Preventing Unauthorized Access to Customer Data

Phase	1A
Author	Shahrukh Ahmed
Document Status	COMPLETE

- Objectives:
- Assumption 1: Basic Profile Permissions with View All Access
  - Configurations
  - Outcomes
- Assumption 2: Record Types and Sharing Rules
  - Configurations
  - Outcomes
- Assumption 3: Master-Detail Relationship with Account
  - Configurations
  - Outcomes
- Assumption 4: Validation Rule for Financial Records
  - Configurations
  - Outcomes

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 or are assigned via `OwnerId`.

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: Master-Detail Relationship with Account

Configurations

1. **Profiles**:
   - **Relationship Manager Profile**:
     - **Transaction Field-Level Security**: Access to all fields.
   - **Agent Profile**:
     - **Object Permissions**: `Read` (no `Edit` or `Delete`).
     - **Transaction Field-Level Security**: Hide financial fields.

2. **Organization-Wide Defaults (OWD) for Account**:
    - Set `Account` object to **Private**.
    - Enable **Grant Access Using Hierarchies**.
3. **Data Model**:
    - **Account-Transaction Relationship**:
        - Create a **Master-Detail** relationship between `Account` (parent) and `Transaction` (child).

Outcomes

- **Objective 1**:
    - Financial transactions inherit restrictions from `Account` (accessible only to managers).
- **Objective 2**:
    - Agents see transactions only if they have access to the parent `Account` but wont see financial fields

---

Assumption 4: Validation Rule for Financial Records

Configurations

1. Either Assumption 1 or 2 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.