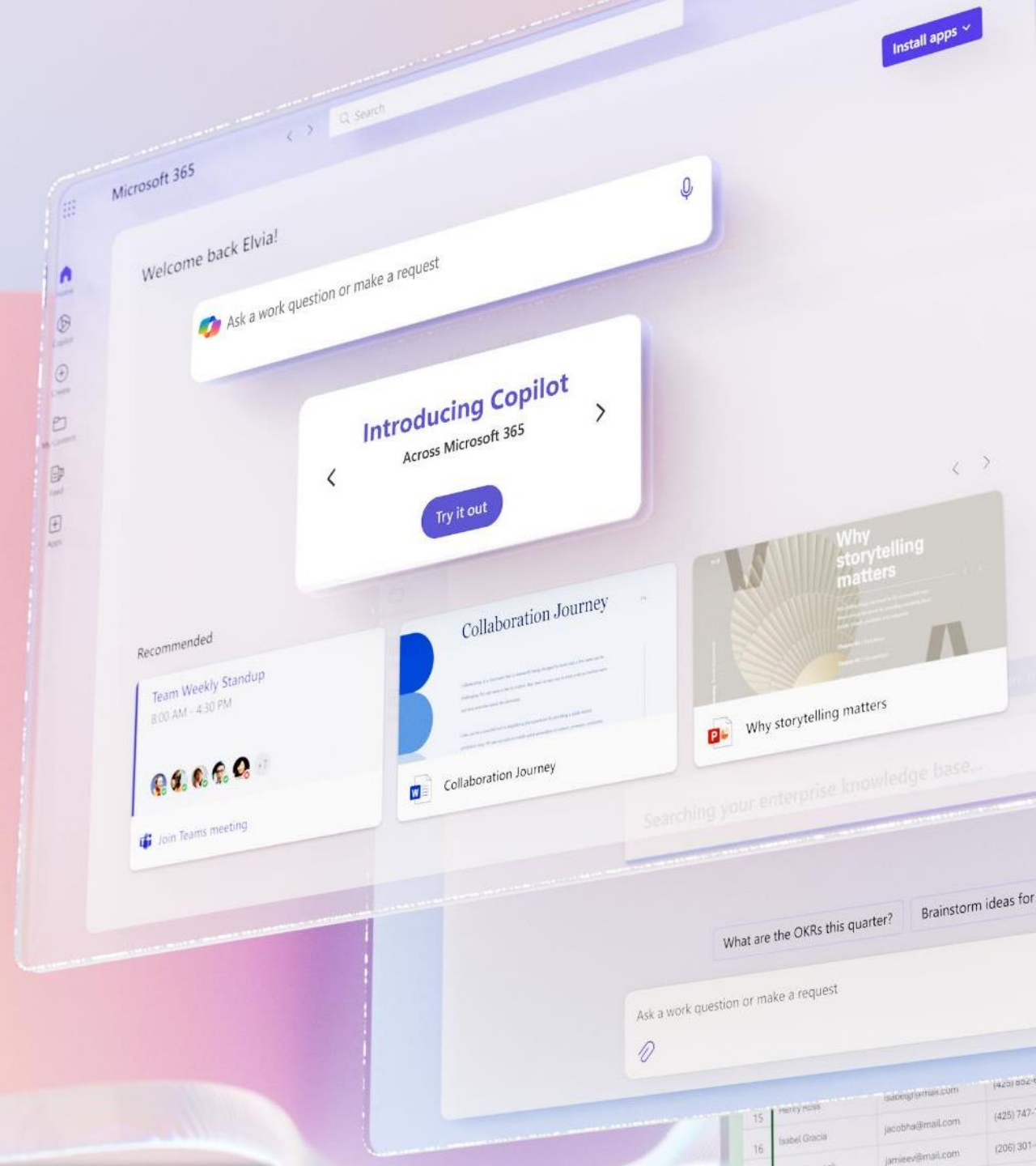


# Secure and govern data in the age of AI

## Overview of Copilot for Microsoft 365

21 May 2024

Erfan Setork | Principal Technical Specialist, Compliance  
Natalie Noonan | Global Black Belt, Compliance



# Welcome + Introductions

## Erfan Setork

Principal Technical Specialist, Compliance

[erfansetork@microsoft.com](mailto:erfansetork@microsoft.com) | [Linkedin](#)



- Leads data protection and data governance strategies for prominent US healthcare providers and payers
- 10+ years as a former IT, cybersecurity and compliance analyst within enterprise software companies

## Natalie Noonan

Global Black Belt, Compliance

CIPM (IAPP), IGP (ARMA), CSM, PMP

[nanoonan@microsoft.com](mailto:nanoonan@microsoft.com) | [Linkedin](#)



- Works with Microsoft's customers, partners, and engineering teams to bring customer insights and enhancements into the risk and compliance solutions
- Point of escalation for customers assessing and deploying Microsoft Purview to meet legal, risk, and compliance obligations
- 20+ years as a former program leader, practitioner, and consultant specializing in information governance, ediscovery, and privacy

# Agenda

## Overview

- What is Copilot for M365? What are top information governance problems and risks?
- How do we deploy Copilot securely? Where do we start?

## Readiness

1. How do we get ready for Copilot for M365? >> “plan on a page”
2. Planning your Copilot rollout – enabling data clean-up and governance by design

### **Administrator – Risk and Compliance Controls**

1. Applying retention and deletion controls (e.g., Copilot interactions, recordings and transcripts)
2. Monitoring for ethical and appropriate use
3. Gathering evidence and audit for data investigations and litigation
4. Using specialized tools for data clean-up and data governance

## Demo

### **End User – Prompts and Responses**

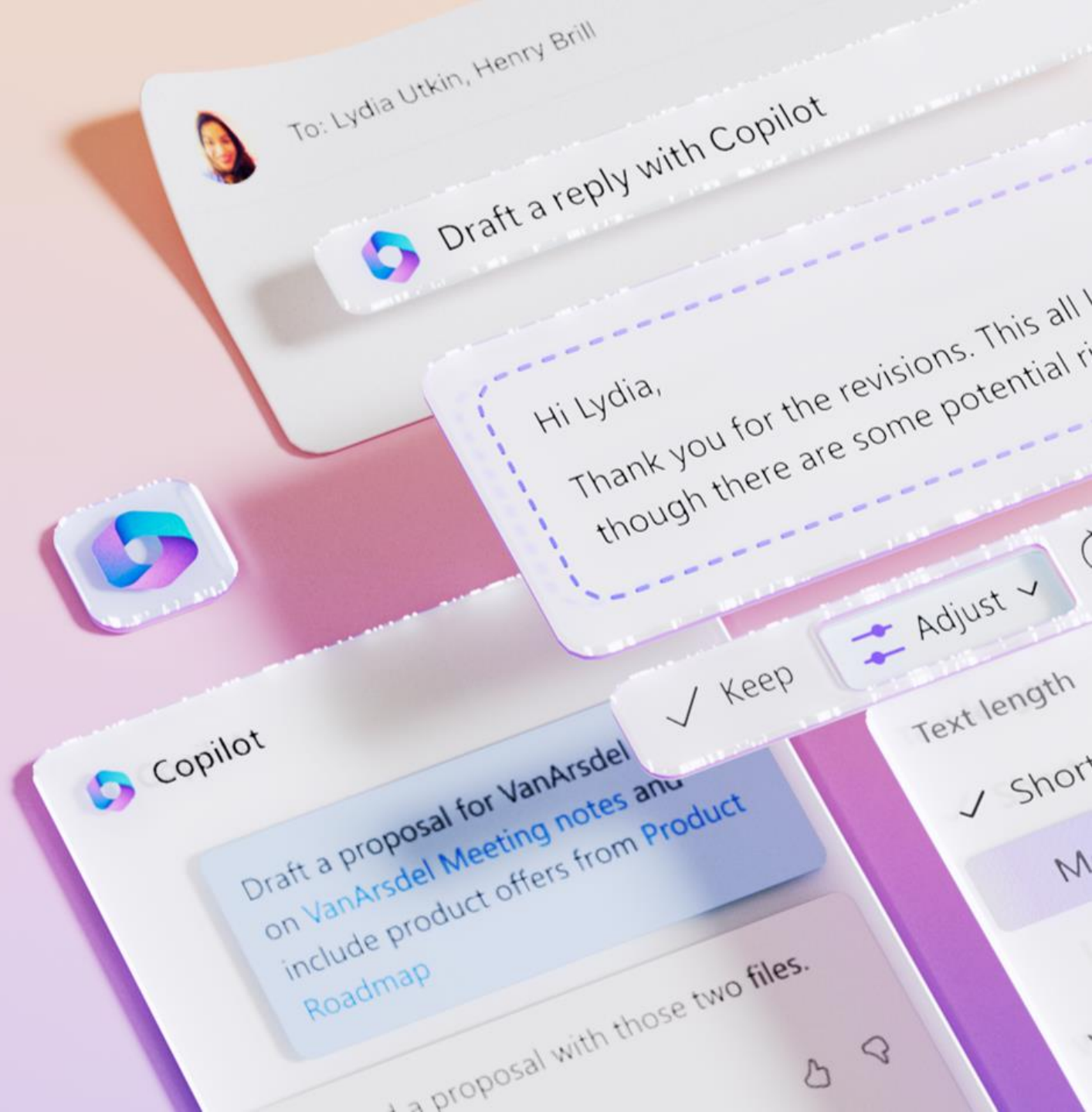
1. Sensitivity labels – applying and enforcing protection (content markings, encryption, privacy, access controls)
2. Label citations – guiding awareness of data sources and classification
3. Label inheritance – driving labels to content created by Copilot
4. Permissions adherence – performing only authorized activities (least privilege access)

## Closing

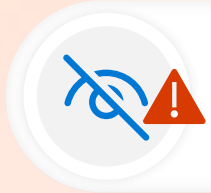
Q&A

# Overview

Copilot for Microsoft 365



# Security and compliance concerns with AI usage

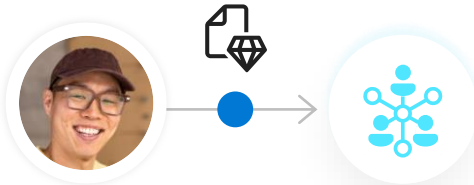


Insufficient visibility into the usage of AI applications can result in security and compliance challenges.

1

## Data leak:

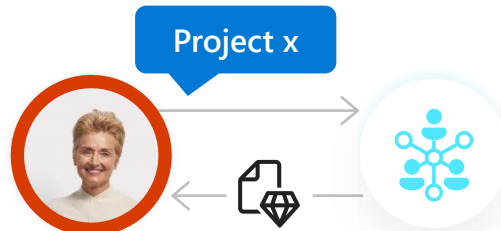
Users may inadvertently leak sensitive data to AI apps



2

## Data oversharing:

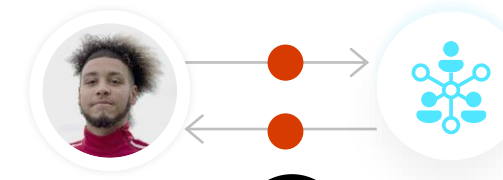
Users may access sensitive data via AI apps they are not authorized to view or edit



3

## Non-compliance usage:

Users use AI apps to generate unethical or other high-risk content



# What is Microsoft Copilot?



[Microsoft Copilot](#) | [Microsoft AI](#)

## Copilot (Edge)



Better interaction with web content

## Microsoft 365

Word



Better reading and writing assistance

Outlook



Better e-mail management

Excel



Better data analysis

PowerPoint



Better presentations

Teams



Better meetings

M365 Chat



Your AI assistant

## Viva



Drive adoption

## Windows



Better interaction with OS, apps, and files

## Copilot for Web

## Copilot for Productivity

## Enhance Copilot for Everyday

## Dynamics



Better sales and customer support

## Fabric



Better data analytics and business intelligence

## Security



Better threat detection, identification, and mitigation

## GitHub



Better code development

## Copilot Studio



Better creation of apps, workflows, and agents

## Copilots for Business

## Copilots for Analytics

## Copilot for Security

## Copilot for Development

## Copilot for Low/No Code Development

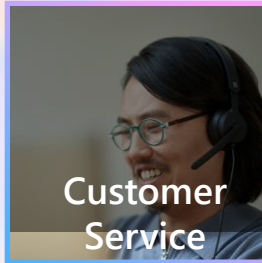
# What are common use cases?



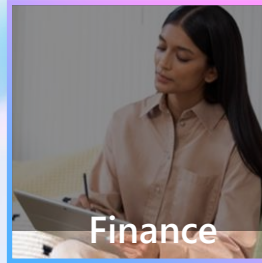
Jumpstart the creative process and generate ideas while writing



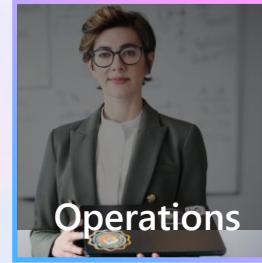
Stay focused on closing deals with an AI assistant for email



Stay coordinated as a team to resolve more customer issues



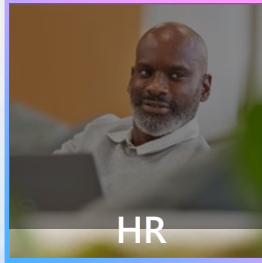
Quickly search data to solve your most complex problems



