Portfolio Security & Access Overview

> Video has been removed from this PDF. Visit the BrightWork 365 knowledge base to view.

Project Management Context

Organizations do not always want to have entirely open access to their portfolio of projects but rather need to take a more granular approach to security and access, while others are fine with users having access to the entire portfolio of projects. BrightWork 365 provides several options to accommodate both of these security requirements through a flexible security and access model that includes business units, portfolios, and projects.

Your browser does not support HTML5 video.

What's In Scope for Security & Access?

- Portfolios
- Programs
- Projects
- Status Reports
- Risks
- Issues
- Actions
- Costs
- SharePoint
- Microsoft Teams
- Power BI with certain exceptions - see section Security and Power BI Reports below
- Custom table support (via customizations)

> **Caution**
>
> - Requests are excluded from security & access models so it is advised to use generic names for confidential requests as the project names will be visible to all users in various places in the app.
> - If you have templates with confidential information, be aware that if you leave the Portfolio and Program fields blank in the templates, all users can potentially read the information.
> - Users with the BrightWork PMO Manager security role have access to everything in BrightWork 365, including confidential projects, regardless of the chosen security model or their assigned business unit.

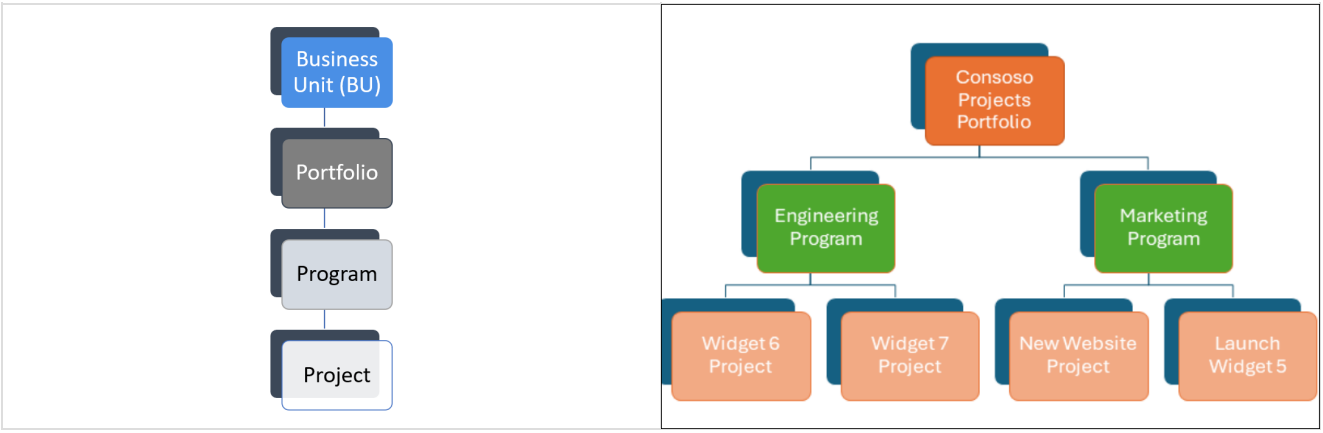
> **Note**
>
> - See Set Up Portfolio Security and Security and Power BI Reports.

- Content Templates take the Business Unit of the project from which they were created. To share a Content Template with project managers who do not have access add them as Team Members to the Content Template.

Security Model 1: Open Access (default model)

In the default open access model, all BrightWork 365 users have access to all portfolios, programs, and projects within the BrightWork 365 app. Note that this open access can be mixed together with a restricted security model as needed - see the other security models noted below.

Example: Single Open Portfolio



- One business unit and one portfolio with access to all app content.
- All users have access to all portfolios, programs, and projects.

Security Model 2: Portfolio Security

The Portfolio Security model explained in this article uses Power Platform business unit membership (see Microsoft article) combined with BrightWork security roles to grant users access to a portfolio attached to a business unit, and all the portfolio's child projects and records.

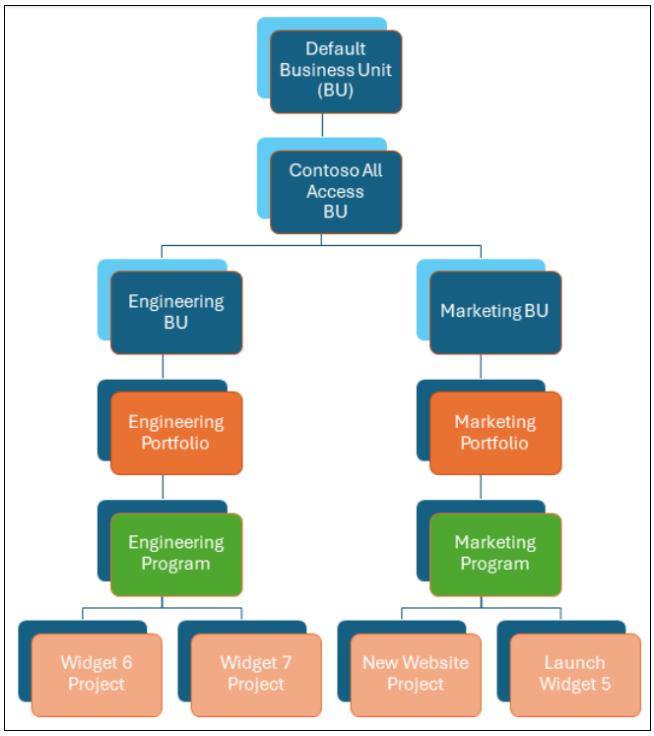
The BrightWork 365 business unit setup for Security and Access can divide access into a Confidential Projects and a Contoso Projects hierarchy ("Contoso" is being used as a sample organization name). Further business units can then be created to minimize access and more easily manage restrictions, as required.

