# Lab Exercise 9 – Security & Governance

### Objective

By the end of this lab, you'll be able to:

- Create and assign **Permission Sets** for Data Cloud access.
- Apply **Field-Level Security (FLS)** to sensitive fields.
- Classify fields using **Data Classification Tags** (sensitivity & compliance).
- View and export **Setup Audit Trail** to monitor configuration changes.
- Understand Salesforce Data Cloud's **AI Tagging & Policy-Based Governance concepts**.

### Step 1: Open Setup and Create a New Permission Set

1. Click the **gear icon → Setup**.
2. In the left search bar, type **"Permission Sets"** and open it.
3. Click **New Permission Set**.
4. Fill in details:

    - **Label:** Data Cloud Restricted Access
    - **API Name:** auto-fills
    - **User License:** choose Salesforce (or Data Cloud Admin if available).
    - **Description:** *Grants access to Data Cloud objects with restricted field visibility*.

5. Click **Save**.

**Step 2: Assign Object Permissions**

1. Within the Permission Set, under **Apps** → **Object Settings**, click **Data Model Objects (DMOs)**.
   - For example, choose **Individual**, **Engagement Event**, or **Customer**.
2. Click the object name, then **Edit**.
3. Enable:
   - **Read** Access → checked
   - **Create/Edit/Delete** → unchecked (for minimal read-only access).
4. Click **Save**.

**Step 3: Apply Field-Level Security (FLS) to a Sensitive Field**

1. Still inside the same Permission Set, scroll down and click **Field Permissions**.
2. Locate a sensitive field such as Email, MobilePhone, or SSN (if available in your DLO/DMO).
3. Click **Edit**.
4. Adjust access:

- **Read Access:** checked
- **Edit Access:** unchecked

5. For fields like SSN or CreditCardNumber, uncheck both Read and Edit Access.
6. Click **Save**.

*This simulates masking sensitive PII for users without data clearance.*

**Step 4: Assign the Permission Set to a User**

1. From the Permission Set detail page, click **Manage Assignments → Add Assignments**.
2. Select your user record and click **Assign**.
3. Click **Done**.
4. Log out and back in (or use another test user) to verify the field restrictions take effect.

**Step 5: Validate Restricted Field Visibility**

1. Open **Data Explorer → Individual DMO**.
2. Attempt to preview records as the user with restricted access.
3. You should notice the sensitive field (e.g., Email or SSN) is **hidden** or not editable.

**Result:** You've successfully implemented FLS through a Permission Set and verified its impact within Data Cloud.

**Hands-on 5.2 — Classify Fields for Governance (Sensitivity & Compliance Tags)**

**Step 1: Open Field Definition**

1. From **Setup**, go to **Object Manager → Individual** (or Customer DMO).
2. Click **Fields & Relationships**.
3. Select a field such as Email or Phone.

**Step 2: Add Data Classification Tags**

1. In the field detail view, scroll down to the **Data Classification** section.
2. Click **Edit**.
3. Assign values:
    - **Data Sensitivity Level:** Confidential
    - **Data Owner:** Sales Ops or Data Governance Team
    - **Compliance Category:** PII (Personal Identifiable Information)
4. Click **Save**.

*These tags help governance teams enforce AI policies and comply with GDPR/CCPA.*

**Step 3: View AI Tagging & Policy-Based Governance (Conceptual Preview)**

1. Go to **Data Cloud Setup → Governance Workspace** (if available in DE).
2. Explore "**AI Tagging**" or "**Policy Management**" sections (read-only in Developer Edition).

3. Observe how Data Cloud labels fields automatically based on sensitivity and usage.

**Result:** You've tagged fields for sensitivity and compliance, making your Data Cloud model governance-ready.

**Hands-on 5.3 — View and Export Setup Audit Trail**

**Step 1: Open Setup Audit Trail**

1. Click **Setup → Quick Find:** View Setup Audit Trail.
2. Click the link to open the **Audit Trail History page**.
3. Review entries for recent activities — you should see items like:

   - *Created Permission Set*
   - *Updated Field-Level Security*
   - *Changed Data Classification Tags*

**Step 2: Export Audit Trail to File**

1. At the top of the page, click **Download Setup Audit Trail**.
2. A .CSV file will download containing the last 6 months of changes.
3. Open it in Excel or Google Sheets and review columns:

   - Action, Section, Created By, Date and Time, Client IP.

4. Filter by your username to see your own changes.

**Result:** You've viewed and exported Setup Audit Trail entries for monitoring system activities — key for governance and compliance.

**Expected Outcomes**

- Understand and apply Permission Set and FLS controls to Data Cloud objects.
- Tag sensitive fields with data classification for governance.
- Retrieve and analyze Setup Audit Trail records.
- Recognize AI tagging and policy management concepts for enterprise-grade governance.