversells and stockouts【91221083353783†L25-L33】 | SLO for reliability |
| **System uptime** | ≥ 99.9 % | Ensures availability for multi‑channel operations | Non‑functional target |
| **Concurrent users** | Support ≥ 200 users | Allows growth while maintaining responsiveness【91221083353783†L25-L33】 | Capacity planning |
| **Tax accuracy** | 100 % compliance | Avoids fines and supports multi‑state expansion【91221083353783†L36-L38】 | Compliance requirement |

## 10 Assumptions and Dependencies

This document assumes that:

1. Network connectivity between warehouses, 3PLs and cloud infrastructure is reliable and redundant.
2. Third‑party services (payment gateways, tax engines, carrier APIs, EDI connections) provide SLAs that are consistent with PCS’s SLOs.
3. Users will receive adequate training and adopt new workflows; change management will address resistance.
4. Data migration from legacy systems will be completed before go‑live, with data cleansed to meet accuracy requirements.
5. The accounting system and other integrated platforms support real‑time or near‑real‑time APIs for synchronisation【91221083353783†L25-L33】.

## 11 Risks and Mitigation

* **Integration Failure:** Complex integrations (e‑commerce, Amazon, POS, 3PL, accounting) might introduce latency or failure points. Mitigation: use robust API middleware, implement retry logic and monitor external services.
* **Infrastructure Limitations:** Under‑provisioned infrastructure could lead to poor performance. Mitigation: conduct capacity planning and load testing; leverage auto‑scaling.
* **Regulatory Changes:** New tax rules or hazmat regulations could require system modifications. Mitigation: design flexible tax and compliance modules; establish a process to monitor regulatory updates.
* **Security Breaches:** Data breaches could impact customer trust and result in fines. Mitigation: employ strong encryption, RBAC, penetration testing and regular security audits.
* **Data Quality Issues:** Inaccurate data from legacy systems or vendors could undermine reliability. Mitigation: implement validation rules, data cleansing and vendor scorecards【91221083353783†L19-L23】.

*End of Document*