Sensitivity Labels and Sharing Guide

Table of Contents

Labeling Principles for Users

Labels for Emails in Outlook

- How To Use
- Labels for Email Descriptions
- Email Recipient's Typical Experience
- Helpful Tips

Labels for Files in Word, PowerPoint, and Excel

- How To Use
- Labels for M365 Files Descriptions
- Sharing Files in M365 101

Labels for Containers such as Teams, SharePoint Sites, and M365 Groups

- How To Use
- Labels for Containers Descriptions
- External Collaboration Manager Role
- Internal Public Container Creator Role

Guest Accounts for External Sharing

- Adding New Guests to the Organization
- Guest Recipient Experience

Labeling Principles for Users

The following are some principles which should be considered when using sensitivity labels.

Sensitivity – The sensitivity of information is directly related to the adverse impacts to a person, organization, or the Nation in the event of unauthorized disclosure. Users should exercise good judgement when determining the sensitivity of information. This is a key principle to consider when labeling files and emails.

Security vs Convenience – Users need to hit the right balance between security and convenience. It can be unhelpful to over-restrict information. But at the same time, users need to appropriately label items that warrant the extra safeguards.

Label Flexibility – Team members and file owners can change the sensitivity label for files as needed, assuming they have the appropriate access to do so. This is necessary if business operations require reducing or adding protection for a particular file. Logs are generated for any time a label is changed. If a label is downgraded, it will ask the user to enter a quick justification.

Labeling vs Sharing – There is a distinction between labeling and sharing. Labeling can add extra safeguards. Sharing gives access to others within the confines of the safeguards.

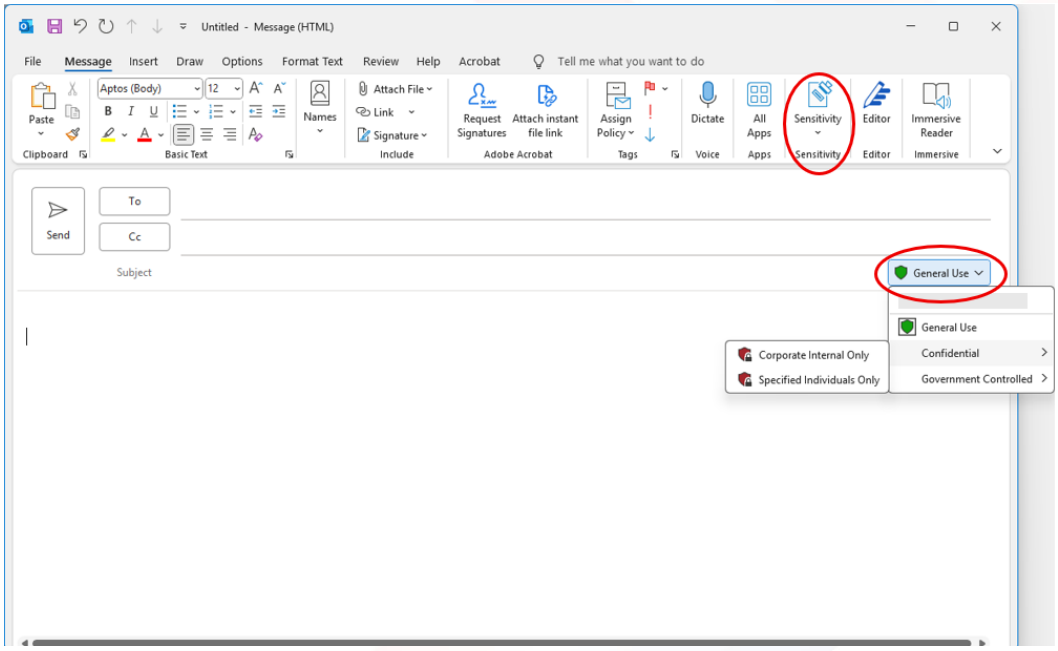
Proper CUI Labeling – Make the most use of the DoD CUI registry at DoD CUI Program > CUI Registry New and your government representatives to accurately label CUI. Although several technical protections are automatically implemented by the IT system, several responsibilities remain with the end user, such as appropriate dissemination controls and more.

Labels for Emails in Outlook

Sensitivity labels in Outlook are a flexible solution for encrypting emails and adding additional safeguards.

