Preventing Unauthorized Access to Customer Data

Phase	1A
Author	Shahrukh Ahmed
Document Status	COMPLETE

Objectives:

1. **Objective 1**: Ensure only relationship managers can view financial details (transactions).
2. **Objective 2**: Ensure agents only see customer records (transactions) assigned to them.

Assumption 1: Basic Profile Permissions with View All Access

Configurations

1. **Profiles**:
   - **Relationship Manager Profile**:
     - **Object Permissions**: `View All`, `Read`, `Edit` on the `Transaction` object.
     - **Field-Level Security**: Full access to all fields.
   - **Agent Profile**:
     - **Object Permissions**: `Read` on the `Transaction` object (no `View All`, `Read`).
     - **Field-Level Security**: Hide sensitive financial fields (e.g., `Amount`, `Payment_Details`).
2. **Organization-Wide Defaults (OWD)**:
   - Set `Transaction` object to **Private**.
   - Enable **Grant Access Using Hierarchies**.
3. **Role Hierarchy**:
   - Relationship Managers are placed **above** Agents in the hierarchy.
4. **Sharing Model**:
   - Agents can only view records where they are the **Owner**.

Outcomes

- **Objective 1**:
  - Managers see all transactions due to `View All` permission (overrides OWD).
- **Objective 2**:
  - Agents see only records they own.

Assumption 2: Record Types and Sharing Rules

Configurations

1. **Profiles**:
   - **Relationship Manager Profile**:
     - **Object Permissions**: `Read`, `Edit` (no `View All`).
     - **Field-Level Security**: Access to all fields.
   - **Agent Profile**:
     - **Object Permissions**: `Read` (no `Edit` or `Delete`).
     - **Field-Level Security**: Hide financial fields.
2. **Record Types**:
   - Create two record types for the `Transaction` object:
     i. **Financial** (visible only to managers).
     ii. **Customer** (visible to agents).
3. **Organization-Wide Defaults (OWD)**:
   - Set `Transaction` object to **Private**.
   - Enable **Grant Access Using Hierarchies**.
4. **Sharing Rules**:
   - **For Managers**:
     - **Rule Name**: `Share Financial Transactions to Managers`.
     - **Criteria**: `Record Type = Financial`.
     - **Access Level**: `Read/Edit`.

Outcomes

- **Objective 1**:
  - Managers see all `Financial` record type transactions via sharing rules.
- **Objective 2**:
  - Agents see only `Customer` record type transactions assigned to them.

Assumption 3: Restrict Agents to See Only Custom Transactions

Configurations

1. **Profiles:**
   - **Relationship Manager Profile:**
     - Full access to both **Financial** and **Custom** Transactions.
   - **Agent Profile:**
     - Access restricted to **Custom Transactions** only.
     - Financial fields are hidden via **Field-Level Security (FLS)**.

2. **Organization-Wide Defaults (OWD):**
    - `Transaction__c` is controlled by its parent (`Account`) due to **Master-Detail** relationship.
    - `Account` is **Private**, ensuring transactions are only accessible through account-level sharing.
3. **Record Types:**
    - **Financial Transactions** → Only visible to Relationship Managers.
    - **Custom Transactions** → Accessible by both Managers and Agents.
4. **Restriction Rule:**
    - Applied to **Agents** to limit access to only **Custom Transactions**, even if transactions are shared through hierarchy or manual sharing.
5. **Field-Level Security (FLS):**
    - Financial fields are hidden from Agents.

Outcomes

- **Objective 1:**
    - **Managers retain full access** to all transactions, including **Financial** and **Custom** records.
- **Objective 2:**
    - **Agents can only see Custom Transactions**, even if they have access to the parent Account.
    - **Financial Transactions remain hidden** in List Views, Reports, and SOQL queries.

Assumption 4: Validation Rule for Financial Records

Configurations

1. Either Assumption 1, 2, and 3 can be implemented with this validation. If a financial record is mistakenly assigned to an agent, this validation will prevent it.
2. **Validation Rule**:
    - **Rule Name**: `Prevent_Agent_Assignment_To_Financial_Records`.
    - **Formula**:

    ```
    AND(
      $User.Profile.Name = "Customer Service Agent",
      RecordType.DeveloperName = "Financial"
    )
    ```

    - **Error Message**: "Agents cannot be assigned to financial transactions. Contact a Relationship Manager."

Outcomes

- Blocks agents from being assigned to `Financial` record type transactions.