Phase 9: Reporting, Dashboards & Security Review

Goal: To create meaningful reports and dashboards for monitoring parking slot utilization and to perform a security review ensuring that system data remains protected and accessible only to the right users.

Step 1: Creating Reports

- Navigated to **Reports tab** in Salesforce.
- Built custom reports for:
    1. **Slot Utilization Report** – shows how many hours each slot is occupied vs free.
    2. **Reservations by Employee Report** – lists reservations made by each employee.
    3. **Reservations by Department Report** – helps manager analyze departmental parking usage.
- Saved reports in a **“Parking Reports” folder** for easy access.

Outcome: Managers can track utilization and employees’ booking patterns.

Step 2: Defining Custom Report Types

- Created a **Custom Report Type**:
    - Primary Object: Parking Slot
    - Related Object: Reservation
- This allows generating combined reports like:
    - Slot utilization by employee.
    - Which slots are most/least booked.

Outcome: Flexible reporting capability across Parking Slots and Reservations.

Step 3: Building Dashboards

- Created a **Slot Utilization Dashboard** with components:

  - Pie Chart: Slots Available vs Reserved.
  - Bar Graph: Reservations per Department.
  - Gauge: Overall Slot Occupancy %.
- Created a **Manager's Dashboard** with components:
  - Line Chart: Daily reservations trend.
  - Table: Top 5 most used slots.
- Added dashboards to **Home Page Layout** for real-time monitoring.

Outcome: Visual insights for quick decision-making.

Step 4: Configuring Dynamic Dashboards

- Enabled **Dynamic Dashboards** so that:
  - Employees see only their own reservations.
  - Managers see reservations of all employees.
- Restricted dashboard data visibility using roles & sharing settings.

Outcome: Personalized dashboard experience for each user type.

Step 5: Reviewing Sharing Settings

- **Parking Slot Object:** Set to **Public Read Only** – everyone can view slots.
- **Reservation Object:** Set to **Private** – only owner and manager can view details.
- Configured **Sharing Rules** so that security staff can see necessary reservations.

Outcome: Data is shared only with relevant users, protecting employee privacy.

Step 6: Applying Field-Level Security

- Restricted access to sensitive employee information (like Employee ID).
- Ensured that only HR/Admin roles can see personal details.

- Employees and Security Staff see only necessary booking info.

Outcome: Prevents unnecessary exposure of confidential employee data.

Step 7: Session & Login Security

- Configured **Session Timeout** to 30 minutes of inactivity.
- Set **Login IP Ranges** so that access is allowed only from company's office network.
- Enabled **Two-Factor Authentication** for Managers and Admins.

Outcome: Prevents unauthorized system access from outside the organization.

Step 8: Security & Audit Trail

- Enabled **Audit Trail** in Salesforce to track all changes in configuration.
- Reviewed user activity logs to ensure compliance.
- Verified that all critical operations (like reservation approvals) are logged.

Outcome: Full visibility into system usage and configuration changes.

Final Output of Phase 9

✓ **Reports created** for slot utilization, employee, and department analysis.
✓ **Dashboards built** for managers and employees with real-time updates.
✓ **Dynamic Dashboards** ensure personalized data views.
✓ **Sharing & Field-Level Security** implemented to protect data.
✓ **Session, IP Restrictions & Audit Trail** strengthen system security.