

# CIS Microsoft Dynamics 365 Power Platform

v1.0.0 - 12-20-2022

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

# Table of Contents

<b>Terms of Use .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>4</b>
Intended Audience.....	4
Consensus Guidance .....	5
Typographical Conventions.....	6
<b>Recommendation Definitions.....</b>	<b>7</b>
Title.....	7
Assessment Status.....	7
Automated .....	7
Manual.....	7
Profile .....	7
Description.....	7
Rationale Statement .....	7
Impact Statement.....	8
Audit Procedure.....	8
Remediation Procedure.....	8
Default Value.....	8
References .....	8
CIS Critical Security Controls® (CIS Controls®) .....	8
Additional Information.....	8
Profile Definitions .....	9
Acknowledgements .....	10
<b>Recommendations .....</b>	<b>11</b>
<b>1 Accounts and Authentication .....</b>	<b>11</b>
1.1 (L1) Ensure 'User access to environments is controlled with Security Groups' (Manual) .....	12
1.2 (L1) Ensure 'User sessions are terminated upon time limit exceeded and user logoff' (Manual) .....	14
1.3 (L1) Ensure 'Administrative accounts are separate, unassigned, and cloud-only' (Manual) .....	17
1.4 (L2) Ensure 'Multifactor authentication for all users' is 'Enabled' (Manual).....	20
<b>2 Permissions .....</b>	<b>23</b>
2.1 (L1) Ensure 'Creation of new trial, production, and sandbox environments' is restricted to 'Administrators' (Manual).....	24
2.2 (L1) Ensure 'Security roles provide access to the minimum amount of business data required' (Manual) .....	28
2.3 (L1) Ensure 'Set blocked file extensions' is configured to match the enterprise block list (Manual) .....	30
2.4 (L2) Ensure 'Access to the environment is restricted by location' (Manual) .....	32

2.5 (L1) Ensure 'Cross-tenant isolation is enabled for Power Platform Apps and Flows' (Manual) .....	34
<b>3 Data Management .....</b>	<b>39</b>
3.1 (L2) Ensure 'Environments with Critical Data are Encrypted with Customer Managed Keys' (Manual) .....	40
3.2 (L1) Ensure 'Extract customer data privileges from Microsoft Dynamics 365 is controlled' (Manual) .....	43
3.3 (L1) Ensure 'Dynamics 365 restricts incoming email actions for public queue mailboxes' (Manual) .....	45
3.4 (L1) Ensure 'DLP policies are enabled and restrict the connectors usage' (Manual) .....	48
<b>4 Logging and Auditing .....</b>	<b>50</b>
4.1 (L1) Ensure 'System Administrator security role changes are reviewed periodically' (Manual) .....	51
4.2 (L1) Ensure 'Environment Activity logging is Enabled' (Manual) .....	53
4.3 (L1) Ensure 'App creation notification is enabled in the environment' (Manual) .....	55
<b><i>Appendix: Summary Table .....</i></b>	<b><i>57</i></b>
<b><i>Appendix: Change History .....</i></b>	<b><i>59</i></b>

# Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Dynamics 365 Power Platform running in the Cloud on any OS. This guide was tested against Microsoft Dynamics 365. To obtain the latest version of this guide, please visit <http://cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto:feedback@cisecurity.org).

## Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft 365.

## Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i>&lt;italic font in brackets&gt;</i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
<b>Note</b>	Additional information or caveats

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.



## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - Corporate/Enterprise Environment (general use)**

Items in this profile intend to:

- be the starting baseline for most organizations;
- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)**

This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability;
- may negatively inhibit the utility or performance of the technology; and
- limit the ability of remote management/access.

**Note:** Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied.

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

The Center for Internet Security extends special recognition and thanks to **Kai Markl** and **Joao Espirito** Santo from Siemens, for their collaboration developing the configuration recommendations contained in this document.

### **Editor**

Jennifer Jarose

### **Author**

Joao Espirito Santo

Kai Markl

### **Contributor**

Caleb Eifert

Alfranio Oliveira

# Recommendations

## 1 Accounts and Authentication

This section contains recommendations related to accounts and authentication.

## *1.1 (L1) Ensure 'User access to environments is controlled with Security Groups' (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

If the organization has multiple Microsoft Dataverse environments, security groups can be used to control which licensed users can be a member of a particular environment.

### **Rationale:**

Limiting the access and permissions for the accounts that needs access to the information, reduces the risk of having users with improper access to data in the environment.

### **Impact:**

Users with legitimate needs to an environment might not be able to access the environment if they are not part of the correct security group.

### **Audit:**

Verify that user access to environments is controlled with security groups.  
In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Edit** on the Details pane of the environment.
3. Select the pencil icon under **Security group**.
4. Ensure the appropriate group(s) are selected.

### **Remediation:**

Ensure that user access to environments is controlled with security groups.  
In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Edit** on the Details pane of the environment.
3. Select the pencil icon under **Security group**.
4. Select the appropriate security group.
5. Select **Done** followed by **Save**.


**Default Value:**

N/A

**References:**

1. <https://docs.microsoft.com/en-us/power-platform/admin/control-user-access>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

## *1.2 (L1) Ensure 'User sessions are terminated upon time limit exceeded and user logoff' (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

The Dynamics 365 platform can be configured with a user session expiration time and inactivity timeout.

