MICROSOFT TEAMS

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 TEAMS

Microsoft 365 (M365) Teams is a cloud-based text and live chat workspace that supports video calls, chat messaging, screen sharing, and file sharing. This secure configuration baseline (SCB) provides specific policies to strengthen Microsoft Teams' security.

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

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

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

1.1 LICENSE COMPLIANCE AND COPYRIGHT

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

1.2 ASSUMPTIONS

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

1.3 KEY TERMINOLOGY

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

Access to Teams can be controlled by the user type. In this baseline, the types of users are defined as follows:

- **Internal users**: Members of the agency's M365 tenant.

- **External users**: Members of a different M365 tenant.
- **Business to Business (B2B) guest users**: External users who are formally invited to collaborate with the team and added to the agency's Azure Active Directory (Azure AD) as guest users. These users authenticate with their home organization/tenant and are granted access to the team by virtue of being listed as guest users on the tenant's Azure AD.
- **Unmanaged users**: Users who are not members of any M365 tenant or organization (e.g., personal Microsoft accounts).
- **Anonymous users**: Teams users joining calls who are not authenticated through the agency's tenant; these users include unmanaged users, external users (except for B2B guests), and true anonymous users (i.e., users who are not logged in to any Microsoft or organization account, such as dial-in users[1]).

Note: These terms vary in use across Microsoft documentation.

2. BASELINE POLICIES

2.1 MEETING POLICIES

This section helps reduce security risks posed by the external participants during meetings. In this instance, the term "external participants" includes external users, B2B guest users, unmanaged users, and anonymous users.

This section helps reduce security risks related to the user permissions for recording Teams meetings and events. These policies and user permissions apply to meetings hosted by a user, as well as during one-on-one calls and group calls started by a user. Agencies should comply with any other applicable policies or legislation in addition to this guidance.

2.2 POLICIES

2.2.1 MS.TEAMS.1.1v1

External meeting participants SHOULD NOT be enabled to request control of shared desktops or windows.

- *Rationale:* An external participant with control of a shared screen could potentially perform unauthorized actions on the shared screen. This policy reduces that risk by removing an external participant's ability to request control. However, if an agency has a legitimate use case to grant this control, it may be done on a case-by-case basis.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) meeting policy, as well as custom meeting policies.

2.2.2 MS.TEAMS.1.2v1

Anonymous users SHALL NOT be enabled to start meetings.

[1] Note that B2B guest users and all anonymous users except for external users appear in Teams calls as *John Doe (Guest)*. To avoid potential confusion, true guest users are always referred to as B2B guest users in this document.

- *Rationale:* For agencies that implemented custom policies providing more flexibility to some users to automatically admit "everyone" to a meeting - this policy provides protection from anonymous users starting meeting to scrape internal contacts.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) meeting policy, and custom meeting policies if they exist.

2.2.3 MS.TEAMS.1.3v1

Anonymous users and dial-in callers SHOULD NOT be admitted automatically.

- *Rationale:* Automatically allowing admittance to anonymous and dial-in users diminishes control of meeting participation and invites potential data breach. This policy reduces that risk by requiring all anonymous and dial-in users to wait in a lobby until admitted by an authorized meeting participant. If the agency has a use case to admit members of specific trusted organizations and/or B2B guests automatically, custom policies may be created and assigned to authorized meeting organizers.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) meeting policy. Custom meeting policies MAY be created to allow specific users more flexibility. For example, B2B guest users and trusted partner members may be admitted automatically into meetings organized by authorized users.

2.2.4 MS.TEAMS.1.4v1

Internal users SHOULD be admitted automatically.

- *Rationale:* Requiring internal users to wait in the lobby for explicit admission can lead to admit fatigue. This policy enables internal users to be automatically admitted to the meeting through global policy.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) meeting policy. Custom meeting policies MAY be created to allow specific users more flexibility.

2.2.5 MS.TEAMS.1.5v1

Dial-in users SHOULD NOT be enabled to bypass the lobby.