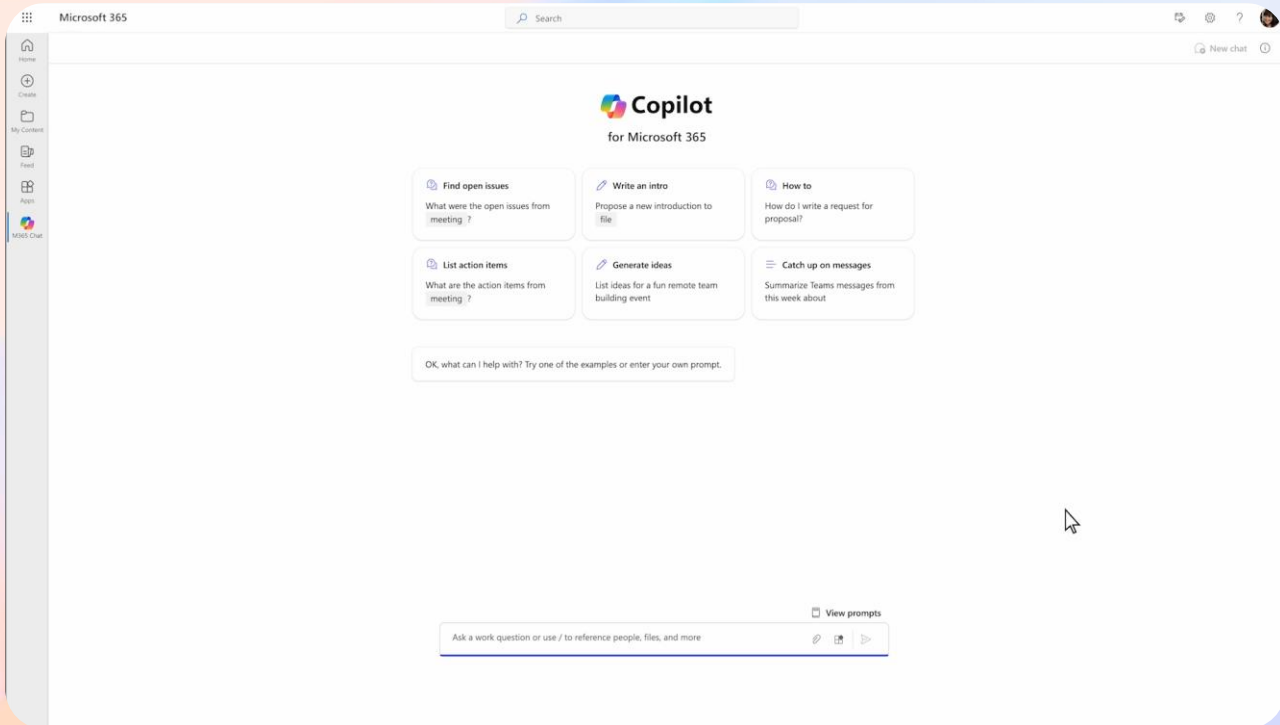
Simplify quality reporting and data validation



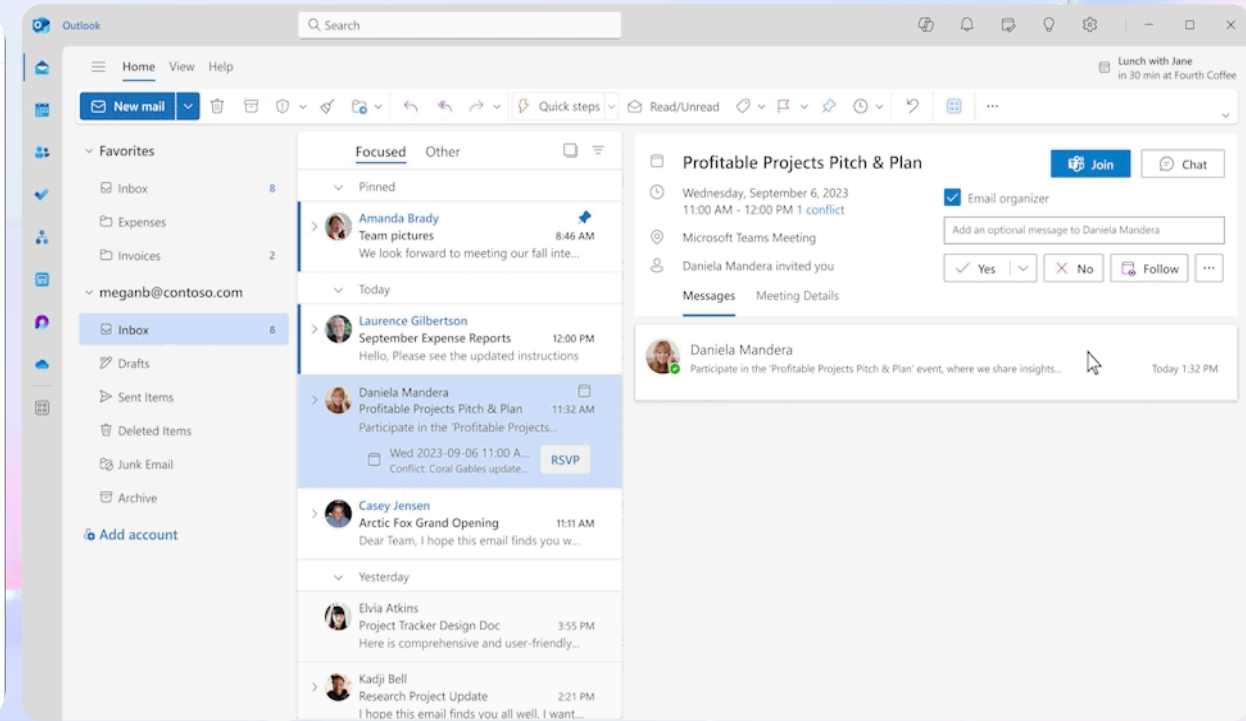
Effectively manage shared projects and track progress



Store, access, and prioritize notes in a fraction of the time



Copilot for Microsoft 365



Copilot in Outlook

# Comparing Personal, Work and Copilot for M365

	Copilot	Copilot	Copilot for Microsoft 365
	Personal (consumer)	Web (enterprise/web)	Work (enterprise/tenant)
GPT Large Language Model	●	●	●
AI-Powered Web Search, Answers & Content Generation	●	●	●
Commercial Data Protection		●	●
Enterprise Security, Privacy & Compliance			●
Microsoft 365 Graph (content & context)			●
Microsoft 365 Apps			●
Prompts retained	●		●
Prompts potentially used to tune LLM	●		

# Technical Readiness



# How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements



Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

- 1 Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
- 2 Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
- 3 Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
- 4 Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
- 5 Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)

Identify those who can help

- ✓ Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.  
[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

1

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

Identify those who can help

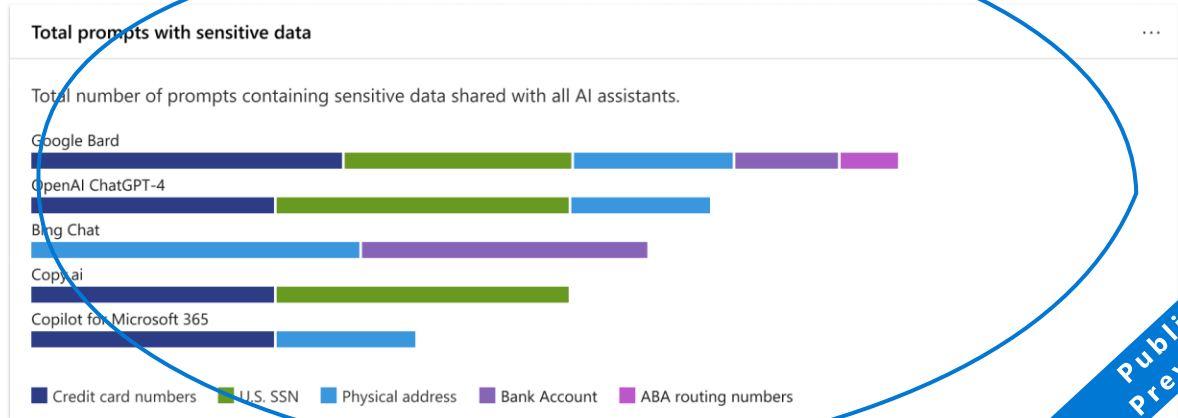
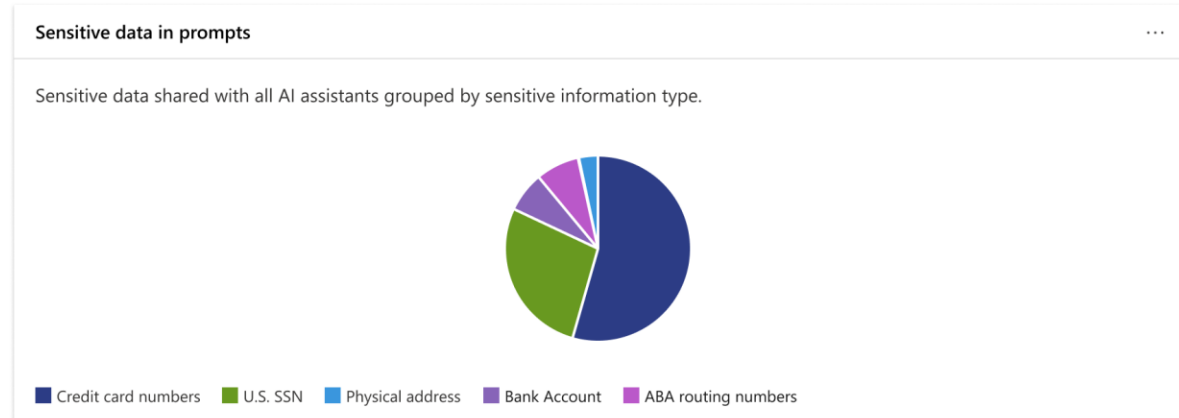
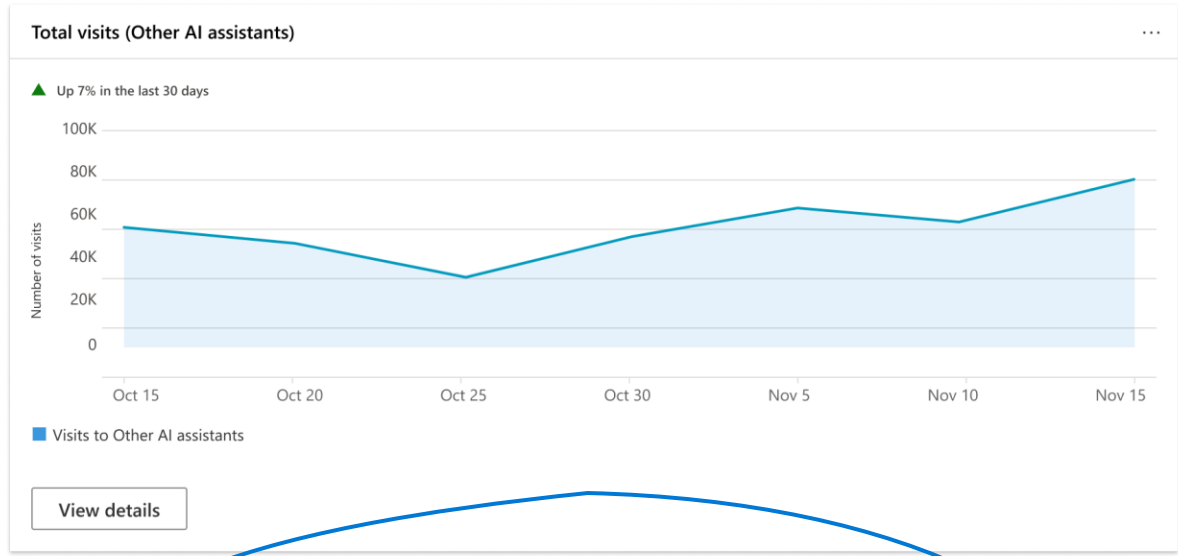
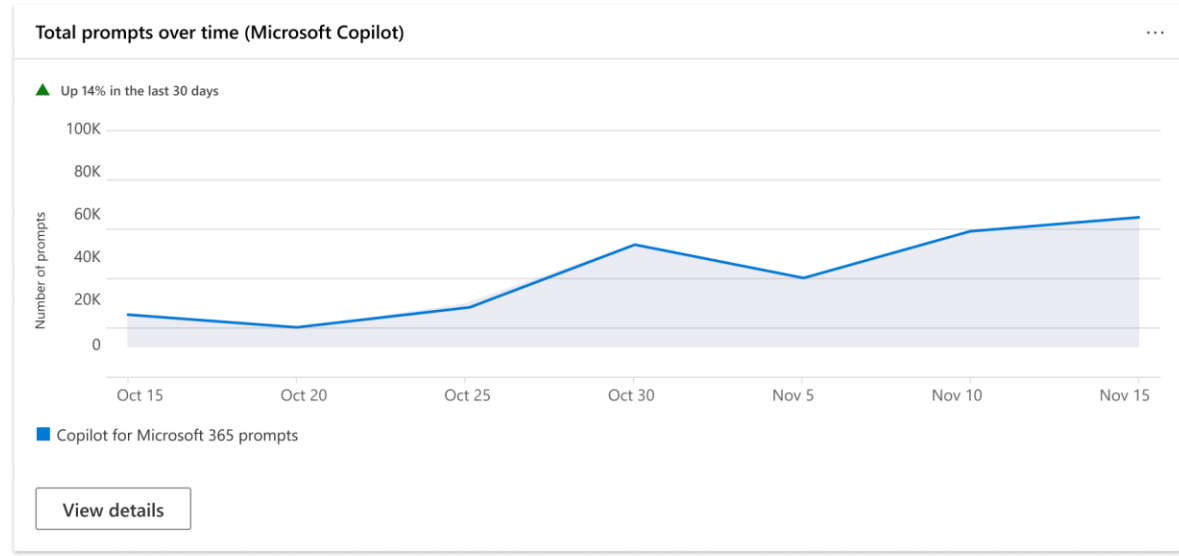
- 1 Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
  - 2 Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
  - 3 Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
  - 4 Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
  - 5 Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)
- ✓ Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.  
[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# AI hub (preview)



Analytics Policies Activity explorer

AI hub in Microsoft Purview provides insights to help security teams gain comprehensive visibility into data security risks (e.g., prompts containing sensitive data in consumer generative AI).