The recommended state for this setting is: 120 minutes.

### **Rationale:**

By default, the timeout for a user's session is set to 24 hours which means the user is not required to re-enter their login details for up to 24 hours.

Whenever a Dynamics 365 user sessions is started, a unique session ID and other session information are generated. Such information can be used by a malicious user to hijack the session. By terminating sessions upon user logoff and idle time limit, the underlying session information is invalidated. Therefore, the potential for the session to be hijacked is removed.

### **Impact:**

User session will be terminated after two hours.

### **Audit:**

Verify that user sessions are terminated upon user logoff and when the idle time limit is exceeded.

In the Power Platform Admin Center:

1. Log in to `https://admin.powerplatform.microsoft.com` and select the appropriate environment.
2. Select `Settings`.
3. Expand `Product` then select `Privacy + Security`.
4. Under `Session Expiration` ensure the slider is set to `On`.

Confirm the length and timeout as determined by organizational policy.

5. Under `Inactivity timeout` ensure the slider is set to `On`.

Confirm the duration for timeout and warning as determined by organizational policy.

6. Click `Save`.

**Remediation:**

Ensure that user sessions are terminated upon user logoff and when the idle time limit is exceeded.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings**.
3. Expand **Product** then select **Privacy + Security**.
4. Under **Session Expiration** move the slider to **On**.

Enter the session length and timeout as determined by organizational policy.

5. Under **Inactivity timeout** move the slider to **On**.

Enter the duration for timeout and warning as determined by organizational policy.

6. Click **Save**.

**Note:** These settings apply to all users in the environment.

**Default Value:**







- Maximum Session Length: 1440 minutes
- Minimum Session Length: 60 minutes
- How long before session expires before showing timeout warning: 20 minutes
- The updated settings will be effective the next time the user signs into the application.

**References:**

1. <https://docs.microsoft.com/en-us/power-platform/admin/user-session-management>



**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.3 Configure Automatic Session Locking on Enterprise Assets</u></b> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.			
v7	<b><u>16.11 Lock Workstation Sessions After Inactivity</u></b> Automatically lock workstation sessions after a standard period of inactivity.			

### *1.3 (L1) Ensure 'Administrative accounts are separate, unassigned, and cloud-only' (Manual)*

#### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

#### **Description:**

Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings.

Each system administrator should utilize two (2) separate accounts, an administrator account to perform administrative tasks and a separate account for daily activities such as checking email. Users should only sign in with system administrator account to perform administrative tasks in the environment.

#### **Rationale:**

Users with the system administrator role automatically have access to records, system, and custom entities. Creating separate administrative accounts can reduce the risk of credential theft and other types of attacks.

#### **Impact:**

Administrative users will have to switch accounts utilizing the login/logout functionality when performing administrative tasks.

#### **Audit:**

Verify there are separate administrative accounts being utilized.

In the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a Global Administrator.
2. Select `Users > Active users` then sort by the `User type` column.
3. Verify that Administrators have a dedicated administrative and regular user account.

## Remediation:

Ensure each administrator has an administrative and regular user account.

In the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a Global Administrator.
2. Go to `Users` and then `Active users` and select `Add a user`.
3. Fill out the appropriate fields for Name, user, domain, password etc.
4. When prompted to assign licenses select `Create user without product license (not recommended)`, then click `Next`.
5. Under the `Option settings` choose `Admin center access` followed by the appropriate role then click `Next`.
6. Select `Finish adding`.

**Note:** Take into account the proper and valid licensing requirements and attribute the security roles inside power platform with the least privilege approach.

## Default Value:

N/A

## References:

1. <https://docs.microsoft.com/en-us/power-platform/admin/create-users#create-a-user-account>
2. <https://docs.microsoft.com/en-us/power-platform/admin/prevent-elevation-security-role-privilege>
3. <https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide>







## Additional Information:

The following setting should also be considered:

- Don't stay signed in with a system administrator account

Staying signed in with a system administrator account when specific administrative tasks are not being performed can increase exposure to phishing attacks. System administrators should sign in as needed to do specific tasks and then sign out.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

## *1.4 (L2) Ensure 'Multifactor authentication for all users' is 'Enabled' (Manual)*

### **Profile Applicability:**

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

### **Description:**

Enable multifactor authentication (MFA) for all users in the Microsoft 365 tenant. MFA is an authentication method which requires the user to provide two (or more) pieces of information to gain access to the system or application.

There are several options for MFA within the Microsoft 365 tenant:

- Authentication code received via text message to a registered mobile phone number.
- Mobile authentication application like Microsoft Authenticator.

### **Rationale:**

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Users will be prompted to authenticate with a second factor upon logging in to Microsoft 365 services.

### **Impact:**

Implementation of multifactor authentication for all users will necessitate a change to users' routine. All users will be required to enroll in multifactor authentication using a mobile phone or an authentication application. After enrollment, use of multifactor authentication will be required for future authentication to the environment.

## Audit:

Verify the multifactor authentication is configured for all users.