- *Rationale:* Automatically admitting dial-in users reduces control over who can participate in a meeting and increases potential for data breaches. This policy reduces the risk by requiring all dial-in users to wait in a lobby until they are admitted by an authorized meeting participant.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) meeting policy, as well as custom meeting policies.

2.2.6 MS.TEAMS.1.6v1

Meeting recording SHOULD be disabled.

- *Rationale:* Allowing any user to record a Teams meeting or group call may lead to unauthorized disclosure of shared information, including audio, video, and shared screens. By disabling the meeting recording setting in the Global (Org-wide default) meeting policy, an agency limits information exposure.
- *Last modified*: July 2023
- *Note*: This policy applies to the Global (Org-wide default) meeting policy, as well as custom meeting policies. Custom policies MAY be created to allow more flexibility for specific users.

2.2.7 MS.TEAMS.1.7v1

Record an event SHOULD be set to **Organizer can record**.

- *Rationale:* The security risk of the default settings for Live Events is Live Events can be recorded by all participants by default. Limiting recording permissions to only the organizer minimizes the security risk to the organizer's discretion for these Live Events.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) meeting policy, as well as custom meeting policies. Custom policies MAY be created to allow more flexibility for specific users.

2.3 RESOURCES

- Manage who can present and request control in Microsoft Teams | Microsoft Learn
- Meeting policy settings | Microsoft Learn
- Teams cloud meeting recording | Microsoft Learn
- Assign policies in Teams – getting started | Microsoft Learn
- Live Event Recording Policies | Microsoft Learn

2.4 LICENSE REQUIREMENTS

- N/A.

2.5 IMPLEMENTATION

2.5.1 MS.TEAMS.1.1v1 Instructions

To help ensure external participants do not have the ability to request control of the shared desktop or window in the meeting:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Content sharing** section, set **External participants can give or request control** to **Off**.
5. If custom policies were created, repeat these steps for each policy, selecting the appropriate policy in step 3.

2.5.2 MS.TEAMS.1.2v1 Instructions

To configure settings for anonymous users:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Meeting join & lobby** section, set **Anonymous users and dial-in callers can start a meeting** to **Off**.
5. If custom policies were created, repeat these steps for each policy, selecting the appropriate policy in step 3.

2.5.3 MS.TEAMS.1.3v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Meeting policies**.
3. Select the **Global (Org-wide default)** policy.

4. Under the **Meeting join & lobby** section, ensure **Who can bypass the lobby** is **not** set to **Everyone**. Bypassing the lobby should be set to **People in my org**, though other options may be used if needed.
5. In the same section, set **People dialing in can bypass the lobby** to **Off**.

2.5.4 MS.TEAMS.1.4v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Meeting join & lobby** section, ensure **Who can bypass the lobby** is set to **People in my org**.
5. In the same section, set **People dialing in can bypass the lobby** to **Off**.

2.5.5 MS.TEAMS.1.5v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Meeting join & lobby** section, set **People dialing in can bypass the lobby** to **Off**.

2.5.6 MS.TEAMS.1.6v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Recording & transcription** section, set **Meeting recording** to **Off**.
5. Select **Save**.

2.5.7 MS.TEAMS.1.7v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings > Live events policies**.
3. Select **Global (Org-wide default)** policy.
4. Set **Record an event** to **Organizer can record**.
5. Click **Save**.
6. If custom policies were created, repeat these steps for each policy, selecting the appropriate policy in step 3.

3. EXTERNAL USER ACCESS

This section helps reduce security risks related to external and unmanaged user access. In this instance, external users refer to members of a different M365 tenant, and unmanaged users refer to users who are not members of any M365 tenant or organization.

External access allows external users to look up internal users by their email address to initiate chats and calls entirely within Teams. Blocking external access prevents external users from using Teams as an avenue for reconnaissance or phishing. Even with external access disabled, external users will still be able to join Teams calls, assuming anonymous join is enabled. Depending on agency need, if both external access and anonymous join are blocked—neither required nor recommended by this baseline—external collaborators would only be able to attend meetings if added as B2B guest users.

