MICROSOFT DEFENDER

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.0

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

REVISION HISTORY

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

CONTENTS

1. CISA M365 SECURITY CONFIGURATION BASELINE FOR DEFENDER

Microsoft 365 (M365) Defender is a cloud-based enterprise defense suite that coordinates prevention, detection, investigation, and response. This set of tools and features are used to detect many types of attacks.

This baseline focuses on the features of Defender for Office 365, but some settings are actually configured in the Microsoft Purview compliance portal. However, for simplicity, both the M365 Defender and Microsoft Purview compliance portal items are contained in this baseline.

Generally, use of Microsoft Defender is not required by the baselines of the core M365 products (Exchange Online, Teams, etc.). This baseline serves as a guide should an agency elect to use Defender as their tool of choice. Please note that some of the controls in the core baselines require the use of a dedicated security tool, such as Defender.

In addition to these controls, agencies should consider using a cloud access security broker to secure their environments as they adopt zero trust principles.

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 agency has identified a set of user accounts that are considered sensitive accounts. See Key Terminology for a detailed description of sensitive accounts.

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 RFC 2119.

The following are key terms and descriptions used in this document.

- Sensitive Accounts: This term denotes a set of user accounts that have access to sensitive and high-value information. As a result, these accounts may be at a higher risk of being targeted.

2. BASELINE POLICIES

2.1 PRESET SECURITY PROFILES

Microsoft Defender defines three preset security profiles: built-in protection, standard, and strict. These preset policies are informed by Microsoft's observations and are designed to strike the balance between usability and security. They allow administrators to enable the full feature set of Defender by simply adding users to the policies rather than manually configuring each setting.

Within the standard and strict preset policies, users can be enrolled in Exchange Online Protection (EOP) and Defender for Office 365 protection. Additionally, preset policies support configuration of impersonation protection.

2.2 POLICIES

2.2.1 MS.DEFENDER.1.1v1

The standard and strict preset security policies SHALL be enabled.

- *Rationale:* Defender includes a large number of features and settings to protect users against threats. Using the preset security policies, administrators can help ensure all new and existing users automatically have secure defaults applied.
- *Last modified:* June 2023

2.2.2 MS.DEFENDER.1.2v1

All users SHALL be added to Exchange Online Protection in either the standard or strict preset security policy.

- *Rationale:* Important user protections are provided by EOP, including anti-spam, anti-malware, and anti-phishing protections. By using the preset policies, administrators can help ensure all new and existing users have secure defaults applied automatically.
- *Last modified:* June 2023
- *Note:*

  - The standard and strict preset security policies must be enabled as directed by MS.DEFENDER.1.1v1 for protections to be applied.
  - Specific user accounts, except for sensitive accounts, MAY be exempt from the preset policies, provided they are added to one or more custom policies offering comparable protection. These users might need flexibility not offered by the preset policies. Their accounts should be added to a custom policy, conforming as closely as possible to the settings used by the preset policies. See the **Resources** section for more details on configuring policies.

2.2.3 MS.DEFENDER.1.3v1

All users SHALL be added to Defender for Office 365 protection in either the standard or strict preset security policy.

- *Rationale:* Important user protections are provided by Defender for Office 365 protection, including safe attachments and safe links. By using the preset policies, administrators can help ensure all new and existing users have secure defaults applied automatically.
- *Last modified:* June 2023
- *Note*:
  - The standard and strict preset security policies must be enabled as directed by MS.DEFENDER.1.1v1 for protections to be applied.
  - Specific user accounts, except for sensitive accounts, MAY be exempt from the preset policies, provided they are added to one or more custom policies offering comparable protection. These users might need flexibility not offered by the preset policies. Their accounts should be added to a custom policy conforming as closely as possible to the settings used by the preset policies. See the **Resources** section for more details on configuring policies.

2.2.4 MS.DEFENDER.1.4v1

Sensitive accounts SHALL be added to Exchange Online Protection in the strict preset security policy.

- *Rationale:* Unauthorized access to a sensitive account may result in greater harm than to a standard user account. Adding sensitive accounts to the strict preset security policy, with its increased protections, better mitigates their elevated risk to email threats.
- *Last modified:* June 2023
- *Note:* The strict preset security policy must be enabled to protect sensitive accounts.

