POWER PLATFORM

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.0

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
1.0	• Creation	CISA	08/13/2023

CONTENTS

1. CISA M365 SECURITY CONFIGURATION BASELINE FOR POWER PLATFORM

Microsoft 365 (M365) Power Platform is a cloud-based enterprise group of applications comprised of a low-code application development toolkit, business intelligence software, a custom chat bot creator, and app connectivity software. This Secure Configuration Baseline (SCB) provides specific policies to help secure Power Platform security.

The Secure Cloud Business Applications (SCuBA) project run by the Cybersecurity and Infrastructure Security Agency (CISA) provides guidance and capabilities to secure federal civilian executive branch (FCEB) agencies' cloud business application environments and protect federal information that is created, accessed, shared, and stored in those environments.

The CISA SCuBA SCBs for M365 help secure federal information assets stored within M365 cloud business application environments through consistent, effective, and manageable security configurations. CISA created baselines tailored to the federal government's threats and risk tolerance with the knowledge that every organization has different threat models and risk tolerance. Non-governmental organizations may also find value in applying these baselines to reduce risks.

The information in this document is being provided "as is" for INFORMATIONAL PURPOSES ONLY. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA. This document does not address, ensure compliance with, or supersede any law, regulation, or other authority. Entities are responsible for complying with any recordkeeping, privacy, and other laws that may apply to the use of technology. This document is not intended to, and does not, create any right or benefit for anyone against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

1.1 LICENSE COMPLIANCE AND COPYRIGHT

Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Sources are linked throughout this document. The United States government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

1.2 ASSUMPTIONS

The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level at a minimum. Therefore, only licenses not included in E3/G3 are listed.

1.3 KEY TERMINOLOGY

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD, "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this document are to be interpreted as described in Request for Comments 2119.

The following section summarizes the various Power Platform applications referenced in this baseline:

1. Power Apps: Low-code application development software used to create custom business applications. The apps can be developed as desktop, mobile, and even web apps. Three different types of Power Apps can be created:
   - Canvas Apps: These are drag and drop-style apps where users drag and add user interface (UI) components to the screen. Users can then connect the components to data sources to display data in the canvas app.
   - Model-Driven Apps: These are apps developed from an existing data source. They can be thought of as the inverse of a canvas app, building from the source rather than the UI. Model-driven apps then connect to the source like canvas apps.
   - Power Pages: These apps are developed to function as either internal or external facing websites.
2. Power Automate: This online tool within Microsoft 365 and add-ins is used to create automated workflows between apps and services to synchronize files, get notifications, and collect data.
3. Power Virtual Agents: These are custom chatbots for use in the stand-alone Power Virtual Agents web app or in a Microsoft Teams channel.
4. Connectors: These are proxies or wrappers around an application programming interface that allow the underlying service to be accessed from Power Automate Workflows, Power Apps, or Azure Logic Apps.
5. Microsoft Dataverse: This is a cloud database management system most often used to store data in SQL-like tables. A Power App would then use a connector to connect to the Dataverse table and perform create, read, update, and delete (CRUD) operations.

2. BASELINE POLICIES

Baseline Policies in this document are targeted toward administrative controls applicable to Power Platform applications at the tenant or Power Platform environment level. Additional Power Platform security settings can be implemented at the app level, connector level, or Dataverse table level. Refer to Power Platform Microsoft Learn documentation for those additional controls.

3. CREATION OF POWER PLATFORM ENVIRONMENTS

By default, any user in the Azure Active Directory (Azure AD) tenant can create additional environments. Enabling these controls will restrict creating new environments to users with the following admin roles: Global admins, Dynamics 365 admins, and Power Platform admins.

3.1 POLICIES

3.1.1 MS.POWERPLATFORM.1.1v1

The ability to create and sandbox environments SHALL be restricted to admins.

- *Rationale:* Users creating new Power Platform environments may inadvertently bypass data loss prevention (DLP) policy settings or misconfigure the security settings of their environment.
- *Last Modified:* June 2023
- *Note*: This control restricts creating environments to users with Global admin, Dynamics 365 service admin, Power Platform service admins, or Delegated admin roles.