External access may be granted on a per-domain basis. This may be desirable in some cases (e.g., for agency-to-agency collaboration). See the Chief Information Officer Council Interagency Collaboration Program Office of Management and Budget MA site for a list of .gov domains for sharing.

Similar to external users, blocking contact with unmanaged Teams users prevents these users from looking up internal users by their email address and initiating chats and calls within Teams. These users would still be able to join calls, assuming anonymous join is enabled. Additionally, unmanaged users may be added to Teams chats if the internal user initiates the contact.

3.1 POLICIES

3.1.1 MS.TEAMS.2.1v1

External access for users SHALL only be enabled on a per-domain basis.

- *Rationale:* The default configuration allows members to communicate with all external users with similar access permissions. This unrestricted access can lead to data breaches and other security threats. This policy provides protection against threats posed by unrestricted access by allowing communication with only trusted domains.
- *Last modified*: July 2023

3.1.2 MS.TEAMS.2.2v1

Unmanaged users SHALL NOT be enabled to initiate contact with internal users.

- *Rationale:* Allowing contact from unmanaged users can expose users to email and contact address harvesting. This policy provides protection against this type of harvesting.
- *Last modified*: July 2023

3.1.3 MS.TEAMS.2.3v1

Internal users SHOULD NOT be enabled to initiate contact with unmanaged users.

- *Rationale:* Contact with unmanaged users can pose the risk of data leakage and other security threats. This policy provides protection by disabling internal user access to unmanaged users.
- *Last modified*: July 2023
- *Note:* This policy is not applicable to Government Community Cloud (GCC), GCC High, and Department of Defense (DoD) tenants.

3.2 RESOURCES

- IT Admins - Manage external meetings and chat with people and organizations using Microsoft identities | Microsoft Learn
- Teams settings and policies reference | Microsoft Learn
- Use guest access and external access to collaborate with people outside your organization | Microsoft Learn
- Manage chat with external Teams users not managed by an organization | Microsoft Learn

3.3 LICENSE REQUIREMENTS

- N/A

3.4 IMPLEMENTATION

Steps for the unmanaged users are outlined in Manage chat with external Teams users not managed by an organization.

3.4.1 MS.TEAMS.2.1v1 Instructions

To enable external access for only specific domains:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users > External access**.
3. Under **Choose which external domains your users have access to**, select **Allow only specific external domains**.
4. Click **Allow domains** to add allowed external domains. All domains not added in this step will be blocked.
5. Click **Save**.

3.4.2 MS.TEAMS.2.2v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users > External access**.
3. Under **Teams accounts not managed by an organization**, toggle **People in my organization can communicate with Teams users whose accounts aren't managed by an organization** to one of the following:
    I. To completely block contact with unmanaged users, toggle the setting to **Off**.
    II. To allow contact with unmanaged users only if the internal user initiates the contact:
        a) Toggle the setting to **On**.
        b) Clear the check next to **External users with Teams accounts not managed by an organization can contact users in my organization**.

3.4.3 MS.TEAMS.2.3v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users > External access**.
3. To completely block contact with unmanaged users, under **Teams accounts not managed by an organization**, set **People in my organization can communicate with Teams users whose accounts aren't managed by an organization** to **Off**.

4. SKYPE USERS

This section helps reduce security risks related to contact with Skype users. Microsoft is officially retiring Skype for Business Online and wants to give customers information and resources to plan and execute a successful upgrade to Teams. Below are the decommissioning dates by product:

- Skype for Business Online: July 31, 2021
- Skype for Business 2015: April 11, 2023
- Skype for Business 2016: Oct. 14, 2025
- Skype for Business 2019: Oct. 14, 2025
- Skype for Business Server 2015: Oct. 14, 2025
- Skype for Business Server 2019: Oct. 14, 2025
- Skype for Business LTSC 2021: Oct. 13, 2026

4.1 POLICIES

4.1.1 MS.TEAMS.3.1v1

Contact with Skype users SHALL be blocked.

