SP Marketplace
HR Suite Security Guide

Module Version 11.0

Copyrights and Trademarks

Contact SP Marketplace

Email: info@spmarketplace.com

Postal Mail:

SP Marketplace
17319 Penn Valley Drive
Penn Valley, CA 95946

Website: www.SPMarketplace.com

Support: www.SPMarketplace.com/Support

Email: support@spmarketplace.com

Table of Contents

Introduction

In December 2016 SP Marketplace restructured its Human Resource product into several connected and synchronized Products. What was once a single Human Resources site being now five products. This document will detail the security aspects of the SP Marketplace HR Suite of products. There are other customization, design and usability documents that cover the details and guidelines for the HR products, including HR Portal, HR Hiring, HR Onboarding, HR Reviews, and HR Policy Management.

This new structure of multiple sites for Human Resource by function was done to:

1. Simplify the navigation and functions within each individual HR module site.
2. Provide for more specific grouping and selection of HR functionality by customers.
3. Provide full security by utilizing native SharePoint security model for permissions.
4. Improve support by eliminating master page customization to implement security.

SharePoint Permissions

All security will be managed by applying SharePoint permissions at the site, list and, in some cases, the item level. The general structure of access for these sites and the default OOTB permissions at setup is as follows:

All Users	Members of this group will have Read access at the site level and include all SharePoint users by including the special "Everyone except External Users" group. Individual lists within each site may break inheritance from the parent site and assign All users contribute rights to lists as needed.
Managers	Members of this group will have Read access at the site level and contribute access to some lists. Generally, this group contains all managers in the organization.
HR Staff	Members of this group will have Contribute access at the site level and designed to include members of the Human Resources department.
SPMP Admin	Members of this group will have Full Control permissions. It is intended to give permissions to people who will do administration of your site. The account for your SP Marketplace Services Associate will already be in this group.

Cautionary Note

It is critical that NO additional SharePoint Groups or individual people are added to the site permissions for any of the HR Suite products. The permissions and security will be enforced, as designed, as long as the out-of-box groups are used to give employees, managers, HR staff, and SharePoint Administrators access to the HR sites. SP Marketplace recommends that any changes be carefully analyzed and made with our assistance. Please familiarize yourself with the example below that lists the consequences of creating a new group and adding one person to it:

Example

An example of the problem created by adding an additional group to the site permissions is as follows:

1. A new SharePoint Group, called Approvers, is added to the site permissions of the HR Portal and given Contribute permissions.
2. The Employee Documents library will inherit that group and so the Approvers group will now have contribute access to this library.
3. A serious permissions breach happens when subsequently an employee uploads a new confidential document to the Employee Documents Library. This is because whenever a new document is uploaded to any library, it will initially inherit the permission from the library. Now anyone in the Approvers group will have contribute access to this document.
4. The current Smart action that enforces the security design will add the SharePoint Userid for this employee to have access to their own document, remove the All Users group access, and remove the Managers group access, but will not remove the Approvers group access but that was just created and is not specifically removed by the action.
5. Unless a new Smart Action is added to remove the Approvers, the person(s) in the Approvers group will still have contribute access to all employee confidential documents.

HR Portal Security

Employee Lists

For security reasons the original Employee List has been split into two synchronized lists of employee data. The first, called Employee List, contains general non-confidential information such as Last Name, First Name, SharePoint UserID, etc. and the other list, called Employees Confidential, contains privacy and confidential information such as Date of Birth, Salary, Social Security Number, etc.

Employee List

All Users	Read Only access by the All Users group, "Everyone except External users"
Managers	Manager's get access by virtual of All Users
HR Staff	Contribute access only by the HR Staff group.
SPMP Admin	Full Control

Employees Confidential

All Users	No Access
Managers	No Access
HR Staff	Contribute access only by the HR Staff group.
SPMP Admin	Full Control