2.2.5 MS.DEFENDER.1.5v1

Sensitive accounts SHALL be added to Defender for Office 365 protection in the strict preset security policy.

- *Rationale:* Unauthorized access to a sensitive account may result in greater harm than to a standard user account. Adding sensitive accounts to the strict preset security policy, with its increased protections, better mitigates their elevated risk.
- *Last modified:* June 2023
- *Note:* The strict preset security policy must be enabled to protect sensitive accounts.

2.3 RESOURCES

- Use the Microsoft 365 Defender portal to assign Standard and Strict preset security policies to users | Microsoft Learn
- Recommended settings for EOP and Microsoft Defender for Office 365 security | Microsoft Learn
- Configure anti-phishing policies in EOP | Microsoft Learn
- Configure anti-malware policies in EOP | Microsoft Learn
- Configure anti-spam policies in EOP | Microsoft Learn

- Configure anti-phishing policies in Defender for Office 365 | Microsoft Learn
- Set up Safe Attachments policies in Microsoft Defender for Office 365 | Microsoft Learn
- Set up Safe Links policies in Microsoft Defender for Office 365 | Microsoft Learn

2.4 LICENSE REQUIREMENTS

- N/A

2.5 IMPLEMENTATION

2.5.1 MS.DEFENDER.1.1v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration > Policies & Rules.**
3. Select **Threat Policies.**
4. From the **Templated policies** section, select **Preset Security Policies.**
5. Under **Standard protection**, slide the toggle switch to the right so the text next to the toggle reads **Standard protection is on.**
6. Under **Strict protection**, slide the toggle switch to the right so the text next to the toggle reads **Strict protection is on.**

Note: If the toggle slider in step 5 is grayed out, click on **Manage protection settings** instead and configure the policy settings according to Use the Microsoft 365 Defender portal to assign Standard and Strict preset security policies to users | Microsoft Learn.

2.5.2 MS.DEFENDER.1.2v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration > Policies & Rules.**
3. Select **Threat Policies.**
4. From the **Templated policies** section, select **Preset Security Policies.**
5. Under either **Standard protection** or **Strict protection**, select **Manage protection settings.**
6. On the **Apply Exchange Online Protection** page, select **All recipients.**
7. (Optional) Under **Exclude these recipients**, add **Users** and **Groups** to be exempted from the preset policies.
8. Select **Next** on each page until the **Review and confirm your changes** page.
9. On the **Review and confirm your changes** page, select **Confirm.**

2.5.3 MS.DEFENDER.1.3v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration > Policies & Rules.**
3. Select **Threat Policies.**
4. From the **Templated policies** section, select **Preset Security Policies.**
5. Under either **Standard protection** or **Strict protection**, select **Manage protection settings.**
6. Select **Next** until you reach the **Apply Defender for Office 365 protection** page.
7. On the **Apply Defender for Office 365 protection** page, select **All recipients.**
8. (Optional) Under **Exclude these recipients**, add **Users** and **Groups** to be exempted from the preset policies.
9. Select **Next** on each page until the **Review and confirm your changes** page.
10. On the **Review and confirm your changes** page, select **Confirm.**

2.5.4 MS.DEFENDER.1.4v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration** > **Policies & Rules**.
3. Select **Threat Policies**.
4. From the **Templated policies** section, select **Preset Security Policies**.
5. Under **Strict protection**, select **Manage protection settings**.
6. On the **Apply Exchange Online Protection** page, select **Specific recipients**.
7. Add all sensitive accounts via the **User** and **Group** boxes using the names of mailboxes, users, contacts, M365 groups, and distribution groups.
8. Select **Next** on each page until the **Review and confirm your changes** page.
9. On the **Review and confirm your changes page**, select **Confirm**.

