|  |  |  |
| --- | --- | --- |
| Product  Data verse for Teams | Specific Product | Share |
| Tables | Ref: <https://docs.microsoft.com/en-us/learn/modules/get-started-dataverse-teams/3-create-table>  While editing your table within the Power Apps **Build** screen, select **Manage Permissions** from the ribbon menu,  **Full access** - Allows users and groups full access to create new records, read all records, and update or delete records. This level of access should only be granted to users who need full control over the data.  **Collaborate** - Allows the creation of new records and the ability to read existing records, but it denies the ability to update existing records or delete them unless they were created by the user. This level of privilege is beneficial for typical users who shouldn't have administrative level access over the data that they're connecting with, but who still need the ability to create new records in the table and edit or delete records that they created in the past. This level of privilege is the most commonly assigned for most use cases.  **Reference** - Allows the assigned user or group the ability to read from the table but not to interact with the data in any other way. For example, this level of privilege is useful for look-up tables where an administrator should define the data that exists while the users should only be able to read from it as a reference for their work.  **Private** - A unique privilege level because it allows the users or groups to create new records in the table (which **Reference** doesn't), but it doesn't allow users or groups to read records that weren't created by them. It also allows the user or group to update and delete their own records, but not records that were created by other users. This level of privilege is best used in situations where sensitive information is held within the table that shouldn't be exposed to typical users.  **None** - Denies access entirely; the user or group can't view or modify records within the table and they can't delete them.  Ref:<https://docs.microsoft.com/en-us/power-platform/admin/about-teams-environment>   |  |  |  | | --- | --- | --- | | **Persona** | **Description** | **Security role auto-assigned** | | Teams owner | Owners can manage team membership and settings in the team. They have full access to the Dataverse for Teams environment's apps, resources, and data. They can perform environment maintenance tasks such as backup and restore through the Power Platform admin center. | System Administrator | | Teams member | Members can view the Dataverse for Teams environment's resources, run all apps and resources, and create or update their own resources. They have full access to all data. | Teams Member | | Teams guest | Guests are people from outside the tenant that a team owner invites, such as a partner or a customer. They can view and run all resources in the team. By default, guests have full access to records they create and don't have access to other users' records. | Teams Guest | | Global admin / Power Platform admin | These are tenant-level admins who manage the health and maintenance of the tenant's environments. They need not be owners or members of the team, but through their tenant-level admin privileges they can perform environment maintenance tasks such as backup and restore for all Dataverse for Teams environments. Similar to Dataverse, these tenant-level admins will have System Administrator privileges with Read-Write access mode to Dataverse for Teams environments. | System Administrator | | Dynamics 365 admin | These admins need to be owners or members of the team (because every team is linked to an Microsoft 365 group and the Dataverse for Teams environment will always be restricted for access to that Microsoft 365 group) to have System Administrator–level privileges to manage the health and maintenance of the environment. | System Administrator if they are an owner in the team; System Administrator and Teams Member if they are a member in the team. No access if they aren't an owner or member in the team. | | Colleagues with access | Colleagues with access are people in the tenant who aren't in the team but have been invited to run apps in the team. By default, colleagues with access have no access to data. Their data access rights can be granted based on the app or resources that they need to run. Note: when a colleague with access is invited to run apps in a team, the Microsoft 365 group association with the team's Dataverse for Teams environment will be automatically removed to allow app run access to the colleague with access. | Basic User | |
| Power Apps | Teams, (User, UserGroup) + Security Group(Share with colleague) |
| Power Automate | A Microsoft team with a Dataverse for Teams environment. A team is provisioned in the Dataverse for Teams environment when you create an app or bot in Microsoft Teams for the first time or install an app from the Microsoft Power Apps catalog.  Flows that are created in Power Automate for Teams are stored in the default environment and not in Dataverse for Teams.  User, UserGroup as Owners |
| Power Virtual Agent | Team or Organization |
