Data Security

Data security deals with the security or sharing settings of data and visibility between users or group of users across the organization.

Force.com platform provides a flexible, layered sharing model that makes it easy to assign different data sets to different sets of users

Security and Sharing model can be configured entirely using the user interface yet it is implemented at the API level which means any permissions specified for objects, records and fields apply even if a user query or update the data via API calls.

Levels of Data Access

The data access on Salesforce is configured in four levels, following are:

Organization Level

The access to the whole organization is secured at this level by maintaining a list of authorized users, setting password policies, and limiting login access to certain hours and certain locations.

Object Level

Object-level security provides the simplest way to control which users have access to which data. By setting permissions on a particular type of object, you can prevent a group of users from creating, viewing, editing, or deleting any records of that object.

Field Level

Field Level security restricts access to certain fields, even for objects a user already has access to.

Record Level

Record Level security lets users access some records but not others. It is used to control data access with greater precision. Users can have access to view an object, but can be restricted to the individual records.

Note: Always make a table for various types of users and the level of access of data that each user have in your organization to implement a security and sharing model.

Control Access to the Organization

Access to organization can be restricted by four means:

1. Allowing only authorized users to access Salesforce
2. Setting Password Policies
3. Restricting IP ranges for Users.
4. Restricting Login Hours for Users.

User Management

A user is anyone who logs in to Salesforce. Users are employees in your organization.

Every user in Salesforce has a user account. The user account identifies the user, and the account settings determine what features and records the user can access.

Each user account contains at least the following:

Usernames: It must be unique across all Salesforce organizations.

User Licenses: It determines which features the user can access in Salesforce. For example, you can allow users access to standard Salesforce features and Chatter with the standard Salesforce license. But, if you want to grant a user access to only some features in Salesforce, you have a host of licenses to choose from. For example, if you have to grant a user access to Chatter without allowing them to see any data in Salesforce, you can give them a Chatter Free license.

Profiles: It determine what users can do in Salesforce. Profiles should be selected based on a user's job function

Roles: It determine what users can see in Salesforce based on where they are located in the role hierarchy. These are optional but each user can have only one.

Alias: An alias is a short name to identify the user on list pages, reports, or other places where their entire name doesn't fit. By default, the alias is the first letter of the user's first name and the first four letters of their last name.

User record in Salesforce can't be deleted it can be only be deactivated or freeze.

Deactivate a User	Freeze a User
User record cannot be deleted so in order to stop the user from logging in to Salesforce organization administrators need to deactivate them.	A user record cannot be deactivated immediately such as when a user is selected in a custom hierarchy field. So to prevent the user from login in to the organization while administrators perform the steps to deactivate them, they can simply freeze that user's

	record.
Deactivating user records frees up the license assigned to the user. So that now new users can use that license in order to access Salesforce platform features.	Freezing a user does not frees the license assigned to the user.

Managing Password Policies

Password policies are configured to ensure that the user's password is strong and secure.

There are several settings to ensure this:

Password policies: Set password and login policies, such as specifying an amount of time before all user's passwords expire and the level of complexity required for passwords.

User password expiration: Expire the passwords for all the users in your organization, except for users with "Password Never Expires" permission.

User password resets: Reset the password for specified users.

Login attempts and lockout periods: Specifies the number of attempts a user can make and if a user is locked out due to too many failed login attempts, administrator can unlock its access.

Restrict Login Access by IP Address

By default, Salesforce doesn't restrict the location for login access. However, for added security, administrators can restrict it.

Administrators can specify an IP address range for the entire organization as well as for specific user profiles, but the behavior is very different for each option.

If login IP range is set at:

Organization level: Users who log in outside the set range are shown a login challenge. If they complete the challenge question, typically by entering an activation code sent to their mobile device or email address, login access is granted. This method does not restrict access, entirely, for users outside of the set IP range. Here the set IP range is called the "trusted" IP range.

Profile level: Users outside the permitted range are always denied for the access.

Restrict Login Access by Time

By default, Salesforce doesn't restrict the time for login access. However, for added security, administrators can restrict it.

Restricting login access by time can only be achieved at profile level. For each profile, administrators can specify the hours when users can log in. For example, for employees who only need to access customer data during business hours, you can deny login access during evening hours and weekends.

If users are logged in when their login hours end, they can continue to view their current page, but they can't take any further action.

Object Level Security:

Object Level Security provides the simplest way to control data access. It prevents user or group of users from creating, viewing, editing or deleting any records of an object by setting permissions on that object.

