SFDC Security Model Org
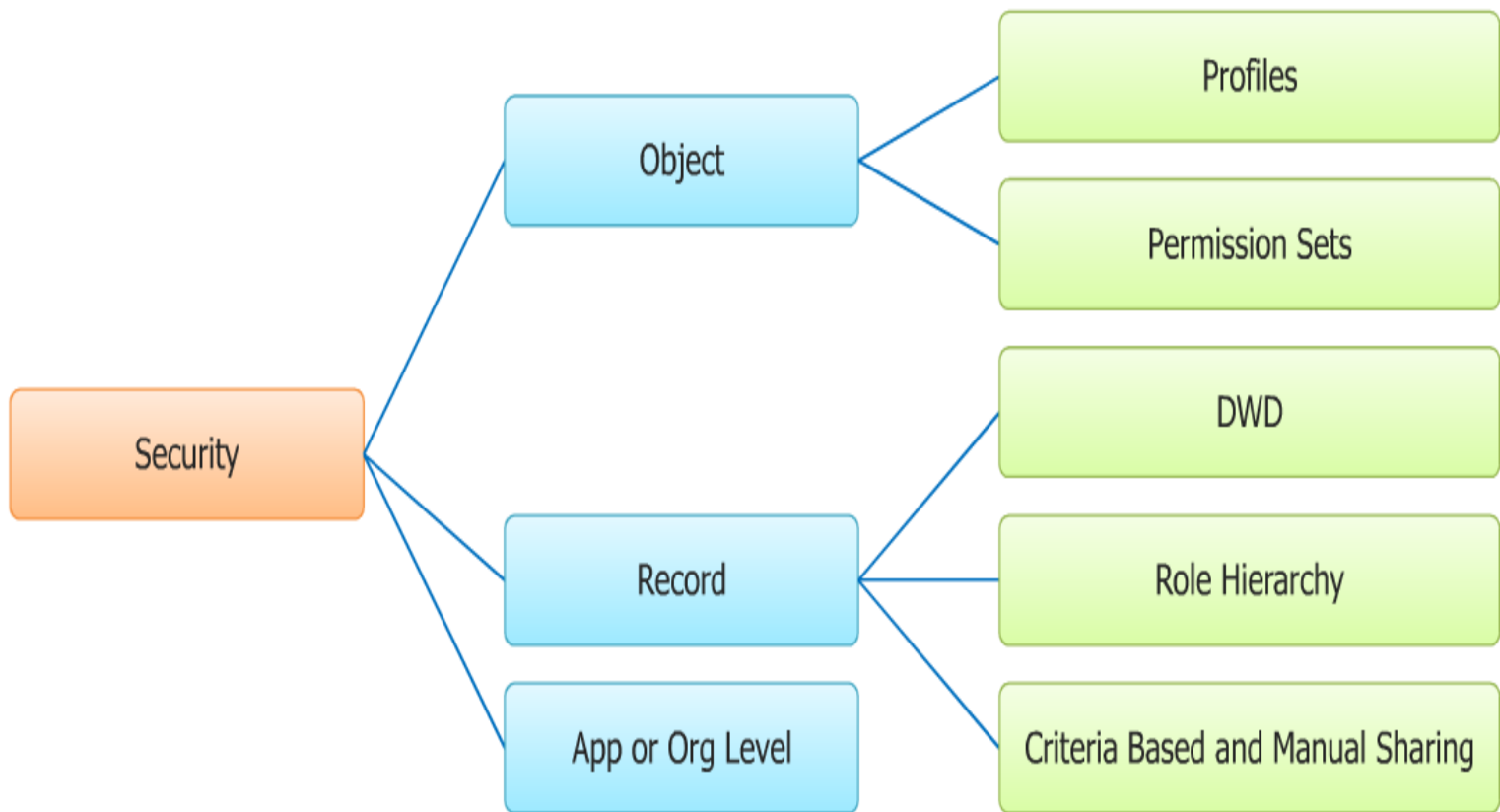
Part 1 –Profiles and permission sets

Objectives

At the end of this module, you will be able to understand:

→Security – Analogy

→System (org) level security

→User administration and troubleshooting by user and admin

→Object level security

→Record level and Field-Level security

→Understand the difference between object and record level
security

→Various features available to implement object and record level

Roles and Profiles

Role controls Data (Record) Visibility
What records can John Sales see ?

Profile controls Object/Field permissions
What CRUD permissions does John have on objects and fields ?

> **Profile**
> Can I access the
> **Account Object (Table)**

John Sales

Account Id	Name	City	State
001U000000B..	ABC Corp	Spokane	WA
001U000000V..	Acme	Atlanta	GA
001U000000X..	X Net	San Francisco	CA
001U000000Y..	Universal Air	Dallas	TX

What are Profiles ?

Defines a user's permission to perform different functions within salesforce.com.

- What objects (accounts, leads, contacts etc.) can I access ?
- What page layouts can I see ?
- What fields can I access ?
- Which tabs can I view ?
- Which record types can I see ?
- Which Apex Classes are accessible for me ?
- Which Visualforce Pages can I access ?

