Hierarchy and inheritance permissions in SharePoint

By default, permissions on lists, libraries, folders, etc. are inherited from their parent site. You can, however, break this inheritance for any secure object at a lower level in the hierarchy by editing the permissions (that is, creating a unique permission assignment) on that secure object.

Websites themselves are securable objects on which permissions can be assigned. You can configure sub-sites to inherit permissions from a parent site or break the inheritance and create unique permissions for a particular site. Inheriting permissions is an easy way to manage a group of websites; however, if a sub-site manages permissions from its parent, that set of permissions is shared. This means that owners of sub-sites that inherit permissions from the parent site can edit the permissions of the parent. Ensure that any changes you make to the permissions on the parent site are appropriate for the parent site and all sub-sites that inherit those permissions.

In the above image:

- **Subsite 1** inherits permissions from the Top-Level Site. This means that changes made to SharePoint groups and permission levels on the Top-Level Site also affect Subsite 1.
- **Subsite 2** is also inheriting permissions from its parent (Subsite 1). However, because Subsite 1 is also inheriting permissions from its parent, changes made to SharePoint groups and permissions levels on the Top-Level Site affect Subsite 2 also. This is because you cannot manage permissions on a sub-site that is inheriting permissions. Instead, you either manage the permissions of the parent (i.e. Top-Level Site) or you break the inheritance and create unique permissions.
- **Subsite 3** has unique permissions. This means that it does not inherit permissions from its parent site. Therefore, any changes made to the permission levels and SharePoint groups on Subsite 3 do not affect its parent site.
- **Subsite 4** is inheriting permissions from Subsite 3, so any changes to permission levels or SharePoint groups on Subsite 3 affect both sites.

Each site contains additional securable objects which have a particular position in the site hierarchy, as shown here:
Lower-level securable objects automatically inherit permissions from their parent. For example, a list or library inherits permissions from the site, and list items and documents inherit permissions from the list, library, or folder that contains them. You can break this inheritance at any point in the hierarchy and assign unique permissions. When you break the inheritance from the parent, the securable object from which you broke the inheritance receives a copy of the parent's permissions. You can then edit those permissions to be unique, meaning that any changes you make to the permissions on that securable object do not affect the parent.

**Plan for permission inheritance**

It is easiest to manage permissions at only the site level, whenever possible. This means you should create your site hierarchy in a way that allows you to assign permissions to sites that are appropriate to all securable objects within the site, such as lists, libraries, folders within lists or libraries, documents, and items. Although you can assign unique permissions on any securable object in the site hierarchy, to do so is more cumbersome than inheriting permissions. It gets more difficult when some lists or libraries within a site have fine-grained permissions applied or when some sites have sub-sites with unique permissions and some with inherited permissions.

As much as possible, arrange sites, sub-sites, lists, and libraries so that they can inherit most permissions. Put sensitive data into separate sub-sites, lists, libraries, and so on.

For example, it is much easier to manage permissions using a hierarchy like the one shown in the following example, rather than mixing sensitive and non-sensitive data in the same sites, lists, and libraries.

- **Site A** Group homepage
  - **List A** Non-sensitive data (inherited permissions)
  - **Document Library A** Non-sensitive data (inherited permissions)
  - **Sub-site B** Sensitive data (unique permissions)
    - **List B** Sensitive data (unique permissions)
    - **Document Library B** Sensitive data (unique permissions)

Notice that the list and library in Site A contain non-sensitive data and Sub-site B was created below Site A to contain a list and library for storing sensitive data. In this scenario, you can assign permissions to Site A that are appropriate to List A and Document Library A and create unique permissions on Sub-site B which are appropriate for List B and Document Library B.