3.1.2 MS.POWERPLATFORM.1.2v1

The ability to create trial environments SHALL be restricted to admins.

- *Rationale:* Users creating new Power Platform environments may inadvertently bypass DLP policy settings or misconfigure the security settings of their environment.
- *Last Modified:* June 2023
- *Note*: This control restricts creating environments to users with Global admin, Dynamics 365 service admin, Power Platform service admins, or Delegated admin roles.

3.2 RESOURCES

- Control who can create and manage environments in the Power Platform admin center | Microsoft Learn
- Power Platform | Digital Transformation Agency of Australia
- Microsoft Power Apps Documentation | Power Apps

3.3 LICENSE REQUIREMENTS

- N/A

3.4 IMPLEMENTATION

3.4.1 MS.POWERPLATFORM.1.1v1 instructions

1. Sign in to your tenant environment's respective Power Platform admin center.
2. In the upper-right corner of the Microsoft Power Platform site, select the **Gear icon** (Settings icon).
3. Select **Power Platform settings**.
4. Under **Who can create production and sandbox environments**, select **Only specific admins.**

3.42 MS.POWERPLATFORM.1.2v1 Instructions

1. Follow the instructions in the MS.POWERPLATFORM.1.1v1 instructions up to step **3**.
2. Under **Who can create trial environments**, select **Only specific admins.**

4. POWER PLATFORM DATA LOSS PREVENTION POLICIES

To secure Power Platform environments, DLP policies can be created to restrict the connectors used with Power Apps created in an environment. A DLP policy can be created to affect all or some environments, or exclude certain environments. The more restrictive policy will be enforced when there is a conflict.

Connectors can be separated by creating a DLP policy assigning them to one of three groups: Business, Non-Business, and Blocked. Connectors in different groups cannot be used in the same Power App. Connectors in the Blocked group cannot be used at all. (Note: Some M365 connectors cannot be blocked, such as Teams and SharePoint connectors.)

In the DLP policy, connectors can be configured to restrict read and write permissions to the data source/service. Connectors that cannot be blocked, cannot be configured. Agencies should evaluate the connectors and configure them to fit agency needs and security requirements. The agency should then create a DLP policy to only allow those connectors to be used in Power Platform.

When the Azure AD tenant is created, by default, a Power Platform environment is created in Power Platform. This Power Platform environment will bear the name of the tenant. There is no way to restrict users in the Azure AD tenant from creating Power Apps in the default Power Platform environment. Admins can restrict users from creating apps in all other created environments.

4.1 POLICIES

4.1.1 MS.POWERPLATFORM.2.1v1

A DLP policy SHALL be created to restrict connector access in the default Power Platform environment.

- *Rationale:* All users in the tenant have access to the default Power Platform environment. Those users may inadvertently use connectors that share sensitive information with others who should not have

access to it. Users requiring Power Apps should be directed to conduct development in other Power Platform environments with DLP connector policies customized to suit the user's needs while also maintaining the agency's security posture.
- *Last Modified:* June 2023
- *Note:* The following connectors drive core Power Platform functionality and enable core Office customization scenarios: Approvals, Dynamics 365 Customer Voice, Excel Online (Business), Microsoft Dataverse, Microsoft Dataverse (legacy), Microsoft Teams, Microsoft To -Do (Business), Office 365 Groups, Office 365 Outlook, Office 365 Users, OneDrive for Business, OneNote (Business), Planner, Power Apps Notification, Power BI, SharePoint, Shifts for Microsoft Teams, and Yammer. As such, these connectors remain non-blockable to maintain core user scenarios functions.

4.1.2 MS.POWERPLATFORM.2.2v1

Non-default environments SHOULD have at least one DLP policy affecting them.

