Salesforce Admin Exam Study Guide - Security and Access (10%)

Salesforce Basics: For Complete Beginners

If you're stepping into Salesforce for the first time, don't panic—here's a gigantic, friendly intro to get you pumped, comfy, and ready to dive in.

- **What is Salesforce?**
    - It's an online platform that businesses use to keep everything organized—customer info, sales deals, team tasks—all in one slick, cloud-based spot, no need for tech nightmares or complicated installs.
    - Imagine it as your business's trusty guardian, like a super-smart vault that holds your data, keeps it safe, and helps your team work together without missing a beat.
- **Why It's a Total Lifesaver**:
    - It rescues you from chaos—like losing track of customer notes or fumbling through emails—and puts everything in one neat hub: customer details, sales progress, work jobs. Whether your team's closing deals, helping clients, or planning projects, it's like a teamwork superpower that saves time, cuts confusion, and keeps everyone aligned.
    - As an admin, you're the gatekeeper and guide—setting up who sees what and keeping the org secure, like teaching a robot bouncer your company's VIP list and rules.
- **Key Words to Start With**:
    - **Org**: Your company's own Salesforce universe—like your team's private fortress where all the data lives and the action happens.
    - **Setup**: The control hub (top-right gear icon) where you tweak things—like the security panel of your Salesforce castle, letting you lock doors and hand out keys.
    - **CRM**: Customer Relationship Management—fancy talk for keeping customers happy and organized, which is Salesforce's core mission.
- **What This Topic Is All About**:
    - This section is your crash course in locking down Salesforce—controlling who gets in, what they see, and what they can do. It's like being the security

chief of your org, making sure data stays safe and users get just the right access.

Let’s jump in with a beginner’s excitement and unpack this step-by-step!

Overview

"Security and Access" is all about protecting your Salesforce org—managing who can log in, what data they can see, and what they can change. You’ll learn to set up user permissions, control object and field access, share records, and keep everything secure. It’s 10% of the exam—a critical piece because security is the backbone of trust in Salesforce.

Exam Weight

- **Percentage**: 10%
- **Why It Matters**: If security’s off, sensitive data leaks or users can’t work—either way, it’s a mess. With 10%, it’s a solid chunk of your test score and a daily must-know for keeping your org safe and functional.

Objectives (In Super-Simple Terms)

- Learn how to control who logs in—like giving out keys to the right people.
- Figure out how to limit what users see or change—like locking certain filing cabinets or drawers.
- Get the hang of sharing data—like passing notes to specific teammates—so everyone gets what they need, nothing more.
- Understand how to keep data safe—like setting up alarms—so your org stays secure and trustworthy.

Structure of the Study Guide

- **Definitions**: Big, clear explanations of key terms.
- **Categories**: Topics broken into bite-sized chunks.
- **Bullet Points**: Massive, beginner-friendly summaries with heaps of detail.
- **Tables**: Side-by-side comparisons to keep it simple.

- **Practical Scenarios**: Tons of real-world examples you can picture doing.
- **Study Tips**: Step-by-step ways to master this.

Definitions (Huge Summaries with Tons of Beginner Details)

- **Profile**:
    - **What It Is**: A set of permissions that controls what a user can do—like see Accounts or edit Opportunities.
    - **Details**: Think of it as a job badge—it defines a user's powers in Salesforce, like "Sales Rep" can view and edit deals but not delete them. Every user gets one profile, and it's the baseline for their access—like a rulebook for their role.
- **Role**:
    - **What It Is**: A position in your org's hierarchy—like "Sales Manager" or "Rep"—that decides what records a user can see.
    - **Details**: This is like a family tree—it sets who's above or below whom and controls record access. A "Manager" might see all team records, while a "Rep" sees only theirs. It's about who owns or shares data, not what they can do (that's the profile's job).
- **Permission Set**:
    - **What It Is**: Extra permissions you add to a user—like letting a rep delete records—without changing their profile.
    - **Details**: Imagine it as a booster pack—like giving a superhero an extra gadget. It's a way to tweak access for specific people (e.g., "Let Jane edit Cases too") without messing with the whole "Sales Rep" profile.
- **Object-Level Security**:
    - **What It Is**: Rules that control what users can do with entire data types—like view or edit all Accounts.
    - **Details**: This is like locking a whole filing cabinet—you decide if a profile can "Create," "Read," "Edit," or "Delete" an object (e.g., Opportunities). It's the first gatekeeper for data access.