Public Preview

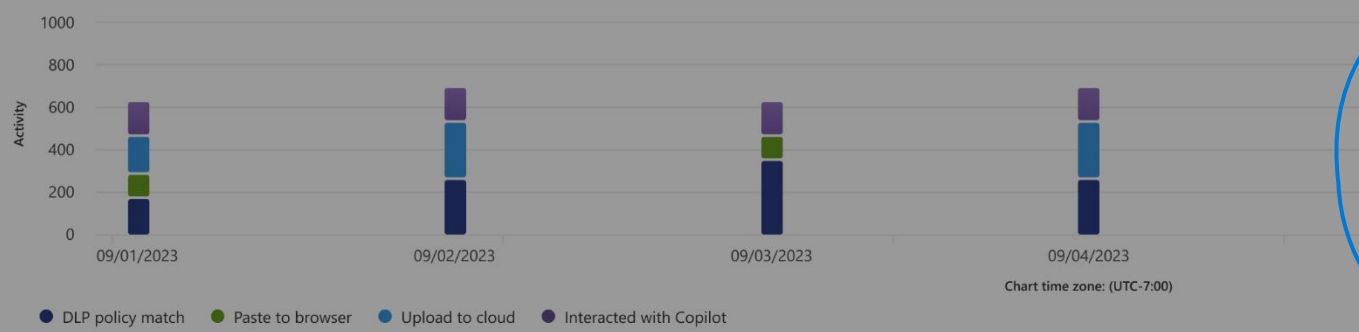
- Home
- Ai Hub**
- Compliance Manager
- Data classification
- Data Connectors
- Alerts
- Reports
- Policies
- Permissions

- Solutions**
- Catalog
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
  - Data lifecycle management
  - Information protection
  - Insider risk management
  - Records management

# AI hub (preview)

Analytics Policies Activity explorer

Activity: All values User: All values DLP policy matched: All values Sensitive info type: All values Add filter Reset all



<input type="checkbox"/>	Activity	User	Time happened	Device full name	Enforcement mode	Sensitive info type	File sensitivity
<input type="checkbox"/>	File upload to cloud	Mona Kane	Sep 01, 2023 3:54 PM	Desktop-3453HD	Audit	Credit card number	Confidential
<input type="checkbox"/>	Paste to browser	Dean Renzo	Sep 01, 2023 3:54 PM	Desktop-363345HD	Audit	Social security number	Confidential
<input type="checkbox"/>	File upload to cloud	Edison Gil	Sep 02, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidential
<input type="checkbox"/>	Interacted with Copilot	Sarah Terry	Sep 03, 2023 3:54 PM		Audit	Credit card number	Confidential
<input type="checkbox"/>	File upload to cloud	Posie Par	Sep 03, 2023 3:54 PM	Desktop-53544EF	Audit	Physical address	Confidential
<input type="checkbox"/>	Interacted with Copilot	Dean Renzo	Sep 05, 2023 3:54 PM		Audit	Social security number	Confidential
<input type="checkbox"/>	Paste to browser	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account	Confidential
<input type="checkbox"/>	Interacted with Copilot	Sarah Terry	Sep 06, 2023 3:54 PM	Desktop-3534345-LD	Audit	Bank account	Confidential
<input type="checkbox"/>	Paste to browser	Mona Kane	Sep 13, 2023 3:54 PM	Desktop-ASFD213	Audit	Credit card number	Confidential

1

## File upload to cloud

### Activity details

**Activity**  
File upload to cloud

**Client IP**  
131.109.147.63

**Target domain**  
bard.google.com

**About this item**

**User**  
Mona.Kane@contoso.com

**Sensitive info type**  
Credit card number

**Rule**  
Audit:UploadToCloud

**Happened**  
Sep 13, 2023 3:54 PM

**Enforcement mode**  
Audit

**JIT triggered**  
False

**Policy**  
AI hub – Data Protection

**Location details**

**Source location type**  
Unknown

**Platform**  
Windows

**Application**  
Desktop-3453HD  
[View device details](#)

**MDAIP device ID**  
33oe9ca0778b9ec2ab7933ac9f7ehsd1987bacd8

[Done](#)



+ New chat

Recent

Extract credit card nu...

Dynamic DLP policies with [Adaptive Protection to prevent sensitive data loss in third-party AI applications.](#)



# Hello again

Tell me what's on your mind, or pick a suggestion.

## Understand

- refactor code
- explain JavaScript code
- rules of a sport

## Create

- supportive response
- mocktail recipe
- revise my writing

## Explore

- comparison shop
- best beaches in...
- date night planning



Enter a prompt here



Washington, USA

# How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

2

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

Identify those who can help

- 1 Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
  - 2 Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
  - 3 Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
  - 4 Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
  - 5 Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)
- ✓ Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.  
[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# Perform data discovery

Optional tasks and tools to aid as part of a data discovery risk assessment depending on licensing and skills

Areas of focus

## Uncover Risks

### Data discovery

- Permissions
- Sensitive and personal data
- Privacy levels
- Data overexposure
- Obsolete data

- Levels of sensitivity
- Application of retention
- Access request procedures
- Data loss procedures
- On/Offboarding procedures

Optional actions

Review existing permissions of Teams and Sites

Use content search to discover sensitive information

Run PowerShell scripts to generate reports

Use Content Explorer to identify sensitive content

Identify data exposition with Defender for Cloud Apps

Use eDiscovery Premium to identify sensitive content

Identify overshared personally identifiable information with Microsoft Priva

Identify sensitive or overexposed content with SharePoint Premium

Microsoft Purview Advanced Rich Reporting

E3

E5

Add-on



We must discover and classify data to understand how it is being used, stored, and shared to implement appropriate safeguards.

## Why does this matter?

**Purpose:** To uncover and report on potential risks of overexposed sensitive data, oversharing of sites and content, and to aid in the preparation of remediation activities

**Procedure:** Run manual procedures, tools, scripts, and building of visual assets to help uncover and present existing risks of data, permissions, and other security, privacy, and information technology concerns to help plan for the remediation activities ahead

**Results:** To obtain knowledge of exposed risks, required activities of remediation, assignment and alignment of resources required, and estimations of time required to implement the necessary controls

- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Trials
- Solutions
  - Catalog
  - App governance
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
  - Data lifecycle management
  - Information protection

# Data classification

Overview Trainable classifiers Sensitive info types EDM classifiers Content explorer Activity explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. [Learn more](#)

Filter on labels, info types, or categories

All locations > SharePoint > <https://m365x10870916.sharepoint.com/sites/Retail>

Ad Slogans.docx

Source Details

The actual number of items in this site/folder might be different from the calculated number that's displayed on the left

Export Search

Name	Sensitive info type	Trainable classifier
Contoso Electronic...	All Full Names	Finance
Electronics Store Tr...	All Full Names	Finance
<input checked="" type="checkbox"/> Ad Slogans.docx		Finance
CE Annual Report.d...	All Full Names	Finance
letter of intent_8.pdf	Types Of M... +1 more	Agreement
term sheet_4.pdf	Australian C... +5 more	Agreement
letter of intent_9.pdf	All Full Na... +2 more	Agreement
term sheet_1.pdf	All Full Na... +2 more	M&A

1 of 2

Use Content Explorer & Activity Explorer to understand what types of sensitive and personal information exists and how it is being used and shared.

Please note contextual summary is not supported for trainable classifiers.

Finance  
Not a match Match

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Roles & Scopes
- Trials
- Solutions
  - Catalog
  - App governance
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
  - Data lifecycle management
  - Information protection
  - Information barriers
  - Insider risk management

# Case 449: Potential IP theft

Active Low 25 risk score

Resolve case Case actions

Case overview Alerts User activity Activity explorer Forensic evidence (preview) Content exp

Filter: Risk category: Any Activity Type: Any Reset all

Sort by: Date occurred

User activity scatter plot 6 Months 3 Months

- Cumulative exfiltration activities**

Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 15/100

467 events: All exfiltration activities with prioritized content: More events than 90% compared to teammates. Priority content includes: 1 SharePoint sites and 2 file extensions.

20 events: Shared SharePoint files externally: More events than 99% compared to users that access same SharePoint sites.

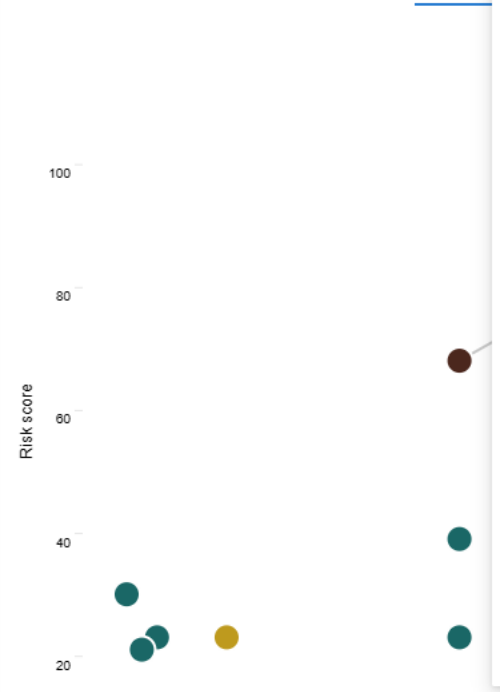
21 events: All exfiltration activities: More events than 30% compared to users with same job title.
- Cumulative exfiltration activities**

Nov 29, 2022 - Nov 30, 2022 (UTC) | Risk score: 45/100

467 events: All exfiltration activities with prioritized content: More events than 90% compared to teammates. Priority content includes: 1 SharePoint sites and 2 file extensions.

20 events: Shared SharePoint files externally: More events than 99% compared to users that access same SharePoint sites.

21 events: All exfiltration activities: More events than 30% compared to users with same job title.



**(4) SEQUENCE: Files collected, obfuscated, exfiltrated and cleaned up**

Nov 21, 2022 - Nov 24, 2022 (UTC) | Risk score: 90/100

- 50 events: Sequence: Files downloaded from SharePoint, renamed, printed, then deleted
- 5 events: Files that have labels applied, including: random name
- 2 events: Files containing sensitive info, including: Credit Cards
- 1 event: File sent to 1 unallowed domain
- 2 events: Files with priority file extensions, including: docx

**Deletion: Files deleted**

Nov 24, 2022 (UTC) | Risk score: 75/100

- 2 events: Files deleted from Windows 10 Machine
- 2 events: Files with priority file extensions, including: docx

**Exfiltration: Files printed**

Nov 23, 2022 (UTC) | Risk score: 45/100

- 2 events: Files printed
- 2 events: Files containing sensitive info, including: Credit Cards

**Obfuscation: Files renamed**

Nov 22, 2022 (UTC) | Risk score: 32/100

- 19 events: Files renamed
- 2 events: Files containing sensitive info, including: Credit Cards
- 12 events: Files with priority file extensions, including: pdf, ppt, docx, txt
- 12 events: Files with priority file extensions modified, including: docx, txt, pdf

**Collection: Files downloaded from SharePoint**

Nov 21, 2022 (UTC) | Risk score: 27/100

- 45 events: Files downloaded from 1 SharePoint site
- 2 events: Files containing sensitive info, including: Credit Cards
- 34 events: Files that have labels applied, including: Confidential



HR event: resignation date set

# How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

3

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

Identify those who can help

- 1 **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
  - 2 **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
  - 3 **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
  - 4 **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
  - 5 **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)
- ✓ **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.  
[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# Strengthen data access controls

Optional tasks and tools to aid with data access remediation depending on licensing and skills

Areas of focus

## Implement Controls

### Data access

- Remediate permissions
- Evaluate data boundaries
- Evaluate and enforce access reviews
- Evaluate and apply expiration policies
- Evaluate and apply conditional access

Manually adjust permissions in Sites and Teams

Temporarily restrict SharePoint site content using Restricted SharePoint Search

Implement Access Reviews to recertify Teams & Group audience

Implement container labeling conditions to new public / private site

Refine group expiration policy for inactive Teams & Group sites

Use SharePoint Premium to restrict access to specific Sites

E3

E5

Add-on



We must discover data access to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices).

## Why does this matter?

**Purpose:** To remediate any existing permission level and access risks along with implementation of future governing practices around access control and review.

**Procedure:** Evaluate and remediate required permission levels and prepare/implement access controls and reviews

1. Engage your IT and SharePoint Administrators to review existing roles, permissions, groups, and privacy levels.
  - [Sharing Policies](#)
  - [Access Control Policies](#)
2. Resolve memberships via site and access reviews to expire sites, set default configurations, set recurring access reviews, etc.
  - Site access reviews
  - Expiration policies
  - Sharing links reports

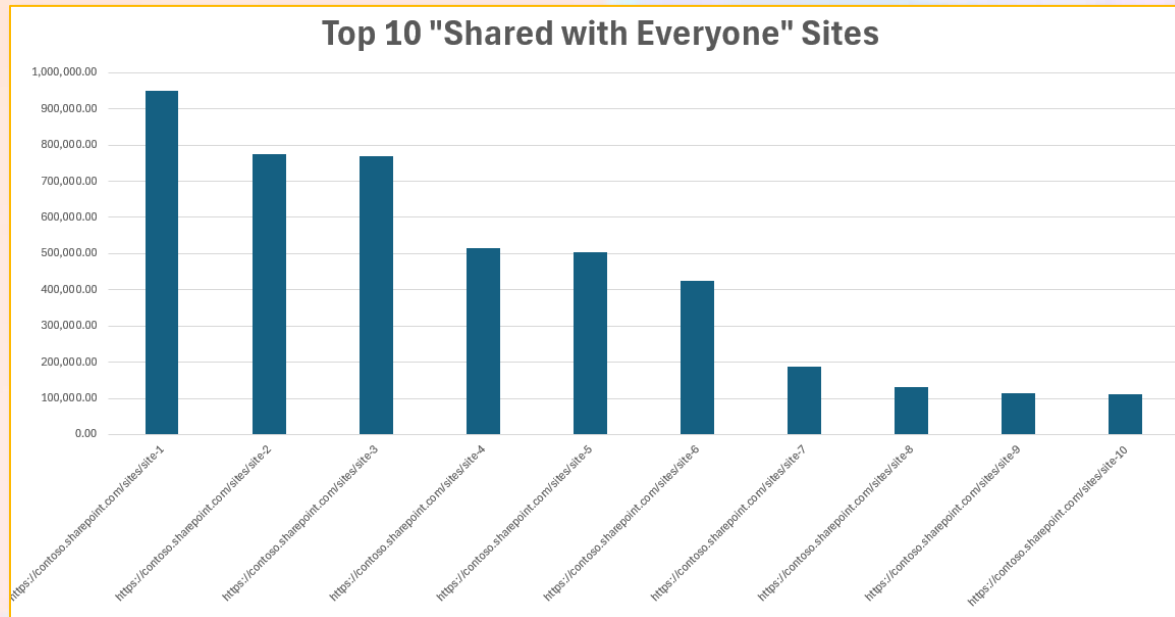
**Results:** Remove legacy permission risks and look to future proof Microsoft 365 long term by implementing processes for continuous content / access reviews.

# Strengthen access controls

SharePoint sharing policies, reports, and access reviews

3

## Sharing policies and reports



1. Remediate top 10 overshared sites.
2. Review site settings – shared w/anyone, public vs. private.
3. Confirm site owners and accountabilities.
4. Kick off access reviews to drive container labels, expirations, etc.
5. Establish go-forward processes (set recurring access reviews, refine sensitivity and retention policies, etc.).

## Implement access reviews



### Ownership Attestation Policy

Your SharePoint site [FY24 HLS Data Security & Privacy Gladiator](#) is due for attestation, which is a Microsoft policy that requires FTE Site Collection Admins (SCAs) to review and renew their sites every 180 days.

If you fail to submit the attestation by **Tuesday, May 7, 2024**, your site will be deleted along with all its associated content.

