# Insurance Distribution — Login & Role Management

## 1. Overview

A secure, standalone authentication and role-management system for an insurance distribution platform. Primary goals:

- Provide admin-created user accounts with role-based access.
- Support a default role-based sales hierarchy plus the ability to customize reporting lines.
- Enforce strong security (MFA, password policies, account lockout) and maintain full audit trails for compliance.
- Support both web and mobile (responsive web / mobile apps).
- Provide org-chart visualization, role-specific dashboards, and exportable reporting & analytics by role/branch/region.

## 2. Objectives & Success Metrics

**Objectives** - Securely authenticate users and protect data with MFA and strong password rules. - Enable managers to view and manage their downline and sales hierarchy. - Provide clear visibility rules so users only see permitted data. - Produce actionable analytics and exportable reports.

**Success metrics** - < 0.5% unauthorized access incidents per year. - MFA adoption > 98% for all active users within 1 month of launch. - Admin onboarding time for new user $\leq$ 2 minutes. - Report export usage rate (CSV/PDF) > 30% among managers.

## 3. Primary Users & Personas

- **Agent** — sells policies, views own performance, sees immediate supervisor.
- **Head of Branch** — manages agents within branch, views branch-level analytics.
- **Training Admin** — manages training records, training-related users visibility.
- **Manager, Business Development (MBD)** — manages team, views regional performance, can update reporting lines.
- **Senior Manager, Business Development (SMBD)** — oversees multiple managers/regions; full visibility of their downline.
- **System Admin** — full system visibility; creates users, assigns roles, overrides lockouts, configures settings.

## 4. Roles & Permissions (high-level)

Permissions are built around the sales hierarchy and can be scoped by branch/region.

- **Agent**

- View/modify own profile
- View own performance and personal reports

- Submit sales activity (leads, opportunities)

- **Head of Branch**

- All Agent permissions for their branch
- View branch reports and org chart

- Edit reporting lines for staff within their branch (if permitted)

- **Training Admin**

- View training statuses for users within scoped branches/regions

- Assign and track training

- **Manager, Business Development**

- View/manage direct reports and their performance
- Propose changes to reporting lines (subject to approval if configured)

- Access manager dashboard and export reports

- **Senior Manager, Business Development**

- All MBD permissions across multiple regions

- Full visibility across their downline

- **System Admin**

- Create/disable users
- Assign roles and branches
- Full visibility and audit access
- Configure security settings (password policy, MFA options, lockout thresholds)

## 5. Hierarchy Model

- Default is **role-based hierarchy** (SMBD -> MBD -> Head of Branch -> Agent).
- Hierarchy is **customizable**: Admins (and scoped managers where allowed) can assign reporting lines manually to reflect real-world exceptions.
- Support for **multiple branches and regions**; users belong to a branch and optionally to a region.
- Visibility rules: users see/manage only their downline and scoped peers unless role has full visibility.

## 6. Org Chart & Visualization

- Interactive org chart (tree/graph) with zoom, expand/collapse nodes, search by name/ID, and drag-to-reassign (admin only).
- Click a node to view user details, performance snapshot, and actions (edit role, reassign manager, view reports).
- Export org chart as PNG/PDF.

## 7. Authentication & Security

- Standalone authentication (no SSO).
- Admin-created accounts only (no self-registration).
- Password policy (industry best practices):
- Minimum 8–12 characters (configurable)
- Must include uppercase, lowercase, number, symbol
- Block common/leaked passwords
- Optional expiration (configurable) and reuse prevention
- Configurable **account lockout** after N failed attempts (default: 5) with time-based unlock and admin override.
- **MFA (configurable per user)**: choices include SMS OTP, email OTP, and authenticator app (TOTP). Users select preferred method at first login or admin forces a default method.
- MFA enforced at first login and optionally for sensitive actions (role change, hierarchy edit, export).
- IP and device logging for security monitoring.

## 8. Audit & Compliance

- Full audit trail for:
- Logins (success/failure, timestamp, IP, device)
- Role assignments and role changes (who changed, before/after, timestamp)
- Hierarchy changes (old manager/new manager, who made change)
- MFA enrollment and verification attempts
- Report exports and data access events
- Audit logs are exportable and immutable (write-once storage with retention policy configurable by admin).