In the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a Global Administrator.
2. Go to Admin centers and click on Azure Active Directory.
3. Select Enterprise applications then, under Security, select Conditional Access.
4. Review the list of policies and ensure that there is a policy that requires the Grant access control with Require multi-factor authentication for All users under Users and groups

Verify the multifactor authentication configuration for administrators, using the M365 SecureScore service:

1. Log in to the Secure Score portal `https://security.microsoft.com` as a Global Administrator or another custom admin role.
2. Click on Require MFA for all users policy to check MFA for all users.
3. It will show the number of users who do not have MFA configured.

This information is also available via the Microsoft Graph Security API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

## Remediation:

Enable multifactor authentication for all users.

In the Microsoft 365 Admin Center:

1. Log in to <https://admin.microsoft.com> as a Global Administrator.
2. Go to Admin centers and click on Azure Active Directory.
3. Select Enterprise applications then, under Security, select Conditional Access.
4. Click New policy
5. Select Cloud apps or actions > All cloud apps (and don't exclude any apps)
6. Go to Assignments > Users and groups > Include > select All users (and do not exclude any user).
7. Access Controls > Grant > Require multi-factor authentication (and nothing else)
8. Conditions > Client Apps > Configure (Yes) > Explicitly select Browser, Mobile apps and desktop clients, Modern authentication clients, Exchange ActiveSync clients, and Other clients
9. Leave all other conditions blank
10. Make sure the policy is enabled
11. Create

## Default Value:

Disabled

## References:

1. <https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 Require MFA for Externally-Exposed Applications</b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 2 Permissions



## *2.1 (L1) Ensure 'Creation of new trial, production, and sandbox environments' is restricted to 'Administrators' (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

An environment is a space to store, manage, and share organizational data, apps, and flows. It also serves as a container to separate apps that may have different roles, security requirements, or target audiences. Power Apps automatically creates a single default environment for each tenant, which is shared by all users in that tenant.

For managing environments centrally and to prevent environment sprawl, it is suggested to limit the ability of environment creation to specific users.

### **Rationale:**

Any PowerApps licensed user can create an environment. If someone in the organization is on a Power Apps or Power Automate per-user plan, they may have permission to create their own environment. These environments can be used and shared by Dynamics 365, Power Apps portals and apps, and Power Automate flows. Environments can store multiple Dataverse tables. Power Platform apps and Dynamics 365 can then connect to, read from, and write to these tables, which would likely be shared across multiple applications/processes.

It is suggested to restrict the power platform environment creation for just administrators and restrict the access for this feature for a limited number of users.

### **Impact:**

Enabling this feature may slow the user's individual productivity, but could also prevent duplicated efforts, inconsistent data, scattered naming conventions, and data leakage.

**Note:** After enabling this feature, only the Tenant Admin or members of the Power Platform Admin Group will be able to create new environments (if non-admins are disabled). Each environment requires 1GB of space before provisioning a new environment.

## Audit:

Verify that the creation of new trial, production, and sandbox environment is restricted to administrators.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select the gear icon in the top right corner then select Power Platform Settings.
3. Under Who can create production and sandbox environments ensure that Only specific admins is selected.

**Note:** This restricts creation to Global admins, Dynamics 365 service admins, Power Platform service admins, and Delegated admins.

4. Under Who can create trial environments ensure that Only specific admins is selected.

**Note:** This restricts creation to Global admins, Dynamics 365 service admins, Power Platform service admins, and Delegated admins.

## Remediation:

Ensure that the creation of new trial, production, and sandbox environment is restricted to administrators.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select the gear icon in the top right corner then select Power Platform Settings.
3. Under Who can create production and sandbox environments select Only specific admins.

**Note:** This restricts creation to Global admins, Dynamics 365 service admins, Power Platform service admins, and Delegated admins

4. Under Who can create trial environments select Only specific admins.

**Note:** This restricts creation to Global admins, Dynamics 365 service admins, Power Platform service admins, and Delegated admins

5. Click Save


**Default Value:**

Everyone / Unrestricted

## References:

1. <https://docs.microsoft.com/en-us/power-platform/admin/control-environment-creation#control-environment-creation-through-powershell>
2. <https://docs.microsoft.com/en-us/power-platform/admin/create-environment>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

## *2.2 (L1) Ensure 'Security roles provide access to the minimum amount of business data required' (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

Users should only have access to data that they really require access to. Make use of the predefined security roles whenever possible and assure the minimum privileges required for the roles and for the users to perform their activities.

### **Rationale:**

Microsoft Dynamics 365 makes use of the Dataverse and role-based security model to help secure the access. It also comes with predefined security roles that can be used for granting user access. If the permission for a predefined role requires customization, copy one that exists and work under the copied role, keeping the integrity of the original role.

It is important to apply the least privilege and need-to-know principle when customizing and granting users and roles permissions. Details in the reference links.

Limiting the access and permissions for the accounts that needs access to the information, reduces the risk of having users with improper access to data in the environment and compromising the integrity/confidentiality of the data.

### **Impact:**

If not configured correctly, users with need-to-know might not have access to business data.

### **Audit:**

Ensure that user access to the environment is controlled with security groups.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select `Settings`.
3. Expand `Users + permissions` then select `Security roles`.
4. Analyze the predefined `Security Roles` to determine which fits the environmental needs.
5. Under the `More actions` click the 3 dots and select `copy` to audit the roles.