How To Use:

When a new email is opened in Outlook, the Sensitivity Labels that have been published by your organization will be available in the following (red circled) locations in an email. Both options are equivalent. Select the appropriate label according to the sensitivity of the information being sent as well as the need for added safeguards. The table on the next page gives a detailed description of the labels for emails and their associated security capabilities. The experience is similar in web Outlook and mobile device Outlook.



Labels for Email Descriptions:

	Label Name	Automated Label Security Actions	Label Intention	Use Case Examples:
	General Use (Default Label)	Emails use standard transport encryption and are not otherwise restricted.	This is the intended label for most general email correspondence. It is flexible and designed for emails that don't require more advanced security controls.	• General collaboration emails • Non-sensitive announcements
	Confidential – Corporate Internal Only	Emails will have an additional layer of encryption. Email body will only be accessible to recipients who are members of your organization.	This label is intended for sensitive internal corporate emails that require additional safeguards to prevent unauthorized access by entities external to your organization.	• Sensitive company announcements • Emails with proprietary information that cannot leave the company
	Confidential – Specific Individuals Only	Emails will have an additional layer of encryption. Email body will only be accessible to the specified email recipients, internal or external to the organization. Recipients will be unable to forward the email to others.	This label is intended for sensitive emails that require additional safeguards to prevent unauthorized access by entities not specifically listed as recipients.	• Emails containing user credentials • Emails with sensitive information such as PII/PHI or legal matters • Emails with highly restricted corporate information
	Government Controlled - CUI	Emails will have an additional layer of encryption. Email body will only be accessible to recipients who are authorized CUI users[2] in your organization as well as CUI-authorized external organizations.[3]	This label is intended for emails that contain government Controlled Unclassified Information (CUI) and therefore require additional safeguards to prevent unauthorized access.	• Emails with information created for or on behalf of the government that are regulated by one of the CUI categories • Emails with Controlled Technical Information, which is a commonly used CUI category
	Government Controlled – CUI/NOFORN[4]	Emails will have an additional layer of encryption. Email body will only be accessible to recipients who are US citizen authorized CUI users[5] in your organization as well as CUI-authorized external organizations.[3]	This label is intended for emails that contain government Controlled Unclassified Information (CUI) that is part of one of the NOFORN categories and therefore requires additional safeguards to prevent unauthorized access.	• Emails with information created for or on behalf of the government that are regulated by one of the NOFORN CUI categories • Emails with ITAR or Intelligence information
	Government Controlled – CUI - Additional Compatibility[6]	Emails will have standard transport encryption. System-enforced access controls will be removed for the purpose of added compatibility with certain recipients. This label will only be used for email when compatibility requires it.	This label is intended for emails that contain government Controlled Unclassified Information (CUI) in the message body or attachment and need additional compatibility with certain recipients.	• Emails with information created for or on behalf of the government that are regulated by one of the CUI categories being sent to authorized recipients that need additional compatibility

[2] Members of your organization can be designated by corporate leadership as authorized CUI users depending on their role. These users will be able to apply the CUI label and can be granted access to CUI files and emails.

[3] Most DoD government organizations are configured as CUI-authorized external organizations by default. More organizations can be added by DefenseX administrators upon corporate leadership request. Partner organizations that need to be able to receive and access CUI will need to be added to the list of CUI-authorized external organizations.

[4] This label is only available on-demand to selected organizations that work with CUI categories with NOFORN restrictions, such as ITAR and intelligence.

[5] Members of your organization can be designated by leadership as US citizens and authorized CUI users for the purpose of accessing NOFORN information.

[6] This label should only be used in cases where recipients need additional compatibility. For example: if an authorized DoD recipient can't open an email sent with the "Government Controlled – CUI" label, try sending again with the "CUI - Additional Compatibility" label. This is because some recipient organizations (very few) do not permit their users to receive emails with additional layers of encryption.

Email Recipient's Typical Experience

There are a few typical experiences that recipients will encounter depending on which sensitivity label is used and what email client/service provider they use. Unique scenarios might arise depending on the email client of a particular recipient. This guide is meant to describe some of the most common scenarios.

- **Outlook Native** - Email opens natively in Desktop Outlook. If using Web Outlook, the experience might be the "Protected Message Portal Link" below.
- **Email Client Native** – Email opens natively in email client.
- **Protected Message Portal Link** – Email will notify recipient they have a protected message awaiting them along with a link to read the message. Recipient will need to click the link and follow the web browser instructions to view and reply to the email. The protected portal will authenticate them via the use of a One Time Passcode sent to their email or via their M365 account natively.