- *Rationale:* Microsoft is officially retiring all forms of Skype as listed above. Allowing contact with Skype users puts agency users at additional security risk. By blocking contact with Skype users, an agency limits access to security threats utilizing the vulnerabilities of the Skype product.
- *Last modified*: July 2023

4.2 RESOURCES

- Configure external meetings and chat with Skype for Business Server | Microsoft Learn
- Skype for Business Online to Be Retired in 2021 | Microsoft Teams Blog

4.3 LICENSE REQUIREMENTS

- N/A

4.4 IMPLEMENTATION

4.4.1 MS.TEAMS.3.1v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users > External access**.
3. Under **Skype users**, set **Allow users in my organization to communicate with Skype users** to **Off**.
4. Click **Save**.

5. TEAMS EMAIL INTEGRATION

This section helps reduce security risks related to Teams email integration. Teams provides an optional feature allowing channels to have an email address and receive email.

5.1 POLICIES

5.1.1 MS.TEAMS.4.1v1

Teams email integration SHALL be disabled.

- *Rationale:* Microsoft Teams email integration associates a Microsoft, not tenant domain, email address with a Teams channel. Channel emails are addressed using the Microsoft-owned domain teams.ms. By disabling Teams email integration, an agency prevents potentially sensitive Teams messages from being sent through external email gateways.
- *Last modified*: July 2023
- *Note:* Teams email integration is not available in GCC, GCC High, or DoD regions.

5.2 RESOURCES

- Email Integration | Microsoft Learn

5.3 LICENSE REQUIREMENTS

- N/A

5.4 IMPLEMENTATION

5.4.1 MS.TEAMS.4.1v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Teams > Teams Settings**.
3. Under the **Email integration** section, set **Users can send emails to a channel email address** to **Off**.

6. APP MANAGEMENT

This section helps reduce security risks related to app integration with Microsoft Teams. Teams can integrate with the following classes of apps:

- *Microsoft apps*: apps published by Microsoft.
- *Third-party apps*: apps not authored by Microsoft, published to the Teams store.
- *Custom apps*: apps not published to the Teams store, such as apps under development, that users sideload into Teams.

6.1 POLICIES

6.1.1 MS.TEAMS.5.1v1

Agencies SHOULD only allow installation of Microsoft apps approved by the agency.

- *Rationale:* Allowing Teams integration with all Microsoft apps can expose the agency to potential vulnerabilities present in those apps. By only allowing specific apps and blocking all others, the agency will better manage its app integration and potential exposure points.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) policy, all custom policies, and the org-wide app settings. Custom policies MAY be created to allow more flexibility for specific users.

6.1.2 MS.TEAMS.5.2v1

Agencies SHOULD only allow installation of third-party apps approved by the agency.

- *Rationale:* Allowing Teams integration with third-party apps can expose the agency to potential vulnerabilities present in an app not managed by the agency. By allowing only specific apps approved by the agency and blocking all others, the agency can limit its exposure to third-party app vulnerabilities.
- *Last modified*: July 2023
- *Note:* This policy applies to the Global (Org-wide default) policy, all custom policies if they exist, and the org-wide settings. Custom policies MAY be created to allow more flexibility for specific users. Third-party apps are not available in GCC, GCC High, or DoD regions.

6.1.3 MS.TEAMS.5.3v1

Agencies SHOULD only allow installation of custom apps approved by the agency.

- *Rationale:* Allowing custom apps integration can expose the agency to potential vulnerabilities present in an app not managed by the agency. By allowing only specific apps approved by the agency and blocking all others, the agency can limit its exposure to custom app vulnerabilities.
- *Last modified*: July 2023

- *Note:* This policy applies to the Global (Org-wide default) policy, all custom policies if they exist, and the org-wide settings. Custom policies MAY be created to allow more flexibility for specific users. Custom apps are not available in GCC, GCC High, or DoD regions.