There are two ways of setting object permissions:

1. **Profiles:**
   It determines the objects a user can access and the permissions a user has on any object record.
2. **Permission Sets:**

   It provides additional permissions and access settings to users

Profiles

Profile is a collection of settings and permissions that determine which data and features in the platform users have access to. Settings determine what users can see for example apps, tabs, fields and record types whereas Permission determine what users can do for example create or edit records of a certain type, run reports and customize the app.

Profiles Control:

- Object Permission
- Field Permission
- User Permission
- Tab Settings
- App Settings
- Apex class access
- Visualforce page access
- Page Layouts

- Record Types
- Login Hours
- Login IP Ranges

Profiles are typically defined by a user's job function but anything that makes sense in an org can be created as a profile.

The platform includes a set of standard profiles.Each of the standard profiles includes a default set of permissions for all of the standard objects available on the platform.

Some of them are:

1. **Standard User:**Standard User profile has Read, Edit and Delete permissions to most standard objects.
2. **Read Only:**Read only user had permissions exactly similar to standard user but limits the access to read only.
3. **Marketing User:**Permissions of Standard User+ Additional Permissions.
4. **Contract Manager:** Permissions of Standard User + Additional Permissions.
5. **Solution Manger:** Permissions of Standard User + Additional Permissions.
6. **System Administrator:** The System Administrator profile has the widest access to data and the greatest ability to configure and customize Salesforce. The System Administrator profile also includes two special permissions namely "View All Data" and "Modify All Data".

When a custom object is created most profiles except those with modify all data permission do not give access to that custom object.

Note: Object permissions on Standard profile cannot be edited.

So to overcome through this it is good to make copies/clones of standard profiles and then customize the copies to fit the needs of the organization.

The profiles functionality in an org depends on the user license type

Note: Every profile should have at least one visible app.

Note: If an app is visible, its tab won't show up unless a profile has permissions to view the associated objects.

Note: A profile can be assigned to many users but user can be assigned to only one profile at a time.

Permission Sets

Permission set is also a collection of settings and permissions that determine user's access to various tools and functions on the platform.

Settings and permissions available in permission sets are also found in profiles but permission sets extend the functionality of users without changing their profiles.

Use permission sets to grant additional access to specific users on top of their existing profile permissions, without having to modify existing profile, create new profiles or grant an administrator profile where it's not necessary.

Permission Sets Control:

- Object Permission
- Field Permission
- User Permission
- Tab Settings
- App Settings
- Apex class access
- Visualforce Page access

There are couple of ways to use permission sets:

1. To grant access to custom objects or entire apps.
2. To grant permissions-temporarily or long term-to specific fields

Permissions are additive which means we can't remove a user's existing permissions by assigning a permission set we can only add permissions.

To limit access for a user or group of users, ensure that their base profile as well as any of their permission sets limits this type of access.

License type cannot be changed once assigned. And it is not mandatory while creating permission sets.

Profile	Permission Sets
Profiles have most restrictive settings and permission a user assigned to this profile should have.	Permission Sets extend the access settings and permissions provided by the profile.
A user can have only one profile assigned.	Users can have more than one permissions sets.
Profiles are restrictive.	Permission Sets are additive.
Every user must be assigned to a profile.	It is not necessary for every user to have a permission set.

Field Level Security

Field level security controls whether a user can see, edit or delete the value for a particular field on an object unlike page layouts which only control the visibility of field on detail and edit pages of an object.

It secures the visibility of fields in any part of the app including related lists, list views, reports and search results.

Field level security can be applied to multiple fields on a single profile or permission set and can also be applied to a single field on all profiles.

Record Level Security

Record level security determines which individual records users can view and edit in each object they have access to in their profile.

The permission on a record is always evaluated according to a combination of object, field and record level security permission.

When object- versus record-level permissions conflict, the most restrictive settings win.

To implement record level security the administrator need to answer following questions:

1. Should the users have open access to every record or a subset?
2. If it's a subset then what rules should determine whether the user can access them?

Salesforce provides 4 ways to implement record-level security:

1. Organization-Wide Default:

Organization-Wide default or Organization-Wide sharing settings determine the baseline level of access for all records of an object.
Organization-wide defaults can never grant users more access than they have through their object permissions.

Organization-Wide defaults should be most restrictive in record level security because other record level security implementations only grant additional accesses, they cannot restrict the access of records provided by Organization-Wide defaults.