## 9. Dashboards & Reporting

- Role-based dashboards (different default dashboards per role) with configurable widgets.
- Built-in analytics for sales performance by user/role/branch/region and time range.
- Common metrics: policies sold, premium volume, conversion rate, pipeline value, training completion.
- Report filters: role, branch, region, team, custom date ranges.
- Exports: CSV, Excel (.xlsx), PDF. Scheduled exports (daily/weekly) available to managers and admins.
- Access controls on exports: only roles with permission may export sensitive data.

## 10. Mobile & Web

- Responsive web app for browsing and management.
- Mobile-first design for agents (lightweight views for sales entry, personal dashboard).
- Native app-ready APIs (if mobile app will be native later).

## 11. Admin Workflows

- Admin creates user: select role, branch, manager, contact info, provisional password, MFA requirement.
- Onboarding email (secure link) for initial password set and MFA enrollment.
- Admin dashboard: bulk user upload (CSV), bulk role/branch changes, account deactivation/reactivation.
- Approvals: optional workflow for hierarchy change approvals (configurable on/off).

## 12. Integrations & APIs

- RESTful API endpoints for authentication, user management, hierarchy CRUD, audit logs, and reporting exports.
- Webhooks for critical events (user created, role changed, hierarchy changed, failed login threshold reached).
- Data export endpoints for BI tools.

## 13. Data Model (high level)

- User: id, name, email, phone, role_id, branch_id, region_id, manager_id, status, created_at, last_login
- Role: id, name, permissions (scoped)
- Branch: id, name, region_id
- Region: id, name
- HierarchyChangeAudit: id, user_id, old_manager_id, new_manager_id, changed_by, timestamp
- AuthAudit: id, user_id, event_type, ip, device, timestamp, meta
- Reports/Exports: id, created_by, type, filters, created_at

## 14. Non-functional Requirements

- **Availability**: 99.9% SLA for auth and hierarchy services.
- **Performance**: auth response < 500ms; org chart rendering for up to 5,000 nodes within acceptable UX limits (pagination/virtualization for very large organizations).
- **Scalability**: horizontally scalable services and stateless auth endpoints.
- **Security**: data encrypted at rest and in transit (TLS), secrets stored in vault.
- **Compliance**: support for audit retention policies, GDPR-friendly data deletion workflows.

## 15. Acceptance Criteria (examples)

- Admin can create a new user and assign role/branch/manager; user receives onboarding email and completes MFA enrollment.

- A manager can view a paginated org chart of their downline and export a CSV of their team's performance.
- System enforces password rules and locks account after 5 failed attempts; admin can unlock.
- All role and hierarchy changes appear in audit logs with before/after values and user who made the change.

## 16. Roadmap & Phases

**Phase 1 (MVP)** - Admin user creation - Authentication (password + configurable MFA) - Role assignment and basic hierarchy (role-based + manual overrides) - Role-based dashboards (basic) - Audit logging for core events

**Phase 2** - Org chart visualization + drag-to-reassign (admin) - Reporting & analytics (basic reports) + export (CSV/XLSX) - Branch/region support and scoped visibility

**Phase 3** - PDF export for org chart and reports - Scheduled exports & webhooks - Advanced analytics, filters, and KPI widgets

## 17. Risks & Mitigations

- **Risk**: MFA delivery (SMS) unreliable in certain regions.
  **Mitigation**: Offer multiple MFA options (TOTP, email) and allow admin to enforce preferred methods.

- **Risk**: Very large orgs may make org chart slow.
  **Mitigation**: Use virtualization, server-side pagination, and summary nodes for collapsed branches.

- **Risk**: Sensitive data export misuse.
  **Mitigation**: Access controls on export, export audit logs, and rate limits.

## 18. Next Steps

1. Review and confirm roles & permissions matrix in detail (map every action to role).
2. Prioritize MVP features and agree on Phase 1 scope.
3. Design UI wireframes for admin flows, org chart, and role dashboards.
4. Prepare API spec and data migration plan (if existing user data exists).

---

*Prepared for:* Insurance Distribution Platform — Login & Role Management *Prepared by:* Product Requirements Document Writer