CSB
CYBER SECURITY BRUNEI

contact@csb.gov.bn

(673) 245 8002

Simpang 69, Jalan E-Kerajaan
Gadong BE1110, Negara Brunei Darussalam

www.csb.gov.bn

SECURITY GUIDELINES ON USING ONLINE COLLABORATION TOOL *MICROSOFT TEAMS*

9 August 2021

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

NDFL
NATIONAL DIGITAL FORENSICS LABORATORY

CYBERWATCH CENTRE

DOCUMENT CHANGE HISTORY

Version	**Date**	**Change Description**
1.00	*31/3/2020*	*Initial draft*
1.10	*1/4/2020*	*Content added*
1.20	*2/4/2020*	*Minor editing*
1.30	*6/4/2020*	*Minor editing*
1.40	*6/3/2021*	*Content added*
1.50	*9/8/2021*	*Content added*

Table of Contents

INTRODUCTION

Online collaboration provides an organization with a platform to communicate and collaborate entirely, connecting more people and processing more information internally or externally at a quick decision-making rate. The tool can be called into action as a contingency plan when an emergency crisis occurs or it can be part of the organization's modernization, digitization and transformation strategy to innovate the delivery of public services by making its internal processes more efficient and effective. As a result, time is saved, work gets done more quickly and information becomes knowledge which is more easily transferrable across the department and cross sectorial.

However, using collaboration tools online can present security risks to the organization's networks and computing systems. Any organizations embarking for this online business solution are required to refer to their **respective data classification policies** for additional security guidelines in managing and handling organization official classified information specifically and must already put in place an organization-wide **Cloud Policy** as these tools are almost exclusively on the cloud.

The online collaboration tools are getting more sophisticated with a variety of features to suit different groups of people and the users are required to be familiar with the product features, functionalities or configuration and customize them to minimize the security risks prior to using the product for organization's use.

This security guideline shall be revised from time to time or be supplemented with updated advisories and recommendations to further improve the security and minimize the risks to the organization in using online collaboration.

PURPOSE

The purpose of this document is to provide guidelines for the organization to enhance the security environment, features and configuration when using Microsoft Team as the preferred communication and collaboration workspace to address the organization online business solution.

INTENDED AUDIENCE

This document is intended for use by all organization personnel in the organization who are authorized and have been familiar in using the product for official online use.

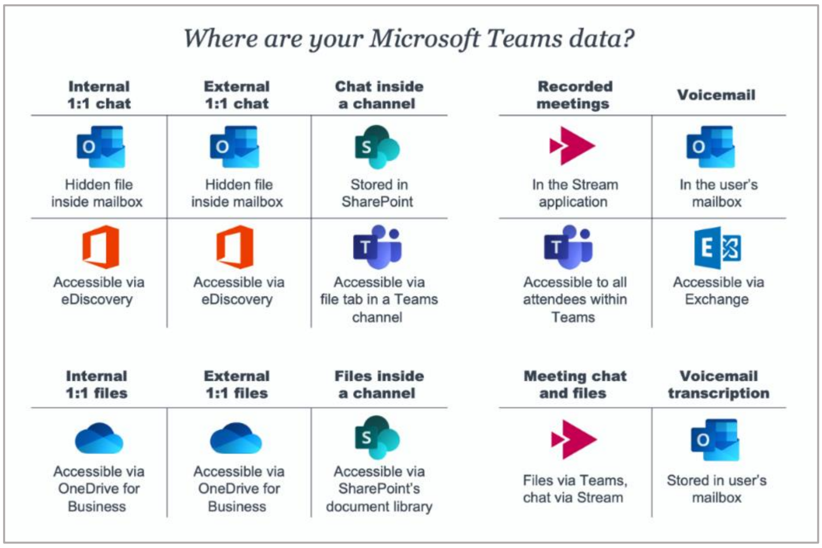
WHAT IS MICROSOFT TEAMS

Microsoft Teams is a unified communication and collaboration platform that combines persistent workplace chat, video meetings, file storage (including collaboration on files), and application integration. The service integrates with an organization's Office 365 subscription office productivity suite and features extensions that can integrate with non-Microsoft products.