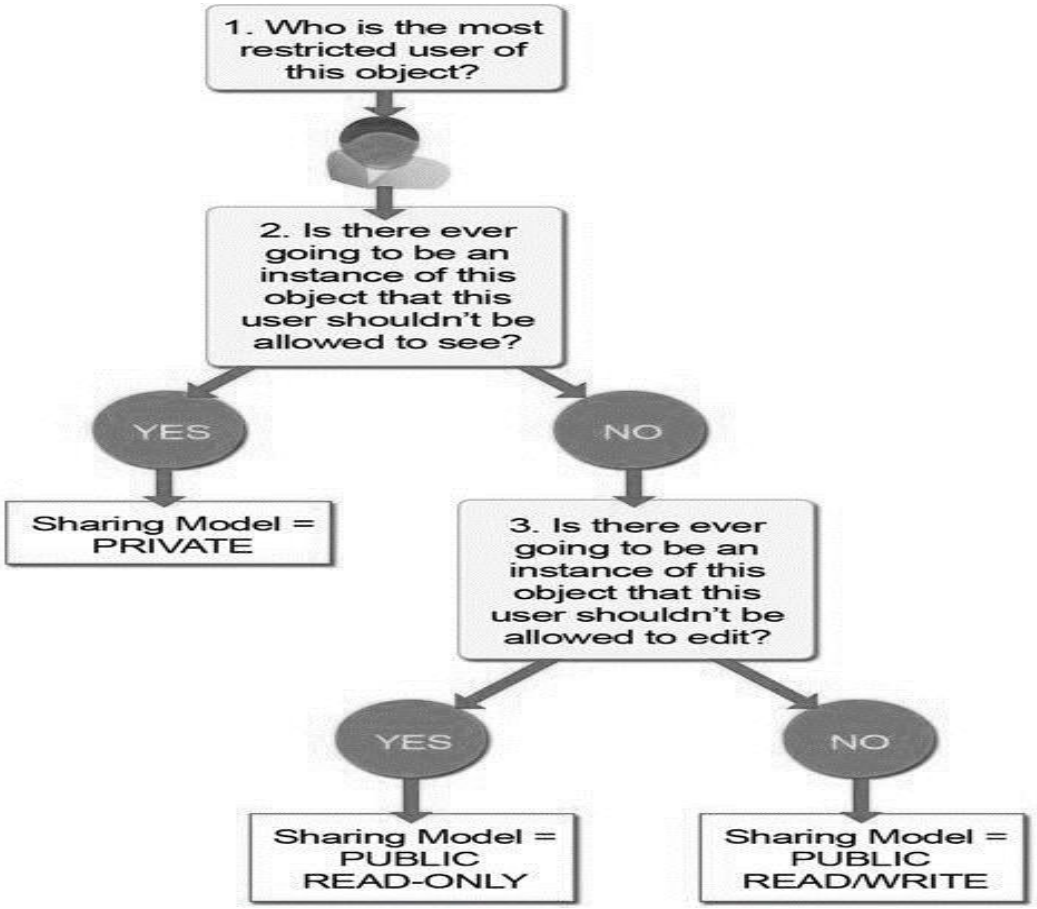
Organization-Wide defaults can be set to any of the 3 below:

1. Public Read/Write
   All users can view, edit, and report on all records.
2. Public Read-Only

All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records.

3. Private
   Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.

To determine the org-wide default of an object consider the below diagram:



The data may be too restrictive for some users according to org-wide defaults but it can be opened for users who need it using role-hierarchies, sharing rules and manual sharing.

A sharing recalculation gets started to apply access changes to records whenever an update is made for Organization-Wide Default settings. An email is sent by Salesforce whenever its gets completed or we can see the update on Setup Audit Trail as well.

2. Role Hierarchy:

Every Salesforce org maintains a role hierarchy for the organization using Salesforce. This role hierarchy defines the hierarchy of the users working in the organization.

Role Hierarchies can be used to extend the record access automatically so that:

- A Manager will always have access to the same data as his/her employees regardless or the org-wide defaults settings.
- Users who tend to need access to the same types of records can be grouped together. (These groups can be used as Roles & Sub-Ordinates in Sharing Rules).

Role hierarchies don't have to match your org chart exactly. Instead, each role in the hierarchy should just represent a level of data access that a user or group of users need.

Depending on organization's sharing settings, roles can control the level of visibility that users have into organization's data. Users at any given role level can view, edit, and report on all data owned by or shared with users below them in the role hierarchy, unless organization's sharing model for an object specifies otherwise.

Note: If the "Grant Access using Hierarchies" option is disabled for a custom object then only record owner and users granted access by the org-wide defaults have access to object's records. However users such as with the "View All" and "Modify All" object permissions and the "View All Data" and "Modify All Data" system permissions can still access records they do not own.

"Grant Access using Hierarchies" option is enabled for all objects and it can only be changed for custom objects.

