**Smart Expense Tracker**

**PHASE 9: REPORTING, DASHBOARDS & SECURITY REVIEW**

**1. Reports (Tabular, Summary, Matrix, Joined)**

Various reports were created to analyze expenses and provide actionable insights.

**Implementation:**

* **Tabular Reports:** Generated simple lists, such as all expenses submitted in the last 7 days.
* **Summary Reports:** Grouped expenses by **Category** and **Status** to track spending patterns and approvals.
* **Matrix Reports:** Analyzed expenses by **Vendor** vs. **Month** to identify high-spending vendors over time.
* **Joined Reports:** Combined multiple report types to compare **Employee expenses vs. Finance approvals**.

**2. Report Types**

Custom report types were defined to meet cross-object reporting requirements.

**Implementation:**

* Created report types linking **Users, Expense\_\_c, and Expense\_Report\_\_c** to generate insights across employees and reports.

**3. Dashboards**

Dashboards were built to visualize expense trends and support decision-making.

**Implementation:**

* Displayed **Total Expenses by Month, Top 5 Vendors, and Category-wise Spending**.
* Included **pie charts, bar graphs, and tables** for quick financial analysis.

**4. Dynamic Dashboards**

Dynamic dashboards were configured to provide personalized views for different roles.

**Implementation:**

* **Employees:** View only their own expenses and totals.
* **Finance Team:** View all employee expenses and pending approvals.
* **Admins:** Access consolidated dashboards for overall monitoring.

**5. Sharing Settings**

Organization-wide sharing settings were configured to protect expense records.

**Implementation:**

* **Private** access for Expense\_\_c to ensure employees see only their own expenses.
* **Sharing Rules** created for managers and finance teams to access team-related expenses.

**6. Field Level Security**

Sensitive financial fields were restricted based on user roles.

**Implementation:**

* Fields like Amount\_\_c and Status\_\_c visible only to Finance Team and Admins.
* Employees could view and edit only their own expense details.

**7. Session Settings**

Session security settings were enforced to maintain system integrity.

**Implementation:**

* Enabled session timeout and re-login after inactivity.
* Enforced password complexity rules to strengthen user security.

**8. Login IP Ranges**

IP restrictions were applied for controlled system access.

**Implementation:**

* Allowed employees and finance staff to log in only from secure office networks or authorized VPNs.

**9. Audit Trail**

Audit trail was enabled to maintain accountability.

**Implementation:**

* Logged all administrative actions, configuration changes, and expense record updates.
* Provided transparency for compliance and audits.