		Recipient's Expected Experience by Email Provider			
Email Label		**Internal to Your Organization**	**Most Commercial Email Services (commercial Outlook, Gmail, etc.) (External)**	**GCC High M365 Desktop Outlook (External)**	**DoD or other US Gov organization (External)**
	General Use (Default Label)	Outlook Native	Email Client Native	Outlook Native	Outlook Native
	Confidential – Corporate Internal Only	Outlook Native	N/A	N/A	N/A
	Confidential – Specific Individuals Only	Outlook Native	Protected Message Portal Link	Outlook Native	Outlook Native
	Government Controlled - CUI	Outlook Native	Protected Message Portal Link	Outlook Native	Outlook Native
	Government Controlled – CUI/NOFORN	Outlook Native	Protected Message Portal Link	Outlook Native	Outlook Native
	Government Controlled – CUI - Additional Compatibility	Outlook Native	Email Client Native	Outlook Native	Outlook Native

Helpful Tips

Notify Recipient – Many recipients are unaccustomed to using encrypted emails or protected message portals. It is helpful to give them a preparatory "heads up" via normal email first to let them know you will be sending an encrypted message to them. This way they are not surprised when they see an encrypted email notification or a message directing them to the protected message portal.

Use Protected Emails for Securely Sending and Receiving Attachments – Protected emails such as *Confidential – Specific Individuals Only* or *Government Controlled – CUI* can be a helpful tool for securely sending or receiving attached files. For example: If you are requesting an external recipient to send you a sensitive file, you can send them a protected email, and they can attach the file to their Reply. The file will be securely delivered to you in their Reply email.

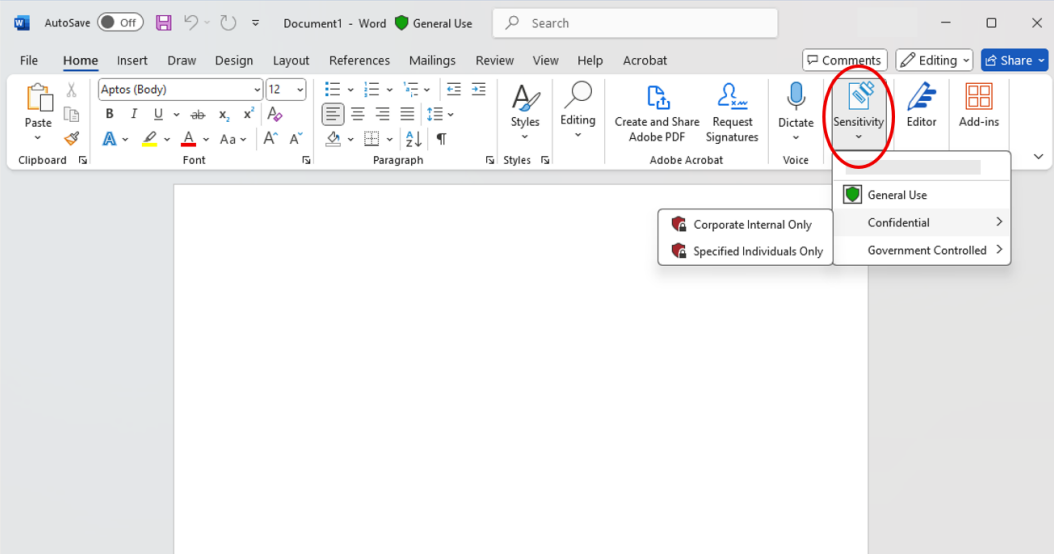
Use Protected Emails Only When Needed – Using additional email protections that are associated with sensitivity labels such as *Confidential – Specific Individuals Only* or *Government Controlled – CUI* should only be done when the information contained warrants the additional protections. Emails with additional protections have reduced flexibility and usability when compared to standard (*General Use*) email and therefore should only be used when needed.

Labels for Files in Word, PowerPoint, and Excel

Sensitivity labels for Files provide additional protection to sensitive content in M365 files, such as Power Point, Word, and Excel.

How To Use:

When a file is opened, click on the sensitivity icon on the top right. The sensitivity labels that have been published by your organization will be available in the following (red circled) location in an M365 file.



