

All Partners Access Network

# APAN SharePoint Governance – Registration List Permissions

December 27, 2023



# 1. CONTENTS

<b>2. OVERVIEW .....</b>	<b>3</b>
2.1. DOCUMENT OBJECTIVE .....	3
2.2. REVISION HISTORY .....	3
2.3. RELATED DOCUMENTS .....	3
<b>3. APAN SHAREPOINT SECURITY OVERVIEW .....</b>	<b>4</b>
3.1. SECURITY MODEL.....	4
3.2. APAN ACTIVE DIRECTORY SECURITY GROUPS.....	4
3.3. SUBSITE SECURITY INHERITANCE.....	4
3.4. LIST/LIBRARY LEVEL SECURITY .....	4
<b>4. SHAREPOINT CUSTOM REGISTRATION LIST .....</b>	<b>5</b>
4.1. PURPOSE .....	5
4.2. SETUP LIST PERMISSION .....	5
4.3. BREAK PERMISSIONS INHERITANCE .....	5
4.4. CONFIGURE ITEM-LEVEL PERMISSIONS FOR REGISTRATION LIST .....	7

## 2. OVERVIEW

### 2.1. DOCUMENT OBJECTIVE

The main objective of this document is to provide guidelines for setting “Guest Registration Lists” within SharePoint. This document will also provide the necessary guidelines and steps in creating new registration lists across all site collections.

### 2.2. REVISION HISTORY

Revision	Date	Description	Revised By
1	3 December 2019	SharePoint Registration Lists Guidelines	Sayed Jaffar
2	27 December 2023	APAN SharePoint Registration List Configurations	Sayed Jaffar

### 2.3. RELATED DOCUMENTS

Document Name	Revision	Author
N/A	N/A	N/A

## 3. APAN SHAREPOINT SECURITY OVERVIEW

### 3.1. SECURITY MODEL

APAN has implemented a pre-configured security model for its SharePoint sites. In SharePoint, security groups are specific objects with "users" as members, each having its own configurable settings. These settings encompass details such as group ownership and permissions related to user addition or removal. The table provided offers an overview and description of the different pre-configured security groups and their associated permission levels.

Security Group	Permission Level	Authority
Site Owners	Full Control	Can add/edit/delete content, delete sites, and set up permissions for a given site
Site Members	Contribute	Can add/edit/delete content on a site
Site Visitors	Read	Can only read and download content
Everyone (used for Registration List permissions)	Contribute No Delete	Same as Contribute without the ability to delete item

Additional SharePoint security groups can be created at the discretion of a **Site Owner** or a **Site Collection Administrator (SCA)**. However, this practice is discouraged and should be minimized as much as possible.

### 3.2. APAN ACTIVE DIRECTORY SECURITY GROUPS

The table below captures all the existing global security groups for APAN SharePoint Farm

Group Name	Description
Everyone (All Users)	All users that are registered with APAN

### 3.3. SUBSITE SECURITY INHERITANCE

All Site Collections allow the creation of subsites in their respective site collections. Site Collection Admins (SCA) and Knowledge Mangers (KMs) must make **Subsite Site Owners** aware of the dangers of **security inheritance**. If possible, security inheritance must be broken between a subsite and a parent site collection.

### 3.4. LIST/LIBRARY LEVEL SECURITY

When applicable, unique list/library or file and folder security can be set, however, the practice shall be avoided or minimized as much as possible. In those cases where certain files or folders must be hidden from a group of users, it is preferable to create a new site with unique security.

## 4. SHAREPOINT CUSTOM REGISTRATION LIST

### 4.1. PURPOSE

Guest Registration List refers to a custom list created to register users for a specific event/exercise/training etc. Within APAN context, these lists refer to custom lists setup by Site Owners to pre-register guests before a particular exercise or event. Since the users are not approved to be a member of the respective site, therefore a new security mechanism is needed for the guest registration lists to ensure that security and content of the site is secured while authenticated users are allowed to access a specific list within the site. The following criteria needs to be met as part of the solution provided in these guidelines:

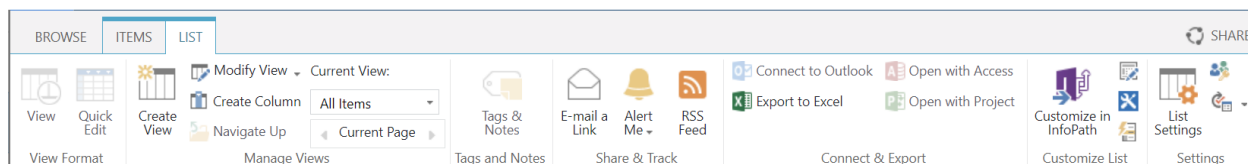
1. Registered Users can complete registration.
2. The registering users can view their own registration submissions (and only their own)
3. Site owners can view all registrations in lists that they own
4. No non-members can upload content to a site.
5. The information contained in this list should not be searchable.

