Salesforce Data Security Model is a three-layer system granting users access to the record instead of restricting users' access. Salesforce uses the data model of Objects, Fields, and Records to store its data and has specific security criteria for each level.

Objects – tables in a database

Fields – columns of the table

Records – rows inside a table

Object-level-security

Before allowing a user access, Salesforce verifies that a user has permission to see the Object. Object-level access can be managed with Profiles and Permission Sets.

Profiles – Profiles are Salesforce's original way to control access to Objects and Fields, and it is the lowest level since profiles control access to page layouts and login restrictions. The best practice is configuring profiles for minimum access and using permission sets and permission set groups to grant a User more access.

Note: You can only grant access. You cannot restrict access with profiles & permission sets!

Permission sets and Permission Set Groups – best practice methods recommend granting permissions to Objects and Fields with permission sets. Permission Sets are more flexible, upgradeable, and can be packaged and deployed to multiple Users simultaneously. For example, you can add permission sets to tasks performed by a group of Users, like Sales Managers who do tasks like managing leads and approving opportunities. Permissions to perform these tasks can be added to Users as needed to grow the User's permissions as required.

A Permission Set Group is used to create a group of users that perform a similar task, like Managers, Sales, and Service teams that offer the Users access to specific Objects and Fields depending on job functions and needs.

In Summary, you can add Permissions to a User to grant additional access to Objects and Fields. Permissions can be granted to a single user, and a group of Users can be granted permissions simultaneously with a Permission Set Group, giving access to multiple Users at once.

Field-Level Security

The next layer in the Salesforce data model is Field-level security. Just because a user has access to an Object does not mean that the User has access to edit the field or see all the fields on an Object. Field-level security can grant read/write access to individual fields on an Object. Fields can also be set to hidden, and a User must have access to the field to see it.

Note: The best practice is to use field-level security to hide a field instead of removing a field from a record page or page layout. Use Field-level security to grant or restrict access through permission sets.

Record-Level Security

Referred to as the Salesforce Sharing model, record-sharing, or simply as sharing, is the last layer of the data security model security. Salesforce provides five record-level security methods to share and access records at this level.

Note: by default, a User can only see the record they own.

1. **Organization-Wide sharing** -Salesforce has a field in Objects called “OwnerId” that states which User is the Owner of that record. Most of the time, this is the User that created the record, and for the records, they create, the User has full CRUD (Create, Read, Update, Delete) access. Ownership can also be granted to a group of Users, for example, queues.

OWD set to **Private** – means Users can only see records that they own

OWD set to **Public Read Only** – any User can read the records, but only the Owner can update or delete them.

OWD set to **Public Read/Write** – Any User can read and update, but not delete the record

2. Role Hierarchies – Role hierarchy states that a User has access to all their records plus the records of their subordinates. For example, a sales Manager would access his team’s records.

3. Sharing Rules – Since Role Hierarchy rules only allow us to share records in a vertical structure, what if we need to share with another manager or another lateral role, for example, a sales team sharing with a service team? This is an excellent example of where sharing rules come in. There are two different types of sharing rules. Ownership-based and Criteria-based

Ownership-based sharing rules are shared based on User Role and Role-and-Subordinate, and public group ownerships. An example of this is a Sales Team sharing with the Service Team.

Criteria-based rules let User share access to records based on the value of a field instead of ownership of the record. For example, records can be shared with a team for a particular territory.

Note: There is a particular type of criteria-based sharing as well called. **Guest User Sharing** Rules – These types of sharing rules are read-only records shared with unauthenticated guest Users.

4. **Manual Sharing** – Manual Sharing is a way for individual users to share records with others. This permission is accessed through the sharing button on the records details page. Only available in OWD security that is set to Private or Public Read-only.

5. **Apex Sharing** – This is when records are not shareable in the standard Salesforce User Interface (UI) and must be written in Apex code. The development team writes an Apex trigger to perform the Apex Sharing