# Role‑Based Access Control (RBAC) Matrix & Permissions Document

**Document Version:** 1.0  
**Prepared By:** [Your Name]  
**Date:** 28 September 2025

## 1 Purpose and Scope

This document defines the Role‑Based Access Control (RBAC) matrix for PineCone Pro Supplies’ new ERP/Inventory Management System (ERP/IMS). RBAC restricts system access based on user roles rather than individual identities, ensuring that employees access only the information they need to do their jobs【752228629016174†L121-L132】. By associating permissions with roles instead of users, the organization simplifies audits, enforces least‑privilege principles and protects sensitive data【752228629016174†L121-L135】. The scope of this document encompasses all core modules of the ERP/IMS identified in the business case—product information management, inventory and warehouse control, order management, purchasing and vendor management, lot/expiry and serial tracking, shipping, returns, tax and accounting integration, and analytics【91221083353783†L4-L45】.

## 2 RBAC Principles and Methodology

RBAC assigns access permissions to users based on roles that reflect job functions and responsibilities【752228629016174†L120-L132】. A role is a predefined set of permissions; users are granted one or more roles, and roles bind users to specific privileges【752228629016174†L140-L144】. The following principles guide PCS’s RBAC implementation:

1. **Least Privilege:** Each role should grant the minimum level of access necessary to perform required tasks【752228629016174†L121-L135】. Access to create, edit, approve or delete data is restricted to those whose job requires it.
2. **Separation of Duties:** Critical functions—such as ordering inventory and approving purchase orders—are split across multiple roles to reduce fraud and errors.
3. **Top‑Down and Bottom‑Up Role Definition:** Roles should be defined both top‑down (from business goals) and bottom‑up (from analysis of how users access systems)【866495138654908†L528-L541】. Business managers identify functional access needs, while IT analyses existing usage patterns to refine roles.
4. **Principle of Least Privilege Mapping:** After analysing the workforce and inventory of resources, permissions are mapped to roles according to least privilege【866495138654908†L528-L541】.
5. **Governance and Policy:** A decision‑making body must maintain roles, policies, risk‑management strategies, and re‑evaluation guidelines【866495138654908†L549-L564】.
6. **Periodic Review:** Roles, permissions and assignments must be reviewed regularly—at least annually—to ensure they align with evolving business needs and to avoid role explosion【866495138654908†L585-L599】.

## 3 Roles and Responsibilities

The table below summarises the primary roles within PCS and their core responsibilities. These roles reflect the personas defined in the product requirements and should serve as the basis for access control.

| Role | Description & Responsibilities | Key Modules |
| --- | --- | --- |
| **Owner/General Manager (GM)** | Oversees business performance, approves high‑value purchases, reviews dashboards and financial reports; has final authority on policy changes and user roles. | All modules (read); Purchasing/Vendor approval; Accounting; Analytics |
| **Operations Manager** | Manages warehouse operations, slotting strategies, cycle counts and carrier performance. Oversees shipping, inventory adjustments and cross‑dock operations. | Inventory & Warehouse; Shipping & Rate Shopping; Returns; Analytics |
| **Purchasing Lead** | Maintains vendor relationships, manages MOQs and lead times, creates and approves purchase orders within limits, analyses demand forecasts and vendor performance. | Purchasing & Vendor Management; Inventory (view); Lot/Serial (view); Accounting (view) |
| **Warehouse Associate (RF)** | Executes receiving, put‑away, picking, cycle counts and return inspections via RF devices. Handles lot/serial capture, bin transfers and cross‑dock shipments. | Inventory & Warehouse; Lot/Serial; Shipping; Returns |
| **Customer Service Representative (CSR)** | Handles customer interactions, edits orders, initiates RMAs, processes refunds and communicates order status. | Order Management; Returns/RMA; Shipping (view); Analytics (view) |
| **E‑Commerce Manager** | Manages product catalog and pricing, coordinates promotions and channel synchronisation across the web store, B2B portal, POS and Amazon. Oversees product data quality and unit conversions. | Product Information Management; Order Management (view); Analytics |
| **Accountant** | Oversees financial reconciliation, tax filings and journal exports. Handles AR/AP, revenue recognition, bank reconciliation and tax compliance. | Accounting Integration; Tax & Reporting; Purchasing (view); Order Management (view) |
| **IT Administrator** | Manages system configuration, user provisioning, role assignments and integrations. Maintains security policies, data backups and disaster recovery. | All modules (administrative); Security & RBAC configuration |
| **Auditor / Read‑Only User** | Reviews system data for compliance and audit purposes without making changes. | All modules (read only) |