### Make sure to review the following before attesting.

- **Microsoft policies and guidelines.** Confirm the group and site complies with [Microsoft 365 Usage Guidelines](#).
  - **SharePoint site sensitivity label.** Make sure that the sensitivity label of your site aligns with its content. You can refer to the [Classify your data](#) page to learn more about what to consider when labeling your data as either Highly Confidential, Confidential, or General. Note: Public and Non-Business data labels apply only to files.
  - **Permissions to content within the site.** Ensure that members of this site are protecting content stored in the SharePoint site by properly classifying and applying permissions based on its business need and impact. Review that any file-, folder-, or site-specific permissions, and link sharing remains appropriate.
  - **Owner and Internal Membership.** Ensure the assigned owners and members of the site are appropriate. It is important to periodically review site ownership since occasionally people move onto other roles that are no longer associated with your site.
  - **External Membership.** Review your site's external membership for guests periodically, and revoke access for guests who no longer need it.
  - **Microsoft Corporate Document Retention Policy and Litigation Hold.** Confirm that the documents stored on the SharePoint site comply with the [Microsoft Document Retention Policy](#) and [Microsoft Corporate Retention Schedule](#). For questions about retention requirements, email [corprm@microsoft.com](mailto:corprm@microsoft.com). If you no longer need the site and intend to delete it or let it expire, email [litdoc@microsoft.com](mailto:litdoc@microsoft.com) to confirm whether it is under litigation hold.
- As an accountable owner of this SharePoint site I confirm that I have taken all the actions to ensure that my site is compliant with Microsoft policies. By clicking on submit I am aware that my site will be renewed for another 180 days.

I attest

[Data Privacy Notice](#)

Need technical assistance? Visit [aka.ms/TechWeb](https://aka.ms/TechWeb) to choose the support option that's right for you.

# How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

4

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

Identify those who can help

- 1 **Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
  - 2 **Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
  - 3 **Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
  - 4 **Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
  - 5 **Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)
- ✓ **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.  
[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# Prioritize deployment of data security controls

Optional tasks and tools to aid with data security depending on licensing and skills

Areas of focus

## Implement Controls

### Data security

- Prevent data loss
- Protect data
- Mitigate insider risk
- Evaluate and apply additional encryption

Optional actions

Implement data loss prevention policies for mail, files, and Sites

Manually apply sensitivity labels to Microsoft Teams and Sites

Implement data loss prevention policies for Microsoft Teams and third-party cloud apps

Auto-apply sensitivity labels to Microsoft Teams and Sites

Create data overexposure policies using Microsoft Priva

Apply encryption options to content, sites, and containers

E3

E5

Add-on



We must identify and protect sensitive data to control access and encourage safe data handling.

## Why does this matter?

**Purpose:** To implement data security controls to further detect, classify, protect, and prevent future data loss of any existing or future sensitive assets

**Procedures:** Once data classification schema is defined, apply levels of sensitivity to content and sites with the appropriate levels assigned to each. Apply data loss prevention policies aligned to the goals set forth of your overall data security program.

**Results:** Sensitive data is classified, protected, and discoverable to aid in the protection of oversharing and inadvertent data loss

- Home
  - Users
  - Devices
  - Teams & groups
  - Roles
  - Resources
  - Billing
  - Copilot**
  - Support
  - Settings
  - Setup
  - Reports
  - Health
- 
- Admin centers
- Identity
  - All admin centers
- 
- Show all

Home > Copilot

# Copilot

Copilot combines the power of AI with your organization's data to help everyone get more work done. Manage how users in your organization interact with Copilot for Microsoft 365, Security Copilot, and more.

## Settings

Name ↑	Description
Microsoft Copilot	Manage how your organization interacts with Copilot
Data security and compliance	Manage how Copilot references documents and data
Plugins	Go to Integrated App settings to control how Copilot interacts with other apps
Public web content	Allow Copilot for Microsoft 365 to reference public web content
Copilot for Sales	Choose whether users can see Copilot for Sales
Security Copilot	Go to Microsoft Security Copilot to manage Security Copilot



## Data security and compliance

Secure and protect Copilot interactions and data across Microsoft 365 using solutions in the Microsoft Purview compliance portal.

### Sensitivity labels

Label and protect your organization's data that's processed and generated by Copilot, while making sure that user productivity isn't hindered.

[Go to Microsoft Purview to manage sensitivity labels](#)

### Retention policies

Manage your data lifecycle by deciding how long to keep Copilot interactions and whether they should be deleted after a certain time.

[Go to Microsoft Purview to manage retention policies](#)

### Communication compliance

Capture Copilot interactions to review potential regulatory and business conduct violations.

[Go to Microsoft Purview to manage communications compliance](#)

### Audit

Search for audit records of Copilot interactions performed by users and admins.

[Go to Microsoft Purview to search audit records](#)

### eDiscovery

Search Copilot interaction content within your organization, preserve content, and export search results for further analysis

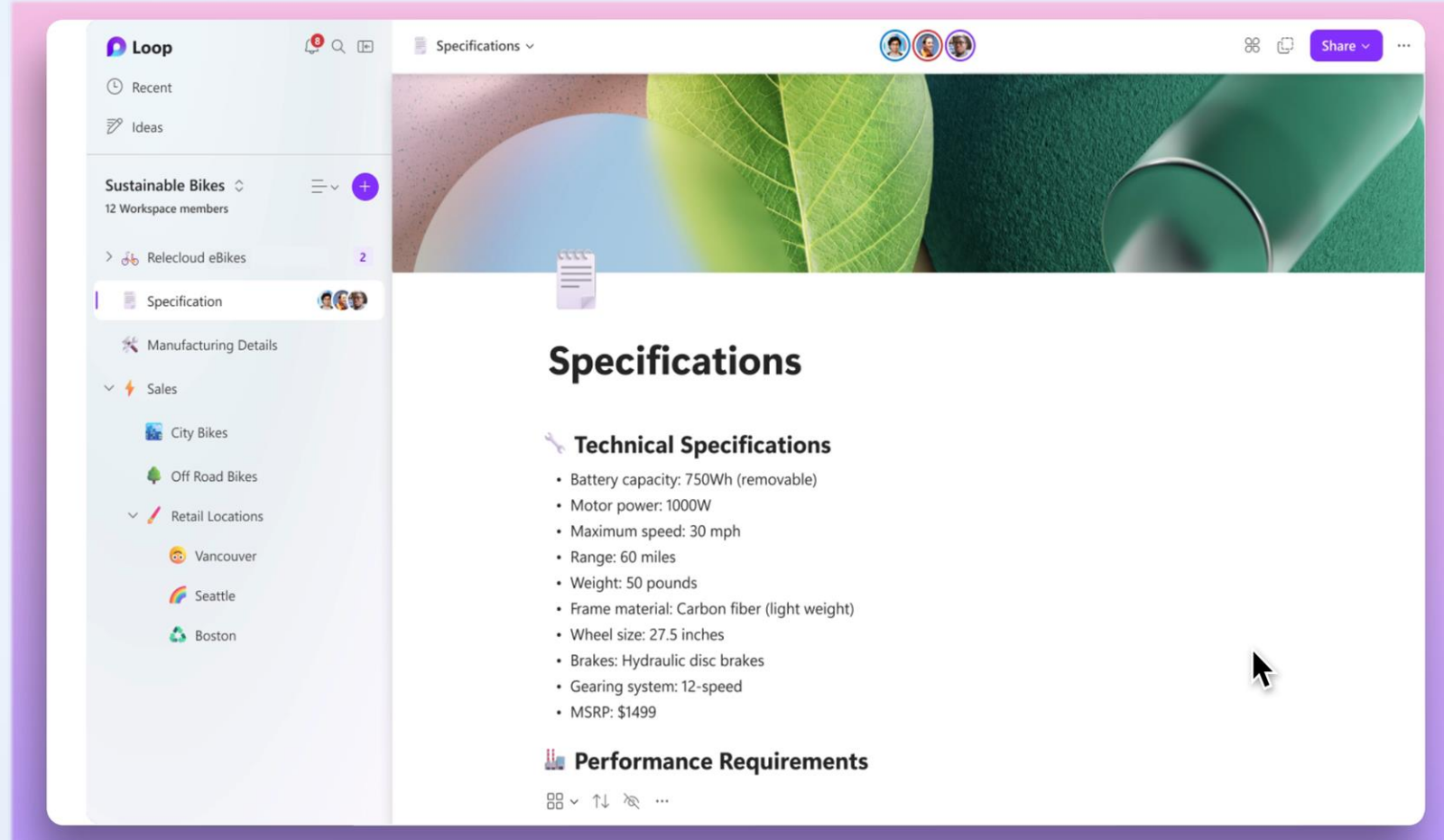
[Go to Microsoft Purview to manage eDiscovery](#)



# Demo

## Administrator – Risk and Compliance Controls

1. Applying retention and deletion controls (e.g., Copilot interactions, recordings and transcripts)
2. Gathering evidence and audit for data investigations and litigation
3. Monitoring for ethical and appropriate use
4. Using specialized tools for data clean-up and data governance



- Name
- Administrative Units
- Type**
- Locations
- Retention settings
- Finish

Create retention policies that identify **how long** the content is retained or deleted based on **where the Teams content is stored**.

- Teams Chats
- Teams Channels (Standard or Private)
- One Drive for Business
- SharePoint Online
- Exchange

<input type="checkbox"/> Off	OneDrive accounts	all document libraries (including default ones like Site Assets). <a href="#">More details</a>		
<input type="checkbox"/> Off	Microsoft 365 Group mailboxes & sites	All files in users' OneDrive accounts. <a href="#">More details</a>		
<input type="checkbox"/> Off	Exchange public folders	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. <a href="#">More details</a>		
<input type="checkbox"/> Off	Skype for Business	Items from all Exchange public folders in your organization.		
<input type="checkbox"/> Off	Teams channel messages	Skype conversations for the users you choose.		
<input type="checkbox"/> Off	Teams private channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. <a href="#">More details</a>		
<input checked="" type="checkbox"/> On	Teams chats and Microsoft 365 Copilot interactions	Messages from individual chats, group chats, meeting chats, bot chats, and Microsoft 365 Copilot interactions. <a href="#">More details</a>	All users	None Edit
<input type="checkbox"/> Off	Viva Engage community messages	Messages from Teams private channels. <a href="#">More details</a>		
<input type="checkbox"/> Off	Viva Engage user messages	Messages from Viva Engage community discussions. <a href="#">More details</a>		
<input type="checkbox"/> Off	Viva Engage user messages	Private messages and community message		

**Data Lifecycle Management** | Apply retention and deletion policies for Copilot prompts and responses; retain what is valuable, remove what is not.

Query-based auto-apply policies use the same search index for Data Lifecycle Management as [eDiscovery content search](#) to identify content. You can also run an auto-labeling policy in [simulation mode](#) to see the results reported to refine your rules for accuracy if needed, or gradually increase the scope of your auto-labeling policy before deployment.



As an Information Governance and eDiscovery leader, I need to enable proper retention and discovery of Teams meetings and other Copilot content.

- We want to retain what is meaningful and a business record.
- We value keeping meetings, conversations, and information shared in context.
- We want to dispose of what is of low or short-term value.

Meetings, Call Records, Intelligent Recaps, Transcripts, Translations...

M365 Copilot



She uses **name mentions and speaker markers** to hear about the task directly. And reviews the content shared using **screenshare markers and Chapters**.

First, Amanda skims the highlights on the Recap tab such as **AI-generated notes and suggested tasks**.

She notices a **task** was assigned to her

In order to start making progress on her task, she asks Copilot to organize the options discussed into a pros and cons table

Copilot 11:43 AM

4 and cons of option 1: Drive campaign traffic to generic Sign up page:

Pros	Cons
Wider range of potential leads	Less persuasive
Simpler, faster sign-up process	Difficult to segment audience
Streamlines multiple campaigns	Less engaging

The table helps Amanda identify her preferred route, but she is curious how the rest of the team feels about that option. She asks Copilot **how did the team react to option 2** to get a better sense of their sentiments during the meeting.

Ask a question about this meeting

5

Data Lifecycle Management | Auto-apply retention labels to matching content (e.g., meeting recordings and transcripts)

# Audit

[Learn about audit](#)

New Search Classic Search Audit retention policies (Preview)

Searches completed: **22** Active searches: **0** Active unfiltered searches: **0**

### Date and time range (UTC) \*

Start: Nov 06 2023 00:00

End: Nov 07 2023 00:00

### Keyword Search

Enter the keyword to search for

### Admin Units

Choose which Admin Units to search for

**Search** Clear all

**Activities - friendly names**

Interacted with Copilot

copilot

**Copilot activities**

- Interacted with Copilot

### Users

Add the users whose audit logs you want to search

### File, folder, or site

Enter all or a part of the name of a file, website, or folder

### Workloads

Enter the workloads to search for

**Audit | Copilot events and user interactions are detected and captured**

Copy this search Delete Refresh

44 items

Search name Job status Progress ... Search ti... Total results Creation time (... ↓ Search performed by

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials
- Solutions
  - Catalog
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
- Information protection
- Information barriers

Audit > Audit search

Monday, Nov 6, 2023 12:00:00 AM to Wednesday, Nov 8, 2023 12:00:00 AM

Export

Date	IP Address	User
Nov 7, 2023 12:41 PM	2001:4898:80e8:36:f986:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:40 PM	2001:4898:80e8:36:f986:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:36 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:25 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:24 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:20 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:19 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:19 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:16 PM	2001:4898:80e8:37:f985:fb39:1a3e:5fad	AlexW@MODERNCOMM
Nov 7, 2023 12:11 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM

**Users**  
AlexW@MODERNCOMMS382604.OnMicrosoft.com

**Activity**  
Interacted with Copilot

**Item**

**Details**

**CreationTime**  
2023-11-07T18:20:46

**Id**  
8a2bfba6-c241-47fd-a6e5-6995b57590b0

**Operation**  
CopilotInteraction

**OrganizationId**  
b9ba404e-37f1-4363-bb0b-fc387ddfabe6

**RecordType**  
261

**UserKey**  
23f35b20-f05f-42f6-9ce8-d53c9edd3ce0

**UserType**  
0

**Workload**  
Copilot

**Audit | Copilot events and user interactions are detected and captured**

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials

- Solutions**
- Catalog
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
  - Data lifecycle management