## Remediation:

Change user roles to meet environment needs via security groups.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings**.
3. Expand **Users + permissions** then select **Security roles**.
4. Edit the **Security Role** to fit environmental needs.

## References:

1. <https://learn.microsoft.com/en-us/dynamics365/customerengagement/on-premises/developer/security-dev/how-role-based-security-control-access-entities?view=op-9-1>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

## *2.3 (L1) Ensure 'Set blocked file extensions' is configured to match the enterprise block list (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

This setting prevents the upload or download of certain attachment types that are considered dangerous.

### **Rationale:**

Dynamics 365 comes with a predefined extensions list that is blocked in the tool; it is required to have it as restricted as possible, allowing just the extensions that are required for business purposes. Consider updating the blocked extensions periodically.

### **Impact:**

File types that are legitimate might be blocked.

### **Audit:**

Verify the 'Set blocked file extensions' is configured to match the organizations block list.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings**.
3. Expand **Product** then select **Privacy + Security**.
4. Review the list extensions to ensure it matches the organizations block list.

### **Remediation:**

Ensure the 'Set blocked file extensions' is configured to match the organizations block list.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings**.
3. Expand **Product** then select **Privacy + Security**.
4. Add extensions as relevant to the organization.

**Default Value:**

ade; adp; app; asa; ashx; asmx; asp; bas; bat; cdx; cer; chm; class; cmd; com; config; cpl; crt; csh; dll; exe; fxp; hlp; hta; htr; htw; ida; idc; idq; inf; ins; isp; its; jar; js; jse; ksh; lnk; mad; maf; mag; mam; maq; mar; mas; mat; mau; mav; maw; mda; mdb; mde; mdt; mdw; mdz; msc; msh; msh1; msh1xml; msh2; msh2xml; mshxml; msi; msp; mst; ops; pcd; pif; prf; prg; printer; pst; reg; rem; scf; scr; sct; shb; shs; shtm; shtml; soap; stm; tmp; url; vb; vbe; vbs; vsmacros; vss; vst; vsw; ws; wsc; wsf; wsh

**References:**

1. <https://docs.microsoft.com/en-us/power-platform/admin/settings-privacy-security>



## *2.4 (L2) Ensure 'Access to the environment is restricted by location' (Manual)*

### **Profile Applicability:**

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

### **Description:**

Location condition in Azure AD Conditional Access, controls access to cloud apps based on the network location of a user. The location condition is commonly used to block access from countries/regions where organizations know traffic should not come from.

Restrict access to users by location to reduce unauthorized access.

### **Rationale:**

Conditional access policies controls access to cloud apps based on the network location of a user. It then blocks access from countries/regions where it knows traffic should not come from reducing the risk of a breach.

### **Impact:**

When location restrictions are set in a user's profile and the user tries to sign in from a blocked location, access to customer engagement apps (Dynamics 365 Sales, Dynamics 365 Customer Service, Dynamics 365 Field Service, Dynamics 365 Marketing, Dynamics 365 Project Service Automation), and Finance and Operations apps are denied.

### **Requirements for using conditional access:**

- A subscription to Azure Active Directory Premium.
- A federated Azure Active Directory tenant.

### **Audit:**

Verify that access to the environment is restricted by location.

In the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a Global Administrator or Conditional Access administrator.
2. Go to Admin centers and click on Azure Active Directory.
3. Select Enterprise applications then, under Security, select Conditional Access.
4. Ensure a policy exists to restrict location.

## Remediation:

Ensure access to the environment is restricted by location.

In the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a Global Administrator or Conditional Access administrator.
2. Go to Admin centers and click on Azure Active Directory.
3. Select Enterprise applications then, under Security, select Conditional Access.
4. Click New policy and create a name.
5. Go to Assignments > Users or workload identity > Users and groups >
6. Under Include > select All users (and do not exclude any user).
7. Under Exclude, select Users and groups, add the organizations emergency access or break-glass accounts.
8. Select Cloud apps or actions > Include and click Select apps
9. Choose Microsoft Dataverse Application or Microsoft Dynamics ERP for Finance and Operations application.
10. Select Conditions > Location configure to Yes
11. Under Include select Selected locations
  - a. Select the blocked location created for the organization.
  - b. Click Select.
12. Select Access controls > click Block Access and click Select.
13. Confirm the settings and set Enable policy to Report-only.
14. Click Create to create and enable the policy.

## Default Value:

N/A

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location#create-a-conditional-access-policy>
2. <https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules>

## *2.5 (L1) Ensure 'Cross-tenant isolation is enabled for Power Platform Apps and Flows' (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

Microsoft Power Platform has a rich ecosystem of connectors based on Azure Active Directory (Azure AD) that allow authorized Azure AD users to build compelling apps and flows establishing connections to the business data available through these data stores.

Tenant isolation makes it easy for administrators to ensure that these connectors can be harnessed in a safe and secure way within the tenant while minimizing the risk of data exfiltration outside the tenant. Tenant isolation allows admins to effectively govern the movement of tenant data from Azure AD authorized data sources to and from their tenant.

With tenant isolation On, all tenants are restricted. 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. Rules can be used to add exceptions.

