Permissions to Security Groups Worksheet

*What are permissions?*

*Permissions are the actions a user can take.*

*What is a security group?*

*A security group is a collection of permissions.*

*As part of this migration, a Security Group has been created for each permission currently used in your ClearCompany account. For example, anyone who had the recruiter permission will now be a part of the recruiter security group. If someone had multiple permissions, they will now belong to multiple security groups– one for each permission.*

*This worksheet is designed to help you review your current setup, evaluate the permissions of each role your organization uses, and group similar roles together. Once complete, security groups will be automatically assigned based on a user’s role–eliminating the need to manually set permissions for each new hire.*

*This change also makes it easier to manage future updates as new permissions are added to ClearCompany.*

## Step 1: Your Current Role: Permission Structure

*Resource: Instructions to pull permissions/role report*

Use this section to identify your existing roles and their associated permissions.

|  |  |  |
| --- | --- | --- |
| **Role Name** | **Current Permission(s) Assigned** | **Notes**  **(e.g. who typically holds this role, specific use cases)** |
| *Sales Manager* | *Hiring Manager*  *Task Assignee* | *Any manager across departments that are not human resources can be added to requisitions as hiring managers and asked to complete/approve documents during onboarding.* |
| *Catering Manager* | *Hiring Manager* | *Although this role does not currently have the task assignee permission there is a chance that they will need to complete onboarding paperwork for a new hire in the future.* |
| *IT Team Lead* | *User Admin,* | *Responsible for* |

Tip: Include all roles–even if they are currently empty or rarely used. This ensures you are set up for long term success.

## Step 2: Identifying your Ideal State: Role-Based Security Groups

*Resource:* [*Adding Security Groups to Roles*](https://clearco.zendesk.com/hc/en-us/articles/23266030137499-Security-Groups-Add-or-Update-another-User-s-Permissions#h_01HQPCHD0Y3QP7ST7Q7Y2CM4EQ)

Start grouping similar roles together based on what permissions they need.

|  |  |
| --- | --- |
| **Security Group Name** | **Role(s) to Include in this Group** |
| Employee | All Employees will receive this security group |
| Manager | Sales Manager |
|  | Catering Manager |
|  | Office Manager |
| Talent Acquisition/Recruiter Group | Recruiter |
|  | Talent Acquisition Coordinator |
| Onboarding Group | Onboarding Coordinator |
|  | HR Generalist |

Tip: Assign security groups at the role level, rather than managing permissions for each individual.

## Step 3: Mapping Current Permissions to Security Groups

*Consider how your existing permissions will translate into the new security group model.*

**Employee Security Group:** Every organization will have an employee security group that all employees are added to automatically. By default, it includes only the basic Employee permission.

If all employees need access to other permissions, those permissions should be added to the Employee Security Group.

* For performance & Goal clients: Add Goal Alignment and Performance Management.
* For LMS clients: Add Learning.

**CEO Access:** Any user who previously had the CEO permission will automatically be given the CEO designation on the user page within ClearCompany. If more than one user had the CEO permissions, all of them will receive the designation.

If you manually assign the CEO designation to a different user after the migration, that user will become the only one with the designation and it will be removed from all other users.

**Vendor Access:** If you currently have vendors accessing your system, they will now appear with a non-employee vendor designation on the user page within ClearCompany.

A security group should not be created for vendor access, and vendor users cannot be assigned any additional permissions beyond their vendor designation.

|  |  |
| --- | --- |
| **Security Group Name** | **Permission(s)** |
| Employee | Employee |
|  | Goal Alignment |
|  | Performance Management |
| Recruiter Group | Recruiter |
|  | Hiring Manager |
|  | Offer Letter Sender |
|  | Background Check |
| Manager Group | Hiring Manager |
|  | Task Assignee |

**Example for Review**

Scenario: Someone with recruiter permission + user admin permission + background check permission (3 permissions)

|  |  |  |
| --- | --- | --- |
| **Employee** | **Current Permissions** | **New Security Group** |
| *Emily Anderson, TA Coordinator* | *Employee* | *Employee Group* |
|  | *Recruiter* | *Recruiter Group* |
|  | *Hiring Manager* |  |
|  | *Offer Letter Sender* |  |
|  | *Background Check* |  |
|  | *Onboarding Coordinator* | *Onboarding Coordinator Group* |
|  | *Task Assignee* |  |
| *Tom Jensen, Catering Manager* | *Employee* | *Employee Group* |
|  | *Hiring Manager* | *Manager Group* |
|  | *Task Assignee* |  |

If all employees within the TA Coordinator role have the same permissions/security groups, you can assign the TA coordinator role to the associated Security Groups.

## Inbound SFTP

This section applies only to organizations that are already set up to use an inbound SFTP file to manage user data within ClearCompany and have chosen to create security groups to be assigned based on roles following the migration to the security group structure.

As part of this transition, you (or your third party provider) will need to adjust the inbound STP file that is sent to ClearCompany. When you are ready to remove the single-permission security groups created by the migration process and begin using your role-based security groups, it is important to coordinate the timing of these changes.

Before removing the single-permission security groups:

* The inbound SFTP file must be updated to remove the individual permission columns.
* Instead, the file should include the role column that lists each user’s assigned role, which will then drive their access via the new security groups.
* If the permission columns are not removed, the system will continue to recreate the single-permission security groups.

Please work with your internal team or third party provider to ensure the necessary updates are made before making the switch to role based security group assignments.