- **Field-Level Security (FLS)**:
    - **What It Is**: Rules that control what users can see or change in specific fields—like hiding “Salary” on Contacts.
    - **Details**: This is like locking drawers inside the cabinet—you can make a field “Visible” (see it), “Read-Only” (see but not touch), or “Hidden” (no access). It’s finer control after object permissions.
- **Organization-Wide Defaults (OWD)**:
    - **What It Is**: The baseline sharing rule for an object—like “Private” so only owners see records.
    - **Details**: Think of it as the default lock on your org’s doors—it sets how private or open an object (e.g., Accounts) is for everyone. Options like “Private,” “Public Read Only,” or “Public Read/Write” decide who sees what before extra sharing kicks in.
- **Sharing Rule**:
    - **What It Is**: A way to open up access—like letting “Sales Team” see all “West Region” Accounts.
    - **Details**: This is like passing a spare key—it overrides OWD to share records with specific roles, groups, or users based on rules (e.g., “If Region = West, share with Sales”). It’s how you loosen tight defaults.

Categories

- **Security Tools**: The big ways you control access and protect data.
    - Profiles and Permission Sets
    - Roles and Hierarchies
    - Object and Field-Level Security
    - Sharing Settings (OWD, Sharing Rules)

Detailed Breakdown (Bullet Points with Massive Beginner Summaries)

1. Security Tools

- **Profiles and Permission Sets**
    - **Summary**: Tools to define what users can do—like view, edit, or delete records—and add extra permissions for specific people.
    - **Details**:
        - These are your user rulebooks—profiles set the baseline, and permission sets tweak it. Profiles are like job titles with standard powers (e.g., “Sales Rep” can edit Opportunities), while permission sets are like bonus cards (e.g., “Let this rep delete too”).
        - **How You Set It Up**: Go to Setup > Users section:
            - **Profiles**:
                - **What It Does**: Controls app, object, field, and system permissions for a group.
                - **Details**: Setup > Users > Profiles:
                    - **Create/Edit**: Click “New Profile” (clone “Standard User”) or edit existing (e.g., “Sales Rep”):
                        - **App Permissions**: Like “Visible” for “Sales” app—decides what apps they see.
                        - **Object Permissions**: Set “CRUD” (Create, Read, Update, Delete)—like “Read/Edit” on Accounts, “No Delete.”
                        - **System Permissions**: Like “View All Data” (rare, for admins) or “Customize Application” (build stuff).
                        - **Tab Settings**: Like “Default On” for “Leads”—shows in navigation.
                    - **Assign**: Link to users—Setup > Users > [User] > Edit > Profile = “Sales Rep.”

        - **Why It's Cool**: One profile fits many—like all reps get "Sales Rep" with same access. Keeps it simple and consistent.
        - **Example**: Clone "Standard User" to "Support Agent"—set "Read/Edit" on Cases, "Read Only" on Accounts, "Visible" for "Service" app—agents are set.
    - **Permission Sets**:
        - **What It Does**: Adds specific permissions without changing profiles.
        - **Details**: Setup > Users > Permission Sets > "New":
            - **Name**: Like "Case Deleter"—easy to spot.
            - **Permissions**: Check boxes—like "Delete" on Cases or "View Reports."
            - **Assign**: Setup > Users > [User] > Permission Set Assignments > Add "Case Deleter."
        - **Why It's Cool**: Flexible—like giving one rep "Export Reports" without making all reps exporters. Stack multiple sets per user.
        - **Example**: Rep Jane needs to delete Leads—create "Lead Deleter" set, add "Delete" on Leads, assign to Jane—she's special now.
- **Why It's Great**: Profiles keep it broad, permission sets make it personal—like a uniform for the team and a badge for the star player. Together, they control everything from apps to buttons.
- **What's Tricky**: Too many profiles get messy—stick to a few (e.g., 5-10). Permission sets pile up—track who's got what. Test access—reps might still miss stuff if fields or sharing block them.
- **Real-Life Example**: Sales team needs basic access—set "Sales Rep" profile with "Read/Edit" on Opportunities, "Visible" for "Sales" app. Manager needs more—add "Report Exporter" permission set—team's covered.