2.5.5 MS.DEFENDER.1.5v1Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration** > **Policies & Rules**.
3. Select **Threat Policies**.
4. From the **Templated policies** section, select **Preset Security Policies**.
5. Under **Strict protection**, select **Manage protection settings**.
6. Select **Next** until you reach the **Apply Defender for Office 365 protection** page.
7. On the **Apply Defender for Office 365 protection** page, select **Specific recipients** or **Previously selected recipients** if sensitive accounts were already set on the EOP page.
8. If adding sensitive accounts separately via **Specific recipients**, add all sensitive accounts via the **User** and **Group** boxes using the names of mailboxes, users, contacts, M365 groups, and distribution groups.
9. (Optional) Under **Exclude these recipients**, add **Users** and **Groups** to be exempted from the preset policies.
10. Select **Next** on each page until the **Review and confirm your changes** page.
11. On the **Review and confirm your changes** page, select **Confirm**.

3. IMPERSONATION PROTECTION

Impersonation protection checks incoming emails to see if the sender address is similar to the users or domains on an agency-defined list. If the sender address is significantly similar, as to indicate an impersonation attempt, the email is quarantined.

3.1 POLICIES

3.1.1 MS.DEFENDER.2.1v1

- *Rationale:* User impersonation, especially of users with access to sensitive or high-value information and resources, has the potential to result in serious harm. Impersonation protection mitigates this risk. By configuring impersonation protection in both preset policies, administrators can help protect email recipients from impersonated emails, regardless of whether they are added to the standard or strict policy.
- *Last modified:* June 2023
- *Note:* The standard and strict preset security policies must be enabled to protect accounts.

3.1.2 MS.DEFENDER.2.2v1

Domain impersonation protection SHOULD be enabled for domains owned by the agency in both the standard and strict preset policies.

- *Rationale:* Configuring domain impersonation protection for all agency domains reduces the risk of a user being deceived by a look-alike domain. By configuring impersonation protection in both preset policies, administrators can help protect email recipients from impersonated emails, regardless of whether they are added to the standard or strict policy.
- *Last modified*: June 2023
- *Note:* The standard and strict preset security policies must be enabled to protect agency domains.

3.1.3 MS.DEFENDER.2.3v1

Domain impersonation protection SHOULD be added for important partners in both the standard and strict preset policies.

- *Rationale:* Configuring domain impersonation protection for domains owned by important partners reduces the risk of a user being deceived by a look-alike domain. By configuring impersonation protection in both preset policies, administrators can help protect email recipients from impersonated emails, regardless of whether they are added to the standard or strict policy.
- *Last modified*: June 2023
- *Note:* The standard and strict preset security policies must be enabled to protect partner domains.

3.2 RESOURCES

- Impersonation settings in anti-phishing policies in Microsoft Defender for Office 365 | Microsoft Learn
- Use the Microsoft 365 Defender portal to assign Standard and Strict preset security policies to users | Microsoft Learn

3.3 LICENSE REQUIREMENTS

- Impersonation protection and advanced phishing thresholds require Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3. As of April 25, 2023, anti-phishing for user and domain impersonation, and spoof intelligence are not yet available in M365 Government Community Cloud High (GCC High) and M365 Department of Defense (DoD) environments. See Platform features | Microsoft Learn for current offerings.

3.4 IMPLEMENTATION

3.4.1 MS.DEFENDER.2.1v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration > Policies & Rules**.
3. Select **Threat Policies**.
4. From the **Templated policies section**, select **Preset Security Policies**.
5. Under **Standard protection** or **Strict protection**, select **Manage protection settings**.
6. Select **Next** until you reach the **Impersonation Protection** page, then select **Next** once more.
7. On the **Protected custom users** page, add a name and valid email address for each sensitive account, and click **Add** after each.
8. Select **Next** until you reach the **Trusted senders and domains** page.
9. (Optional) Add specific email addresses here to not flag as impersonation when sending messages and prevent false positives. Click **Add** after each.
10. Select **Next** on each page until the **Review and confirm your changes** page.
11. On the **Review and confirm your changes** page, select **Confirm**.

3.4.2 MS.DEFENDER.2.2v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration** > **Policies & Rules**.
3. Select **Threat Policies**.
4. From the **Templated policies** section, select **Preset Security Policies**.
5. Under **Standard protection** or **Strict protection**, select **Manage protection settings**.
6. Select **Next** until you reach the **Impersonation Protection** page, then select **Next** once more.
7. On the **Protected custom domains** page, add each agency domain, and click **Add** after each.
8. Select **Next** until you reach the **Trusted senders and domains** page.
9. (Optional) Add specific domains here to not flag as impersonation when sending messages and prevent false positives. Click **Add** after each.
10. Select **Next** on each page until the **Review and confirm your changes** page.
11. On the **Review and confirm your changes** page, select **Confirm**.

