Data Security

Monday, August 08, 2016 10:21 AM

Overview of Data Security
Prior to setting up access, it's important you have designed and implemented the data model.
Have an understanding of each field and who needs to see them.
The security and sharing model is implemented entirely at the API level. This ensures the security of your data is protected regardless of how it is accessed.

Access is layered
Org Access
Object Access - Profile level
Record Access - Role Hierarchy
Field Access - Field-Level Security

- **Organization-wide defaults** specify the default level of access users have to each other's records. You use organization-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** open up access to those higher in the hierarchy so they inherit access 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** enable you to make automatic exceptions to organization-wide defaults for particular groups of users, to give them access 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 organization-wide sharing settings, role hierarchies, or sharing rules, it can be useful in some situations, for example, if a recruiter going on vacation needs to temporarily assign ownership of a job application to another employee.

Audit features include:
Record Modification Fields
Login History
Field History Tracking
Setup Audit Trail