- **Roles and Hierarchies**

- **Summary**: A system to decide who sees records based on their spot in the org—like managers seeing team data, reps seeing only theirs.
- **Details**:
    - This is your org's ladder—it's about record ownership and visibility, not actions (that's profiles). Roles like "CEO" or "Sales Rep - West" form a hierarchy where higher-ups see everything below them—like a boss peeking at all team files.
    - **How You Set It Up**: Setup > Users > Roles:
        - **Create Roles**:
            - **What It Does**: Builds the hierarchy—like "CEO > Sales Director > Sales Rep."
            - **Details**: Click "Set Up Roles":
                - **Add Role**: Name it—like "Sales Rep - East"—and set its parent (e.g., "Sales Manager - East").
                - **Hierarchy**: Stack them—like "CEO" at top, "Sales Director" below, "Reps" under that.
                - **Assign**: Setup > Users > [User] > Edit > Role = "Sales Rep - East."
            - **Why It's Cool**: Higher roles see all records below—like a Sales Director sees all Reps' Opportunities if OWD allows (more on that later).
            - **Example**: Build "CEO > VP Sales > Sales Manager > Sales Rep - West"—Rep owns their deals, Manager sees all West deals, VP sees all sales.
        - **Role vs. Profile**:
            - **Details**: Role = what records (e.g., "My Accounts" vs. "Team Accounts"). Profile = what actions (e.g., "Edit Accounts"). A "Sales Rep" profile with "Sales Rep - West" role means they edit only their West records—combo matters.

        - **Why It's Great**: It's like a family tree—keeps data flowing up naturally. A rep owns their Leads, but their boss sees them too—perfect for oversight without micromanaging.
        - **What's Tricky**: No role = no hierarchy access—users see only their stuff unless shared. Too many roles clog it—keep it lean (e.g., 10-15 max). Test it—hierarchy alone won't help if OWD is "Private."
        - **Real-Life Example**: Sales org—set "VP Sales > East Manager > East Reps"—Rep owns "Acme Inc." Account, Manager sees it, VP sees all East—data flows up smoothly.
- **Object and Field-Level Security**
    - **Summary**: Rules to control access to entire data types (objects) and specific pieces (fields)—like who can edit Accounts or see "Revenue."
    - **Details**:
        - This is your data gatekeeper—object-level sets the big permissions (e.g., "Edit Opportunities"), field-level fine-tunes it (e.g., "Hide Salary"). Together, they lock down what users touch or peek at.
        - **How You Set It Up**:
            - **Object-Level Security**:
                - **What It Does**: Sets "CRUD" (Create, Read, Update, Delete) for objects—like "Read Only" on Cases.
                - **Details**: Setup > Users > Profiles > [Profile] > Object Settings:
                    - Click an object—like "Accounts."
                    - Check boxes—like "Read," "Create," "Edit," "Delete"—or leave blank for no access.
                    - Example: "Sales Rep" gets "Read/Edit" on Opportunities, no "Delete"—keeps deals safe.
                - **Why It's Cool**: Broad control—like "Support Agents get Cases, not Opportunities"—keeps roles focused.
            - **Field-Level Security (FLS)**:

            - **What It Does**: Locks specific fields—like “Visible” or “Hidden” for “Annual Revenue.”
            - **Details**: Setup > Object Manager > [Object] > Fields & Relationships > [Field] > Set Field-Level Security:
                - **Visible**: Check if they see it—like “Phone” for reps.
                - **Read-Only**: Uncheck “Edit” if they can’t change it—like “Created Date.”
                - **Hidden**: Uncheck “Visible” if it’s off-limits—like “Salary” for non-HR.
                - Example: “Revenue” Hidden for “Sales Rep,” Visible for “Manager”—sensitive stuff stays secret.
            - **Why It’s Cool**: Granular—like “Reps see Account Name, not Billing Info”—protects privacy.
        - **Why It’s Great**: It’s like a two-layer lock—objects block the big stuff, fields hide the details. A rep might edit Accounts but not “Revenue”—keeps data safe and clean.
        - **What’s Tricky**: FLS overrides object perms—if “Edit” on Accounts but “Read-Only” on “Name,” they can’t change it. Test every profile—reps might see less than you think.
        - **Real-Life Example**: Sales team—set “Sales Rep” profile with “Read/Edit” on Accounts, FLS hides “Annual Revenue”—reps work Accounts, managers see financials.
- **Sharing Settings (OWD, Sharing Rules)**
    - **Summary**: Tools to set default access (OWD) and share records (Sharing Rules)—like making Accounts private or opening them to teams.
    - **Details**:
        - This is your data-sharing blueprint—OWD sets the base lock, Sharing Rules open doors. Together, they decide who sees records beyond ownership or hierarchy.

