Phase 10: Security & Access Control – SmartPropertyPortal

Objective

To implement robust, role-based access control across SmartPropertyPortal using Salesforce's declarative and automated security features. This ensures that users interact only with the data relevant to their role, while protecting sensitive fields and enabling scalable sharing.

Deployment Summary

Role Hierarchy Configuration

- Created custom roles:
- `Portal Admin` → Full access to all records and dashboards
- `Lead Manager` → Access to all buyer leads and agent assignments
- `Sales Agent` → Access limited to owned or shared properties and appointments
- Roles were added under appropriate parent roles to enable upward visibility

Impact: Enabled record-level visibility and reporting hierarchy for agents and managers.

Public Groups Setup

- Defined groups:
- `Assigned Agents` → Used for sharing appointments and property records
- `Lead Reviewers` → Used for sharing high-interest leads with analysts
- Groups included users by role and profile for dynamic access control

Impact: Simplified sharing rule targeting and workflow alerts.

Permission Sets

- Created modular permission sets:
- `Property Manager Access` → Full CRUD on Property__c
- `Appointment Viewer` → Read-only access to Appointment__c
- `Lead Analyst Access` → View/export Lead__c data
- Assigned via manual mapping and automated policies

Impact: Decoupled access from profiles, enabling flexible user provisioning.

Sharing Rules

- Configured object-level sharing:
- `Property__c`: Shared "Available" records with `Sales Agent` role
- `Appointment__c`: Shared records with `Assigned Agents` group
- `Lead__c`: Shared "High Interest" leads with `Lead Reviewers` group

Impact: Automated record visibility based on business criteria.

Field-Level Security

- Restricted sensitive fields:
- `Price` field hidden from `Sales Agent` profile
- `Buyer Contact` field set to read-only for non-admins
- Configured via profile-level field access and page layout controls

Impact: Protected sensitive financial and personal data from unauthorized access. ---

User Access Policies (Automated Assignment)

- Created policies to auto-assign:
- `Property Manager Access` to users with role = `Portal Admin`
- `Lead Reviewers` group to users with title = “Analyst”
- Used filters based on role, title, and department

Impact: Reduced manual provisioning and ensured consistent access control.

Session & Login Security

- Set session timeout to 30 minutes for agent-level users
- Restricted login IP ranges for internal users
- Enabled audit trail for login history and access attempts

Impact: Strengthened org-level security and compliance posture.

THANK YOU