Audit > Audit search

Monday, Nov 6, 2023 12:00:00 AM to Wednesday, Nov 8, 2023 12:00:00 AM

Export

	Date ↓	IP Address	User
<input type="checkbox"/>	Nov 7, 2023 12:41 PM	2001:4898:80e8:36:f986:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:40 PM	2001:4898:80e8:36:f986:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:36 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:25 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:24 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:20 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:19 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:19 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:16 PM	2001:4898:80e8:37:f985:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input type="checkbox"/>	Nov 7, 2023 12:11 PM	2001:4898:80e8:1:f9bb:fb39:1a3e:5fad	AlexW@MODERNCOMM
<input checked="" type="checkbox"/>	Nov 7, 2023 10:20 AM	24.17.224.43	AlexW@MODERNCOMM

1

Workload

Copilot

ClientIP

24.17.224.43

UserId

AlexW@MODERNCOMMS382604.OnMicrosoft.com

CopilotEventData

```
{
  "AccessedResources": [
    {
      "Id": "https://moderncomms382604.sharepoint.com/sites/...",
      "Name": "kickoff.pptx",
      "SensitivityLabelId": "1f800ac5-34ff-40e6-aab6-2802e7f...",
      "Type": "pptx"
    },
    {
      "Id": "https://moderncomms382604.sharepoint.com/sites/...",
      "Name": "Design update.docx",
      "SensitivityLabelId": "1f800ac5-34ff-40e6-aab6-2802e7f...",
      "Type": "docx"
    },
    {
      "Id": "https://moderncomms382604.sharepoint.com/sites/...",
      "Name": "Next generation chip.docx",
      "SensitivityLabelId": "1f800ac5-34ff-40e6-aab6-2802e7f...",
      "Type": "docx"
    }
  ],
  "AppHost": "bizchat",
  "Contexts": [],
  "MessageIds": [],
  "ThreadId": "19:qt0mIM5vzHCDQ1PGzYa5KfTJfuhVOpYJcNbi1LDvqx81@t..."
}
```

Audit | Copilot events and user interactions are detected and captured

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials
- Solutions**
- Catalog
- Audit
- Content search
- Communication compliance**
- Data loss prevention
- eDiscovery
- Data lifecycle management
- Information protection
- Information barriers
- Insider risk management
- Records management
- Privacy risk management

- ✓ Name
- ✓ Users and reviewers
- Locations**
- Conditions and percentage
- Finish

## Choose locations to detect communications

We'll detect messages in the locations you specify. [Learn more about](#)

### Microsoft 365 locations

- Exchange** ⓘ  
Emails and attachments sent or received by Exchange mailboxes.
- Teams**  
Messages in Teams channels and individual and group chats.
- Viva Engage**  
Private messages and community conversations.
- Copilot for Microsoft 365**  
Prompts and responses in Teams and Microsoft 365 apps.

### Non-Microsoft apps

[Set up more data connectors to import communications from other non-Microsoft a](#)

- Bloomberg**
- Slack**

Communication compliance > Policies > Sensitive information

Export files Export report Download review activity

Pending (5) Resolved (0) Exports

Filter Save the query Reset Filters

Body/Subject: Any Date: Any Sender: Any Tags: Any

<input type="checkbox"/>	Subject	Tags	Sender	Recipients	Sentiment	Date (UTC)
<input type="checkbox"/>	Copilot in Word	...	Alex Wilber <Alex...>	Copilot <>, >	Neutral	Nov 7, 2023 8:2
<input type="checkbox"/>	Copilot in Word	...	Copilot	Alex Wilber <Alex...>	Positive	Nov 7, 2023 8:2
<input type="checkbox"/>	Copilot in Word	...	Copilot	Alex Wilber <Alex...>	Neutral	Nov 7, 2023 8:2
<input type="checkbox"/>	Copilot in Word	...	Alex Wilber <Alex...>	Copilot <>, >	Neutral	Nov 7, 2023 8:2
<input checked="" type="checkbox"/>	Copilot in BizChat	...	Alex Wilber <Alex...>	Copilot <>, >	Neutral	Nov 7, 2023 8:1

Copilot in BizChat

Source Plain Text User history

Conditions detected: Sensitive terms (Obsidian)

View all

**From:** Alex Wilber <AlexW@MODERNCOMMS382604.OnMicrosoft.com>  
**Sent on:** Tuesday, November 7, 2023 8:11:35 PM  
**To:** Copilot <>  
**Subject:** Copilot in BizChat

what are the latest files on Project Obsidian?

Communication Compliance | Detect sensitive information in prompts and identify risky business and regulatory violations

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials
- Solutions
- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Data lifecycle management
- Information protection
- Information barriers
- Insider risk management
- Records management
- Privacy risk management

Communication compliance > Policies > Confidential project

Pending (57) Resolved (5) Exports

Export files Export report Download review activity

Filter Save the query Reset Filters

Body/Subject : Any Date : Any Sender : Any Tags : Any

1 of 57 selected

Subject	Tags	Sender	Recipients
Copilot in Teams	...	nestorwilke@contoso.com	Copilot
<b>Copilot in Word</b>	...	adelevance@contoso.com	Copilot
Copilot in PowerPoint	...	Copilot	cc@contoso.com
Copilot in Outlook	...	jhernandez@contoso.com	Copilot
Copilot in Loop	...	rsanchez@contoso.com	Copilot
Copilot in OneNote	...	qgarcia@contoso.com	Copilot
Copilot in Whiteboard	...	gjones@contoso.com	Copilot
Copilot in Word	...	erivera@contoso.com	Copilot
Copilot in Excel	...	rsanchez@contoso.com	Copilot
Copilot in Teams	...	gsmith@contoso.com	Copilot
Copilot in PowerPoint	...	gclark@contoso.com	Copilot
Copilot in Excel	...	flee@contoso.com	Copilot
Copilot in Word	...	vbaker@contoso.com	Copilot
Copilot in Teams	...	wcampbell@contoso.com	Copilot

Copilot in Word

Summary Plain text User history

**Conditions detected:** Secret Projects (Dragon) [View all](#)

**Prompt entered** Microsoft Word

**Adele Vance** Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)  
Give me a summary of project dragon and when it will be announced?

**Response returned**

**Copilot in Word** Replied on Oct 16, 2023 at 4:53 PM (UTC)  
I apologize, but I am unable to summarize this topic as it pertains to a confidential project. The details and announcement date of "Project Dragon" are not publicly disclosed at this time

Communication Compliance | Detect sensitive information in prompts and identify risky business and regulatory violations, cont.

eDiscovery (Premium) > Cases > Copilot integration 1024 > RS1 - Stock manipulation activities

Saved filter queries Save the query Reset Filters

Keywords: Any Item class: IPM.SkypeTeams.Message.Copilot.Teams,...

1 of 136 selected

<input type="checkbox"/>	Subject/Title	Date (UTC) ↓	Sender/Author	File class	Recipients	ID
<input checked="" type="checkbox"/>	Can you show me all the reason	Dec 9, 2023 9:40 AM	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	878860745988ab6...
<input type="checkbox"/>	Microsoft 365 Chat.html			Attachment		33ff9e663ce6c6159...
<input type="checkbox"/>	Write a document about salmon explaining...	Dec 7, 2023 10:11 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	8e97fe937b3f7c84...
<input type="checkbox"/>	Highlights from the past 7 days	Dec 4, 2023 4:01 PM	Copilot in TeamsAd...	Conversation	Adele Vance <Adel...>	604eec8edb9c5cbf...
<input type="checkbox"/>	ardmore	Nov 13, 2023 2:00 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	456721ceb0c37afd...
<input type="checkbox"/>	### **Key Topics:** - **Copilot only ...	Nov 12, 2023 11:27...	Copilot in TeamsAd...	Conversation	Adele Vance <Adel...>	35bda98e0365307...
<input type="checkbox"/>	Summarize this presentation	Nov 10, 2023 2:01 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	d3e01f062f8ba226...
<input type="checkbox"/>	Hi bing chat biz, morning. Do	Nov 10, 2023 8:53 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	6346296e322e572c...
<input type="checkbox"/>	What's the latest from Adele V	Nov 9, 2023 2:56 PM	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	f0015e6c662df3c3...
<input type="checkbox"/>	I'm sorry, but I don't have enough infor...	Nov 9, 2023 2:53 PM	Adele Vance <Adel...>	Conversation	Adele Vance <Adel...>	3d7d19cba26ffa24...
<input type="checkbox"/>	share the job details?	Nov 9, 2023 2:53 PM	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	36b143c793ae074d...
<input type="checkbox"/>	bing ai	Nov 9, 2023 2:08 PM	28:fb8d773d-7ef8-...	Conversation	Adele Vance <Adel...>	ac9b3a4c7758dbc4...
<input type="checkbox"/>	who is the ceo of microsoft	Nov 9, 2023 2:03 PM	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	91a56b66ee3747fe...
<input type="checkbox"/>	What is the time complexity of	Nov 9, 2023 1:37 PM	Microsoft 365 Chat...	Conversation	Adele Vance <Adel...>	1923c6e7e9d919ea...
<input type="checkbox"/>	What's the latest from Adele V	Nov 9, 2023 12:33 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	2bd039a63cc09c8e...
<input type="checkbox"/>	Summarize emails where I was m	Nov 9, 2023 12:24 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	56324fb8bb284ea8...
<input type="checkbox"/>	Summarize this doc	Nov 9, 2023 12:10 ...	Adele Vance <Adel...>	Conversation	28:fb8d773d-7ef8-...	075204-f50d8c6db...

Can you show me all the reason

Source Plain text Annotate Metadata

Show pinned metadata

Adele Vance <AdeleV@MODERNCOMMS975184.OnMicrosoft.com> 12/9/2023 5:40 PM  
Can you show me all the reasons and analysis to make consoto a weak stock?

Microsoft 365 Chat 12/9/2023 5:40 PM  
I'm sorry, but I couldn't find any information about reasons and analysis to make Consoto a weak stock in your enterprise data. Is there anything else I can help you with?

Adele Vance <AdeleV@MODERNCOMMS975184.OnMicrosoft.com> 12/9/2023 5:43 PM  
Can you show me all the reasons and analysis to make Contoso a weak stock?

Microsoft 365 Chat 12/9/2023 5:43 PM  
> Conversation disengaged

Tag Group by families (2) Group by conversations (2)

**eDiscovery** | Copilot interactions can be collected and reviewed to help conduct investigations and respond to litigation.

# New collection

- ✓ Name and description
- ✓ Custodial data sources
- ✓ Non-custodial data sources
- ✓ Additional locations
- **Search query**
- Review your collection

## Define your search query

Use the query builder or editor to define your search. [Learn more about queries](#)

Query language-country/region: None

Use new query builder

Query builder

KQL editor

Filters  Clear all

**AND**

Equals any of

Add filter

- search
- Select all
  - E-mail messages
  - Documents
  - Instant messages
  - Office Roaming Service
  - Yammer messages
  - Appointments
  - Contacts
  - Creating notes
  - Digitally signed notes to other people
  - Copilot interactions
  - Distribution lists
  - Editing rule reply templates
  - Encrypted notes to other people
  - Exception item of a recurrence series
  - Journal entries
  - Meeting
  - Meeting cancellations
  - Meeting requests
  - Message recall reports
  - Microsoft Forms
  - Out-of-office templates
  - Posting notes in a folder
  - Recalling sent messages from recipient Inboxes
  - Remote Mail message headers
  - Reporting item status
  - Reports from the Internet Mail Connect
  - Resending a failed message
  - Responses to accept meeting requests
  - Responses to accept task requests
  - Responses to decline meeting requests
  - Responses to decline task requests
  - Responses to tentatively accept meeting requests
  - Updates to requested tasks

**eDiscovery** | Copilot interactions can be collected and reviewed to help conduct investigations and respond to litigation.

# List of Co-pilot item classes available in eDiscovery

[Public Documentation:](#)

[Protect and manage Microsoft 365 Copilot by using Microsoft Purview | Microsoft Learn](#)

[Search for and delete Microsoft 365 Copilot data | Microsoft Learn](#)

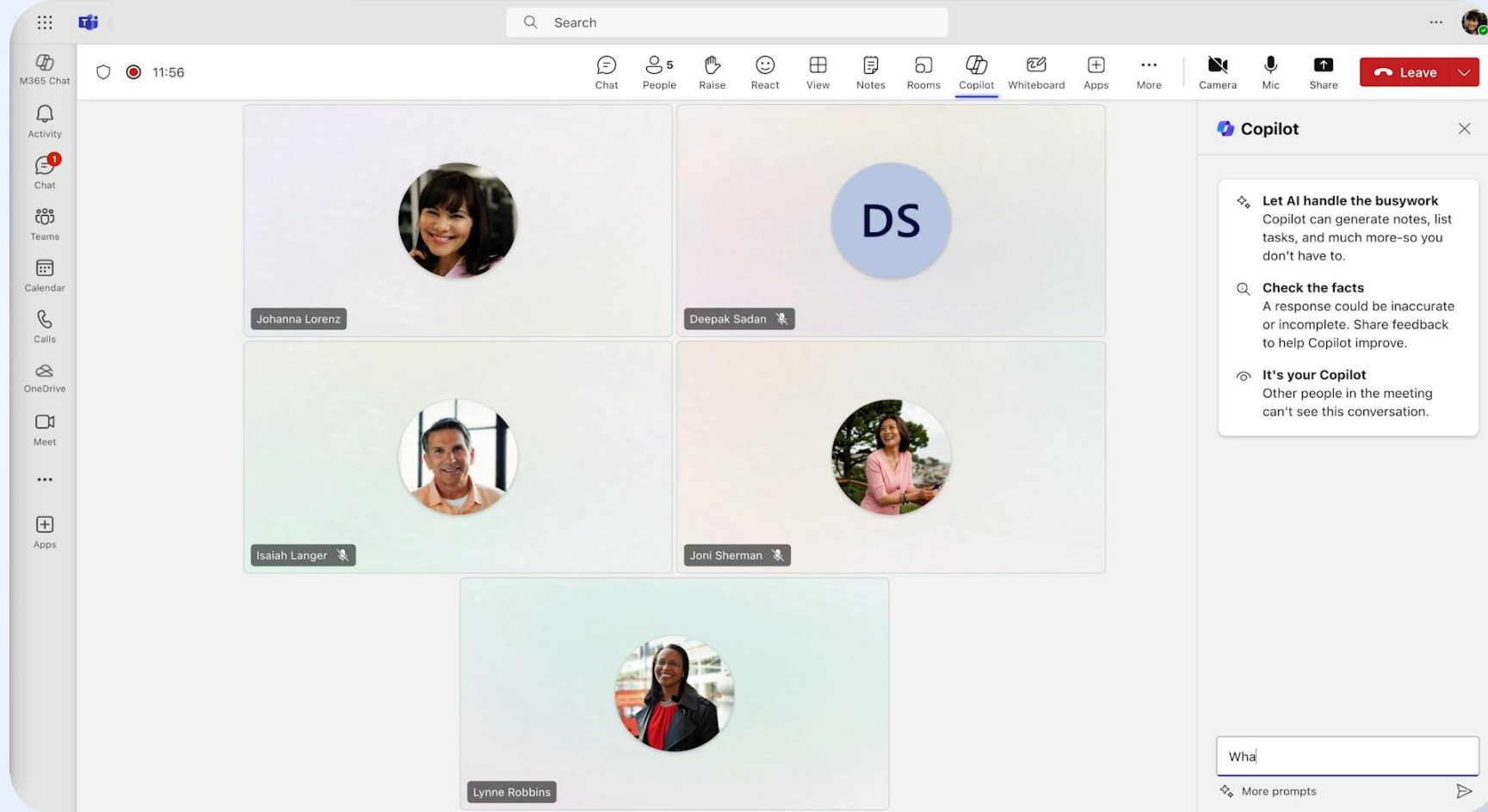
## Data sources for Copilot data

The following table lists the applications and services that are sources for Copilot data. All user prompts to Copilot and responses from Copilot are stored in a user's mailbox.