**Note:** Power Platform tenant isolation is different from Azure AD-wide tenant restriction. It doesn't 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.

### **Rationale:**

Cross-tenant isolation restricts how other tenants connect. Applied at the connector level, cross-tenant isolation blocks inbound or outbound connections for canvas apps and flows.

An attacker can compromise an account and create a connection in order to maintain persistent access to the user's account.

**Impact:**

Restricting outbound connections means that a user is blocked from connecting to a third-party tenant. (Restricting outbound cross-tenant connections can be done using tenant restrictions that apply to all Azure Active Directory (Azure AD) software as a service (SaaS) cloud apps, or at the connector level, which would block outbound connections just for canvas apps and flows.)

Restricting inbound connections means that a user in a third-party tenant is blocked from creating a connection to the tenant. (Restricting inbound cross-tenant connections requires a support ticket—this restriction then only applies to Power Apps and Power Automate.)

Enable the configurations below will prevent communication with any other tenant.

**Warning:** Perform an impact analysis before implementation.

**Requirements for using cross-tenant isolation:**

- A subscription to Azure Active Directory Premium.
- A federated Azure Active Directory tenant.

Admins can specify an explicit allowlist of tenants that they want to enable inbound, outbound, or both, which will bypass tenant isolation controls when configured. Admins can use a special pattern “\*” to allow all tenants in a specific direction when tenant isolation is turned on. All other cross-tenant connections except the ones in the allowlist are rejected by Power Platform.

**Audit:**

Verify that cross-tenant isolation is enabled.

In the Power Platform Admin Center:

- Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
- Select Tenant isolation (preview).
- Confirm that tenant isolation is `on`.

## Remediation:

Ensure that tenant restrictions for outbound connections are setup:

There are two steps to get started with tenant restrictions. First, make sure that clients can connect to the right addresses. Second, configure proxy infrastructure.

### 1. URLs and IP addresses:

- a) To use tenant restrictions, clients must be able to connect to the following Azure AD URLs to authenticate: `login.microsoftonline.com`, `login.microsoft.com`, and `login.windows.net`.
- b) Additionally, to access Office 365, clients must also be able to connect to the fully qualified domain names (FQDNs), URLs, and IP addresses defined in [Office 365 URLs and IP address ranges](#).

### 2. Proxy configuration and requirements:

- a) The following configuration is required to enable tenant restrictions through the proxy infrastructure. This guidance is generic, refer to the proxy vendor's documentation for specific implementation steps.
- b) Prerequisites:
  1. The proxy must be able to perform TLS interception, HTTP header insertion, and filter destinations using FQDNs/URLs.
  2. Clients must trust the certificate chain presented by the proxy for TLS communications. For example, if certificates from an internal public key infrastructure (PKI) are used, the internal issuing root certificate authority certificate must be trusted.
  3. Azure AD Premium 1 licenses are required for use of Tenant Restrictions.
- c) Configuration:
  1. For each outgoing request to `login.microsoftonline.com`, `login.microsoft.com`, and `login.windows.net`, insert two HTTP headers: `Restrict-Access-To-Tenants` and `Restrict-Access-Context`.

**Note:** Do not include subdomains under \*.login.microsoftonline.com in the proxy configuration. Doing so will include device.login.microsoftonline.com and will interfere with Client Certificate authentication, which is used in Device Registration and Device-based Conditional Access scenarios. Configure the proxy server to exclude device.login.microsoftonline.com and enterpriseregistration.windows.net from TLS break-and-inspect and header injection.

**3. The headers should include the following elements:**

1. For Restrict-Access-To-Tenants, use a value of permitted tenant list, which is a comma-separated list of tenants that allow users to access. Any domain that is registered with a tenant can be used to identify the tenant in this list, as well as the directory ID itself. For an example of all three ways of describing a tenant, the name/value pair to allow Contoso, Fabrikam, and Microsoft looks like: Restrict-Access-To-Tenants: contoso.com,fabrikam.onmicrosoft.com,72f988bf-86f1-41af-91ab-2d7cd011db47
2. For Restrict-Access-Context, use a value of a single directory ID, declaring which tenant is setting the tenant restrictions.

**Example:** Declare Contoso as the tenant that set the tenant restrictions policy, the name/value pair looks like: Restrict-Access-Context: 456ff232-3512-5h23-b3b3-3236w0826f3d. Use the environments directory ID here to get logs for these authentications. If any directory ID other than the environments being set up, those sign-in logs will appear in another tenant, with all personal information removed. For more information, see Admin experience.

To prevent users from inserting their own HTTP header with non-approved tenants, the proxy needs to replace the Restrict-Access-To-Tenants header if it is already present in the incoming request.

Clients must be forced to use the proxy for all requests to login.microsoftonline.com, login.microsoft.com, and login.windows.net. For example, if PAC files are used to direct clients to use the proxy, end users shouldn't be able to edit or disable the PAC files.

**4. Inbound Connections:**

1. Browse to the Power Platform admin center, select Help + support.
2. Under the New support request option, fill out the information required regarding the environment.

**Default Value:**

Tenant isolation is not activated by default.