User   1 Profile
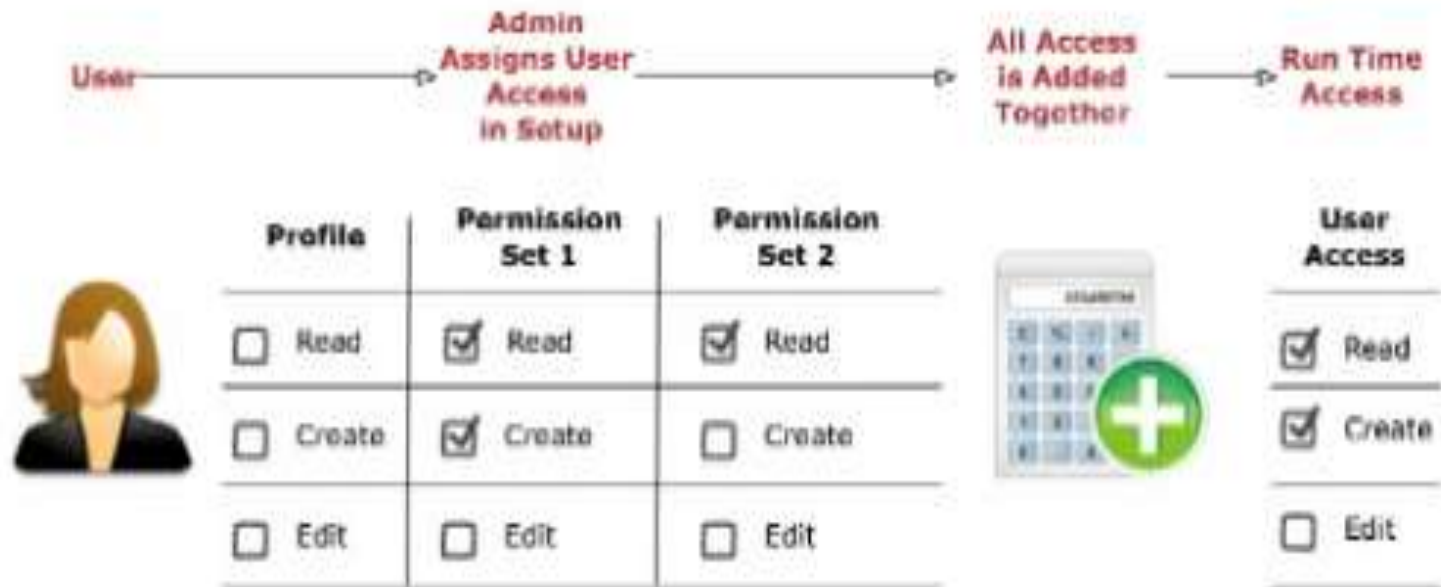
☐ Read

+   ☐ Create

☐ Edit

What's a permission set?

	Profile	Permission Set 1	Permission Set 2	User Access
	☐ Read	☑ Read	☑ Read	☑ Read
	☐ Create	☑ Create	☐ Create	☑ Create
	☐ Edit	☐ Edit	☐ Edit	☐ Edit

User → Admin Assigns User Access in Setup → All Access is Added Together → Run Time Access

A collection of CRUD permissions and settings

Extends user's access without creating a new profile

User access controlled by Profile + Permission Sets

Creating Profiles

Salesforce ships with default system admin profile and some additionla

Create new profile by cloning the system admin profile and then reducing access as system admin has all accees

Ensure that new profiles don't have view all ,modify all disabled at object level

Ensure that new profiles also have edit readonly fields permission disabled

Security at org Level

System Level or Org Level security - Users and Profiles and User License type

→ All SF users should have a valid user account to login to salesforce

→While creating a new user the following info has to be selected or entered – Profile, License, username(unique across all orgs!), lastname, alias etc

→User License determines the different features the user has access to

→Profiles are the most important feature in SF and you need to create a profile first before you can create an user

→Profiles are linked to User license type and this is mandatory

→There are many standard profiles available and they can be cloned to create custom profiles. You cannot create custom profiles directly.

→A given user can be associated with only one profile and license combination at a point of time

Security at org Level

System Level or Org Level security - Users and Profiles and User License type

To use enhanced profile editor: Go to Setup → Customize → User Interface → select the checkbox "Enhanced Profile User Interface" and click "Save"

→Before creating an user first decide the profile + license type combination and proceed

→Once user id is created the user gets an email and they can set password

→Password policy is controlled at profile level , Login hours can also be controlled

→Login IP range can be controlled at org level and profile level

→If login IP is set a org level and user logs outside this ip range he gets an activation code and he can get access once he provides the code

→Profile IP is very strict and user cannot login outside this ip range

Object Level security:Permission sets

→Permission sets and Profiles can be used together

→Profile should be used to provide bare minimum permissions and then additional permissions can be given using permission sets

→PSet can only be used to grant but cannot deny !!

→One user can be part of only one profile at a point of time, but a user can be part of many permission sets

→An org can have up to 1000 permission sets

→PSet need not be associated with license types

→Permissions sets can be used for any short-term requirements and then revoke later

→Profiles and permission sets help handle both app level and object level security settings

→It is advisable to keep the number of profiles to a minimum say less than 10-15 for an organization with multiple departments and global user base

→Identify common functions and permissions that are required and create profiles and then extend additional functionality with permission sets

→In case of our student app, we can have a role called Professors and we can have a permission set Principal and add some additional permissions

Principal permissions = Professor (Profile) + Principal (Permission set)