The platform may contain vulnerabilities, default settings and configurations which may compromise the security of the product and can pose serious implications to the users. This guideline shall provide some recommendations on how to secure Microsoft Teams for use by the government; consolidated from various sources and best practices currently in use.

LOCATING TEAMS CHAT AND FILES

Microsoft Teams allows for both internal and external chat. Teams users can also chat inside a larger channel or one on one. Unlike many other collaboration tools (including Skype), Microsoft Teams' persistent chat makes it easy to find an ongoing conversation inside a given channel or chat. But as can be seen, all those chats and files don't remain solely in Teams.



Where are your Microsoft Teams data?

Internal 1:1 chat	External 1:1 chat	Chat inside a channel	Recorded meetings	Voicemail
Hidden file inside mailbox	Hidden file inside mailbox	Stored in SharePoint	In the Stream application	In the user's mailbox
Accessible via eDiscovery	Accessible via eDiscovery	Accessible via file tab in a Teams channel	Accessible to all attendees within Teams	Accessible via Exchange

Internal 1:1 files	External 1:1 files	Files inside a channel	Meeting chat and files	Voicemail transcription
Accessible via OneDrive for Business	Accessible via OneDrive for Business	Accessible via SharePoint's document library	Files via Teams, chat via Stream	Stored in user's mailbox

[*] *VULNERABILITIES DISCOVERED*

Microsoft Teams is becoming a popular choice as an alternative to Slack. A common risk associated with Teams is when the user is tricked into placing a malicious DLL file prepared by an attacker in a specific folder. The problem affects most Windows desktop apps that use the **Squirrel** installation and update framework, which uses **NuGet** packages.

Vulnerabilities:

Microsoft Teams DLL Loading Remote Code Execution Vulnerability

CVE-ID: CVE-2019-5922

Description:

Microsoft Teams installation folders contain an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries (CWE-427) and allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.

Microsoft states that the root cause of this vulnerability is "Application Directory (App Dir) DLL planting", thus there is no plan to release any security updates to address this issue.

Impact:

Arbitrary code may be executed with the privilege of the user invoking the installer.

[*] *This issue should be dealt with by CIOs and CTOs*

Recommendations:

- Save the installer into a newly created directory and confirm there are no unrelated files in the directory then invoke the installer.
- Make sure there are no suspicious files in the directory where the installer is saved.
- If your organization uses shared directories to place installers for organizational operations, make sure that the shared directory is set to read-only for non-administrative users.
- Download the latest version of Microsoft Teams.
- Make sure to download from trusted resources.

Remarks:

- This vulnerability was fixed in Teams version 1.2.00.21068.
- Microsoft Teams iOS Information Disclosure Vulnerability

CVE-2021-24114

Impact:

- Allows a remote attacker to gain access to potentially sensitive information.
- The vulnerability exists due to excessive data output by the application in Microsoft Teams for iOS. A remote authenticated attacker can gain unauthorized access to sensitive information on the system.

Recommendations:

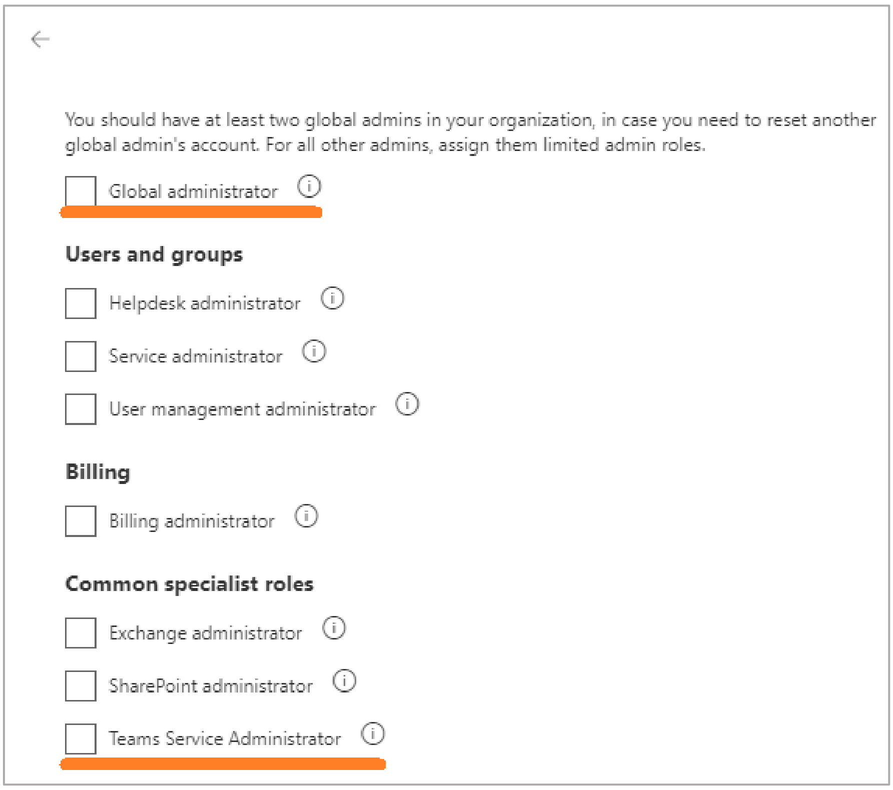
- Urgently apply the latest Microsoft patches to all systems across the organization

MICROSOFT TEAMS SECURITY CHECKLIST

Below is a Security Checklist that needs to be considered in using the Microsoft Teams platform:

GLOBAL TEAMS MANAGEMENT

This role is crucial in setting up all the features and functionalities that come with Teams as well as managing the overall Teams environment. To globally manage Microsoft Teams, there must be either a Teams Service Administrator or a Global Administrator in an organisation.



You should have at least two global admins in your organization, in case you need to reset another global admin's account. For all other admins, assign them limited admin roles.

□ Global administrator

Users and groups

□ Helpdesk administrator

□ Service administrator

□ User management administrator

Billing

□ Billing administrator

Common specialist roles

□ Exchange administrator

□ SharePoint administrator

□ Teams Service Administrator

A Microsoft Teams Service Administrator cannot see or manage all the Teams from within Teams. The Administrator must go to https://admin.teams.microsoft.com/ to manage everything including security. This may be a partial bias from being able to manage and see sites within SharePoint as a SharePoint site collection administrator but in a similar fashion a SharePoint site collection admin can only see their site collection and cannot see everything; only a Microsoft SharePoint Service Administrator can from within SharePoint admin console.

EXTERNAL GUEST ACCESS

External access means that people with email addresses that are not mapped at the domain level can access Microsoft Teams as a guest.

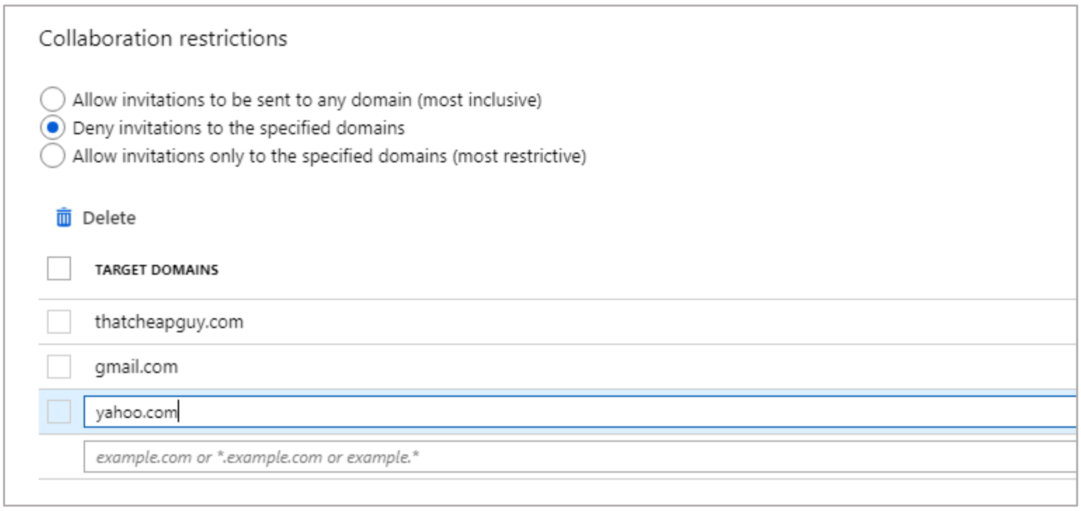
Guests have some limitations compared to Team members. Those primary limitations are:

- Use OneDrive for Business
- Search for people not in Teams
- Use a calendar to schedule meetings
- View the organizational chart
- Create or configure a Team
- Search for Teams
- Upload files directly in a Chat
- Add Apps
- Manage Security

By default, guest access is not enabled within Microsoft Teams. If the organisation wants to enable guest access, the organisation's Teams Service Administrator or a Global Administrator are the one allowed to enable it.

To prevent data leaks from your organisation, restrict domain viewing, and review invitations from your Tenant.

To do this click on **"**Deny invitations to the specified domains**"** under Collaboration restrictions.



Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)
● Deny invitations to the specified domains
○ Allow invitations only to the specified domains (most restrictive)

Delete

□	**TARGET DOMAINS**
□	thatcheapguy.com
□	gmail.com
□	yahoo.com
	*example.com or *.example.com or example.**

To enable Microsoft Teams Guest Access:

1. Go here: https://admin.teams.microsoft.com/
2. On the left-hand menu, click Org-wide settings, then Guest Access
3. Once you enable guest access in Teams, the following features can be configured on or off for guests:
    1. Making private calls
    2. Using IP video
    3. The default screen sharing mode
    4. Ability to start an instant meeting using Meet Now
    5. Edit or delete sent messages
    6. Ability to use Chat
    7. Using GIFs in conversations as well as how safe/mature you want GIFs to be
    8. Using memes or stickers in conversations
    9. Allowing immersive reader

EXTERNAL ACCESS

In Microsoft Teams, external access for people outside the organization is called Guest Access. External Access within Microsoft Teams has a different technical meaning.

External Access will allow an entire domain to use the chat and calls within the organisation Teams. For instance, if the organisation is @xx.gov.bn and the organisation wants all users with an email of @xx.com to be able to chat and call within the organisations Teams, then this is considered as External Access.

By default, all external domains can chat within Microsoft Teams. The organisation can however allow and restrict specific domains on a case-by-case basis if the organisation does not want to allow chatting with specific users.

External Access Users are currently more restricted than Guest Users within Teams. Meetings, messages, file sharing and more cannot be done by External Access Users since it is only for chat or calling only.

To Allow or Block Domains within Microsoft Teams External Access:

1. Go here: https://admin.teams.microsoft.com/
2. On the left-hand menu, click Org-wide settings, then External Access
3. Enable 'Users can communicate with Skype for Business and Teams users'
   Click 'Add a domain' and add the external domain you wish to allow or block. For example, acme.com

SAFE ATTACHMENTS

Safe Attachments for Microsoft Teams provides an additional layer of protection for files that have already been scanned at upload time by the common virus detection engine in Microsoft 365. Safe Attachments for Microsoft Teams helps detect and block existing files that are identified as malicious in team sites and document libraries.

Safe Attachments for Microsoft Teams is not enabled by default. To turn it on, go to https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-atp-for-spo-odb-and-teams?view=o365-worldwide.

HOW SAFE ATTACHMENTS FOR MICROSOFT TEAMS WORKS

When Safe Attachments for Microsoft Teams is enabled and identifies a file as malicious, the file is locked using direct integration with the file stores.

Although the blocked file is still listed in the document library and in web, mobile, or desktop applications, people cannot open, copy, move, or share the file. But they can delete the blocked file.

Recommendations:

Although cybercriminals continue to find new ways to trick people with malware, there are steps you can take to help protect you and your computer.