6.2 RESOURCES

- Use app permission policies to control user access to apps | Microsoft Learn
- Upload your app in Microsoft Teams | Microsoft Learn

6.3 LICENSE REQUIREMENTS

- N/A

6.4 IMPLEMENTATION

6.4.1 MS.TEAMS.5.1v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Teams apps > Permission policies**.
3. Select **Global (Org-wide default)**.
4. Under **Microsoft apps**, select **Allow specific apps and block all others** or **Block all apps**.
5. Click **Allow apps**.
6. Search and Click **Add** to all appropriate Microsoft Apps.
7. Click **Allow**.
8. Click **Save**.
9. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3.

6.4.2 MS.TEAMS.5.2v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Teams apps > Manage apps**.
3. Select **Org-wide app settings** button to access pop-up options.
    I. Under **Third-party apps** turn off **Third-party apps**.
    II. Click **Save**.
4. Select **Teams apps > Permission policies**.
5. Select **Global (Org-wide default)**.
6. Set **Third-party apps** to **Block all apps**, unless specific apps have been approved by the agency, in which case select **Allow specific apps and block all others**.
7. Click **Save**.
8. If custom policies have been created, repeat steps 4 to 7 for each policy, selecting the appropriate policy in step 5.

6.4.3 MS.TEAMS.5.3v1 Instructions

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Teams apps > Manage apps**.
3. Select **Org-wide app settings** button to access pop-up options.
    I. Under **Custom apps** turn off **Interaction with custom apps**.
    II. Click **Save**.
4. Select **Teams apps > Permission policies**.
5. Select **Global (Org-wide default)**.

6. Set **Custom apps** to **Block all apps**, unless specific apps have been approved by the agency, in which case select **Allow specific apps and block all others**.
7. Click **Save**.
8. If custom policies have been created, repeat steps 4 to 7 for each policy, selecting the appropriate policy in step 5.

7. DATA LOSS PREVENTION

Data loss prevention (DLP) helps prevent both accidental leakage of sensitive information as well as intentional exfiltration of data. DLP forms an integral part of securing Microsoft Teams. There are several commercial DLP solutions available documenting support for M365. Microsoft itself offers DLP services, controlled within the Microsoft Purview compliance portal. Agencies may select any service that fits their needs and meets the requirements outlined in this baseline setting. The DLP solution selected by an agency should offer services comparable to those offered by Microsoft.

Though using Microsoft's DLP solution is not strictly required, guidance for configuring Microsoft's DLP solution can be found in following section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- Data Loss Prevention | CISA M365 Security Configuration Baseline for Defender for Office 365

7.1 POLICIES

7.1.1 MS.TEAMS.6.1v1

A DLP solution SHALL be enabled. The selected DLP solution SHOULD offer services comparable to the native DLP solution offered by Microsoft.

- *Rationale:* Teams users may inadvertently disclose sensitive information to unauthorized individuals. Data loss prevention policies provide a way for agencies to detect and prevent unauthorized disclosures.
- *Last modified*: July 2023

7.1.2 MS.TEAMS.6.2v1

The DLP solution SHALL protect personally identifiable information (PII) and sensitive information, as defined by the agency. At a minimum, sharing of credit card numbers, taxpayer identification numbers (TINs), and Social Security numbers (SSNs) via email SHALL be restricted.

- *Rationale:* Teams users may inadvertently share sensitive information with others who should not have access to it. Data loss prevention policies provide a way for agencies to detect and prevent unauthorized sharing of sensitive information.
- *Last modified*: July 2023

7.2 RESOURCES

- Plan for data loss prevention (DLP) | Microsoft Learn
- Personally identifiable information (PII) | NIST
- Sensitive information | NIST

7.3 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.

7.4 IMPLEMENTATION

7.4.1 MS.TEAMS.6.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for DLP for additional guidance.

7.4.2 MS.TEAMS.6.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for DLP for additional guidance.

8. MALWARE SCANNING

Malware scanning protects M365 Teams assets from malicious software. Several commercial anti-malware solutions detect and prevent computer viruses, malware, and other malicious software from being introduced into M365 Teams. Agencies may select any product that meets the requirements outlined in this baseline policy group. If the agency is using Microsoft Defender to implement malware scanning, see the following policies of the CISA M365 Security Configuration Baseline for Defender for Office 365 for additional guidance.