3.4.3 MS.DEFENDER.2.3v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. In the left-hand menu, go to **Email & Collaboration** > **Policies & Rules**.
3. Select **Threat Policies**.
4. From the **Templated policies** section, select **Preset Security Policies**.
5. Under **Standard protection** or **Strict protection**, select **Manage protection settings**.
6. Select **Next** until you reach the **Impersonation Protection** page, then select **Next** once more.
7. On the **Protected custom domains** page, add each partner domain, and click **Add** after each.
8. Select **Next** on each page until the **Review and confirm your changes** page.
9. On the **Review and confirm your changes** page, select **Confirm**.

4. SAFE ATTACHMENTS

The Safe Attachments feature will scan messages for attachments with malicious content. All messages with attachments not already flagged by anti-malware protections in EOP are downloaded to a Microsoft virtual environment for further analysis. Safe Attachments then uses machine learning and other analysis techniques to detect malicious intent. While Safe Attachments for Exchange Online is automatically configured in the preset policies, separate action is needed to enable it for other products.

4.1 POLICIES

4.1.1 MS.DEFENDER.3.1v1

Safe attachments SHOULD be enabled for SharePoint, OneDrive, and Microsoft Teams.

- *Rationale:* Clicking malicious links makes users vulnerable to attacks, and this danger is not limited to links in emails. Other Microsoft products, such as Microsoft Teams, can be used to present users with malicious links. As such, it is important to protect users on these other Microsoft products as well.
- *Last modified*: June 2023

4.2 RESOURCES

- Safe Attachments in Microsoft Defender for Office 365 | Microsoft Learn
- Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams | Microsoft Learn

4.3 LICENSE REQUIREMENTS

- Requires Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3.

4.4 IMPLEMENTATION

4.4.1 MS.DEFENDER.3.1v1 Instructions

To enable Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, follow the instructions listed at Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams | Microsoft Learn.

1. Sign in to **Microsoft 365 Defender**.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under **Policies**, select **Safe Attachments**.
5. Select **Global settings**.
6. Toggle the **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams** slider to **On**.

5. DATA LOSS PREVENTION

There are several approaches to securing sensitive information, such as warning users, encryption, or blocking attempts to share. Agency policies for sensitive information, such as personally identifiable information (PII), should dictate how that information is handled and inform associated data loss prevention (DLP) policies. Defender can detect sensitive information and associates a default confidence level with this detection based on the sensitive information type matched. Confidence levels are used to reduce false positives in detecting access to sensitive information. Agencies may choose to use the default confidence levels or adjust the levels in custom DLP policies to fit their environment and needs.

5.1 POLICIES

5.1.1 MS.DEFENDER.4.1v1

A custom policy SHALL be configured to protect PII and sensitive information, as defined by the agency. At a minimum, credit card numbers, U.S. Individual Taxpayer Identification Numbers (ITIN), and U.S. Social Security numbers (SSN) SHALL be blocked.

- *Rationale:* Users may inadvertently 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

5.1.2 MS.DEFENDER.4.2v1

The custom policy SHOULD be applied to Exchange, OneDrive, SharePoint, Teams chat, and Devices.

- *Rationale:* Unauthorized disclosures may happen through M365 services or endpoint devices. DLP policies should cover all affected locations to be effective.
- *Last modified*: June 2023
- *Note:* The custom policy referenced here is the same policy configured in MS.DEFENDER.4.1v1.

5.1.3 MS.DEFENDER.4.3v1

The action for the custom policy SHOULD be set to block sharing sensitive information with everyone.

- *Rationale:* Access to sensitive information should be prohibited unless explicitly allowed. Specific exemptions can be made based on agency policies and valid business justifications.
- *Last modified*: June 2023
- *Note:* The custom policy referenced here is the same policy configured in MS.DEFENDER.4.1v1.