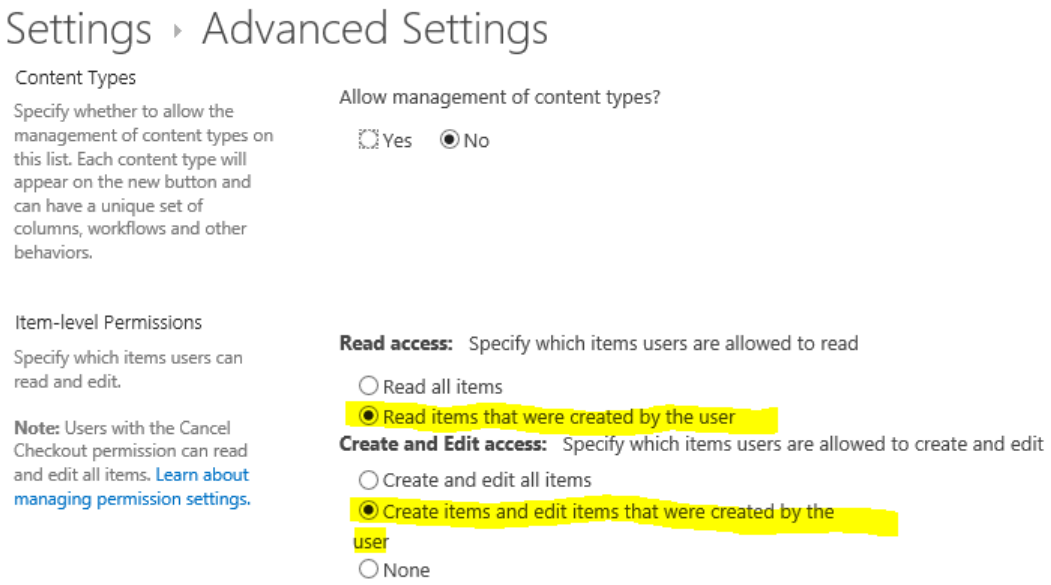
Employee Data Management

All users can see their own employee information by submitting a request and their information will be sent them by Email. They can also submit a request to change their information in the confidential employee list but will not be able to view it directly. This design avoids the need to provide item level security on the confidential employee list.

In addition, the Manager (based on the Reports to field in the employee record in the Employee List) can request that Employee information, for people that he is designated as the Manager, be emailed to his email account. And the Manager can submit change requests that will update his employees' information without giving the manager direct access to the Employee Confidential list.

Service Request List

The Service Request list is designed to provide item level security so that, other than the HR Staff, only the requestor of a service request can see or edit service requests that he is designated as the Requester. To provide this level of security, All Users group will be given Contribute permissions to the Service Request List and the List level permissions setting will be set to Item level security as shown below:

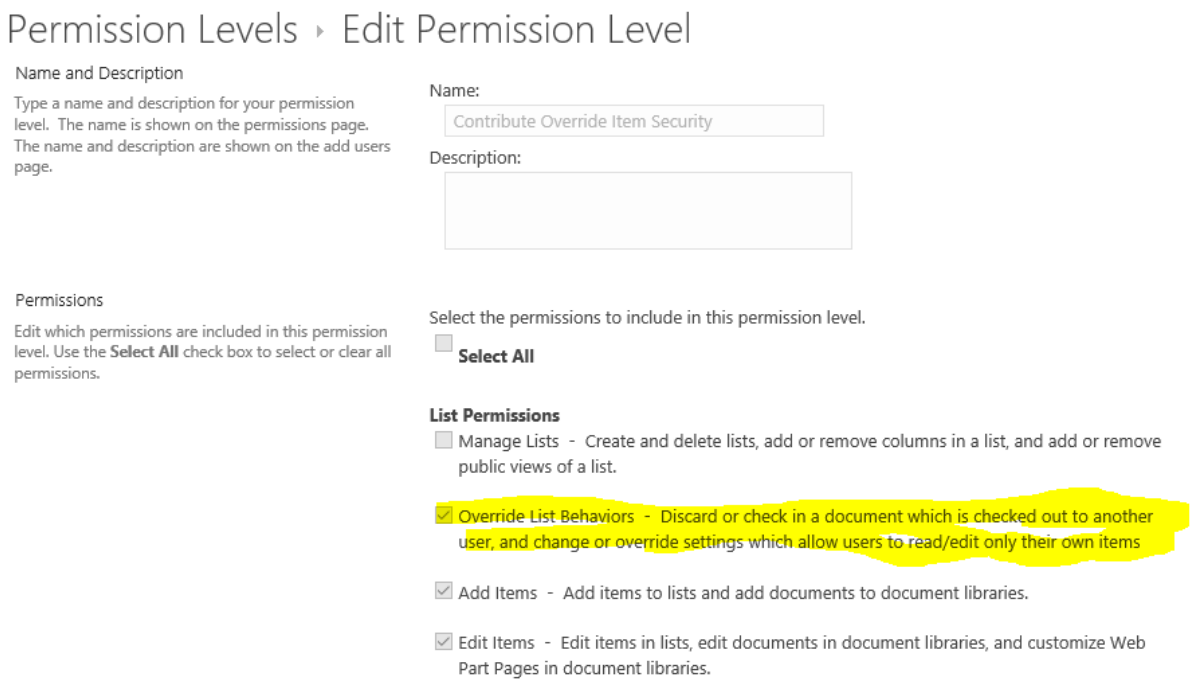


Additional Lists

There are 3 other lists that are also setup with List Item level security in the Advanced Settings and no surrogate capability will be provided for those lists. All three of these lists are used to submit/update the employee list when they are created. Editing and changes items in these lists will NOT update the Employee List. But they can be used by HR Staff to track changes that have been submitted.

1. Employee Update Info – used thru the employee portal to submit updates to the users Employee list information.
2. Manager Employee Change Request – used by managers to update Employee list information. Not accessible by employees
3. New Employee – used by the Onboarding site to create new employee items

When using this list setting, for the HR Staff group to be able to edit Service Requests, they must have the Override List Behaviors Permission. So as part of the OOTB installation of the HR sites a new permission level (Contribute Overwrite Item Security) will be created and assigned to the HR Staff Group as shown below:



To allow a surrogate to create a Service Request for the Requester, there is a Smart Action on the Service Request list that will change the author (Created By) field to be the same as the Requester if that is not already true. This is needed because the above settings for Item level list permissions is based solely on the Created By field and not the Requester or any other person field in the item.

