Phase 4: Security & Access Control

Project Title: Customer Support Ticket Management System

- Security and access control play a vital role in the successful implementation of any enterprise-level Salesforce application.
- Since the Customer Support Ticket Management System handles sensitive customer information, issue descriptions, and internal support processes, it is essential to ensure that data is protected from unauthorized access.
- This Phase focuses on designing and implementing a structured security model using Salesforce's built-in security mechanisms.

1.Importance of Security in Customer Support Systems

- Customer support systems manage critical business data, including customer contact information, issue details, and service history.
- Improper access to this data can result in data breaches, loss of customer trust, and legal compliance issues.

Key reasons why security is essential in this system include:

- Protection of customer personal and contact information
- Prevention of unauthorized modification of support tickets
- Controlled access to administrative configurations
- Accountability through role-based access
- Compliance with organizational data security standards

By implementing a well-defined security framework, the Customer Support Ticket Management System ensures that only authorized users can view or modify sensitive data.

2.User Roles

The system is designed with clearly defined user roles to control access based on responsibilities.

System Administrator

The System Administrator has complete control over the Salesforce org and is responsible for:

- Managing users, roles, and profiles
- Configuring custom objects, fields, and automation
- Monitoring system performance and security settings

- Ensuring data integrity and compliance

This role has full access to all objects and configuration settings.

Support Agent

Support Agents are responsible for resolving customer issues. Their access is limited to operational tasks.

Responsibilities include:

- Viewing assigned support tickets
- Updating ticket status and resolution details
- Communicating with customers regarding issue resolution

Support Agents do not have access to administrative or configuration settings, ensuring system security.

Support Manager

Support Managers oversee the support process and monitor team performance.

Responsibilities include:

- Viewing all support tickets across the organization
- Monitoring ticket status, escalations, and resolution time
- Analyzing reports and dashboards

Support Managers have broader visibility but limited modification rights.

3.Object-Level Security

Object-level security determines which users can create, read, update, or delete records for each object.

This structure ensures:

- Only administrators can manage master data
- Agents focus on ticket resolution
- Managers have visibility without unnecessary control

4.Field-Level Security

Field-level security (FLS) restricts access to sensitive fields within objects. This prevents users from viewing or editing data beyond their responsibilities.

Examples of field-level security implementation include:

- Support Agents can edit **Status** and **Priority** fields
- Sensitive system fields are restricted to Administrators
- Support Managers have read-only access to most ticket fields

Field-level security ensures data accuracy and prevents unauthorized modifications.

5.Record-Level Security & Sharing Rules

Record-level security controls which individual records users can access.

Ownership-Based Access

- Support Agents can access tickets assigned to them
- Ticket ownership determines visibility

Manager Visibility

- Support Managers have access to all tickets for monitoring and escalation

Organization-Wide Defaults

- Default sharing is set to **Private** for Support Tickets
- Access is extended using roles and sharing rules

This approach ensures strict control over record visibility while supporting managerial oversight.

6.Authentication and Login Security

Salesforce provides robust authentication mechanisms to protect user access.

Key security features include:

- Username and password authentication
- Email verification
- Role-based login access
- Session timeout controls

These mechanisms ensure that only authenticated users can access the system.

7.Data Protection and Compliance

The implemented security model supports organizational compliance by:

- Protecting customer data from unauthorized access
- Maintaining audit trails through record history
- Ensuring accountability for ticket updates
- Supporting internal data protection policies

This enhances trust and reliability in the Customer Support Ticket Management System.

8.Benefits of Security & Access Control Implementation

The security framework provides several benefits:

- **Improved Data Confidentiality:** Sensitive information is protected
- **Controlled Access:** Users access only what they need
- **Reduced Risk:** Minimizes accidental or malicious data changes
- **Operational Clarity:** Clear role boundaries improve efficiency
- **Scalability:** Security model can scale with organization growth