5.1.4 MS.DEFENDER.4.4v1

Notifications to inform users and help educate them on the proper use of sensitive information SHOULD be enabled in the custom policy.

- *Rationale:* Some users may not be aware of agency policies on proper use of sensitive information. Enabling notifications provides positive feedback to users when accessing sensitive information.
- *Last modified*: June 2023
- *Note:* The custom policy referenced here is the same policy configured in MS.DEFENDER.4.1v1.

5.1.5 DEFENDER.4.5v1

A list of apps that are restricted from accessing files protected by DLP policy SHOULD be defined.

- *Rationale:* Some apps may inappropriately share accessed files or not conform to agency policies for access to sensitive information. Defining a list of those apps makes it possible to use DLP policies to restrict those apps' access to sensitive information on endpoints using Defender.
- *Last modified*: June 2023

5.1.6 MS.DEFENDER.4.6v1

The custom policy SHOULD include an action to block access to sensitive information by restricted apps and unwanted Bluetooth applications.

- *Rationale:* Some apps may inappropriately share accessed files or not conform to agency policies for access to sensitive information. Defining a DLP policy with an action to block access from restricted apps and unwanted Bluetooth applications prevents unauthorized disclosure by those programs.
- Last modified: June 2023
- Note:
  - The custom policy referenced here is the same policy configured in MS.DEFENDER.4.1v1.
  - This action can only be included if at least one device is onboarded to the agency tenant. Otherwise, the option to block restricted apps will not be available.

5.2 RESOURCES

- Plan for data loss prevention (DLP) | Microsoft Learn
- Data loss prevention in Exchange Online | Microsoft Learn
- Personally identifiable information (PII) | NIST
- Sensitive information | NIST
- Get started with Endpoint data loss prevention - Microsoft Purview (compliance) | Microsoft Learn

5.3 LICENSE REQUIREMENTS

- DLP for Teams requires an E5 or G5 license. See Microsoft Purview Data Loss Prevention: Data Loss Prevention for Teams | Microsoft Learn for more information.
- DLP for Endpoint requires an E5 or G5 license. See Get started with Endpoint data loss prevention - Microsoft Purview (compliance) | Microsoft Learn for more information.

5.4 IMPLEMENTATION

5.4.1 MS.DEFENDER.4.1v1 Instructions

1. Sign in to the **Microsoft Purview compliance portal**.
2. Under the **Solutions** section on the left-hand menu, select **Data loss prevention**.
3. Select **Policies** from the top of the page.
4. Select **Create policy**.
5. From the **Categories** list, select **Custom**.
6. From the **Templates** list, select **Custom policy** and then click **Next**.
7. Edit the name and description of the policy if desired, then click **Next**.
8. Under **Choose locations to apply the policy**, set **Status** to **On** for at least the Exchange email, OneDrive accounts, SharePoint sites, Teams chat and channel messages, and Devices locations, then click **Next**.
9. Under **Define policy settings**, select **Create or customize advanced DLP rules**, and then click **Next**.
10. Click **Create rule**. Assign the rule an appropriate name and description.
11. Click **Add condition**, then **Content contains**.
12. Click **Add**, then **Sensitive info types**.
13. Add information types that protect information sensitive to the agency. At a minimum, the agency should protect:
    - Credit card numbers
    - U.S. Individual Taxpayer Identification Numbers (ITIN)
    - U.S. Social Security Numbers (SSN)
    - All agency-defined PII and sensitive information
14. Click **Add**.
15. Under **Actions**, click **Add an action**.
16. Check **Restrict Access or encrypt the content in Microsoft 365 locations**.
17. Under this action, select **Block Everyone**.
18. Under **User notifications**, turn on **Use notifications to inform your users and help educate them on the proper use of sensitive info**.
19. Click **Save**, then **Next**.
20. Select **Turn it on right away**, then click **Next**.
21. Click **Submit**.

5.4.2 MS.DEFENDER.4.2v1 Instructions

See MS.DEFENDER.4.1v1 instructions step 8 for details on enforcing DLP policy in specific M365 service locations.

5.4.3 MS.DEFENDER.4.3v1 instructions

See MS.DEFENDER.4.1v1 instructions steps 15-17 for details on configuring DLP policy to block sharing sensitive information with everyone.