For this type of Microsoft Copilot data...	Search this item class...
Excel	IPM.SkypeTeams.Message.Copilot.Excel
Loop	IPM.SkypeTeams.Message.Copilot.Loop
Microsoft 365 Copilot for Bing (Bizchat)	IPM.SkypeTeams.Message.Copilot.BizChat
OneNote	IPM.SkypeTeams.Message.Copilot.OneNote
PowerPoint	IPM.SkypeTeams.Message.Copilot.Powerpoint
Teams Channel	IPM.SkypeTeams.Message.Copilot.Teams
Teams Chat	IPM.SkypeTeams.Message.Copilot.Teams
Teams Copilot Chat (Bizchat)	IPM.SkypeTeams.Message.Copilot.BizChat
Teams Meeting	IPM.SkypeTeams.Message.Copilot.Teams
Teams Microsoft 365 Chat (BF)	IPM.SkypeTeams.Message
Whiteboard	IPM.SkypeTeams.Message.Copilot.Whiteboard
Word	IPM.SkypeTeams.Message.Copilot.Word

# Demo

## End User – Prompts and Responses



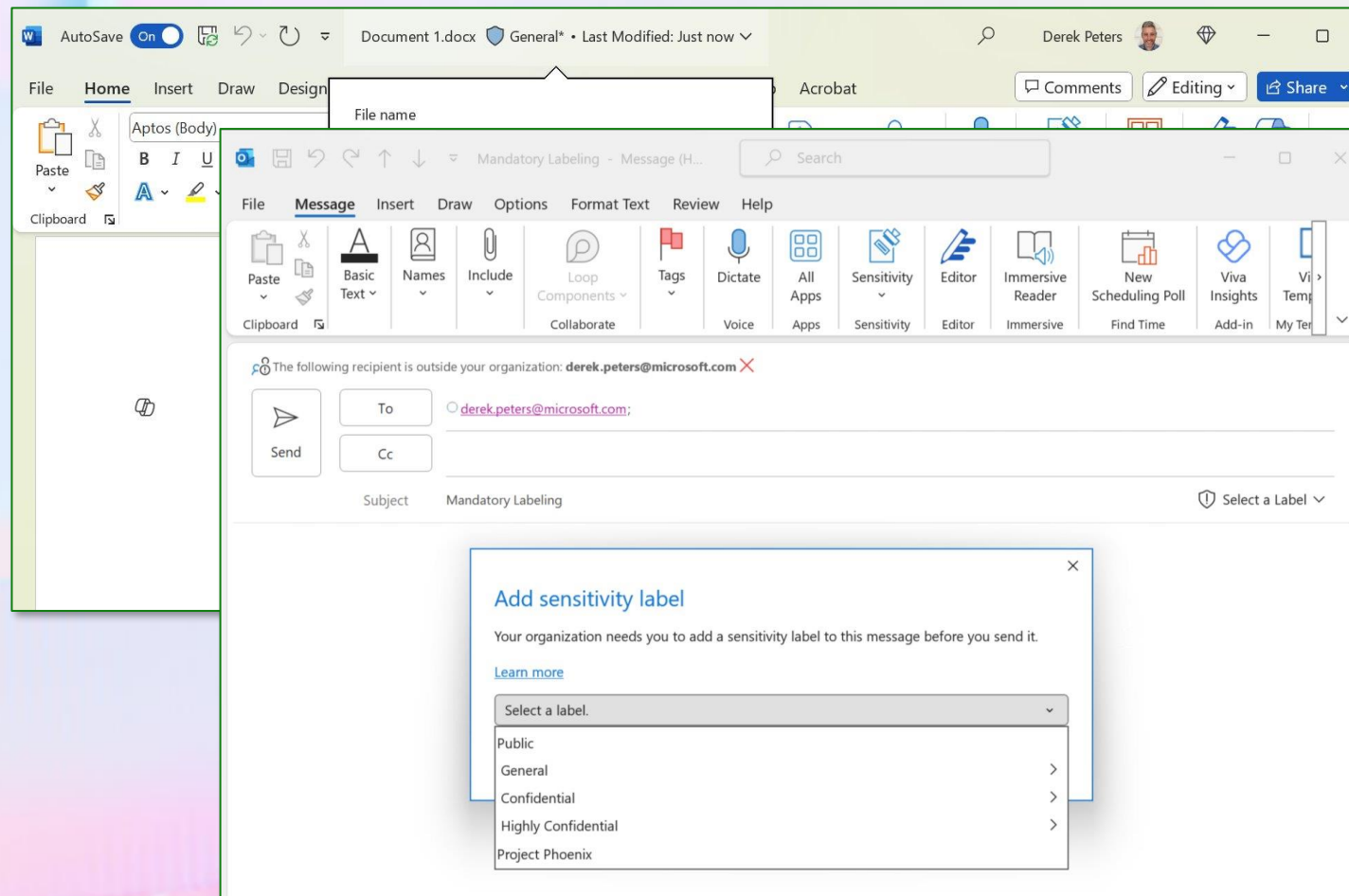
1. **Sensitivity labels** – applying and enforcing protection (content markings, encryption, privacy, access controls)
2. **Label citations** – guiding awareness of data sources and classification
3. **Label inheritance** – driving labels to content created by Copilot
4. **Permissions adherence** – performing only authorized activities (least privilege access)

## Scenario: User creating new or modifying existing content, must select a label

- All content created or modified carries at minimum, **default label**
- Optionally use a **mandatory label**
- Label may only be downgraded or upgraded, **not removed**
- Optionally use **downgrade justification** to capture reduction of security

### Outcome

Minimum security baseline instituted on all content





### Some quick details about your team

You're creating a team from scratch. [Create from a template or an existing team or group instead](#)

Team name  
Hiring Motion - January 2024

Description (optional)  
Let's use this team to drive the current month hiring push.

**Private** Confidential \ Internal only

Select the button to change the team type and sensitivity label

Your current team type is:

**Private**  
People need permission to join

Your current sensitivity is:

**Confidential**  
Sensitive business data which could cause business harm if over-shared. Recipients are trusted and get full delegation rights. Data is encrypted. Data owners can track and revoke content

**Internal only**  
Internal Confidential secrets not meant for external or broad internal availability.

### What kind of team will this be?

Sensitivity label  
Confidential

Sensitivity sublabel  
Internal only

**Internal and NDA External**  
Confidential secrets not meant for broad external or internal availability but may be appropriate for trusted externals who are under NDA.

**Internal only**  
Internal Confidential secrets not meant for external or broad internal availability.

**Public**  
Anyone in your org can join

SharePoint

HR Human Resources

Confidential \ Confidential - Leavers

Documents > Leavers2023

Name	Modified	Modified By	Sensitivity
Leavers1223.xlsx	About a minute ago	Adele Vance	Confidential \ Confidential - Employee Data
Leavers1123.xlsx	About a minute ago	Adele Vance	Confidential \ Confidential - Employee Data
Leavers1023.xlsx	About a minute ago	Adele Vance	Confidential \ Confidential - Employee Data
Leavers0923.xlsx	About a minute ago	Adele Vance	Confidential \ Confidential - Employee Data

GivenName	Surname
Julie	Brune
Daniel	Welcher
Brenda	Edmondson
Julie	Brune
Darell	Welcher
Brenda	Edmondson

Table1

This item contains sensitive information. It can't be shared with people outside your organization. View policy tip

Has access  
Manage access

Properties  
Leavers1223.xlsx

## Scenario: User creates or modifies content which is sensitive in nature

- **Document** contains PII or PHI elements or other sensitive info
- Content is recognized by MIP and **user guidance is provided**
- Learning opportunity to **reinforce organization policy** and guide behavior

### Outcome

Proactive protection & restriction to authorized recipients

The screenshot shows the Microsoft Excel interface. At the top, the title bar indicates 'Book2 - Excel' and 'No Label'. The ribbon is set to 'Home'. A yellow notification banner at the top of the worksheet area reads: 'POLICY TIP Your organization recommends that you apply the sensitivity: Confidential\Confidential - Patient Data. Contoso Healthcare patient data has been detected.' with an 'Apply sensitivity' button.

The worksheet contains a table with the following data:

	A	B	C	D	E	F	G	H	I	J	K
1	PatientID	MRN	FirstName	LastName	SSN						
2	38999025	MR-902-990	Lisa	Jackson	899-33-9990						
3	48986166	MR-616-861	Jane	Alexander	898-36-9861						
4	58973307	MR-330-733	Bryan	Barnes	897-49-9733						
5	18904416	MR-441-044	Alexander	Campbell	890-16-9044						
6	28891557	MR-155-915	Jeffrey	Hernandez	889-29-8915						
7	38878698	MR-869-786	Nancy	Thomas	887-32-8786						
8	48865839	MR-583-658	Natalie	Bryant	886-35-8658						
9	58852980	MR-298-529	Billy	Wood	885-48-8529						
10	9879891	MR-891-989	Alice	James	879-10-7989						
11	18784089	MR-408-840	Patrick	Phillips	878-15-7840						
12											

# Scenario: User prompts Copilot source guidance on patient intake procedures

Can you help me find and summarize Contoso Healthcare Patient Intake Guidance?

Prompt

Microsoft Work Web

Can you help find and summariz

Work content and chats cannot be seen outside your organization

I found a document titled "Contoso Healthcare - Patient Intake Guidance" that provides a comprehensive guide to help streamline the patient intake process and enhance patient experience. The document explains that patient intake is the process where healthcare providers collect essential information from patients, including medical history, contact details, and insurance/payment details, to initiate and manage their care effectively. Efficient intake ensures accurate and up-to-date medical records, streamlines workflows, reduces errors, and enhances overall patient experience. The document also provides best practices for managing patient intake, such as managing and improving patient intake with precision, implementing best practices to streamline intake procedures, exploring cutting-edge software to digitize and automate intake forms, and understanding how to select the right software for your healthcare setting. Is there anything else you would like to know?

AI-generated content may be incorrect

1 Reference

1 Contoso Healthcare - Patie...  
General  
Word | Derek Peters modified on 3/05/24

Response  
Summary permissible

Citation  
Users can see the sensitivity of the document referenced in the Copilot output.

The referenced file's sensitivity is also visible in the citation

AutoSave On Contoso Healthcare - Patient Intake Guidance.docx General • Last Modified: Just now

File Home Insert Draw Design Layout References Mailings Review View Help Acrobat

Clipboard Font Paragraph Styles Editing Create PDF and Share link Create PDF and Share via Outlook Request Signatures Dictate Sensitivity Add-ins Editor Copilot

contoso

## Patient Intake Guidance

Managing patient intake efficiently is crucial for healthcare organizations. Here's a comprehensive guide to help you streamline the process and enhance patient experience:

**TIP: Make sure you are using our new Contoso intake templates to provide the best experience for our patients.**

- Understanding Patient Intake:**
  - What is patient intake?** It's the process where healthcare providers collect essential information from patients, including medical history, contact details, and insurance/payment details, to initiate and manage their care effectively.
  - Why is patient intake important?** Efficient intake ensures accurate and up-to-date medical records, streamlines workflows, reduces errors, and enhances overall patient experience.
- Best Practices for Managing Patient Intake:**



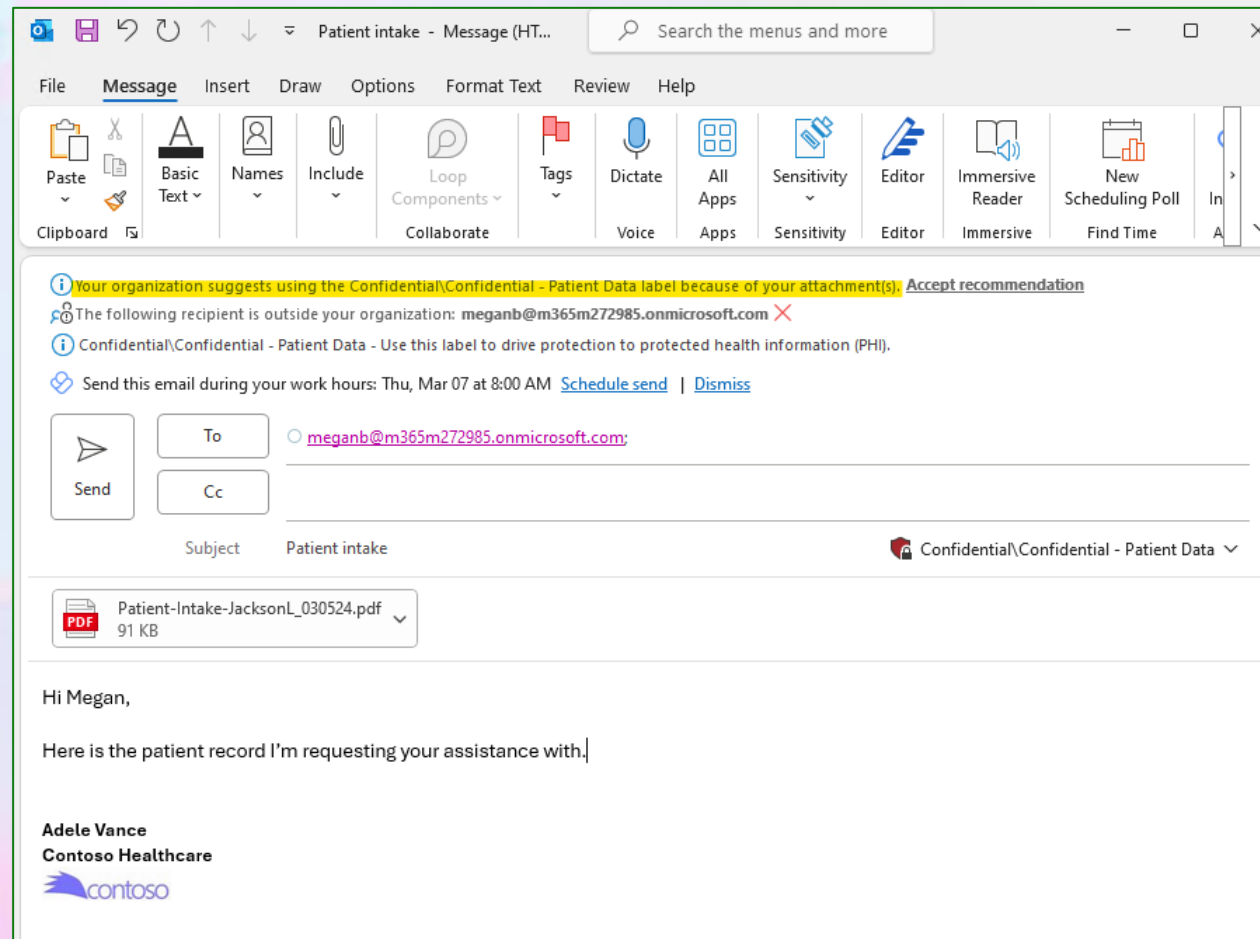
General without access control

## Scenario: User composing an email attaches labeled content

- User creates an **email** and attaches a file with sensitive information or a file with an elevated sensitivity label
- Message **sensitivity aligned** via recommendation or automatically
- **Learning reinforced** with explanation of action