## References:

1. <https://docs.microsoft.com/en-us/power-platform/admin/cross-tenant-restrictions>
2. <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions>
3. <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions#admin-experience>
4. <https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>

## 3 Data Management



### *3.1 (L2) Ensure 'Environments with Critical Data are Encrypted with Customer Managed Keys' (Manual)*

#### **Profile Applicability:**

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

#### **Description:**

All environments of Microsoft Dataverse use SQL Server Transparent Data Encryption (TDE) to perform real-time encryption of data when written to disk, also known as encryption at rest.

By default, Microsoft stores and manages the database encryption key for environments. The manage keys feature in the Microsoft Power Platform admin center gives administrators the ability to self-manage the database encryption key that is associated with the Dataverse tenant.

Enable sensitive data encryption at rest using Customer Managed Keys rather than Microsoft Managed keys.

**Note:** This feature is only available in tenants with 1,000 or more users. An exception to this recommendation will be needed for those tenants that have under 1,000 users.

#### **Rationale:**

By default, Microsoft stores and manages the database encryption key for organizational environments, so administrators don't have to. The manage keys feature in the Microsoft Power Platform admin center gives administrators the ability to self-manage the database encryption key that is associated with the Dataverse tenant.

#### **Impact:**

Using Customer Managed Keys may also incur additional man-hour requirements to create, store, manage, and protect the keys as needed.

**Note:** It is strongly recommended that a copy of the encryption key is made and stored in a safe place. The key may need to be entered again to ensure that certain features keep working and the data is retrievable. For more information, see Data Encryption.

Changing the encryption key can take a long time in a large database. Run this operation during off-peak hours if the system is busy or when working with a large amount of data.

**Note #2:** This feature is only available in tenants with 1,000 or more users. An exception to this recommendation will be needed for those tenants that have under 1,000 users.

**Audit:**

Ensure that Customer Managed Keys are utilized.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings** at the top of the screen.
3. Expand **Encryption** then select **Data encryption**

A new window will open and may be slow to load

4. Ensure Encryption status is set to **Active**
5. Ensure self-managed encryption keys are utilized.
6. Click **Close** (data will not be re-encrypted).

**Remediation:**

Configure Customer Managed Keys.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings** at the top of the screen.
3. Expand **Encryption** then select **Data encryption**

A new window will open and may be slow to load

4. Ensure Encryption status is set to **Active**
5. Under **Change Encryption Key** insert the new key followed by **Change**




**Note:** It is important to safeguard the encryption key.

6. Click **Close**

**References:**

1. <https://docs.microsoft.com/en-us/power-platform/admin/data-encryption>
2. <https://docs.microsoft.com/en-us/power-platform/admin/manage-encryption-key>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## 3.2 (L1) Ensure 'Extract customer data privileges from Microsoft Dynamics 365 is controlled' (Manual)

### Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### Description:

Ensure that privileges related to customer data extraction are well tailored for the business needs considering the minimum privileges required.

### Rationale:

When users are able to export data deliberately, data governance and security can become an impossible activity and can also lead data leakage.

### Impact:

If not configured correctly, users with need-to-know might not have access to the data.

### Audit:

Ensure that the extract customer data privileges from Microsoft Dynamics 365 controlled.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select `Settings`
3. Expand `Users + permissions` then click `Security roles`.
4. Select `Edit` under `More Actions` for each security role
5. Select the `Business Management` tab then review the permissions under `Privacy Related Privileges`.
6. Ensure that the appropriate privileges are assigned based on organizational policy.

## Remediation:

To configure the extract customer data privileges from Microsoft Dynamics 365 privilege, use the Power Platform Admin Center:







1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings**
3. Expand **Users + permissions** then click **Security roles**.
4. Select **Edit** under **More Actions** for each security role
5. Select the **Business Management** tab then review the permissions under **Privacy Related Privileges**.
6. Enable or disable privilege based on organizational policy.

**Note:** Enabling these privileges will allow users to extract customer data from Microsoft Dynamics 365. For more information, review the corresponding user documentation.

## References:

1. <https://docs.microsoft.com/en-us/power-platform/admin/create-edit-security-role>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### *3.3 (L1) Ensure 'Dynamics 365 restricts incoming email actions for public queue mailboxes' (Manual)*

#### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

#### **Description:**

Microsoft Dynamics 365 can be used in Outlook to track email messages, contacts, tasks, and appointments. When an email message, contact, task, or appointment record is tracked, a copy of that record is saved as an activity in Dynamics 365 for Customer Engagement and synchronized with the Outlook record.

This can be viewed and edited in Dynamics 365 for Outlook or Customer Engagement. If Outlook is synced to a mobile device, the mobile device will also have access to these records.

Options to automatically track email messages:

Email messages from Dynamics 365 apps Leads, Contacts, and Accounts: Tracks email messages only if they originate from someone with a Dynamics 365 for Customer Engagement lead, contact, or account record.

The recommended state for this setting is: Email messages from Dynamics 365 apps Leads, Contacts, and Accounts

#### **Rationale:**

An unauthenticated attacker can create arbitrary contacts and email activities within the Dynamics 365 system. This can lead to several problems of varying severity:

- Spam and reduction of data quality.
- Denial of Service (DoS).
- Sophisticated attacks aiming at human error. For example, an attacker may create a new contact that has the same name as an already existing contact.
- A Dynamics 365 application user may accidentally choose the attacker-controlled contact for communication instead of the legitimate one and thereby cause exposure of sensitive information.

