Green Energy Usage Monitor - Phase 2

Phase 2 Completion Document

Step 1: Define Clear Role Requirements

The first step was to define what each role—Manager, Technician, and Customer—should be able to do within the Salesforce system.

- The Manager has full access to manage all operations, approve user requests, and view detailed reports.
- The Technician has access specifically to maintenance-related tasks and updates on technical issues to carry out their responsibilities effectively.
- The Customer is given limited access, primarily to view their own data and submit or view service requests related to their accounts.

Step 2: Create or Confirm Profiles for Each Role

For these roles, profiles were created or confirmed in Salesforce by cloning standard profiles and customizing them:

- The Standard User profile was cloned and customized for the Manager and Technician roles to adjust access and permissions accordingly.
- A limited profile similar to the Customer Community User was cloned or created for the Customer role to restrict access strictly to appropriate data and functionality. These profiles act as templates that govern user permissions and accessibility aligned with their respective roles.

Step 3: Assign Object Access Permissions for Standard Objects

Since no custom objects were created, the focus was on standard Salesforce objects.

- Managers were given full Create, Read, Update, and Delete (CRUD) permissions on Accounts, Contacts, Cases, and Tasks/Events to manage customer data and business operations fully.
- Technicians received read-only permission on Account records, limited read and edit access on related Contacts, and read/edit access for assigned Cases and Tasks to handle maintenance efficiently.

- Customers were restricted to read only their own Accounts, allowed to read and edit their own Contact records, and permitted to create and view their own Cases, with minimal or no access to Tasks.

Step 4: Configure Field-Level Security

Field-level security was reviewed and configured to protect sensitive data across objects such as Account, Contact, and Case. Managers were granted full visibility and edit rights on relevant fields. Technician profiles were limited to technical and relevant fields, some as read-only. Customer profiles were restricted to visibility of necessary fields related to their own data, with sensitive internal fields hidden to safeguard information security.

Step 5: Set Tab Visibility in Profiles

Profiles were customized to display tabs relevant only to each role's functions. Managers were able to see all Sales and Service-related tabs, Technicians saw tabs related to Cases, Tasks, and Accounts necessary for maintenance duties, and Customers were given minimal access to tabs related to service requests or portals specific to customer use.

Step 6: Assign Profiles to Users

Users created for the project were assigned profiles based on their defined roles. This assignment was verified to ensure that users could not escalate their permissions beyond the intended level, maintaining strict role-based access control.

Step 7: Configure Business Hours and Holidays

Business hours and holiday schedules were verified and configured to control the timing of workflow processes and approval requests accurately. Public holidays were added to prevent automated actions from triggering on non-working days, ensuring the system aligns with operational calendars.

Step 8: Setup Sharing Rules

The organization-wide defaults were set to restrict data visibility, predominantly selecting "Private" access to minimize exposure by default. Sharing rules were then established to extend access according to role requirements: Customers can see only their own records, Technicians see records related to their assigned cases or accounts, and Managers have broader visibility across all related data.

Step 9: Test User Access

Testing of user access was conducted using the "Login As" feature to simulate login as different role users—Manager, Technician, and Customer. This testing confirmed users could

only view and modify data permitted by their profiles and associated sharing rules. Tab visibility and field-level restrictions were also verified to be in effect as configured.