DATA SECURITY IN SALESFORCE

APOCALYPSE TRAINING FROM STEVE ROSS

HTTPS://WWW.LINKEDIN.COM/IN/SROSSFBT/

TRAILHEAD MODULE:

HTTPS://TRAILHEAD.SALESFORCE.COM/EN/CONTENT/LEARN/MODULES/DATA_SECURITY

TRAILHEAD MODULE: HTTPS://TRAILHEAD.SALESFORCE.COM/EN/CONTENT/LEARN/MODULES/DATA_SECURITY

- Data Security in Salesforce is simply controlling who sees what.
- For some organizations this more important than others (small start up vs a bank).
- Best to set this up early as it will be more challenging later
- Think in terms of groups of users; what they need to do and what they need to see
- Will always be a balance between convenience and security
- Salesforce makes it much easier to 'open up' than to close down
- I feel being too strict will have far fewer negative consequences than being too open.

LEVELS OF ACCESS

- Org wide access: Examples: Trust/Block users based on IP Address, password policies. Many of these are more advanced topics. For now, just know that level exists.
- We can set permissions at Object, field and record level. CRUD (create, read, update and delete)
- Permissions can be broad based or fine grained. Examples: Marketing interns can't see opportunities. Sales Reps can't view salary information on user records.
- **Object Level access**: Setting permissions for a specific object (i.e./ Accounts, Contacts, Opportunities) Should users be able to edit accounts? Create Opportunities?
- **Field level access**: An employee can't read the max salary value on an open position.

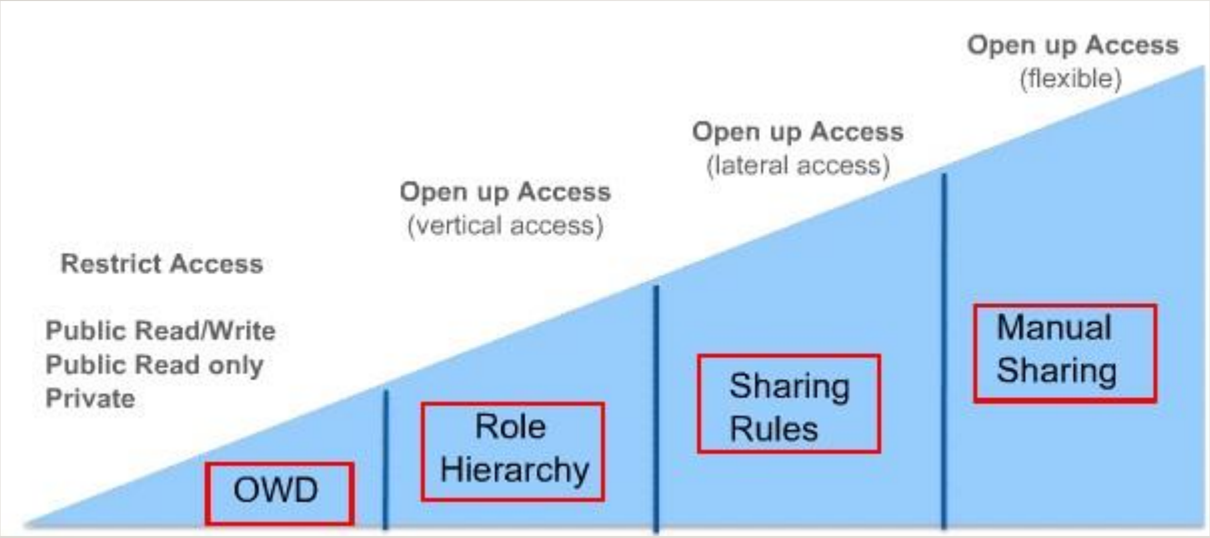
LEVELS OF ACCESS

- **Record level access**: What you can see and what you can do. Examples: Inside sales can't update leads they don't own. Sales Reps can create accounts.
- All records in Salesforce have an owner, which are users (*with one exception*) and this makes CRED (or CRUD) decisions little more complicated. Here are the scenarios:

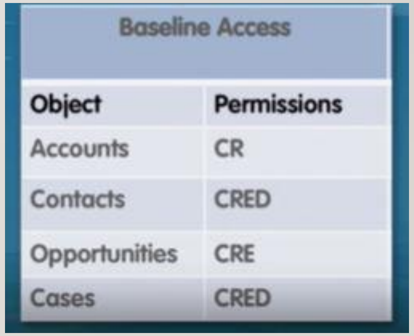
Records I own	Records Others Own	We Own?
God level of access (Create, edit & delete). I can do as I please!	I may or may not be able to read or edit your records.	We are working as a team and can both edit.