## 4 Modules and Functional Areas

PCS’s ERP/IMS is composed of the following modules. Each module corresponds to a set of permissions that can be granted independently. The descriptions below reference the primary features document【91221083353783†L4-L45】.

| Module | Description | Source |
| --- | --- | --- |
| **Product Information Management (PIM)** | Centralised master data management for 12 000+ SKUs, including kits/bundles, unit conversions, hazardous classifications and pricing【91221083353783†L4-L7】. Ensures consistent product data across the web, B2B portal, POS and Amazon. | Primary Feature【91221083353783†L4-L7】 |
| **Inventory & Warehouse Control** | Tracks stock across multiple warehouses (Greensboro DC, Charlotte cross‑dock, Reno 3PL) with bin/zone management, RF scanning and cycle counts to achieve 98 % inventory accuracy【91221083353783†L9-L12】. | Primary Feature【91221083353783†L9-L12】 |
| **Order Management & Payments/Fraud** | Orchestrates B2B and B2C orders from web, portal, POS and Amazon, including payment processing and fraud screening; meets a sub‑24‑hour service‑level target for 95 % of orders【91221083353783†L14-L17】. | Primary Feature【91221083353783†L14-L17】 |
| **Purchasing & Vendor Management** | Provides vendor scorecards, handles MOQs and lead‑time data, automates POs using reorder points and EOQ, and supports ASN receiving and drop‑ship【91221083353783†L19-L23】. | Primary Feature【91221083353783†L19-L23】 |
| **Lot/Expiry & Serial Tracking** | Tracks lot numbers and expiration dates for finishing chemicals and serial numbers for high‑value tools to enable recalls and warranty/service management【91221083353783†L25-L27】. | Primary Feature【91221083353783†L25-L27】 |
| **Shipping & Rate Shopping** | Integrates with carriers to compare shipping rates, manage hazmat documentation and support cross‑dock/3PL workflows【91221083353783†L29-L31】. | Primary Feature【91221083353783†L29-L31】 |
| **Returns/RMA Workflow** | Provides a standardised returns process with disposition codes (restock, refurbish or scrap) to improve inventory accuracy【91221083353783†L32-L34】. | Primary Feature【91221083353783†L32-L34】 |
| **Tax Calculation & Reporting** | Automates county‑level sales tax for North Carolina and prepares for multi‑state expansion; manages hazardous‑materials compliance and audit trails【91221083353783†L36-L38】. | Primary Feature【91221083353783†L36-L38】 |
| **Basic Accounting Integration** | Synchronizes general ledger, accounts payable and accounts receivable so that financials, purchasing and sales feed the same ledgers【91221083353783†L40-L41】. | Primary Feature【91221083353783†L40-L41】 |
| **Operational Analytics & Alerts** | Provides dashboards and alerts for key performance indicators such as cycle‑count accuracy, order fulfilment times, vendor performance and tax liabilities【91221083353783†L44-L45】. | Primary Feature【91221083353783†L44-L45】 |

## 5 Permissions Matrix

The matrix below specifies the level of access that each role has to each module. Permissions are defined as follows:

* **N** – No Access: Cannot view data or perform actions in the module.
* **R** – Read Only: Can view data and run reports but cannot create or modify records.
* **C** – Create/Edit: Can create, edit and delete records within the module but cannot approve high‑value transactions.
* **A** – Approve: Can approve transactions (e.g., purchase orders, returns) and perform administrative actions such as changing status, releasing holds or finalising reconciliations.
* **F** – Full Control: Full access including create/edit, approve, delete, configure and manage settings.