The New Employee list is a list that All Users have contribute access and is used by the HR Onboarding site to create a new employee in the Employee list. There are Smart Actions defined for this list that run with elevated permissions that allow a new item to be created in the Employee List from this New Employee List.

Since the primary users of the HR Department site will be members of the Human Resources department there may be other Lists and Libraries that should be changed to remove All Users group even Read access to those Lists and Libraries. This can be done easily after the OOTB installation by breaking the inheritance on each of those Lists or Libraries and removing the All Users group.

The Benefits list will also have Item Level Security specified at the List Level similar to Service Requests. Thru the use of Smart Actions the Created By field will be set to the Sharepoint Userid specified for the benefit item so HR Staff can create a benefit for an employee and that employee will still be able to see his benefits in the Employee portal

Employee Documents

The Employee Documents library which is a child list to the Employees Confidential list has Item Level Security on each document managed thru Smart Actions. In general each document has unique permissions that restrict the document to the HR Staff Group, the SPMP Admin Group and the employee who "owns" the document.

HR Hiring Security

The OOTB installation of HR Hiring has no item level security permissions. Some customers may need tighter level security such as only allowing managers to see and edit their Requisitions, Applicants and Candidates but that will require further customization and is not provided as part of the OOTB installation.

Managers and HR Staff members are the primary users of this site and employees only normally access the site to participate in the Interview process. Both the Managers Group and the HR Staff group will be given Contribute access to the entire SPMP HR Hiring site. The All Users group will be given Read access to the HR Hiring Site and only contribute access to the Interviews list and the Candidate Feedback list.

For those customers who want to restrict access to Requisitions, Applicants and Candidates to only Managers and HR Staff, the simplest customization would be to remove All Users from any access to the HR Hiring site and handle any Interviews and candidate feedback to members in the All Users group manually outside the HR Hiring site.

More complex item level security in this area of Employee candidate interviews thru customization could get rather tricky and complex. Because in order to interview a candidate for a requisition the interviewer most likely needs at least read access to both the Candidate item and to the Requisition.

HR Onboarding Security

The SPMP HR Onboarding has only one list/library that has List level or Item level permissions and that library is the Employee Documents library,

Employee Documents

Since the documents that a new employee needs to complete may contain private or other sensitive information, access to each document needs to be restricted to the new employee who uploads the document (the Creator) the HR Staff Group and the SPMP Admin group.

In the OOTB site there will be no ability for a surrogate to upload documents for the new employee but this could be provided thru customization. If a customer is using the HR Onboarding process then most customers will have the new employee perform the upload of the document into the Employee Documents library.

Since document libraries do not support the List Item level permissions setting in the Advanced settings like lists have, smart actions are used to remove all user access to each document except for members of the HR Staff group, the SPMP Admin Group and the person who created the document.

In terms of general users (All Users) the only list that they have contribute access to is the On Board Tasks list. The Onboard lists itself is designed to be managed by members of the HR Staff group and All users will only have read access to that list and all other lists in the site except for tasks.

HR Reviews Security

SPMP HR Reviews has the most complex item level security of all the HR Suite of sites. HR Reviews need item level security and should only be seen and editable by the Employee, their Manager and the Approvers for the review. Smart actions are used on the Reviews document library to enforce this level of item level security.

The Employee list which, in this site, contains the history of reviews also has Item level security enforced thru Smart Actions. Employees can only see their Employee List item, Managers can see only all of the Employee List items where they are in the "Reports To" person field and HR Staff group members can see all Employee list items.

Change management in terms of Item level security is NOT automated, is not supported except by manual changes. While there is a desire for Item Level security, the impacts of change management are rarely considered.

An example of this is when a group of employees has a change in management, the new manager will get immediate access to the items in the Employee list for these employees but the old manager will still have access. In order to remove access by the old manager the item level security setting must be manually changed and the old manager removed item by item.

It is possible to automate this process thru customization but it requires that any change in the Reports to field is managed by a transactional list (something like a Change Manager list) that processes the changes (and has Smart Actions that can delete the old manager and add a new manager).

Whenever dealing with Item Level Security there are many other change scenarios other than a change of managers that must be handled manually. An example would be that the Approver of a review is on a month of vacation and wants to delegate his approval to someone else just for this time period.

Some more examples that are not handled except thru manual Item level security changes:

1. An employee changes managers - both the new manager and the old manager can see his review history and reviews
2. A manager changes job, is no longer a manager and get replaced by a new manager -- that old no longer manager will still be able to see all the review history and reviews
3. A review approver wants to delegate his review approvals to someone else for the next 15 days -- not doable without manual changes

HR Policy Management Security

The primary user of Policy Management will be the HR Staff, consequently the All Users group will ONLY have access to 2 lists (Read access to the Policies document library and Contribute access to the Policy Acknowledgement tasks). However, the All Users group will also be given Read access to the following elements that are used, indirectly.

- Site Pages
- Site Assets
- SPJS-DynamicFormsForSharepoint
- SPJS-vLookupSettings
- Announcements