**Phase 2: Org Setup & Configuration**

**Project: Phishing Awareness Training Tracker**

**Objective**

The objective of this phase was to configure the Salesforce Developer Edition org for the project. This included setting up company details, defining user roles, assigning profiles, configuring security with OWD and sharing rules, and verifying that the data visibility model works as expected.

**Dev Org Setup**

A Salesforce **Developer Edition** org was provisioned for the project. This edition provides access to custom objects, flows, Apex, dashboards, and Agentforce, which are sufficient for development and testing.

**Company Profile Setup**

* **Company Name:** Phishing Awareness Tracker
* **Default Time Zone:** Asia/Kolkata (GMT +05:30)
* **Default Locale:** English (India)
* **Default Currency:** INR

A screenshot of a computer

AI-generated content may be incorrect.

**User Setup, Roles & Profiles**

* **Roles Created:**
  + CEO (root)  
      ↳ HR  
       ↳ Security  
        ↳ Manager  
         ↳ Employee

A screenshot of a computer

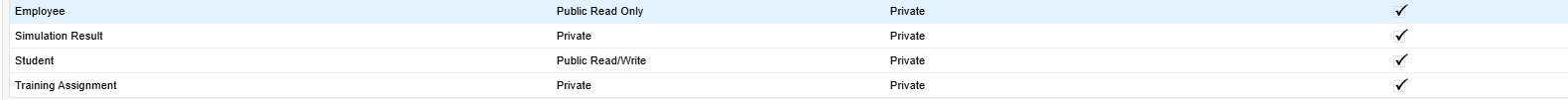
AI-generated content may be incorrect.

* **Users Created:** One user for each role (Employee, Manager, HR, Security) for testing record visibility.
* **Profiles:** For simplicity, **Standard User** profile was assigned to all roles.



**OWD & Sharing Rules**

* **Organization-Wide Defaults:**
  + Employee → Public Read Only
  + Training Assignment → Private
  + Simulation Result → Private



* **Sharing Rules:** Configured so that Managers can access Training Assignments and Simulation Results owned by their direct reports.

A screenshot of a computer

AI-generated content may be incorrect.

**Login Access Policies**

Enabled *“Administrators Can Log in as Any User”* to allow testing of visibility and permissions under different roles.

**Deployment**

Since the project uses a Developer Edition org, changes will be deployed using an **Unmanaged Package** if needed in the future.