The high-level steps to implement are as follows (further details in other article sections below):

1. Create business units and a business unit hierarchy.
2. Assign BrightWork 365 users to a home business unit.
3. Assign users security roles in their home business unit.
4. (Optional) Assign users the same security role they have in their home business unit in secondary business units as needed.
5. Create portfolios that will act as the top parent levels of the hierarchy in BrightWork 365.
6. Within each portfolio select an Owning Business Unit.
7. Assign programs to parent portfolios associated with the business unit desired for the program and its child projects.

After the above steps are completed, users will have access to the portfolios, programs, and projects that are associated with the business units in which they have been given security roles.

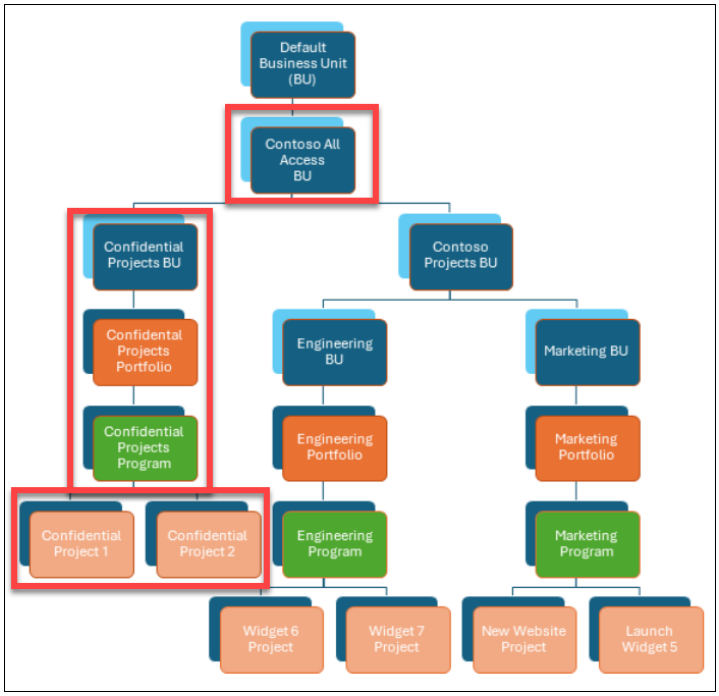
Example: Projects Secured by Department



- Engineering users are added to the Engineering business unit and only see its portfolio, program, and projects.
- Marketing users are added to the Marketing business unit and only see its portfolio, program, and projects.

> **Tip** A user can be given the same security roles in both the Engineering and Marketing business units so that they have access to both sets of portfolios, programs, and projects.

Example: Portfolio Security with Confidential Projects

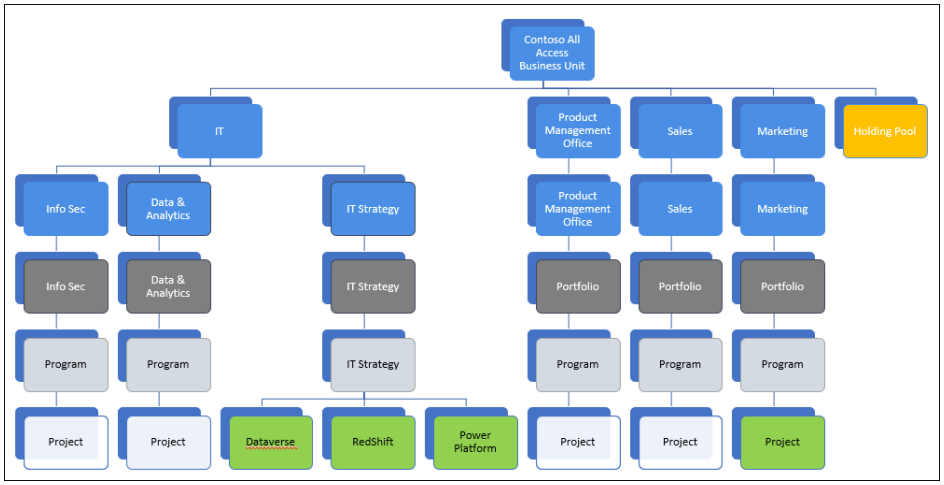


- Users who need access to all confidential and non-confidential projects would be in the parent Contoso All Access business unit.
- Users who need to see only non-confidential projects would be in the Contoso Projects business unit.
- If users should only be given access to individual confidential projects by exception instead of all projects in the Confidential Projects portfolio, give them access to the individual projects from within each project using Project Security and Access.
    - This exception project access is managed by the Access Level in each project team member record in each individual confidential project.

Security Model 3: Holding Pool

In the Holding Pool model, most users only get access to the projects in which they have been added as a Team Member. This can be accomplished with the project security option which provides this capability. For more information see Project Security & Access.

Example: Portfolio & Project Access by Exception Using Holding Pool without Confidential Projects Business Unit



- A select group of users are given membership in an All Access business unit.
- Majority of users placed in a Holding Pool business unit that has no portfolio, program, or project access. These users are given access to individual projects by exception as needed.