| Power BI | Ref: <https://docs.microsoft.com/en-us/learn/modules/dataverse-teams-power-bi/5-share-options>  Reports that are published to Power BI workspaces automatically grant access to everyone who is a member of the workspace  -**People in your organization**  **-People with existing access**  **-Specific people -** specific people, groups, or external guests in your organization's Microsoft Azure Active Directory (Azure AD)  From the **Managed permissions** panel, you can review **Links giving access** and who has **Direct access** permissions to the report.  Permissions are at workspace, reports level.  **Power BI Security Roles** - <https://docs.microsoft.com/en-us/power-bi/collaborate-share/service-roles-new-workspaces>  **Power BI Data Set permissions** - <https://docs.microsoft.com/en-us/power-bi/connect-data/service-datasets-permissions>  **Power BI Row level security** - <https://docs.microsoft.com/en-us/power-bi/enterprise/service-admin-rls> |
| Power Virtual Agent |  | Who can Edit Bot?  Ref: <https://docs.microsoft.com/en-us/learn/modules/implement-power-virtual-agents/2-environments>  To create a bot in an environment where you don't have access, you'll need to be a system administrator  Or Contact Administrator and   * Create a bot in the environment (this step will install the necessary Power Virtual Agents solutions). * Assign the security role of "bot author" to you in the environment.   You can share your bot with other users so that multiple users can edit, manage, and collaborate on a bot.  Ref: <https://docs.microsoft.com/en-us/learn/modules/implement-power-virtual-agents/6-administer>  **Bot author**, **Bot contributor**, and **Bot transcript viewer** are the three security roles for Power Virtual Agents that you can manage at Microsoft Power Platform admin center.  You can assign the **Environment maker** security role when sharing a bot with a user who doesn't have sufficient environment permissions to run Power Virtual Agents.  When you are sharing the bot, if the specified user doesn't have sufficient permissions to use Power Virtual Agents in the environment, you will be notified that the **Environment maker** security role will be assigned to the person so that they can use the bot.  --------  Who can use the BOT?  The **Access** and **Authentication** options control who can access your bot. You can select one of two groups:   * **All bot managers** - This selection allows only bot managers to chat with the bot. You can share your bot so that other bot managers can access it. * **Everyone in my organization (Organization name)** - This selection allows everyone in the organization to access and chat with your bot. Users who are outside of the organization will see an error when chatting with the bot.   Authentication for users  - No Authentication  - Only for teams  - Manual (for any channels including teams)  - Manual using Az Active Directory V2  - Generic Oauth2  **Web channel security** |
| Dataverse Security Roles |  | Ref: <https://docs.microsoft.com/en-us/power-platform/admin/database-security>  <https://docs.microsoft.com/en-us/learn/modules/create-manage-environments/4-roles>  <https://docs.microsoft.com/en-us/learn/modules/get-started-security-roles/4a-security-role> |
| Tables |  | Ref: <https://docs.microsoft.com/en-us/learn/modules/get-started-with-powerapps-common-data-service/2-learn-about-entities>  **User or team owned**: Actions that can be performed on these rows can be controlled at the user level.  **Organization-owned**: Access to the data is controlled at the organization level. |
| Env Default or built in roles |  | System Administrator  Environment Maker  When you add a user to an environment, they are assigned two roles by default.  Dataverse User (this role is created when you instantiate an instance of a Dataverse database and all users in the environment are assigned this role)  Environment Maker |
| Dataverse |  | Ref: <https://docs.microsoft.com/en-us/learn/modules/get-started-security-roles/4-security-concepts>  Role Based Security  Business Units  Entity Record Ownership (Organization and User)  Teams(Owned by BU)  Column Level Security  Hierarchy Security to control access (Manager and Position)  Ref: <https://docs.microsoft.com/en-us/learn/modules/get-started-security-roles/6a-teams>  Configure Dataverse Teams for Security |
| Record Level Privileges |  | Ref: <https://docs.microsoft.com/en-us/learn/modules/get-started-security-roles/5-custom> |
| Flow |  | Ref: https://docs.microsoft.com/en-us/learn/modules/get-started-flows/8-flow-share-flows  Owner- name, email address, or group name of the person or group  Co-Owner-Microsoft Lists(SharePoint users must have Edit permission or be a member of the Members or Owners group to run flows in SharePoint.)  Owner can Add or remove other owners (but not the flow's creator).  If you remove an owner whose credentials are used to access Power Automate services, be sure to update the credentials for those connections, so that the flow continues to work correctly. |
| Model Driven Apps |  | Ref: <https://docs.microsoft.com/en-us/learn/modules/get-started-with-model-driven-apps-in-powerapps/5-control-security-when-sharing-model-driven-apps>  Can be shared with User, Group |
| Canvas App |  | Ref: <https://docs.microsoft.com/en-us/learn/modules/manage-apps-in-powerapps/2-share-apps>  User (Everyone), AD Security Group  By default, the user receives the User permission. If you want the user to also be able to edit the app, then select the co-owner check box. The following is a description of both permissions:   * **Co-owner** - Users can use, edit, and share the app, but can't delete or change the owner. * **User** - Users can view and use the app, but they can't change it. |