- MS.DEFENDER.3.1v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
  - Safe attachments SHOULD be enabled for SharePoint, OneDrive, and Microsoft Teams.

8.1 POLICIES

8.1.1 MS.TEAMS.7.1v1

Attachments included with Teams messages SHOULD be scanned for malware.

- *Rationale:* Teams can be used as a mechanism for delivering malware. In many cases, malware can be detected through scanning, reducing the risk for end users.
- *Last modified*: July 2023

8.1.2 MS.TEAMS.7.2v1

Users SHOULD be prevented from opening or downloading files detected as malware.

- *Rationale:* Teams can be used as a mechanism for delivering malware. In many cases, malware can be detected through scanning, reducing the risk for end users.
- *Last modified*: July 2023

8.2 RESOURCES

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

8.3 LICENSE REQUIREMENTS

- If using Microsoft Defender, 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.

8.4 IMPLEMENTATION

8.4.1 MS.TEAMS.7.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for Safe Attachments for additional guidance.

8.4.2 MS.TEAMS.7.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for Safe Attachments for additional guidance.

9. LINK PROTECTION

Several technologies exist for protecting users from malicious links included in emails. For example, Microsoft Defender accomplishes this by prepending:

https://*.safelinks.protection.outlook.com/?url=

to any URLs included in emails. By prepending the safe links URL, Microsoft can proxy the initial URL through their scanning service. Their proxy can perform the following actions:

- Compare the URL with a blocklist.
- Compare the URL with a list of know malicious sites.
- If the URL points to a downloadable file, apply real-time file scanning.

If all checks pass, the user is redirected to the original URL.

Microsoft Defender includes link-scanning capabilities. Using Microsoft Defender is not strictly required for this purpose; any product fulfilling the requirements outlined in this baseline policy group may be used. If the agency uses Microsoft Defender to meet this baseline policy group, see the following policy of the CISA M365 Security Configuration Baseline for Defender for Office 365 for additional guidance.

- MS.DEFENDER.1.3v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
  - All users SHALL be added to Defender for Office 365 Protection in either the standard or strict preset security policy.

9.1 POLICIES

9.1.1 MS.TEAMS.8.1v1

URL comparison with a blocklist SHOULD be enabled.

- *Rationale:* Users may be directed to malicious websites via links in Teams. Blocking access to known malicious URLs can help prevent users from accessing known malicious websites.
- *Last modified*: July 2023

9.1.2 MS.TEAMS.8.2v1

User click tracking SHOULD be enabled.

- *Rationale:* Users may click on malicious links in Teams, leading to compromise or authorized data disclosure. Enabling user click tracking lets agencies know if a malicious link may have been visited after the fact to help tailor a response to a potential incident.
- *Last modified*: July 2023

9.2 RESOURCES

- Recommended settings for EOP and Microsoft Defender for Office 365 security | Microsoft Learn
- Set up Safe Links policies in Microsoft Defender for Office 365 | Microsoft Learn

9.3 LICENSE REQUIREMENTS

- N/A

9.4 IMPLEMENTATION

9.4.1 MS.TEAMS.8.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for standard or strict preset security policy for additional guidance.

9.4.2 MS.TEAMS.8.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for standard or strict preset security policy for additional guidance.

APPENDIX A: CUSTOM MEETING POLICIES

If there is a legitimate business need, custom meeting policies can be defined with *specific* users assigned to them. For example, custom meeting policies can be configured with *specific* users having permission to record meetings. To allow specific users the ability to record meetings:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings** > **Meeting policies**.
3. Create a new policy by selecting **Add**. Give this new policy a name and appropriate description.
4. Under the **Recording & transcription** section, set **Cloud recording** to **On**.
5. Select **Save**.
6. After selecting **Save**, a table displays the set of policies. Select the row containing the new policy, then select **Manage users**.
7. Assign the users who need the ability to record to this policy.
8. Select **Apply**.