5.4.4 MS.DEFENDER.4.4v1 instructions

See MS.DEFENDER.4.1v1 instructions steps 18-19 for details on configuring DLP policy to notify users when accessing sensitive information.

5.4.5 MS.DEFENDER.4.5v1 Instructions

1. Sign in to the **Microsoft Purview compliance portal**.
2. Under **Solutions**, select **Data loss prevention**.

3. Go to **Endpoint DLP Settings**.
4. Go to **Restricted apps and app groups**.
5. Click **Add or edit Restricted Apps**.
6. Enter an app and executable name to disallow said app from accessing protected files and log the incident.
7. Return and click **Unallowed Bluetooth apps**.
8. Click **Add or edit unallowed Bluetooth apps**.
9. Enter an app and executable name to disallow said app from accessing protected files and log the incident.

5.4.6 MS.DEFENDER.4.6v1 Instructions

If restricted app and unwanted Bluetooth app restrictions are desired, associated devices must be onboarded with Defender for Endpoint before the instructions below can be completed.

1. Sign in to the **Microsoft Purview compliance portal**.
2. Under **Solutions**, select **Data loss prevention**.
3. Select **Policies** from the top of the page.
4. Find the custom DLP policy configured under MS.DEFENDER.4.1v1 instructions in the list and click the Policy name to select.
5. Select **Edit Policy**.
6. Click **Next** on each page in the policy wizard until you reach the Advanced DLP rules page.
7. Select the relevant rule and click the pencil icon to edit it.
8. Under **Actions**, click **Add an action**.
9. Choose **Audit or restrict activities on device.**
10. Under **File activities for all apps**, select **Apply restrictions to specific activity**.
11. Check the box next to **Copy or move using unallowed Bluetooth app** and set its action to **Block**.
12. Under **Restricted app activities**, check the **Access by restricted apps** box and set the action drop-down to **Block**.
13. Click **Save** to save the changes.
14. Click **Next** on each page until reaching the **Review your policy and create it** page.
15. Review the policy and click **Submit** to complete the policy changes.

6. ALERTS

There are several pre-built alert policies available pertaining to various apps in the M365 suite. These alerts give administrators better real-time insight into possible security incidents. Guidance on specific alerts to configure can be found in the linked section of the CISA M365 Security Configuration Baseline for Exchange Online.

- MS.EXO.16.1v1 | CISA M365 Security Configuration Baseline for Exchange Online

6.1 POLICIES

6.1.1 MS.DEFENDER.5.1v1

At a minimum, the alerts required by the CISA M365 Security Configuration Baseline for Exchange Online SHALL be enabled.

- *Rationale:* Potentially malicious or service-impacting events may go undetected without a means of detecting these events. Setting up a mechanism to alert administrators to the list of events above draws attention to them to minimize any impact to users and the agency.
- Last modified: June 2023

6.1.2 MS.DEFENDER.5.2v1

The alerts SHOULD be sent to a monitored address or incorporated into a SIEM.

- *Rationale:* Suspicious or malicious events, if not resolved promptly, may have a greater impact to users and the agency. Sending alerts to a monitored email address or Security Information and Event Management (SIEM) system helps ensure events are acted upon in a timely manner to limit overall impact.
- *Last modified*: June 2023

6.2 RESOURCES

- Alert policies in Microsoft 365 | Microsoft Learn

6.3 LICENSE REQUIREMENTS

- N/A

6.4 IMPLEMENTATION

6.4.1 MS.DEFENDER.5.1v1 Instructions

1. Sign in to **Microsoft 365 Defender**.
2. Under **Email & collaboration**, select **Policies & rules.**
3. Select **Alert Policy.**
4. Select the checkbox next to each alert to enable as determined by the agency, and at a minimum those referenced in the *CISA M365 Security Configuration Baseline for Exchange Online*.
5. Click the pencil icon from the top menu.
6. Select the **Enable selected policies** action from the **Bulk actions** menu.