Applying a particular sensitivity label to a file does not automatically give the associated population access to the file, but it instead makes them eligible to access the file if it is shared with them. Labeling is not the same as Sharing. For example, applying *Confidential – Corporate Internal Only* to a file on a user's OneDrive does not automatically give the whole organization access to the file, but instead makes them eligible to have access if the file Owner shares it with them. For further information about sharing files, please see the Sharing Files in M365 101 section below. Please see the table below for the security actions and use cases associated with the different sensitivity labels.

Labels for M365 Files Descriptions:

	Label Name	Label Security Actions	Label Intention	Applicable to:
	General Use	Files are restricted by default and use standard at-rest encryption. There are no system-enforced access controls preventing sharing.	This is the intended label for most regular files. It is flexible and designed for files that don't require strict sharing restrictions.	• Files not containing sensitive information • Files that need the ability to be shared broadly, internal or external to organization
	Confidential – Corporate Internal Only	Files will have an additional layer of encryption. Only members of your organization will be eligible to access file content, assuming the file is shared with them.	This label is intended for sensitive internal corporate files that require additional safeguards to prevent unauthorized access by entities external to your organization.	• Files with proprietary information that cannot leave the company • Sensitive company-wide documents
	Confidential – Specific Individuals Only[1]	Files will have an additional layer of encryption. Only specified individuals internal or external[2] to your organization will be eligible for accessing file content, assuming the file is also shared with them.	This label is intended for sensitive files that require additional safeguards to prevent unauthorized access by internal or external users not specified.	• Files with sensitive information such as PII/PHI or legal matters • Files with highly sensitive corporate information
	Government Controlled - CUI	Files will have an additional layer of encryption. Only authorized CUI users[3] in your organization as well as CUI-authorized external organizations[4] will be eligible for accessing file content after the file is shared with them.	This label is intended for files that contain government Controlled Unclassified Information (CUI) and therefore require additional safeguards to prevent unauthorized access.	• Files with information created for or on behalf of the government that is regulated by one of the CUI categories • Files with Controlled Technical Information, which is a commonly used CUI category
	Government Controlled – CUI/NOFORN	Files will have an additional layer of encryption. Only authorized US Citizen CUI users[3] in your organization as well as CUI-authorized external organizations[4] will be eligible for accessing file content, assuming the file is shared with them.	This label is intended for files that contain government Controlled Unclassified Information (CUI) that is part of one of the NOFORN categories and therefore requires additional safeguards to prevent unauthorized access.	• Files with information created for or on behalf of the government that is regulated by one of the NOFORN CUI categories • Files with ITAR or Intelligence information
	Government Controlled – CUI - Additional Compatibility[5]	Files will have standard at-rest encryption. System-enforced access controls will be removed for the purpose of added compatibility for sending to authorized recipients via email or uploading to a web portal. This label will only be used **temporarily** when necessary. Users must immediately revert label to the "Government Controlled – CUI" after file has been sent as an attachment or uploaded.	This label is intended for files that contain government Controlled Unclassified Information (CUI) and need additional compatibility when sending to certain recipients or uploading to a web portal.	• Emails with information created for or on behalf of the government that is regulated by one of the CUI categories being sent to authorized recipients that need additional compatibility

[1] This label is currently only available through the Desktop Apps for Word, PowerPoint, and Excel

[2] Sharing Files that have additional protections with External users makes use of Guest accounts in your organization's M365. Only designated members of your organization have the ability to invite **new** Guests to the organization. Any member can share with **existing** Guests. For more information, see Guest Accounts section of this guide.

[3] Members of your organization can be designated by corporate leadership as authorized CUI users depending on their role. These users will be able to apply the CUI label and can be granted access to CUI files and emails.

[4] Most DoD government organizations are configured as CUI-authorized external organizations by default. More organizations can be added by DefenseX administrators upon corporate leadership requests. Partner organizations that need to be able to receive and access CUI will need to be added to the list of CUI-authorized external organizations.