- *Rationale:* Users may inadvertently use connectors that share sensitive information with others who should not have access to it. DLP policies provide a way for agencies to detect and prevent unauthorized disclosures.
- *Last Modified:* June 2023

4.2 RESOURCES

- Data Policies for Power Automate and Power Apps | Digital Transformation Agency of Australia
- Create a data loss prevention (DLP) policy | Microsoft Learn
- DLP connector classification | Microsoft Learn
- DLP for custom connectors | Microsoft Learn

4.3 LICENSE REQUIREMENTS

- N/A

4.4 IMPLEMENTATION

4.4.1 MS.POWERPLATFORM.2.1v1 Instructions

1. Sign in to your tenant environment's respective Power Platform admin center.
2. On the left pane, select **Policies** > **Data Policies.**
3. Select the **+ New Policy** icon to create a new policy.
4. Give the policy a suitable agency name and click **Next.**
5. At the **Prebuilt connectors** section, search and select the connectors currently in the **Non-business | default** tab containing sensitive data that can be utilized to create flows and apps.
6. Click **Move to Business.** Connectors added to this group cannot share data with connectors in other groups because connectors can reside in only one data group at a time.
7. If necessary (and possible) for the connector, click **Configure connector** at the top of the screen to change connector permissions. This allows greater flexibility for the agency to allow and block certain connector actions for additional customization.
8. For the default environment, move all other connectors to the **Blocked** category. For non-blockable connectors noted above, the Block action will be grayed out and a warning will appear.
9. At the bottom of the screen, select **Next** to move on.
10. Add a custom connector pattern. Custom connectors allow admins to specify an ordered list of Allow and Deny URL patterns for custom connectors. View DLP for custom connectors | Microsoft Learn for more information.
11. Click **Next.**

12. At the **Scope** section for the default environment, select **Add multiple environments** and add the default environment.
13. Select **Next** -> **Create Policy** to finish.

4.4.2 MS.POWERPLATFORM.2.2v1 Instructions

1. Repeat steps 1 to 11 in the MS.POWERPLATFORM.2.1v1 instructions.
2. At the **Scope** section for the default environment, select **Add multiple environments** and select the non-default environments where you wish to enforce a DLP policy. If you wish to apply the DLP policy for all environments, including environments created in the future, select **Add all environments.**
3. Select **Next** -> **Create Policy** to finish.

5. POWER PLATFORM TENANT ISOLATION

Power Platform tenant isolation is different from Azure AD-wide tenant restriction. It does not impact Azure AD-based access outside of Power Platform. Power Platform tenant isolation only works for connectors using Azure AD-based authentication, such as Office 365 Outlook or SharePoint. The default configuration in Power Platform has tenant isolation set to **Off**, allowing for cross-tenant connections to be established. A user from tenant A using a Power App with a connector can seamlessly establish a connection to tenant B if using appropriate Azure AD credentials.

If admins want to allow only a select set of tenants to establish connections to or from their tenant, they can turn on tenant isolation. Once tenant isolation is turned on, inbound (connections to the tenant from external tenants) and outbound (connections from the tenant to external tenants) cross-tenant connections are blocked by Power Platform, even if the user presents valid credentials to the Azure AD-secured data source.

5.1 POLICIES

5.1.1 MS.POWERPLATFORM.3.1v1

Power Platform tenant isolation SHALL be enabled.

- *Rationale:* Provides an additional tenant isolation control on top of Azure AD tenant isolation specifically for Power Platform applications to prevent accidental or malicious cross- tenant information sharing.
- *Last modified*: June 2023

5.1.2 MS.POWERPLATFORM.3.2v1

An inbound/outbound connection allowlist SHOULD be configured.

- *Rationale:* Depending on agency needs, an allowlist can be configured to allow cross- tenant collaboration via connectors.
- *Last modified*: June 2023
- *Note*: The allowlist may be empty if the agency has no need for cross tenant collaboration.

5.2 RESOURCES

- Enable tenant isolation and configure allowlist | Microsoft Learn

5.3 LICENSE REQUIREMENTS

- N/A

5.4 IMPLEMENTATION

5.4.1 MS.POWERPLATFORM.3.1v1 Instructions

1. Sign in to your tenant environment's respective Power Platform admin center.
2. On the left pane, select **Policies -> Tenant Isolation**.
3. Set the slider in the center of the screen to **On,** then click **Save** on the bottom of the screen.