RECORD LEVEL ACCESS

Record level access (access to records you don't own) can be accomplished in a variety of ways and it's a best practice to work from left to right.



OWD Baseline Example

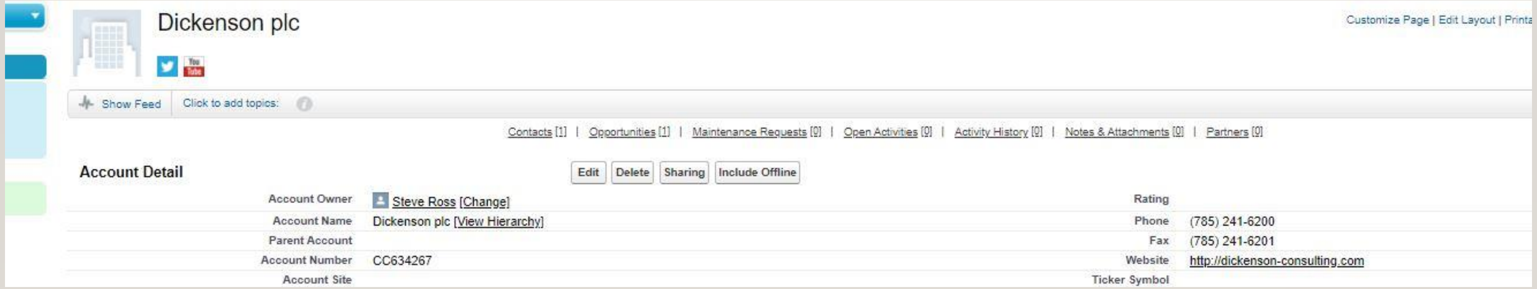


Baseline Access

Object	Permissions
Accounts	CR
Contacts	CRED
Opportunities	CRE
Cases	CRED

RECORD ACCESS: SHARING RULES

- Another way to create access is with automatic exceptions.
- The exceptions can be by owner or by other criteria.
- Let's look at an Example (go to link)
- Manual Sharing: 'One off' sharing for a specific record (classic only?). Use this when record sharing is needed and it's outside of the usual process.


Customize Page | Edit Layout | Printa
Show Feed
Click to add topics:
Contacts [1] | Opportunities [1] | Maintenance Requests [0] | Open Activities [0] | Activity History [0] | Notes & Attachments [0] | Partners [0]
Edit
Delete
Sharing
Include Offline

Dickenson plc

Account Detail

Account Owner	Steve Ross [Change]	Rating	
Account Name	Dickenson plc [View Hierarchy]	Phone	(785) 241-6200
Parent Account		Fax	(785) 241-6201
Account Number	CC634267	Website	http://dickenson-consulting.com
Account Site		Ticker Symbol	

OWD (ORGANIZATIONAL WIDE DEFAULTS)

- OWD is always where you start. This sets the default level of access users have to each others records). It is set per object and options are: Private, Public Read Only, Public red/Write, Public Read/Write/Transfer.
- Set OWD based on the most restrictive use case you have. The golden rule: It is always easier to open up! Looking at the diagram, moving to the right ONLY grants additional access. OWD is the only place to restrict access.

RECORD ACCESS: ROLE HIERARCHY

- Role Hierarchy gives access based on the salesforce role hierarchy. This is defined: Setup > Roles
- The idea is that a manager may need to read/edit records owned by subordinates (users she manages) Example: A Sales Manager needs to read and edit opportunities created by the sales team.
- The role hierarchy is a way to grant access.

Let’s take a look:

OTHER ACCESS: PROFILES & PERMISSION SETS

- All users in Salesforce must have a profile
- Profiles (among other things) determine what you can do with records you own.
- Profiles broad categories that individual users can be assigned: examples Sales Reps, Sales Mgmt., Support, Human Resources.
- Permission set is a specific permission granted to a user or groups of users. Examples: Access to an installed app, view SSN information on candidate records

SETTING UP SECURITY IN AN ORG

- Scenario: ACME Fireworks has just purchased Salesforce and you have been tasked with setting up data security. You have been assigned to setup data security in the new org. How would you start? First Steps? Second Steps?

NEXT STEPS

- The Data Security Module has 7 challenges
- You will need a Trailhead playground to complete this
- I will be giving you an additional challenge on Wed that we will do together. Here is a preview:

Congratulations on completing earning your Data Security Trailhead badge! While the module gave you a good introduction, in that you setup I want to challenge you to take it further with testing your security setup. How would we go about doing this?

RESOURCES

- Who sees what video link: https://help.salesforce.com/articleView?id=security_data_access.htm&type=5