Flux POS & Inventory System

Roles & Permissions Matrix

Applies to: Phase 0 (Walking Skeleton) + Phase 1 (Trimmed MVP)

Date: 2026-02-01

Purpose: Define what each user role can do in Flux. This prevents confusion during development, testing, and real-world use. Permissions are enforced using (1) application rules and (2) Supabase Row Level Security (RLS) scoped by location_id.

Primary roles in Phase 0/1: Owner (Super Admin), Store Manager, Cashier.

Optional role included for completeness: Auditor (read-only). If you decide not to implement Auditor in Phase 0/1, treat this column as Future.

1. Role Definitions

Owner (Super Admin): Full system access. Can see and manage multiple branches/locations, global settings, and all operational modules.

Store Manager: Runs day-to-day operations for a single branch/location: masters, GRN, transfers, stock adjustments, basic reports, and user management inside their branch.

Cashier: POS-focused user. Can create and post sales, search/select customers, and view sales-only information. Restricted from sensitive stock operations.

Auditor (Read-only): View-only access for review and checking. No create/edit/post actions. Scope can be per branch (recommended) or cross-branch if the Owner grants it.

2. Permission Legend

Code	Meaning
ALLOW	User can perform the action.
VIEW	User can only view/search/read. No create/edit/post/delete.
COND	Allowed only with limits or approval (examples: discount limit, void requires manager override, credit limit enforcement).
DENY	Not allowed.

3. Security Enforcement Notes (How Flux enforces this)

Application RBAC: The UI hides and blocks actions outside the user's role. **Database RLS:** All business rows are scoped by location_id so users cannot access other branches. Owner (Super Admin) can be allowed cross-branch access by RLS policy using a JWT claim role = 'super_admin' (recommended).

4. Phase 0 Permissions Matrix (Walking Skeleton)

Phase 0 proves: login, offline-ready PWA shell, core masters, and simple POS sales with safe sync.

Capability / Action	Owner (Super Admin)	Store Manager	Cashier	Auditor
Authentication: log in / log out	ALLOW	ALLOW	ALLOW	ALLOW
Select active location (branch)	ALLOW	ALLOW (own branch)	ALLOW (own branch)	VIEW (assigned)
Locations (branches): create/edit/deactivate	ALLOW	DENY	DENY	VIEW
User management: create/disable/reset users	ALLOW (all branches)	ALLOW (own branch)	DENY	VIEW
Assign user role (Owner/Manager/Cashier)	ALLOW	DENY	DENY	VIEW
Masters - Categories: create/edit/delete	ALLOW	ALLOW (own branch)	DENY	VIEW
Masters - Units: create/edit/delete	ALLOW	ALLOW (own branch)	DENY	VIEW
Masters - Items: create/edit/delete (incl. barcode)	ALLOW	ALLOW (own branch)	DENY	VIEW
POS - Search items, build bill	ALLOW	ALLOW	ALLOW	VIEW
POS - Create sale invoice (draft)	ALLOW	ALLOW	ALLOW	DENY
POS - Post/Finalize sale	ALLOW	ALLOW	ALLOW	DENY
POS - Apply discount	ALLOW	COND (policy)	COND (policy)	DENY
POS - Void/Cancel sale	ALLOW	COND (manager approval)	DENY	DENY
Sales-only reports (today sales, invoice list)	ALLOW (all branches)	ALLOW (own branch)	VIEW (sales-only)	VIEW
Export/Download reports	ALLOW	COND (policy)	DENY	VIEW

Phase 0 constraints (important)

- Cashier must not change inventory masters or perform stock operations. - All actions are restricted by location_id (branch isolation). - Offline sync status is stored only on the client (IndexedDB queue), not inside server tables.

5. Phase 1 Permissions Matrix (Trimmed MVP)

Phase 1 adds: Customers (incl. credit), Purchasing (GRN), Stock Transfers, Batch/Expiry (lots), Stock Adjustments, and basic inventory reporting.

Capability / Action	Owner (Super Admin)	Store Manager	Cashier	Auditor
Customers: create/edit/delete	ALLOW	ALLOW (own branch)	DENY	VIEW
Customers: search/select in POS	ALLOW	ALLOW	ALLOW	VIEW
Set credit terms (credit limit/days)	ALLOW	ALLOW (own branch)	DENY	VIEW
Credit sale: create invoice with customer_id	ALLOW	ALLOW	ALLOW (within limits)	DENY
Credit limit enforcement (block/override)	ALLOW	ALLOW (override)	COND (no override)	DENY
Purchasing - GRN: draft	ALLOW	ALLOW (own branch)	DENY	VIEW
Purchasing - GRN: post (updates stock)	ALLOW	ALLOW (own branch)	DENY	DENY
Manage lots/batches on GRN (batch no + expiry)	ALLOW	ALLOW (own branch)	DENY	VIEW
Stock transfers: create (from -> to)	ALLOW	ALLOW (own branch)	DENY	VIEW
Stock transfers: receive (confirm inbound stock)	ALLOW	ALLOW (own branch)	DENY	VIEW
Stock adjustments: create (reason + lines)	ALLOW	ALLOW (own branch)	DENY	VIEW
Stock adjustments: post (updates stock)	ALLOW	COND (policy/limits)	DENY	DENY
Inventory reports: stock on hand, low stock	ALLOW (all branches)	ALLOW (own branch)	DENY	VIEW
Expiry reports/warnings (lot expiry)	ALLOW (all branches)	ALLOW (own branch)	DENY	VIEW
Transfer reports (in/out history)	ALLOW (all branches)	ALLOW (own branch)	DENY	VIEW
GRN reports (supplier purchases)	ALLOW (all branches)	ALLOW (own branch)	DENY	VIEW
Audit log viewing	ALLOW (all branches)	ALLOW (own branch)	DENY	VIEW

Phase 1 conditional rules (examples you should implement as simple policies)

1) Discount policy: set a max discount percentage for Cashier; Manager/Owner can override. 2) Void policy: Cashier cannot void; Manager can void within allowed window; Owner can always void. 3) Stock adjustment policy: only Manager/Owner can post adjustments; optionally require Owner approval above a threshold.

6. RLS Scoping Rules (must be true for every query and write)

- Every master and transactional table includes location_id (branch isolation). - Store Manager and Cashier: can only read/write rows where location_id equals their assigned location. - Owner: can read/write all locations (policy based on JWT role claim). - Auditor: read-only, scoped by assigned location (recommended).