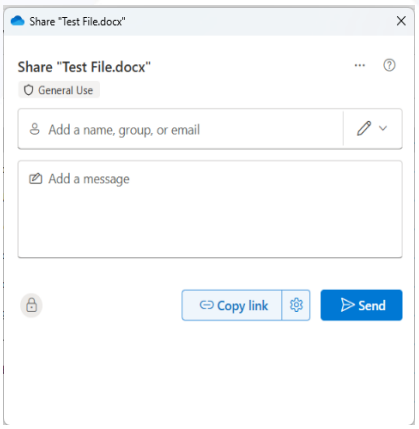
[5] This label was created because some external organizations have security settings that prevent files with additional protection from being sent to them. Additionally, for a CUI file that will have unlimited distribution by an external organization recipient, this is the best label to use.

Sharing Files in M365 101

There are two common ways that many individuals share files in M365.

A. Giving Others Direct Access to Source File

1. This can be done by clicking the **Share** button on any of the M365 apps. Typically, the button will look like this: Share
2. A small window will pop up that allows you to give other users direct access to the file along with an email message.
3. Alternatively, you can also generate a customized sharing link that you can copy and provide to others. This option is often more flexible. You can copy this link into a Teams chat or an Email.



Note: Sharing via this method for users external to your organization requires the use of Guest accounts. Anyone in the organization can share files with existing Guests, but only certain designated individuals can invite new Guests into the organization. See the Guest Accounts for External Sharing section of this Guide for more details regarding this topic.

B. Attaching Files to Emails

1. This can be done by clicking the **Attach File** button on an email Ribbon. This button will provide several options for sources from where to attach the file from. Typically, the button will look like this:
2. When selecting a file that is in your OneDrive or another M365 web location, you will get the option to **Share Link** or **Attach as a Copy**.
    i. Using the **Share Link** is recommended for most internal sharing since it helps prevent duplicates. The Share Link uses the same mechanisms as method A above. Email recipients will be given direct access.
    ii. Attaching a Copy makes a full copy of the file to deliver to the recipient. This is a more compatible method of sharing when sending files external to the organization.

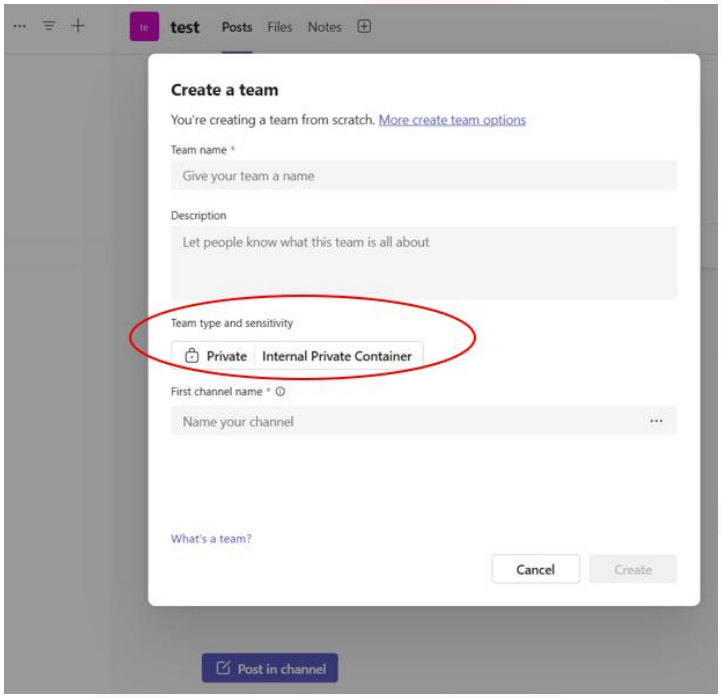
Note: When a file has an additional layer of encryption, as in the case of *Government Controlled – CUI*, the file retains that additional layer of encryption and associated access controls even when it is emailed externally as a copy. External recipients will need to use their Guest accounts to access the file. See the Guest Accounts for External Sharing section of this Guide for more details regarding this topic.

Labels for Containers such as Teams, SharePoint Sites, and M365 Groups

Labels for containers such as Teams, SharePoint sites and M365 groups add additional levels of security. They help the organization have a greater level of awareness regarding where external collaboration is happening and minimize the amount of "public" internal teams that can cause unintended oversharing.

How To Use:

When a new Team, SharePoint Site, or M365 Group is created, the creation wizard will require a sensitivity label to be associated with it. The sensitivity labels that have been published by your organization will be available in the following (red circled) location. The table below describes the sensitivity labels that can be associated with Teams, M365 Groups, and SharePoint Sites.



