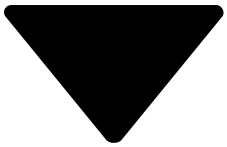
1. Data Security



2. Overview of Data Security

Overview of Data Security

Learning Objectives

After completing this unit, you'll be able to:

- Explain the importance of giving the right people access to the right data.
- List the four levels at which you can control data access.
- Describe a typical scenario for limiting data access at each of the four levels.

Introduction

Choosing the data set each user or group of users can see is one of the key decisions that affects the security of your Salesforce org or app. Once you've designed and implemented your data model, give some thought to the kinds of things your users are doing and the data they need to do it.

Let's say you're building a recruiting app to help manage open positions, candidates, and job applications. You'll have to store confidential data, such as social security numbers, salary amounts, and applicant reviews, that only some types of users should see. You'll want to secure the sensitive data without making life harder for recruiters, hiring managers, and interviewers.

With the Salesforce platform's flexible, layered sharing model, it's easy to assign different data sets to different sets of users. You can balance security and convenience, reduce the risk of stolen or misused data, and still make sure all users can easily get the data they need.

The platform makes it easy to specify which users can view, create, edit, or delete any record or field in the app. You can control access to your whole org, a specific object, a specific field, or even an individual record. By combining security controls at different levels, you can provide just the right level of data access to thousands of users without having to specify permissions for each user individually.

Note

Although you can configure the security and sharing model entirely using the user interface, the model works at the API level. That means any permissions you specify apply even if you query or update the data via API calls. The security of your data is protected, regardless of how users get to it.

Levels of Data Access

You can control which users have access to which data in your whole org, a specific object, a specific field, or an individual record.

Organization

For your whole org, you can maintain a list of authorized users, set password policies, and limit logins to certain hours and locations.

Objects
Access to object-level data is the simplest thing to control. 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. For example, you can use object permissions to ensure that interviewers can view positions and job applications but not edit or delete them.

Fields
You can restrict access to certain fields, even if a user has access to the object. For example, you can make the salary field in a position object invisible to interviewers but visible to hiring managers and recruiters.

Records
You can allow particular users to view an object, but then restrict the individual object records they're allowed to see. For example, an interviewer can see and edit her own reviews, but not the reviews of other interviewers. You can manage record-level access in these four ways.

- ***Organization-wide defaults*** specify the default level of access users have to each others' records. You use org-wide sharing settings to lock down your data to the most restrictive level, and then use the other record-level security and sharing tools to selectively give access to other users.
- ***Role hierarchies*** give access for users higher in the hierarchy to all records owned by users below them in the hierarchy. Role hierarchies don't have to match your organization chart exactly. Instead, each role in the hierarchy should represent a level of data access that a user or group of users needs.
- ***Sharing rules*** are automatic exceptions to organization-wide defaults for particular groups of users, so they can get to records they don't own or can't normally see. Sharing rules, like