| Module | Owner/GM | Ops Mgr | Purchasing Lead | Warehouse Associate | CSR | E‑Comm Mgr | Accountant | IT Admin | Auditor |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PIM** | R | R | R | N | R | F | R | F | R |
| **Inventory & Warehouse** | R | F | R | C | R | R | R | F | R |
| **Order Management** | A | C | R | R | C | R | R | F | R |
| **Purchasing & Vendor Mgmt** | A | R | F | N | N | R | R | F | R |
| **Lot/Expiry & Serial** | R | F | R | C | R | R | R | F | R |
| **Shipping & Rate Shopping** | R | F | R | C | C | R | R | F | R |
| **Returns/RMA Workflow** | A | C | R | C | C | R | R | F | R |
| **Tax Calculation & Reporting** | A | R | R | N | N | R | F | F | R |
| **Basic Accounting Integration** | A | R | R | N | N | R | F | F | R |
| **Operational Analytics & Alerts** | F | F | R | R | R | F | F | F | R |

### Matrix Explanation

* **Owner/GM:** Holds approval authority for purchasing, returns and financial operations. Mostly reads system data but can approve and override where necessary.
* **Operations Manager:** Has full control over inventory, warehouse and shipping modules, including creating and editing records. Reads purchasing and accounting data to plan operations.
* **Purchasing Lead:** Manages vendors and purchase orders end‑to‑end. Can create, edit and approve POs (within delegated authority), view inventory levels and analytics, but cannot edit orders or product data.
* **Warehouse Associate:** Restricted to operational tasks—receiving, picking, counting, shipping and returns. Cannot modify master data or financial records.
* **Customer Service Representative:** Focuses on order adjustments and customer returns; cannot create POs or modify product data.
* **E‑Commerce Manager:** Manages product catalog and promotions; has full access to PIM and analytics. Reads orders and inventory to ensure online stock accuracy.
* **Accountant:** Maintains financial records and tax reporting; has full control over accounting and tax modules, read access to other modules for reconciliation.
* **IT Administrator:** Administers the system and security; has full control across modules but should not be involved in day‑to‑day transactions.
* **Auditor:** Has read‑only access across all modules for compliance and audit purposes.

## 6 Separation of Duties and Approval Workflows

To mitigate risks of fraud and error, the RBAC matrix enforces separation of duties. For example, the Warehouse Associate can receive goods and record inventory transactions but cannot create purchase orders or approve them. The Purchasing Lead can create and edit POs but high‑value POs require approval by the Owner/GM. CSRs can initiate RMAs but cannot approve refunds; approvals are handled by the Accountant or Owner/GM. The IT Administrator configures the system but is not permitted to approve operational transactions, preventing abuse of superuser privileges.

## 7 Governance and Review

Effective RBAC requires an ongoing governance process. PCS should establish a committee of business managers, IT administrators and compliance officers to oversee roles and permissions. This body should maintain project priorities, risk‑management strategies and re‑evaluation guidelines【866495138654908†L549-L564】. Roles should be reviewed at least annually to identify unnecessary privileges, overlapping assignments and role explosion【866495138654908†L585-L608】. Audits of access logs and user feedback can highlight when roles need adjustment. As the business introduces new modules or processes—such as Phase 2 enhancements (forecasting, promotions, kitting, 3PL integration, customer service console and EDI)【91221083353783†L48-L51】—roles and permissions must be updated accordingly.

## 8 Legend

| Code | Meaning |
| --- | --- |
| **N** | No Access – user cannot view or interact with data in the module |
| **R** | Read Only – user can view data, run queries and reports |
| **C** | Create/Edit – user can create, edit and delete records |
| **A** | Approve – user can approve transactions and perform administrative actions |
| **F** | Full Control – user can configure, create, edit, approve and delete within the module |

## 9 Future Considerations

As PCS expands the ERP/IMS in Phase 2, additional roles (e.g., Forecasting Analyst, Promotions Manager, Light Manufacturing Supervisor, 3PL Liaison, Customer Service Console Agent, EDI Coordinator) may be required. The principles outlined in this document—least privilege, separation of duties, governance and review—should guide the creation of new roles. For dynamic or temporary access needs, consider complementing RBAC with attribute‑based access control (ABAC) policies to handle evolving infrastructure【866495138654908†L620-L636】.

*End of Document*