6.4.2 MS.DEFENDER.5.2v1 Instructions

For each enabled alert, to add one or more email recipients:

1. Sign in to **Microsoft 365 Defender**.
2. Under **Email & collaboration**, select **Policies & rules.**
3. Select **Alert Policy.**
4. Click the alert policy to modify.
5. Click the pencil icon next to **Set your recipients.**
6. Check the **Opt-In for email notifications** box.
7. Add one or more email addresses to the **Email recipients** text box.
8. Click **Next.**
9. On the **Review** page, click **Submit** to save the notification settings.

7. AUDIT LOGGING

User activity from M365 services is captured in the organization's unified audit log. These logs are essential for conducting incident response and threat detection activity.

By default, Microsoft retains the audit logs for 180 days. Activity by users with E5 licenses is logged for one year.

However, in accordance with Office of Management and Budget (OMB) Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, M365 audit logs are to be retained for at least 12 months in active storage and an additional 18 months in cold storage. This can be accomplished either by offloading the logs out of the cloud environment or natively through Microsoft by creating an audit log retention policy.

OMB M-21-13 requires Advanced Audit Features be configured in M365. Advanced Audit, now Microsoft Purview Audit (Premium), adds additional event types to the Unified Audit Log.

7.1 POLICIES

7.1.1 MS.DEFENDER.6.1v1

Microsoft Purview Audit (Standard) logging SHALL be enabled.

- *Rationale:* Responding to incidents without detailed information about activities that took place slows response actions. Enabling Microsoft Purview Audit (Standard) helps ensure agencies have visibility into user actions. Furthermore, enabling the unified audit log is required for government agencies by OMB M-21-31 (referred to therein by its former name, Unified Audit Logs).
- *Last modified*: June 2023

7.1.2 MS.DEFENDER.6.2v1

Microsoft Purview Audit (Premium) logging SHALL be enabled for ALL users.

- *Rationale:* Standard logging may not include relevant details necessary for visibility into user actions during an incident. Enabling Microsoft Purview Audit (Premium) captures additional event types not included with Standard. Furthermore, it is required for government agencies by OMB M-21-13 (referred to therein as by its former name, Unified Audit Logs w/Advanced Features).
- *Last modified*: June 2023

7.1.3 MS.DEFENDER.6.3v1

Audit logs SHALL be maintained for at least the minimum duration dictated by OMB M-21-31.

- *Rationale:* Audit logs may no longer be available when needed if they are not retained for a sufficient time. Increased log retention time gives an agency the necessary visibility to investigate incidents that occurred some time ago.
- *Last modified*: June 2023
- *Note*: Purview Audit (Premium) provides a default audit log retention policy, retaining Exchange Online, SharePoint Online, OneDrive for Business, and Azure Active Directory audit records for one year. Additional record types require custom audit retention policies.

7.2 RESOURCES

- OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents | Office of Management and Budget
- Turn auditing on or off | Microsoft Learn
- Create an audit log retention policy | Microsoft Learn
- Search the audit log in the compliance center | Microsoft Learn
- Audit log activities | Microsoft Learn

7.3 LICENSE REQUIREMENTS

- Microsoft Purview Audit (Premium) logging capabilities, including the creation of a custom audit log retention policy, requires E5/G5 licenses or E3/G3 licenses with add-on compliance licenses.
- Additionally, maintaining logs in the M365 environment for longer than one year requires an add-on license. For more information, see Licensing requirements | Microsoft Learn.

7.4 IMPLEMENTATION

7.4.1 MS.DEFENDER.6.1v1 Instructions

To enable auditing via the Microsoft Purview compliance portal:

1. Sign in to the **Microsoft Purview compliance portal**.
2. Under **Solutions**, select **Audit**.
3. If auditing is not enabled, a banner is displayed to notify the administrator to start recording user and admin activity.
4. Click the **Start recording user and admin activity**.

7.4.2 MS.DEFENDER.6.2v1 Instructions

To set up Microsoft Purview Audit (Premium), see Set up Microsoft Purview Audit (Premium) | Microsoft Learn.

7.4.3 MS.DEFENDER.6.3v1 Instructions

To create one or more custom audit retention policies, if the default retention policy is not sufficient for agency needs, follow Create an audit log retention policy instructions. Ensure the duration selected in the retention policies is at least one year, in accordance with OMB M-21-31.