In order to implement security to address the aforementioned requirements, follow the instructions provided in the next section.

### 4.2. SETUP LIST PERMISSION

By default, all lists and libraries inherit permissions from the parent site permissions. In the first step, we will break permission's inheritance between the "Registration List" and the "Parent Site".

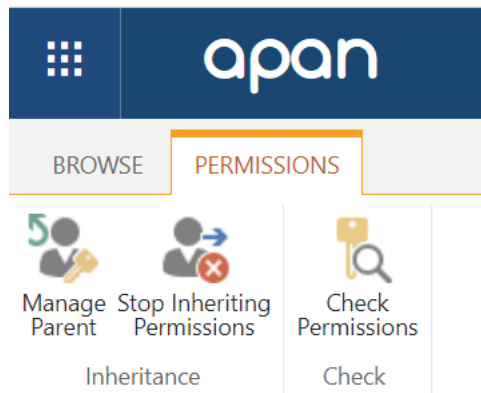
### 4.3. BREAK PERMISSIONS INHERITANCE



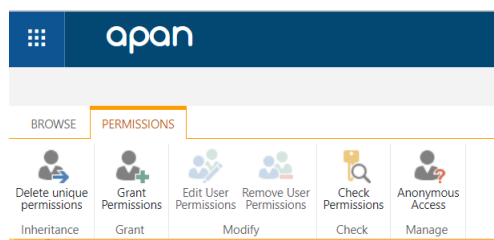
- Navigate to the SharePoint site where your (Registration) List is located
- Click on LIST tab at the top left of the page, and click on LIST SETTINGS

- [List name, description and navigation](#)
- [Versioning settings](#)
- [Advanced settings](#)
- [Validation settings](#)
- [Audience targeting settings](#)
- [Rating settings](#)
- [Form settings](#)
- [Delete this list](#)
- [Save list as template](#)
- [Permissions for this list](#)
- [Workflow Settings](#)
- [Enterprise Metadata and Keywords Settings](#)
- [Generate file plan report](#)
- [Information management policy settings](#)
- [Record declaration settings](#)
- [RSS settings](#)

- Under “Permissions and Management” click on “Permissions for this list”



- If the ribbon displays the list inheriting permissions from Parent Site (as shown above in the screen shot), then click on "Stop Inheriting Permissions" button. This will break the inheritance from the parent site.
- Your Ribbon should now look like the screen-shot below



- Click on “Grant Permissions” and enter “Everyone” in the field showing “Enter names or email addresses...” and then select “Everyone” from the results.
- Click on “SHOW OPTIONS” link to select the desired permission level from the “Select a permission level” dropdown.
- Contribute or Contribute No Delete are the two common permission levels for registration lists.

- Click on “Share” button.
- This will add “Everyone” (All Registered Users) to your registration list permissions.
- Now if a user who does not have permission to your site navigates to this registration list, he/she will be able to access the registration list

## 4.4. CONFIGURE ITEM-LEVEL PERMISSIONS FOR REGISTRATION LIST

The above settings will setup who can access the registration list, but it also allows the authenticated user to access all content within the registration list. To secure the registration list further, the following actions should be performed.

1. Go to [List Settings](#) page, and then click on [Advanced Settings](#) link.
2. On this page, configure all settings according to the image below.

### Settings ▸ Advanced Settings

Content Types

Specify whether to allow the management of content types on this list. Each content type will appear on the new button and can have a unique set of columns, workflows and other behaviors.

Allow management of content types?

☐ Yes ☒ No

Item-level Permissions

Specify which items users can read and edit.

**Note:** Users with the Cancel Checkout permission can read and edit all items. [Learn about managing permission settings.](#)

**Read access:** Specify which items users are allowed to read

☐ Read all items  
☒ Read items that were created by the user

**Create and Edit access:** Specify which items users are allowed to create and edit

☐ Create and edit all items  
☒ Create items and edit items that were created by the user  
☐ None