- Run security software on your computer and keep that software up to date.
- Install the latest software updates on all your devices.
- Use caution with email attachments and files.

MEMBERS OF ADMINS

When adding internal users to Teams, the organisation may want to make certain people Members or Admins depending on their role within the Team. The biggest differences are Admins can create, edit or delete Teams as well as manage security. For some organisations it is beneficial to allow free-flowing Team management as well as security management to not bottleneck those processes. For other organisations, particularly ones that are more regulated, it may be worthwhile to have a very limited number of Teams Owners.

MICROSOFT TEAMS POTENTIAL RISK

Microsoft Teams is a fully integrated platform for Office 365. It allows access to chat channels, apps integration and collaboration between the same or even different organizations.

App integration is a feature in Teams that can be abused by malicious users.

Microsoft Teams, by default, does not provide effective security for malicious content:

- Links in the chat are not scanned at all.
- Files are scanned, but not instantly and only for basic issues. That means that malware can sit in the chat for hours at a time

WEBSITE FEATURE

The "Website" feature in Microsoft Teams by default allows members to add a webpage via URL to the channel's tab. Malicious members can abuse this feature by posting a malicious webpage to the channel's tab.

Other than the Office 365 admin, there are no indications on who has created the tab and its contents. While the attack can only be done by current or invited members, which are assumed trusted users, the possibility of this attack shouldn't be ignored.

The threat or risk is elevated in a scenario when dealing with a large number of users, especially with cross-organization collaboration or online learning situations.

In large settings i.e. school or work, channel permission should be configured by allowing only trusted members to add features to the channel.

RECOMMENDATIONS

- Be cautious when on clicking links posted in Teams
- There is no way of identifying posted contents in the Teams tab. Ask and verify the contents from members who created it if needed.
- Assign proper permissions when creating a Team/Channel.

DATA LOSS PREVENTION

To comply with corporate standards and industry regulations, organizations must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy in the Office 365 Security & Compliance Center, it can identify, monitor, and automatically protect sensitive information across Office 365.

With a DLP policy, it can:

- Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.
- Prevent the accidental sharing of sensitive information.
- Monitor and protect sensitive information in the desktop versions of Excel, PowerPoint, and Word.
- Help users learn how to stay compliant without interrupting their workflow.
- View DLP alerts and reports showing content that matches your organization's DLP policies.

RECOMMENDATIONS

- Files or documents must be password protected.
  - For Windows:
    - Go to File > Info > Protect Document > Encrypt with Password.
    - Type a password, then type it again to confirm it.
    - Save the file to make sure the password takes effect.
  - For MacOS
    - Go to Review > Protect Document.
    - Under Security, you can select whether to enter a password to open the document, modify the document, or both. Enter each password again to confirm.
    - Click OK.

GENERAL RECOMMENDATIONS

Below are some general best practices:

- Create different channels in Teams to direct conversation.
- Allow users to create new Teams but maintain administrative control such as removing users who should not have access to Teams.
- Take advantage of integrations with other software in the organisation such as Zoom, Stream, etc.

- Leverage chatbots to promote daily activity and tasks
- Use PowerShell to manage Teams

File Sharing and Security

- Require multi-factor authentication
- Scan the content for malicious files and links, identifying them in real time
- Enforce least privileged access across Teams and Office 365
- Classify sensitive data and use Microsoft Azure Information Protection (AIP) or any compatible security software for additional protection
- Prevent file download to unmanaged devices
- Audit external sharing

REFERENCES

- *https://www.eswcompany.com/microsoft-teams-security-setup/*
- *https://docs.microsoft.com/en-us/microsoftteams/assign-roles-permissions*
- *https://www.brainstorminc.com/blog/microsoft-teams-how-secure-is-it-really-a-rundown/*
- *https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview*
- *https://www.youtube.com/watch?v=3aZM0Rfjgy4*
- *https://www.darkreading.com/vulnerabilities---threats/the-insecure-state-of-microsoft-teams-security/d/d-id/1339884*