Labels for Containers Descriptions:

Label Name	Label Security Actions	Label Intention	Applicable to:
Internal Private Container (Default Label)	Private container by default. Only members of your organization can be invited to become members. Sharing files located inside the container is restricted to members of your organization.	This label is intended for all collaboration workspaces which will be composed of **only** members from your organization.	• Most team workspaces for internal collaboration • Private workspace for specified individuals
Internal Public Container[1]	Public internal container by default. Any member of your organization can discover and self-join on demand. Sharing files in the container is restricted to members of your organization.	This label is intended for a few company-wide accessible containers. It is not ideal for storing sensitive information.	• Open community interest groups • Public announcement containers
External Collaboration Container[2]	Private container by default. Individuals that are external to your organization can be invited to become members via the use of Guest accounts.[3] Sharing files in the container is restricted to members of your organization and Guest users.	This label is intended for private collaboration workspaces that need to be composed of members of your organization as well as external members.	• Team workspaces for external collaboration with partner organizations or Government organizations

[1] Only a few individuals designated by corporate leadership as Internal Public Container Creators will have the ability to use this label and create these containers. More information regarding this role is found below.

[2] Only a few individuals designated by corporate leadership as External Collaboration Managers will have the ability to use this label and create these containers. More information regarding this role is found below.

[3] See the Guest Accounts for External Sharing section in this guide for more information related to Guest accounts.

External Collaboration Manager Role - This role should be given to a limited number of individuals to improve security. Ideal candidates include team leaders or individuals that have frequent external collaboration needs. These users will have the following additional capabilities:

1. These users will have the ability to create Teams, Sites, and M365 Groups (containers) that Guests can be invited to.
2. They will be able to invite **new** Guests from other organizations to collaborate, including DoD or partner orgs.

Internal Public Container Creator Role - This role should be given to very few individuals from the organization, such as HR individuals and other leadership. Public containers (although internal to the org) can lead to accidental oversharing if used improperly. Users with this role will have the following additional capabilities:

1. They will be able to create public internal Teams and M365 groups that all members of the organization can self-join on demand.

Guest Accounts for External Sharing

Guest accounts are designed to enable external organizations or users access resources in your M365 environment in a secure way for the purpose of collaboration. It enabled "Guests" from other organizations to access your resources via their own organization's credentials. GCC High M365 is designed in a unique way to insulate it from commercial M365 organizations and other cloud environments. For this reason, different actions may need to be taken by IT administrators to enable Guest accounts to be created for particular external organizations. The chart below details the most likely experience when collaborating with individuals or organizations in different cloud environments. Depending on the organization you are wanting to collaborate with, you might encounter one of these scenarios. These can also be influenced by the external organization's security policies.

Cloud Environment	Expected Behavior	Additional Required Actions from IT admins
Organizations in M365 GCC High	Full collaboration natively	N/A
Organizations in M365 DoD	Full collaboration natively[1]	N/A
Organizations in commercial M365	Full collaboration when permitted and configured by both orgs[2]	Cross-Cloud and Cross-Tenant configuration needs to be implemented on both sides
Personal Microsoft Accounts	Collaboration via shared Files, SharePoint sites, and limited Teams functionality	N/A
Gmail Accounts[3]	Collaboration via shared Files, SharePoint sites, and limited Teams functionality	N/A

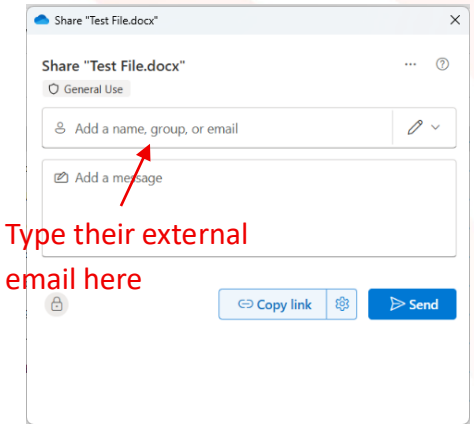
[1] Most DoD organizations have additional security policies that can result in unidirectional Guest account capabilities. For example, a member from a DoD org can have a Guest account in your org, but you cannot have a Guest account in theirs.

[2] Due to Microsoft's compliance requirements in GCC High, collaboration with commercial M365 organizations is disabled by default. It can be enabled by IT admins on both sides and is a simple configuration.

