**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.

## Set Password Policy

You can configure several settings to ensure that your users’ passwords are strong and secure.

**Password policies**

Set password and login policies, such as specifying an amount of time before all users’ passwords expire and the level of complexity required for passwords.

**User password expiration**

Expire the passwords for all the users in your org, except for users with “Password Never Expires” permission.

**User password resets**

Reset the password for specified users.

**Login attempts and lockout periods**

If a user is locked out due to too many failed login attempts, you can unlock the person’s access.