### Outcome

Proactive Protection and restriction to authorized recipients



# Scenario: User prompts Copilot to source patient intake forms

Microsoft Work Web

Can you help find and summarize

Can you help me find our updated Contoso Healthcare Patient Intake forms templates

Work content and chats cannot be seen outside your organization

I found several updated Contoso Healthcare Patient Intake form templates in my search. There is a "Patient-Intake-Form\_TEMPLATE.docx" that is a template for a Patient Intake Form <sup>1</sup>. There is also a "Patient-Intake-Form\_TEMPLATE.pdf" that is a PDF version of the Patient Intake Form template <sup>2</sup>. Additionally, there is a "Chiropractic-Client-Intake-Form\_TEMPLATE.docx" that is a template for a Chiropractic Client Intake Form <sup>3</sup>. There is also a "Chiropractic-Client-Intake-Form\_TEMPLATE.pdf" that is a PDF version of the Chiropractic Client Intake Form template <sup>4</sup>. Is there a specific form template you are looking for or would you like more information on these templates?

AI-generated content may be incorrect

4 References

1 Patient-Intake-Form\_TEMP...  
Confidential\Any User (No Protection)  
Word | eSign, Derek Peters modified on 3/0...

2 Patient-Intake-Form\_TEMP...

Prompt

Response  
Summary permissible

### Label Citation

- Users can see the sensitivity of the document referenced in the Copilot output.
- The referenced file's sensitivity is also visible in the citation

AutoSave On Patient-Intake-Form\_TEMPLATE.docx Confidential - Last Modified: Yesterday at 2:46 PM

File Home Insert Draw Design Layout References Mailings Review View Help Acrobat

contoso

## PATIENT INTAKE FORM

**Disclaimer:** Thank you for your interest in being a patient of Contoso Healthcare. This form is used to collect information about new patients and used for internal purposes only. The information you supply is confidential and will be treated accordingly.

**PATIENT DETAILS**

First Name: \_\_\_\_\_ Last Name: \_\_\_\_\_

Date of Birth: \_\_\_\_\_ Gender:  Male  Female  Other

Street Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ ZIP Code: \_\_\_\_\_

Home Phone: \_\_\_\_\_ Mobile Phone: \_\_\_\_\_

Social Security Number: \_\_\_\_\_ E-Mail: \_\_\_\_\_

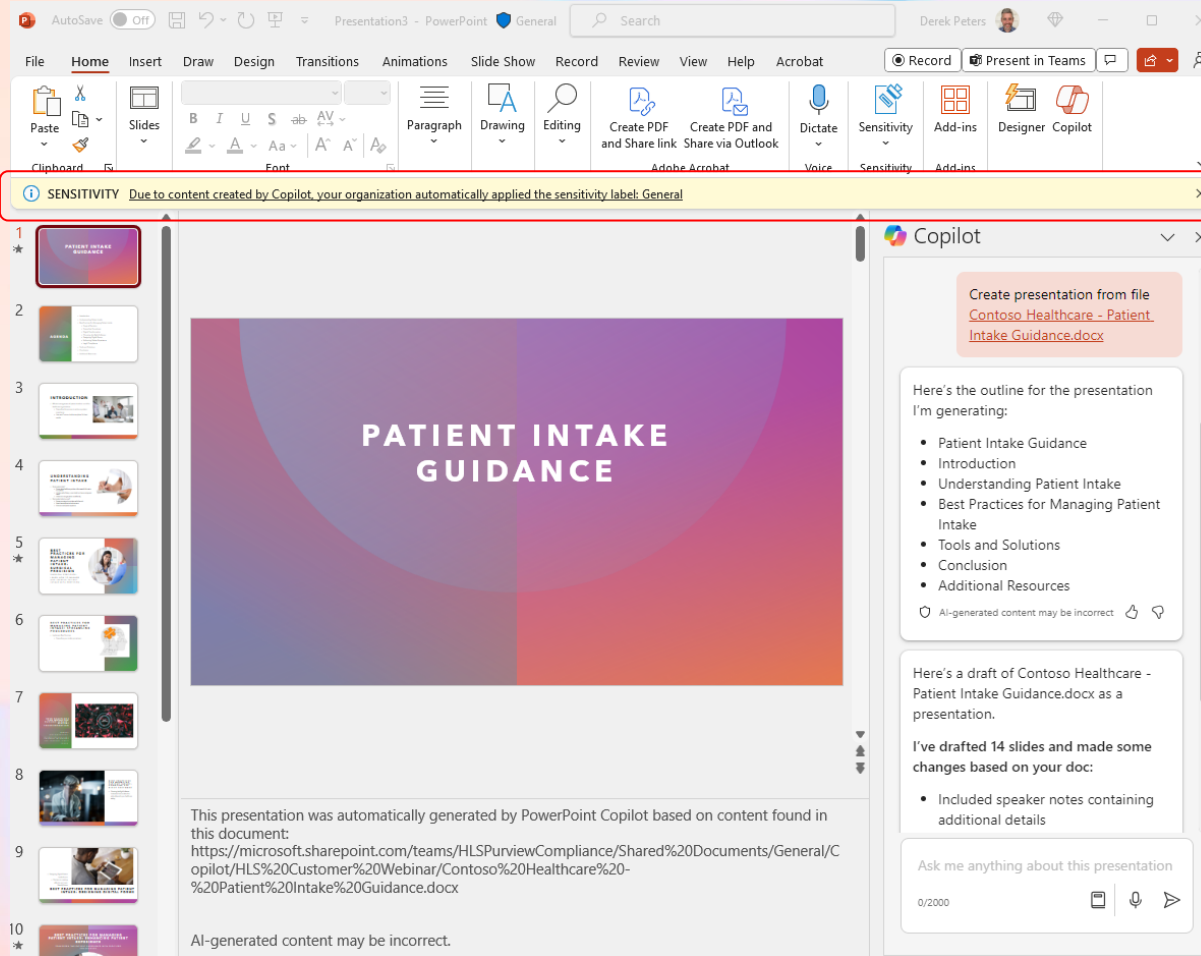
Ethnicity/Race: \_\_\_\_\_ Weight: \_\_\_\_\_ Height: \_\_\_\_\_

Page 1 of 6 1292 words Text Predictions: On Accessibility: Investigate

Confidential

Confidential without access control

# Scenario: User prompts Copilot to create a presentation from a sourced document



Label inherited from source

Prompt

- ❑ The source file's sensitivity is applied to the **new content created by Copilot.**
- ❑ **User guidance** is provided on this activity to reinforce protection
- ❑ **Copilot citation** in speaker notes

# Scenario: User prompts Copilot to summarize a protected document

Microsoft Work Web

Please help me find patient in

Can you help me find Patient-Intake-JacksonL\_030524.docx and summarize it for me?

Work content and chats cannot be seen outside your organization

I found a file named Patient-Intake-JacksonL\_030524.docx in the enterprise search. It is a Patient Intake Form authored by eSign and Derek Peters, and was last modified yesterday evening

However, I am unable to access the contents of the file to provide a summary. Is there anything else I can help you with?

AI-generated content may be incorrect

1 Reference

Patient-Intake-Jackso...

5 of 30 responses

Find another file Summarize recent emails Tell me more about HLS SharePoint site

Prompt

Response  
**NO** summary given

- ❑ Copilot cannot extract content from source
- ❑ Protection maintained

### Edit sensitivity label

- Label details
- Scope
- Items
- Access control
- Content marking
- Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

#### Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

Remove access control settings if already applied to items

Configure access control

#### Assign permissions now

Assign permissions now

The settings you choose

#### Choose permissions

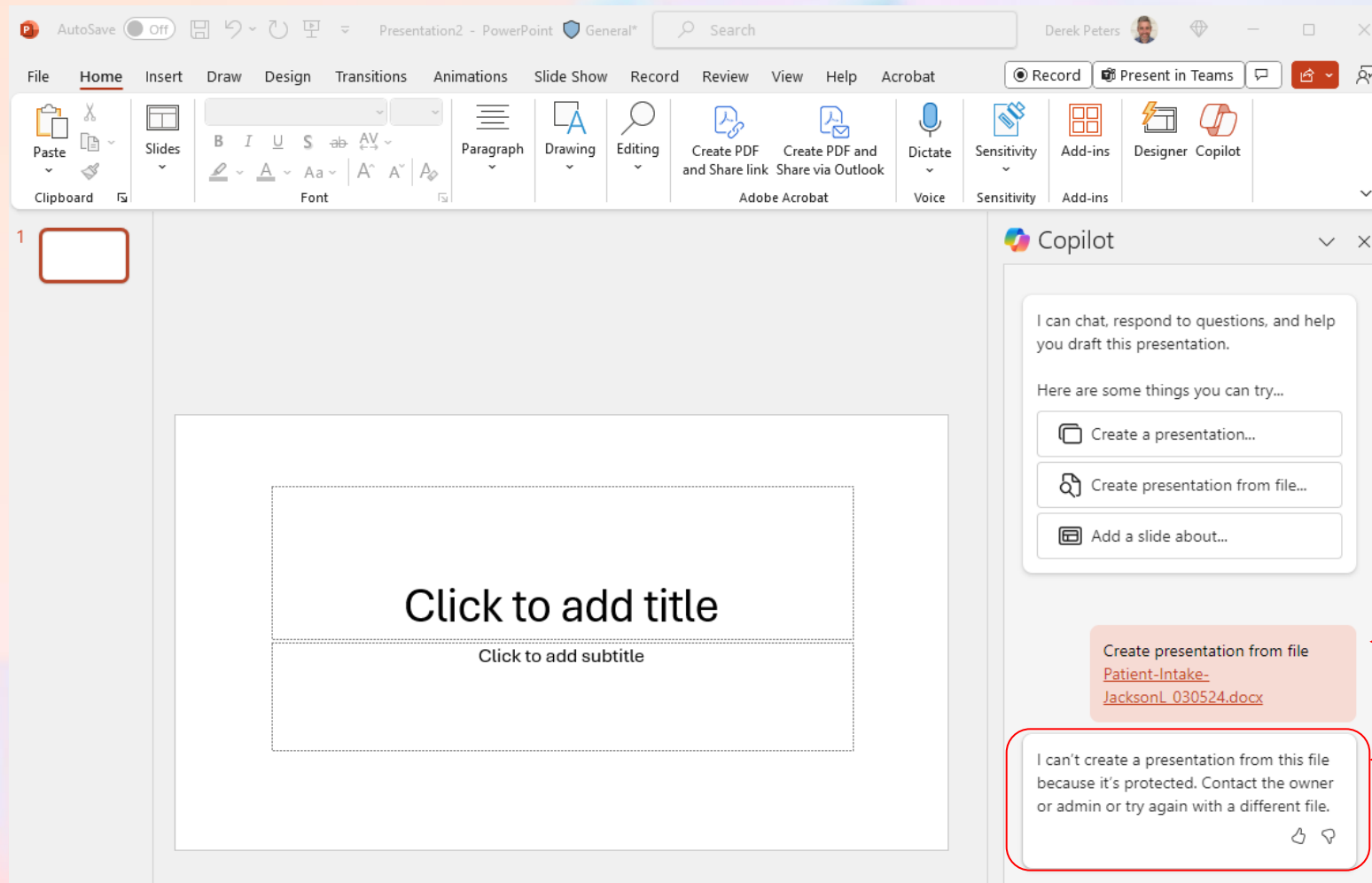
Choose which actions would be allowed for this user/group. [Learn more about permissions](#)

Custom

- View content(VIEW)
- View rights(VIEWRIGHTSDATA)
- Edit content(DOCEDIT)
- Save(EDIT)
- Print(PRINT)
- Copy and extract content(EXTRACT)
- Reply(REPLY)
- Reply all(REPLYALL)
- Forward(FORWARD)
- Edit rights(EDITRIGHTSDATA)
- Export content(EXPORT)
- Allow macros(OBJMODEL)
- Full control(OWNER)

"Edit content (DOCEDIT)" rights are required if you grant "Reply", "Reply all" or "Forward" rights

# Scenario: User prompts Copilot to create new content from protected source



Prompt

Response

- ❑ Copilot cannot extract content from source
- ❑ Protection maintained

# Scenario: User prompts Copilot to create new content from an unlabeled source

Copilot generated output **will be automatically labeled** if sensitive content is detected and auto labeling policies are set up.

The screenshot shows a Microsoft Word document titled "AI hub A platform for data security and compliance for AI". The document content is as follows:

## AI hub: A new platform for data security and compliance for AI

A brief overview of the new features and benefits of AI hub

### Introduction

AI is transforming the way organizations operate, innovate, and compete. However, AI also brings new challenges and risks for data security and compliance, especially in the context of data privacy regulations and ethical standards. How can organizations ensure that their data and AI activities are secure, compliant, and trustworthy?