[3] Microsoft supports the creation of personal Microsoft accounts by using Gmail accounts.

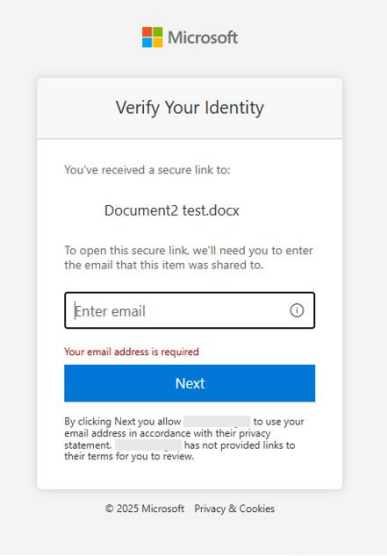
Guest Account Typical Experience

Adding New Guests to the Organization - New Guests can be added to the organization by individuals with the External Collaboration Manager Role. In order to add new Guests to the organization, simply share a file with them from an external collaboration container or add them as a member to that container. The share button will open up the share window. Type in their external email address to the *Add a name, group, or email*. It will warn you that the user is outside of your organization and in many cases give you the option of typing in a display name for that Guest user. Once you click send or add they will be added to the organization as a Guest.

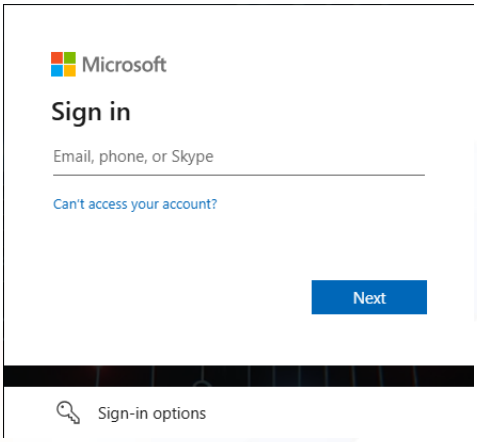


Guest Recipient Experience – When new Guests are added to your organization, they will receive an email inviting them to collaborate. They will be guided through the quick set up for their Guest accounts.

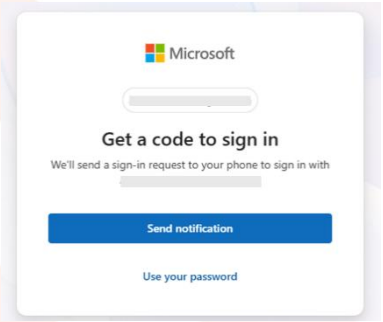
1. They will click the link in their email and it will open a web browser which will ask them to input their email address.



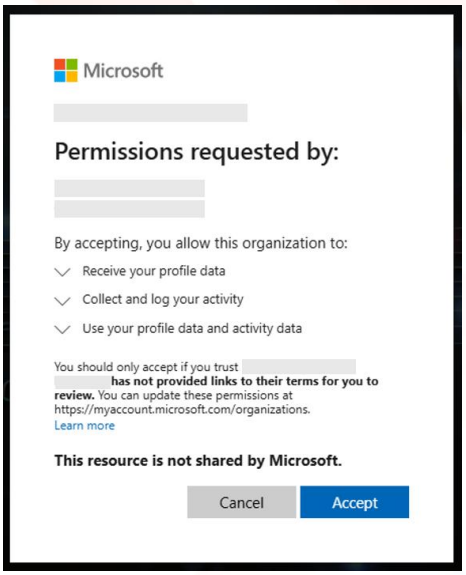
2. Once they type their email address, they will be directed to a Microsoft login screen for your organization. They will type the same email address again and authenticate if they already have credentials.



3. If they have MFA already in place for their account, they will be prompted for it.



4. They will then be directed to Accept the monitoring that your organization has in place in order to access your organization's resource.



5. Once they accept, they will be led through some simple steps to set up MFA as per your organization's requirements either via phone, text, or an authenticator app. At the conclusion of this, they will have access to the resources you shared with them. They will be able to re-access the resources by clicking on the original email link inviting them to collaborate.
6. For more info, see the Microsoft video regarding this: [Work with external guests - Microsoft Support]

Note: For DoD users that are invited as Guests, they will only need to go through an abbreviated version of these steps. This is due to some configurations that have a higher level of trust for them due to their existing security policies.