5.4.2 MS.POWERPLATFORM.3.2v1 instructions

1. Follow steps 1 and 2 in MS.POWERPLATFORM.3.1v1 instructions to arrive at the same page.
2. The tenant isolation allowlist can be configured by clicking **New tenant rule** on the Tenant Isolation page.
3. Select the **Direction** of the rule and add the **Tenant Domain or ID** this rule applies to.
4. If Tenant Isolation is switched **Off**, these rules will not be enforced until Tenant Isolation is turned **On**.

6. POWER APPS CONTENT SECURITY POLICY

Content Security Policy (CSP) is an added security layer that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting, clickjacking, and data injection attacks. When enabled, this setting can apply to all current canvas apps and model-driven apps at the Power Platform environment level.

6.1 POLICIES

6.1.1 MS.POWERPLATFORM.4.1v1

Content Security Policy SHALL be enforced for model-driven and canvas Power Apps.

- *Rationale:* Adds CSP as a defense mechanism for Power Apps against common website attacks.
- *Last Modified:* June 2023

6.2 RESOURCES

- Content Security Policy | Microsoft Learn

6.3 LICENSE REQUIREMENTS

- N/A

6.4 IMPLEMENTATION

6.4.1 MS.POWERPLATFORM.4.1v1 Instructions

1. Sign in to your tenant environment's respective Power Platform admin center.
2. On the left-hand pane, click on **Environments** and then select an environment from the list.
3. Select the **Settings** icon at the top of the page.
4. Click on **Product** ,then click on **Privacy + Security** from the options that appear.
5. At the bottom of the page under the **Content security policy** section, turn the slider **On** for **Model-driven** and **Canvas**.
6. At the same location, set **Enable reporting** to **On** and add an appropriate endpoint for reporting CSP violations.
7. Repeat steps 2 to 6 for all active Power Platform environments.

7. POWER PAGES CREATION

Power Pages, formerly known as Power Portals, are Power Apps specifically designed to act as external facing websites. By default, any user in the tenant can create a Power Page. Admins can restrict the creation of new Power Pages to only admins.

7.1 POLICIES

7.1.1 MS.POWERPLATFORM.5.1v1

The ability to create Power Pages sites SHOULD be restricted to admins.

- *Rationale:* Users may unintentionally misconfigure their Power Pages to expose sensitive information or leave the website in a vulnerable state.
- *Last Modified:* June 2023

7.2 RESOURCES

- Control Portal Creation | Microsoft Learn

7.3 LICENSE REQUIREMENTS

- N/A

7.4 IMPLEMENTATION

7.4.1 MS.POWERPLATFORM.5.1v1 Instructions

1. This setting currently can only be enabled through the Power Apps PowerShell modules.
2. After installing the Power Apps PowerShell modules, run **Add-PowerAppsAccount -Endpoint $YourTenantsEndpoint** to authenticate to your tenant's Power Platform. Discover the valid endpoint parameter here. Commercial tenants use **-Endpoint prod**, Government Community Cloud (GCC) tenants use **-Endpoint usgov,** and so on.
   Then run the following PowerShell command to disable the creation of Power Pages sites by non-administrative users.

APPENDIX A: CROSS-TENANT ACCESS GUIDANCE

Some of the conditional access policies contained in this security baseline, if implemented as described, will impact guest user access to a tenant. For example, the policies require users to perform MFA and originate from a managed device to gain access. These requirements are also enforced for guest users. For these policies to work effectively with guest users, both the home tenant (the one the guest user belongs to) and the resource tenant (the target tenant) may need to configure their Azure AD cross-tenant access settings.

Microsoft's Authentication and Conditional Access for External ID provides an understanding of how MFA and device claims are passed from the home tenant to the resource tenant. To configure the inbound and outbound cross-tenant access settings in Azure AD, refer to Microsoft's Overview: Cross-tenant access with Microsoft Entra External ID.