- **How You Set It Up**: Setup > Security > Sharing Settings:
    - **Organization-Wide Defaults (OWD)**:
        - **What It Does**: Baseline privacy—like "Private" so only owners see records.
        - **Details**: Click "Edit" in Sharing Settings:
            - **Options**:
                - **Private**: Only owner (or hierarchy) sees—like "My Accounts only."
                - **Public Read Only**: All see, none edit—like a library book.
                - **Public Read/Write**: All see and edit—like a shared doc.
            - Set per object—like "Accounts = Private," "Opportunities = Public Read Only."
        - **Why It's Cool**: Locks it down—like "Private" keeps Accounts safe until you share them on purpose.
        - **Example**: Set "Cases = Private"—only case owners (or managers via role) see them—customer privacy locked.
    - **Sharing Rules**:
        - **What It Does**: Opens access—like "Share East Accounts with East Sales."
        - **Details**: Click "New" in Sharing Rules:
            - **Type**:
                - **Owner-Based**: Share by owner—like "Accounts owned by East Reps" to "East Sales" role.
                - **Criteria-Based**: Share by field—like "Accounts where Region = West" to "West Sales."
            - **Access**: "Read Only" or "Read/Write."

        - **Share With**: Roles, groups—like “Sales Team” or “Managers.”
    - **Why It’s Cool**: Flexible—like “West Reps share with West Manager, not East”—targets access where needed.
    - **Example**: “Accounts where Industry = Tech” shared “Read Only” with “Tech Sales” role—team sees relevant clients.
- **Why It’s Great**: OWD keeps it tight, Sharing Rules loosen it just right—like a vault with selective keys. “Private” Accounts with a “Sales Team” rule balance security and teamwork.
- **What’s Tricky**: OWD is strict—change from “Private” to “Public” opens everything, so test first. Sharing Rules pile up—track them or it’s chaos. Roles still need OWD to work right.
- **Real-Life Example**: “Opportunities = Private,” add Sharing Rule “Opportunities where Amount > 50,000” to “Managers” with “Read Only”—reps own deals, managers peek at big ones.

Tables

Table 1: Profiles vs. Roles

What’s Different	Profiles	Roles
Controls	What users do (CRUD)	What records they see
Scope	Apps, objects, fields	Record ownership/hierarchy
Example	“Edit Accounts”	“See team Accounts”
Assigned	One per user	One per user (optional)

Table 2: Object vs. Field-Level Security

What’s Different	Object-Level	Field-Level (FLS)
Scope	Whole object (e.g., Accounts)	Specific fields (e.g., Phone)

What's Different	Object-Level	Field-Level (FLS)
Options	CRUD	Visible, Read-Only, Hidden
Example	"Edit Opportunities"	"Hide Revenue"
Set In	Profile Object Settings	Field Settings

Table 3: OWD vs. Sharing Rules

What's Different	OWD	Sharing Rules
Purpose	Default access for all	Extra access for some
Options	Private, Public R/O, R/W	Read Only, Read/Write
Example	"Accounts = Private"	"Share West Accounts"
Scope	Org-wide	Specific roles/groups

Practical Scenarios

1. **Sales Rep Access**:
    - **Need**: Reps edit Opportunities, not delete.
    - **Solution**: Setup > Profiles > "Sales Rep" > Object Settings > Opportunities = "Read/Edit," no "Delete"—reps work safe.
2. **Manager Oversight**:
    - **Need**: Sales Manager sees all team Leads.
    - **Solution**: Setup > Roles > "Sales Manager > Sales Rep," OWD "Leads = Private"—Manager sees Reps' Leads via hierarchy.
3. **Hide Sensitive Field**:
    - **Need**: Reps don't see "Revenue" on Accounts.
    - **Solution**: Setup > Object Manager > Account > Fields > "Annual Revenue" > FLS Hidden for "Sales Rep"—secret stays safe.
4. **Share Region Accounts**:
    - **Need**: East Sales sees all "East" Accounts.

    - **Solution**: Setup > Sharing Settings > OWD “Accounts = Private,” New Sharing Rule “Region = East” to “East Sales” role, “Read Only”—team shares smart.
5. **Special Permission**:
    - **Need**: One rep exports reports.
    - **Solution**: Setup > Permission Sets > New “Report Exporter,” check “Export Reports,” assign to rep—extra power granted.

Study Tips

- **Hands-On**: Get a free org (developer.salesforce.com)—create a profile, set OWD, add a Sharing Rule, test with a user.
- **Start Simple**: Trailhead’s “Data Security” module—free, with videos and practice.
- **Focus**: Know Profiles (actions), Roles (records), OWD/Sharing (visibility), FLS (fields).
- **Practice**: Try “Limit reps to edit only?” or “Share Accounts by region?”—exam drills.
- **Beginner Boost**: Watch “Salesforce Security Basics” on YouTube; tweak one setting daily—like profile, then role.
- **Time**: Spend 10% here—5 hours of 50—split: 2 on Profiles/Roles, 2 on Sharing, 1 on FLS.