Example document: User Roles

How to use this example document:

This example document could be a starting point for your own user Roles documentation, or just an inspiration to see how others have done it.

The examples below assume an organization with tiered access including state-level organization and local chapters, in which staff of each state and chapter actually log in to use the system – and the system is a CRM running on the organization's main website, powered by WordPress or an equivalent content management system (CMS). Most organizations (perhaps yours) don't have that level of institutional complexity. I recommend you trim this down to make it as simple as possible while still serving your actual needs *at present*. You can (and probably will) need and want to modify it later.

1. Commit yourself not to make any changes to user permissions until you've completed this whole process.
2. Copy this document to one of your own, and strip out the Roles section. Your Roles section will be a blank slate.
3. Read through the other sections of this document to understand how it's meant to work. This will be a durable policy document for your organization.
4. Take time to think about the needs of your various users (those who actually log in). Who are they? What do they need to do in the system? What must they *not* be allowed to do? How can you group them into "clusters" that describe various "classes" of access levels? These clusters will be your system roles.
5. Use this document for inspiration if you like, but begin to document those "clusters" of users as roles in your (now empty) Roles section.
6. Optional but *very* useful: If you thought of some roles but decided not to proceed with them, document that in the section "Examples of "roles" considered but not implemented." Months or years from now, when you or someone on your team *again* proposes such a role (and they will), you'll have a record of your rationale for deciding against that in the beginning. You can always change your policies, but remembering your past rationale can be very informative.
7. Now that you have a formal list of roles, consider every one of your current users. Which of your documented roles should each one have? If you find that some of your users can't do what's needed with the roles you've documented, now is the time to modify your documented roles. Repeat this process until you're confident that your documents roles will actually accommodate your needs. (if you have 10,000 current users, this will sound like a lot of trouble. But compare that to pissing off 10,000 people by being careless at this stage. It's worth being careful.)
8. You're done! You now have a formal policy document describing your system's permissions model. Keep it handy, reference it often, and update it as needed.
9. And for your next trick: it's time to dive in and start updating your system permissions and user roles, with this document closely at hand.

Allen Shaw, Jan 9, 2026

Purpose

The WordPress site at example.com supports the following user roles as a means of segregating user access so that users may be granted access only to functionality on which they have been properly trained, and for which they may reasonably be expected to take responsibility.

Assumptions and expectations

This permission scheme is built around certain assumptions and expectations:

- **Level of detail:**
  Role descriptions in this document are meant to be short, plain-English, and easily understood. The inclusion of greater or lesser detail is a judgement call, but in general: use these descriptions to describe intent and rationale; lists of specific permissions are generally to be avoided.
- **Assigning roles to users:**
  Any user may be granted more than one role, as appropriate for their training and job description. Granting or removing a role to/from any user is an "easy decision" – it will not directly have surprising effects on other users.
- **Altering role permissions:**
  Modification of permissions for any existing role should be undertaken with care – such action can have complex and hard-to-predict effects on existing users.
- **Creating new roles:**
  Creation of new roles will have no direct impact on existing users; however, a proliferation of roles will increase the administrative overhead in managing users and roles; thus creation of new roles merits careful consideration.
- **Maintaining this document:**
  Once these roles (and their attendant permission configurations) are established, any changes to live system permissions should be recorded in this document, in *at least one* of the following ways:
    - Note the specific change in a dated entry in Appendix 1: Logged Permission Changes.

- Update the relevant role description, as far as necessary to remove whatever ambiguity may have led to the situation that required permissions to be changed.

Roles

Once you've copied this document to a draft for your own use, delete this section; it's just here as an example.

Administrator

This is the "super user" role. Users with this role have all possible permissions on the site, including creation and modification of users, roles, permissions; creation and deletion of site images, articles, menus, and all other content; installing or removing plugins; viewing and editing all CRM contacts and configurations.

State Leadership

Users with this role are expected to be leaders in the state org. As such, they should have read/write access to all CRM contacts and other data; access to create website posts and pages; **but they should not have** read/write access to other user accounts, nor to modify advanced CRM configuration.

Communications

Users with this role are expected to facilitate mass communications both with known constituents and with the broader public. As such, they should have access to send mass emails; to view and edit all CRM contacts; and to create, edit, and delete blog posts/articles

Outreach/Membership

Users with this role are expected to facilitate event participation and org membership. As such, they should have access to create and edit events and event participants; create and edit membership types and individual membership records; and to view financial records (since these are relevant to event participation and membership); and to view and edit all CRM contacts (any of whom may be event participants or members at some time).

Chapter Leadership

Users with this role are expected to be leaders in a local chapter. As such, they should have access to create and edit events; and to view (but not edit) contacts according to permissioned relationships.

Examples of "roles" considered but not implemented

Once you've copied this document to a draft for your own use, delete this section; it's just here as an example.

Executive

This was originally described as "Create blog posts, create events, view contacts, etc.", which is essentially equivalent to "Communications + Outreach/Membership." Therefore, this role is not needed. Users who need this level of access should simply be given *both* roles: Communications *and* Outreach/Membership.

Officer

This was originally described as "same as Executive," and was considered a possible future need, based on the notion that we may one day want to split some "Executive" users off into a more- or less-privileged role for officers. Rather than maintaining multiple roles (or combinations of roles) with identical permissions (which creates admin headaches), we'll hold this idea in reserve for the future. If such a new classification of user permissions becomes necessary, we can document and create the role at that time, and easily move users into that role as needed.

Appendix 1: Logged Permission Changes

Use the following table to enter dated records of permissions changed on the live site (see *Assumptions and expectations: Maintaining this document*, above).

Date	Your name	Description of change (name of permission; name of role; added/removed)	Rationale