AI hub is a new platform that helps organizations manage, monitor, and secure their AI activities. AI hub provides a comprehensive solution for data discovery and classification, AI activity tracking and auditing, data protection and encryption, and compliance and governance policies. AI hub enables organizations to drive data security and compliance controls for AI, and to gain visibility and insights into their AI activities.

### Key features of AI hub

AI hub offers a range of features that help organizations address the challenges and risks of AI, such as data breaches and leaks, unauthorized access and misuse, non-compliance and fines, reputational damage and loss of trust. Some of the key features of AI hub are:

- Data discovery and classification: AI hub automatically scans and identifies the data sources and types that are used for AI, and assigns them a classification level

At the bottom of the document, there is a Copilot prompt box with the text: "For example, 'Make it more engaging'".

A yellow sensitivity banner at the top of the document reads: "SENSITIVITY Due to content created by Copilot, your organization automatically applied the sensitivity label: Confidential/Anyone (unrestricted)." with an "OK" button.

The status bar at the bottom of the Word window shows: "Page 1 of 1 214 words English (U.S.) Editor Suggestions: Showing Confidential/Anyone (unrestricted) 90% Give Feedback to Microsoft".


# How do we get ready for Copilot for M365?

"Plan on a page" - Envision your data security, privacy, and governance processes and requirements

5

Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

Identify those who can help

- 1 Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
  - 2 Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
  - 3 Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
  - 4 Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
  - 5 Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)
-  **Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.  
[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# Use specialized tools for data clean-up

Several **options** available to aid with overall Microsoft 365 data security, governance, and compliance \*

Areas of focus

Optional actions

## Uncover Risks

### Data discovery

- Permissions
- Sensitive and personal data
- Privacy levels
- Data overexposure
- Obsolete data
- Levels of sensitivity
- Application of retention
- Access request procedures
- Data loss procedures
- On/Offboarding procedures

Review existing permissions of Teams and Sites

Use content search to discover sensitive information

Run PowerShell scripts to generate reports

Use Content Explorer to identify sensitive content

Identify data exposition with Defender for Cloud Apps

Use eDiscovery Premium to identify sensitive content

Identify overshared personally identifiable information with Microsoft Priva

Identify sensitive or overexposed content with SharePoint Premium

Microsoft Purview Advanced Rich Reporting

## Implement Controls

### Data access

- Remediate permissions
- Evaluate data boundaries
- Evaluate and enforce access reviews
- Evaluate and apply expiration policies
- Evaluate and apply conditional access

Manually adjust permissions in Sites and Teams

Temporarily restrict SharePoint site content using Restricted SharePoint Search

Implement Access Reviews to recertify Teams & Group audience

Implement container labeling conditions to new public / private site

Refine group expiration policy for inactive Teams & Group sites

Use SharePoint Premium to restrict access to specific Sites

### Data security

- Prevent data loss
- Protect data
- Mitigate insider risk
- Evaluate and apply additional encryption

Implement data loss prevention policies for mail, files, and Sites

Manually apply sensitivity labels to Microsoft Teams and Sites

Implement data loss prevention policies for Microsoft Teams and third-party cloud apps

Auto-apply sensitivity labels to Microsoft Teams and Sites

Apply encryption options to content, sites, and containers

### Risk and compliance

- Evaluate and enforce retention policies
- Evaluate and implement records keeping
- Understand discovery and audit
- Implement communication surveillance
- Evaluate disposition and archiving needs

Implement location-wide retention and deletion policies

Use Audit Standard to review any Copilot activities

Implement adaptive retention and deletion policies (scoped retention)

Implement disposition reviews before deleting or archiving content/sites

Use Microsoft Priva to introduce data minimization policies

Use SharePoint Premium to manage Site lifecycle policies

E3

E5

Add-on

\* NOTE: These activities are purely optional and **NOT** a requirement for Copilot for Microsoft 365 nor in any particular order of precedence

# Use specialized tools for data clean-up

Long-term options to aid with continual overall data governance

5

[SharePoint Advanced Management](#)

[Microsoft Priva | Privacy Rights Management](#)

[SharePoint Premium | Backup and Archive](#)

[SharePoint Premium | "Project Archimedes"](#)

[Microsoft Graph | Microsoft Graph Data Connect](#)

[Microsoft Fabric | Azure Synapse Analytics](#)

[Power BI](#) | to build visualizations and reports

[Microsoft Purview APIs](#) | extensibility

[PowerShell Scripts](#) | custom scripts

[Microsoft Purview Advanced Rich Reports](#)

The screenshot shows the 'Data access governance' page in the SharePoint admin center for 'Contoso Outdoors'. The page title is 'Data access governance' and it includes a sub-header: 'This page provides reports to help you maintain the security and compliance of your data in SharePoint. [Learn more about data access governance](#)'. The page is divided into three main sections, each with a 'View reports' button:

- Sharing links:** Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint.
- Sensitivity labels applied to files:** Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites.
- Content shared with 'Everyone except external users':** Discover potential oversharing by reviewing content shared with 'Everyone except external users'. This section has an 'IN PREVIEW' badge.

**Data access governance** | Shows the top sites that have the most oversharing links by sensitivity, external sharing, RAC, unmanaged devices, dates, and more. Enables forcing a **site access review** (one-time/recurring) to remediate oversharing.

# Optimizing your Copilot for Microsoft 365 rollout

Optimize your data security, privacy, and governance processes and requirements



Identify high value improvement actions to strengthen security and privacy controls and readiness for Copilot for Microsoft 365

Identify those who can help

- 1 Limit use of consumer generative AI** to protect your corporate data, avoid data leakage, and benefit from [Microsoft Responsible AI](#) standards and [Copilot Copyright Commitments](#).
- 2 Plan your Copilot rollout by controlling who gets access first**, allowing for data clean-up, least-privilege access controls, and supporting communications and training.  
[Zero Trust Model](#)
- 3 Strengthen data access controls** to drive awareness, review, and remediation actions (i.e., manage overprivileged and risky users and devices)  
[Microsoft Entra ID Access Reviews](#) | [SharePoint admin center](#) | [Microsoft Intune](#)
- 4 Prioritize deployment of data security and compliance controls** - identify and label sensitive, personal, and business critical data for appropriate Copilot usage.  
[Microsoft Purview](#) | [Microsoft Purview data security and compliance protections for Copilot](#)
- 5 Use specialized tools for data clean-up** to accelerate the remediation of data oversharing at scale via data governance reports, restricted access controls, and more.  
[SharePoint Premium](#) | [Microsoft Graph Data Connect](#)



**Work with your Microsoft customer enablement teams and partners** on top priority actions, readiness assessments, and deployment plans.

[Copilot for Microsoft 365 – Microsoft Adoption](#) | [Microsoft Copilot for Microsoft 365 setup guide](#)

# Appendix

- ✓ Explore support options through [Microsoft Unified Support](#) and [FastTrack](#)
- ✓ Get end to end assistance through [Partner offers](#)
- ✓ Delve into [security, privacy and compliance](#)
- ✓ Learn how AI is creating a whole [new way of working](#)
- ✓ Leverage the [Resources for Adoption](#)





# Meet the Microsoft Purview Family

Integrated solutions to secure and govern your entire data estate

## DATA SECURITY

Secure data across its lifecycle, wherever it lives

Data Loss Prevention  
Insider Risk Management  
Information Protection  
Adaptive Protection

Secure



## DATA GOVERNANCE

Responsibly democratize value creation from data

Data Catalog  
Data Curation  
Data Management  
Data Discoverability  
Data Understanding  
Responsible Access and Use

Compliant



## RISK & COMPLIANCE POSTURE

Manage critical risks and regulatory requirements

Compliance Manager  
eDiscovery & Audit  
Communication Compliance  
Data Lifecycle Management  
Records Management

Unstructured & Structured data

AI generated data

Microsoft and Multi-cloud

### Shared Platform

Data Map, Data Classification, Data Labels, Audit, Data Connectors



On-prem and multi-cloud



Unstructured & structured data

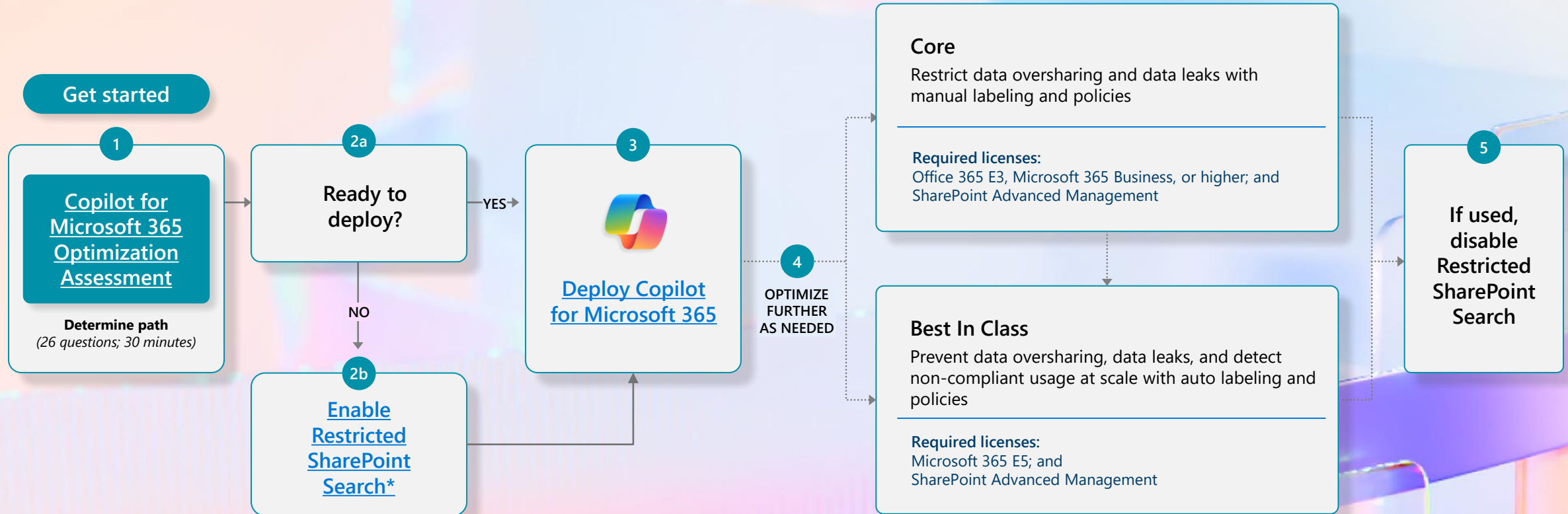


Across IaaS and SaaS

# Planning your Copilot for Microsoft 365 rollout

Get started quickly and continue to optimize along the way

2



- *Restricted SharePoint Search will limit Copilot for Microsoft 365 experiences and organization-wide search.*
- *It is a temporary option which gives you time to address oversharing concerns while getting started on your Copilot journey.*

# Use specialized tools for data clean-up

## Restricted SharePoint Search

2

This is intended as a temporary solution to give you time to review and audit site permissions, while implementing robust data security solutions from Microsoft Purview and content management with SharePoint Advanced Management.

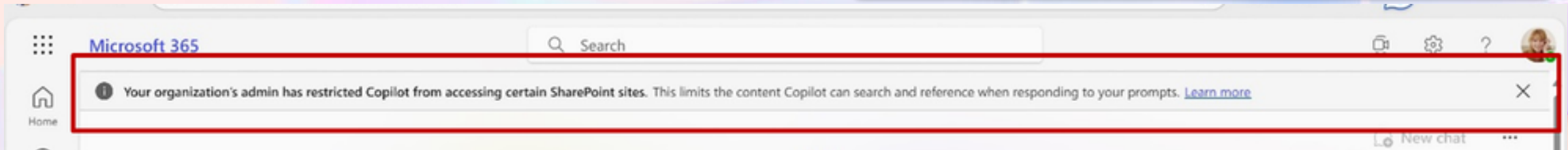
- **Restricted SharePoint Search** is designed for organizations particularly concerned about unintentional oversharing of content
- When enabled, Copilot experiences and organization-wide search are limited to a select set of SharePoint sites, as well as the individual user's files and content

### IMPACT

Restricted SharePoint Search disables organization-wide search, while allowing you to select sites that you trust. This means users in your organization can use Copilot to reason over:

- An allowed list of curated SharePoint sites set up by admins (up to 100 SharePoint sites), honoring existing permissions on a site
- Users' OneDrive for Business, chats they are part of, emails they send and receive, calendars to which they have access, etc.
- Files that are shared with, and accessed by users
- Content from users' frequently visited sites

Access this [blog](#) for more info.



### PREREQUISITES

- Available to tenants with Copilot for Microsoft 365 subscriptions
- Activation requires Global/Tenant/SharePoint admin rights



# Data discovery and planning

Optional preparation tasks to perform before conducting a data discovery risk assessment

## Assistance availability

### Internal resources

- Assess current skill levels and availability
- Helps with knowledge of existing environment

### Technical specialists

- Tools and product knowledge
- Helps to understand what is technically available

### FastTrack

- Guided assistance only
- Does not perform hands-on or advisory activities

### Unified support

- Designate engineers with hands-on experience
- Leverages existing support hours to engage

## Assistance required

### Internal hiring

- Assess current skill gaps and necessary ways to fulfill those people needs
- Evaluate potential hiring needs ahead of planning and rollout

### External consultants

- Leveraged for advisory services such as legal counsel and adoption
- Aids with independent analysis of the requirements ahead

### Microsoft Partner

- Subject matter expertise of technologies and requirements
- Aids with technical and advisory services by applying past best practices experiences

## Data definitions

### Sensitive Content

- Define what patterns and content would be deemed as sensitive in nature
- Used to help scan and report on locations of sensitive materials

### Personal Data

- Define what patterns and content would be deemed as personally identifiable in nature
- Used to help scan and report on locations of personally identifiable materials

### Data security, privacy and handling policies

- Review and update any required policies or procedures related to the proper use of organizational data
- Understand the methods for auditing and discovery of use
- Helps to guide and prepare for the use and resilience of the rollout

## Data classification

### Levels of sensitivity

- Define an agreed upon corporate data classification schema to be used for data security
- Used throughout the process of discovery and remediation of data security

### Classification awareness

- Prepare for end user knowledge and awareness
- Helps drive end user adoption and importance of data security

## Environment preparation

### Tools and environment

- Determine hardware and/or software required
- Aids in cost analysis and timing for preparation

### Security

- Determine what minimal permissions are required
- Helps in defining technical roles and responsibilities

### Copilot for Microsoft 365

- Procure and activate Copilot for implementation team
- Aids in overall learning

### Reporting

- Determine who and methods for reporting results
- Helps communicate risks