If possible, emails should only be converted to Dynamics 365 entities when the sender address is known or considered trustworthy.

#### **Impact:**

Emails from a trustworthy entity might not be converted to Dynamics 365.

## Audit:

Verify that the option `Email messages from Dynamics 365 apps Leads, Contacts, and Accounts` is selected.

In the Power Platform Admin Center:

1. Log in to `https://admin.powerplatform.microsoft.com` and select the appropriate environment.
2. Select `Settings` at the top.
3. Expand `Business` followed by `Queues`.

This will open in a new window.

4. Click on the email boxes to modify.
5. Under `EMAIL SETTINGS` ensure that the `Email messages from Dynamics 365 Leads, Contacts, and Accounts` options is selected.

## Remediation:

Ensure that the option `Email messages from Dynamics 365 apps Leads, Contacts, and Accounts` selected.

In the Power Platform Admin Center:

1. Log in to `https://admin.powerplatform.microsoft.com` and select the appropriate environment.
2. Select `Settings` at the top.
3. Expand `Business` followed by `Queues`

This will open in a new window.

4. Click on the email boxes to modify.
5. Under `EMAIL SETTINGS` set `Convert Incoming Email to Activities` to `Email messages from Dynamics 365 Leads, Contacts, and Accounts`
6. Click `Save`.

**Note:** Avoid setting the option to `All email messages` as Dynamics 365 apps will track junk mail as well as business conversations.

## Default Value:

By default, email in the “Sent Items” folder within Outlook will not automatically appear as tracked in Dynamics 365.

**References:**

1. <https://docs.microsoft.com/en-us/dynamics365/outlook-addin/user-guide/set-option-automatically-track-incoming-outlook-email>
2. <https://docs.microsoft.com/en-us/dynamics365/outlook-addin/user-guide/overview-tracking-records>



### *3.4 (L1) Ensure 'DLP policies are enabled and restrict the connectors usage' (Manual)*

#### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

#### **Description:**

Power Platform data loss prevention policies (DLP) act as guardrails to help prevent users from unintentionally exposing organizational data. These data loss prevention policies enforce rules for which connectors can be used together in apps and flows. The policies can be scoped to one environment, many environments, or tenant-wide

#### **Rationale:**

Power Apps and automation are becoming increasingly connected across multiple data sources and multiple services. Some of these might be external, third-party services and might even include some social networks. Users generally have good intentions, but they can easily overlook the potential for exposure from data leakage to services and audiences that shouldn't have access to the data. Categorize the data connectors into one of three data groups, "Business data only", "No business data allowed" and "Blocked". Users will be prevented from creating flows and apps that combine connectors from the "Business data only" and "No business data allowed" data groups and also will not have access to connectors blocked.

#### **Impact:**

Enabling a Power Platform DLP policy will restrict the connectors usage in the environment. Always ensure to follow appropriate procedures in regard to testing and implementation of DLP policies based on the business needs.

#### **Audit:**

Verify DLP policies are enabled.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com>.
2. Expand **Policies** in the left pane then select **Data policies**
3. Verify that organizational policies are set and applied.

## Remediation:

Ensure DLP policies are enabled.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com>.
2. Expand **Policies** in the left pane then select **Data policies**.
3. Click **New Policy** to initiate the policy wizard.
4. Name the policy, then click next.
5. At the **Custom Connectors** choose which connectors should fit in every data group:
  1. Business
  2. Non-business (Default)
  3. Blocked
  4. Ignore.
6. For the **Scope** ensure to select all applicable environments.
7. Click **Create policy**.

## Default Value:

By default, no DLP policies are implemented in the tenant.

## References:

1. <https://docs.microsoft.com/en-us/power-platform/guidance/adoption/dlp-strategy>
2. <https://docs.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention>
3. <https://docs.microsoft.com/en-us/power-platform/admin/create-dlp-policy>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.13 <u>Deploy a Data Loss Prevention Solution</u></b> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	<b>13.3 <u>Monitor and Block Unauthorized Network Traffic</u></b> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

## 4 Logging and Auditing

## *4.1 (L1) Ensure 'System Administrator security role changes are reviewed periodically' (Manual)*

### **Profile Applicability:**

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### **Description:**

Security roles define how different users access different types of records. To control access to data, security roles can be modified to create new security roles or change which security roles are assigned to each user. Each user can have multiple security roles and are cumulative meaning having more than one security role gives a user every privilege available in every role.

### **Rationale:**

Illicit role group changes could give an attacker access to data that is privileged and perform tasks in the environment.

### **Impact:**

None - there is no impact to users or the system.

### **Audit:**

Verify which users have been added to the System Administrator Security Role.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Edit** on the Details pane of the environment.
3. Select **Settings** at the top of the window.
4. Expand **Users + permissions** then select **Security roles**.
5. Click on **System Administrator** (not the three dots and edit)
6. Review the list of users

## Remediation:

Ensure no unauthorized users have been added to the System Administrator Security Role.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Edit** on the Details pane of the environment.
3. Select **Settings** at the top of the window.
4. Expand **Users + permissions** then select **Security roles**.
5. Click on **System Administrator** (not the three dots and edit)
6. Add/Remove users as appropriate.