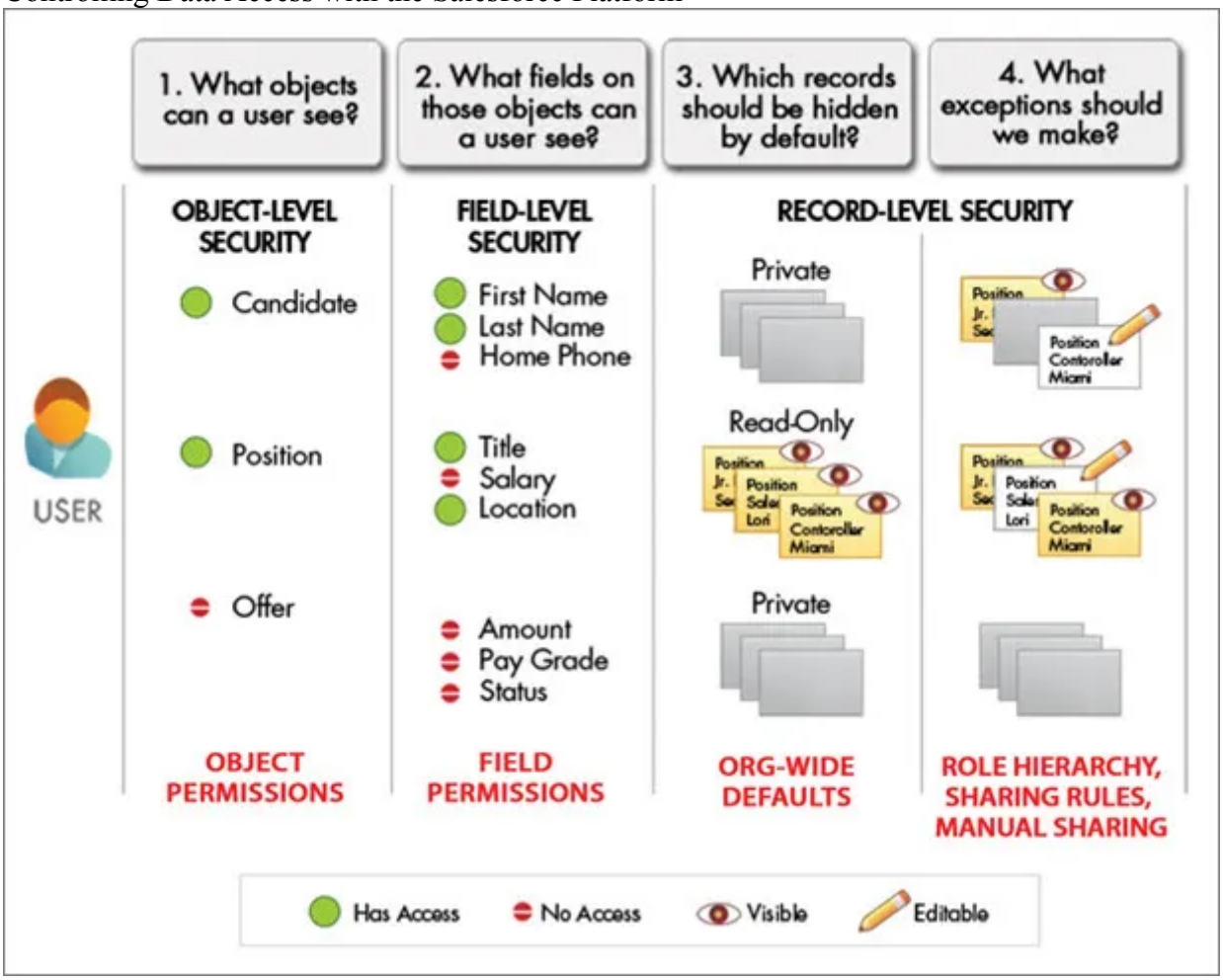
role hierarchies, are only used to give additional users access to records. They can't be stricter than your organization-wide default settings.

- ***Manual sharing*** allows owners of particular records to share them with other users. Although manual sharing isn't automated like org-wide sharing settings, role hierarchies, or sharing rules, it can be useful in some situations, such as when a recruiter going on vacation needs to temporarily assign ownership of a job application to someone else.

Tip

Make a table of the various types of users in your organization. In the table, specify the level of access to data that each type of user for each object and for fields and records within the object. You can then refer to this table as you set up your security model.

Controlling Data Access with the Salesforce Platform



Audit System Use

Auditing provides important information for diagnosing potential security issues or dealing with real ones. Someone in your organization should audit regularly to detect potential abuse. Look for unexpected changes or patterns of use.

Record Modification Fields

All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.

Login History

You can review a list of successful and failed login attempts for the past six months. For more information, see Monitor Login History.

Field History Tracking

You can turn on auditing to automatically track changes in the values of individual fields. Although field-level auditing is available for all custom objects, only some standard objects allow it. For more information, see Field History Tracking.

Setup Audit Trail

The Setup Audit Trail logs when modifications are made to your organization's configuration. For more information, see Monitor Setup Changes.

Resources

- Security Implementation Guide

Quiz Complete!

+100 points

Data Security
100%
Progress: 100%
View more modules