Salesforce Security for Nonprofits: Basics

Kevin Dillon
Senior Consultant, Exponent Partners

Salesforce® security is a dense topic, and can be intimidating. **How do you ensure the appropriate level of access for all your staff and constituents?**

As a consultant for solutions based on the Salesforce platform, I've overseen system security for large and small nonprofits. The finer points can be nuanced. Fortunately, a working understanding of security can take you far when communicating with your implementation partner, or making a tweak later on your own.

Why Use Security

Hide sensitive data: You can hide fields, specific records, or even entire objects from certain users or types of users. At the field level, for example, you could hide social security numbers on a need-to-know basis. At the object level, you might decide the program team should not see fundraising data.

Protect data from being modified inappropriately: Sometimes, there may be data that users should be able to see but not edit. Using Salesforce security settings, you can specify particular fields or objects as read-only for a group of users. For example, you may want your programmatic users to be able to see the donation history of donors, but not to have the ability to edit this information.

An understanding of how to apply some basic principles of security in Salesforce can also mean the difference between major headaches and a smooth experience for each of your users.

Tools for Managing Security

Profiles: Each user must have a profile, which controls both object-level access and field-level access. For object-level access (a.k.a. CRUD or Create, Read, Update, Delete permissions), the profile determines which objects a user has the ability to see, create, edit, and delete records on. Field-level security determines which fields on each object a user has access to and if they are able to edit those fields. **Please note:** there are many other permissions controlled by the profile. I recommend learning more through resources like this Salesforce profile overview or speaking with an implementation partner.

Organization-Wide Defaults: Organization-wide defaults are a more advanced form of security, and are ideal for larger organizations. They are often not necessary for smaller organizations. These defaults establish the default level of access for all users to records within a given object. Sharing rules can be used with organization-wide defaults to share records with a particular group of users (in the same role or public group), while restricting access for other users.

Permission Sets: Permission sets allow you to fine-tune permissions on a user-by-user basis. They grant individual users the permission to view and customize types of records and fields.

Best Practices

1. Promote sharing wherever possible. This helps your staff see information organization-wide. It also fosters greater collaboration among users, often leading to richer and more accurate data. Basic contact information is usually a good starting place to share and establish a point of commonality. Opt for open security (meaning all users can access all data) whenever possible, unless you have a serious need to restrict. Siloed data may also introduce unnecessary

complexity to your system. For example, multiple staff may unknowingly create duplicates of a record, which interferes with reporting and API integrations.

2. Fit your security to the size of your organization. The more layers of security you have, such as *permission sets*, or different *profiles* (explained above), the harder it becomes to manage. You may spend unwanted time adjusting individual permissions. If you have a small set of users, use basic security wherever possible. This means, for example, one profile type, with one additional larger set of permissions for your system administrator.

3. Divide your users by what they need to do. A good strategy is to define what you need each of your users to do, then place them in "buckets" based on the permissions they will need. If you have volunteers who will be accessing the system, for example, perhaps they should not have access to all staff data. These buckets can then be used to determine what profiles need to be created.

4. Identify and secure your most sensitive information. Privacy is a real concern for certain types of data. For example, if you are a health or education organization and have sensitive HIPAA- or FERPA-protected data, you will want to make special note of this. When bringing this type of data into Salesforce, it's advisable to consult with your implementation partner to make sure they apply the appropriate level of security.

5. Document your security model. It will be valuable for you to list why your security model was created and who it was assigned to, and spell out your strategy. (It's just as important to note what you can share as what you can't.) This model provides a map and is helpful for transitioning new staff and system administrators. Further, the document will help you understand the implications of any changes you make to your security from a high level. Make sure to keep it current!

Additional Resources

- Salesforce Security Webinar
- Salesforce Security Workbook
- Salesforce Security Implementation Guide (more in-depth)