Public Groups

A public group consists of a set of users. It can contain individual users, other groups or the users in a particular role or territory plus all the users below that role (subordinates) in the hierarchy.

3. Sharing Rules:

Sharing rules are used to create automatic exceptions to the Organization-Wide Default settings for the users who does not own the record.

Sharing rules should be applied to the objects whose org-wide defaults are set to Public Read-only or Private because sharing rules can only extend the access they cannot restrict the access provided by org-wide defaults.

There are 2 types of sharing rules based on which records to be shared:

1. Owner Based Sharing Rules:

Owner based sharing rules share the records owned by certain users. Owners can be identified through public groups, roles and roles and sub-ordinates.

2. Criteria Based Sharing Rules:
   Criteria based sharing rules share the records that meet a certain criteria.

Before creating sharing rules administrators need to answer these 3 questions:

1. Share which records?
   This identifies the records that need to be shared. They can be categorized based on owner of the records or the criteria that records met.
2. With whom the records needs to be shared?
   Records can be shared with public groups, roles and roles & subordinates.
3. What kind of access should be provided for these records?
   The users with whom the records are shared should have Read-Only or Read/Write access is decided by this question.

Note: As sharing rules cannot restrict the access this is the reason it gives Read-Only and Read/Write as access parameters in sharing rules.

Note: Sharing rules work best when they are defined for a particular group of users that can be determined or predict in advance rather than a set of users that frequently changes.

4. Manual Sharing

In manual sharing, records are shared individually with other users by using the share button on the record.

Sometimes it is not possible to define a consistent group of users who need access to a particular record that is where manual sharing comes in. It allows the users to share the record to users who would not have access to the record any other way.

Only these 4 users can share the record:

- Record Owner
- A user in a role above the owner in the role hierarchy.
- User granted “Full Access” to record.
- Administrator

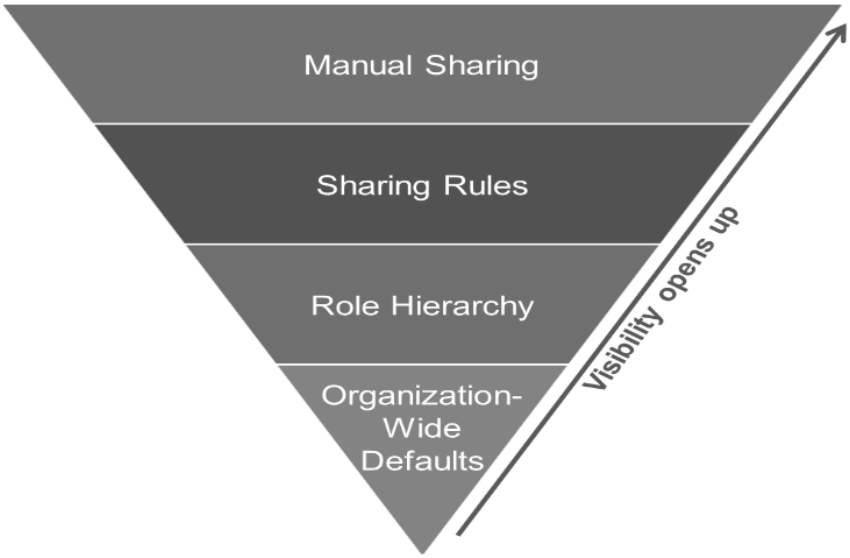
Sometimes granting access to records also includes access to its associated records.

The sharing button is available when your sharing model is either “Private” or “Public Read-Only” for a type of record or related record.

Records can be shared manually with groups, roles, roles & subordinates and individual users.

There are basically 4 access levels that determine the access provided to users

1. Full access:
   Users with full access can view, edit, delete and transfer the record. These users can also extend sharing access to other users.
   Users cannot grant full access to other users.
1. Read/Write:
   Users can view and edit the record and add associated records, notes and attachments to it.
2. Read Only:
   Users can view the record and add associated records to it. They cannot edit the records or add notes and attachments.
3. Private:
   Users cannot access the record in any way.



Different types of groups, users, roles and territories:

Type	Description
Managers Groups	All direct and indirect managers of a user.
Manager Subordinates Groups	A manager and all direct and indirect reports who he or she manages.
Public Groups	All public groups defined by your administrator.
Personal Groups	All personal groups defined by the record owner. Only the record owner can share with his or her personal groups.
Users	All users in your organization. Does not include portal users.
Roles	All roles defined for your organization. This includes all of the users in each role.
Roles and Subordinates	All of the users in the role plus all of the users in roles below that role in the hierarchy. Only available when no portals are enabled for your organization.