## Default Value:

N/A

## References:

1. <https://docs.microsoft.com/en-us/power-platform/admin/database-security>
2. <https://docs.microsoft.com/en-us/power-platform/admin/security-roles-privileges>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

## 4.2 (L1) Ensure 'Environment Activity logging is Enabled' (Manual)

### Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

### Description:

Activity logging track changes to organizational data and maintain a log of those changes.

### Rationale:

Enabling Power Platform Activity logging helps the security teams to investigate activities for regular security operational or forensic purposes. The auditing feature is designed to meet the auditing, compliance, security, and governance policies of many regulated enterprises.

### Impact:

It is required to plan and evaluate the log size for impact to storage/costs.

### Audit:

Verify that the Environment Activity logging is Enabled.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Click **Settings** at the top of the window.
3. Expand **Audit and logs** then select **Audit settings**.
4. Ensure the following are set:
  - a. Start Auditing
  - b. Log access
  - c. Read logs
5. Ensure that the retention for logs to the appropriate timeframe according to organizational policy.

## Remediation:

Ensure that the Environment Activity logging is Enabled.

In the Power Platform Admin Center:

1. Log in to <https://admin.powerplatform.microsoft.com> and select the appropriate environment.
2. Select **Settings** at the top of the window.
3. Expand **Audit and logs** then select **Audit settings**.
4. Select the following:
  - a. **Start**
  - b. **Auditing Log access**
  - c. **Read logs**
5. Set the retention for logs to the appropriate timeframe according to organizational policy.
6. Click **Save**.

**Note:** Logs are found in the Security and Compliance Center







## Default Value:

Disabled.

## References:

1. <https://docs.microsoft.com/en-us/power-platform/admin/enable-use-comprehensive-auditing#enable-auditing>
2. <https://docs.microsoft.com/en-us/power-platform/admin/system-settings-dialog-box-auditing-tab>
3. <https://docs.microsoft.com/en-us/power-platform/admin/logging-powerapps>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

### 4.3 (L1) Ensure 'App creation notification is enabled in the environment' (Manual)

#### Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

#### Description:

App creation alerting can be used to inform admins and stakeholders about specific events, or provide a summary of activity in the environment.

#### Rationale:

Alerting on the creation of apps allows for administrators to look for risky apps that users have created that could cause data spillage or accidental elevation of privilege.

#### Impact:

Alerts will be sent to an individual(s) and could be high in volume.

**Note:** Audit logging must be enabled.

#### Audit:

Verify that App creation notifications are set to enabled.

In the Microsoft 365 Security & Compliance Center:

- Log in to the Microsoft 365 Security & Compliance Center  
<https://compliance.microsoft.com/> as a tenant Administrator.
- Go to Policies > Alert Policy.
- Verify a policy exists for app creation notification.

#### Remediation:

Ensure that App creation notifications are set to enabled.

In the Microsoft 365 Security & Compliance Center:

- Log in to the Microsoft 365 Security & Compliance Center  
<https://compliance.microsoft.com/> as a tenant Administrator.
- Go to Policies > Alert Policy > +New Alert policy.
- Name policy and select the Severity and Category for the policy.
- In the Activity section scroll down to PowerApps app or search for Publish.
- Name the alert and select users (emails) to send alerts to.

Ensure that a notification is triggered when a new app is created in the environment.



**Default Value:**

N/A

**References:**

1. <https://docs.microsoft.com/en-us/power-platform/guidance/adoption/sharing-alerts>

# Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1</b>	<b>Accounts and Authentication</b>		
1.1	(L1) Ensure 'User access to environments is controlled with Security Groups' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	(L1) Ensure 'User sessions are terminated upon time limit exceeded and user logoff' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	(L1) Ensure 'Administrative accounts are separate, unassigned, and cloud-only' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	(L2) Ensure 'Multifactor authentication for all users' is 'Enabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Permissions</b>		
2.1	(L1) Ensure 'Creation of new trial, production, and sandbox environments' is restricted to 'Administrators' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	(L1) Ensure 'Security roles provide access to the minimum amount of business data required' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	(L1) Ensure 'Set blocked file extensions' is configured to match the enterprise block list (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	(L2) Ensure 'Access to the environment is restricted by location' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	(L1) Ensure 'Cross-tenant isolation is enabled for Power Platform Apps and Flows' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Data Management</b>		
3.1	(L2) Ensure 'Environments with Critical Data are Encrypted with Customer Managed Keys' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.2	(L1) Ensure 'Extract customer data privileges from Microsoft Dynamics 365 is controlled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	(L1) Ensure 'Dynamics 365 restricts incoming email actions for public queue mailboxes' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	(L1) Ensure 'DLP policies are enabled and restrict the connectors usage' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Logging and Auditing</b>		
4.1	(L1) Ensure 'System Administrator security role changes are reviewed periodically' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(L1) Ensure 'Environment Activity logging is Enabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	(L1) Ensure 'App creation notification is enabled in the environment' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version
12/20/2022	1.0.0	Initial Public Release