



Microsoft 365
COMMUNITY CONFERENCE

Secure and Govern Microsoft 365 Copilot

Remediate Oversharing, enforce Guardrails, and meet AI Regulations

April 22, 2026

© Copyright Microsoft Corporation. All rights reserved.





Sophie Ke
Sr. PMM



Dave Minasyan
Principal PM



**Microsoft
commitments
and controls**



**Microsoft 365
Copilot is built
on trust**



**Tools
to manage
Copilot data**

Microsoft commitments and controls



We secure your data
at rest and in transit



You control
your data



Your data is not used
to train or enrich
foundation models



You're protected
against AI security and
copyright risks



**Microsoft 365
Copilot is built
on trust**



Microsoft 365 Copilot



Microsoft Purview

Security & Governance

Honors your existing permissions

Supports your lifecycle policies and audit requirements

Protects against data loss and insider risk

Detect and investigation non-compliant and unethical usage

Assess Oversharing risks and apply recommended corrections

Guided assistance to remain compliant with AI Regulations

A complete solution for enterprise-ready AI

Tools to secure and govern Microsoft 365 Copilot



Microsoft Purview

Provides security, compliance, and governance across data and files



SharePoint Advanced Management

Included in  Microsoft 365 Copilot

Provides SharePoint site management and content governance capabilities

Problem summary

Microsoft 365 Copilot builds on the data already in Microsoft 365, prompting organizations to strengthen oversharing, data loss, and insider risks practices to support safe, confident adoption.

If grounding data and Copilot interactions are not secured, it could lead to



Access to information beyond what the user needs for their role



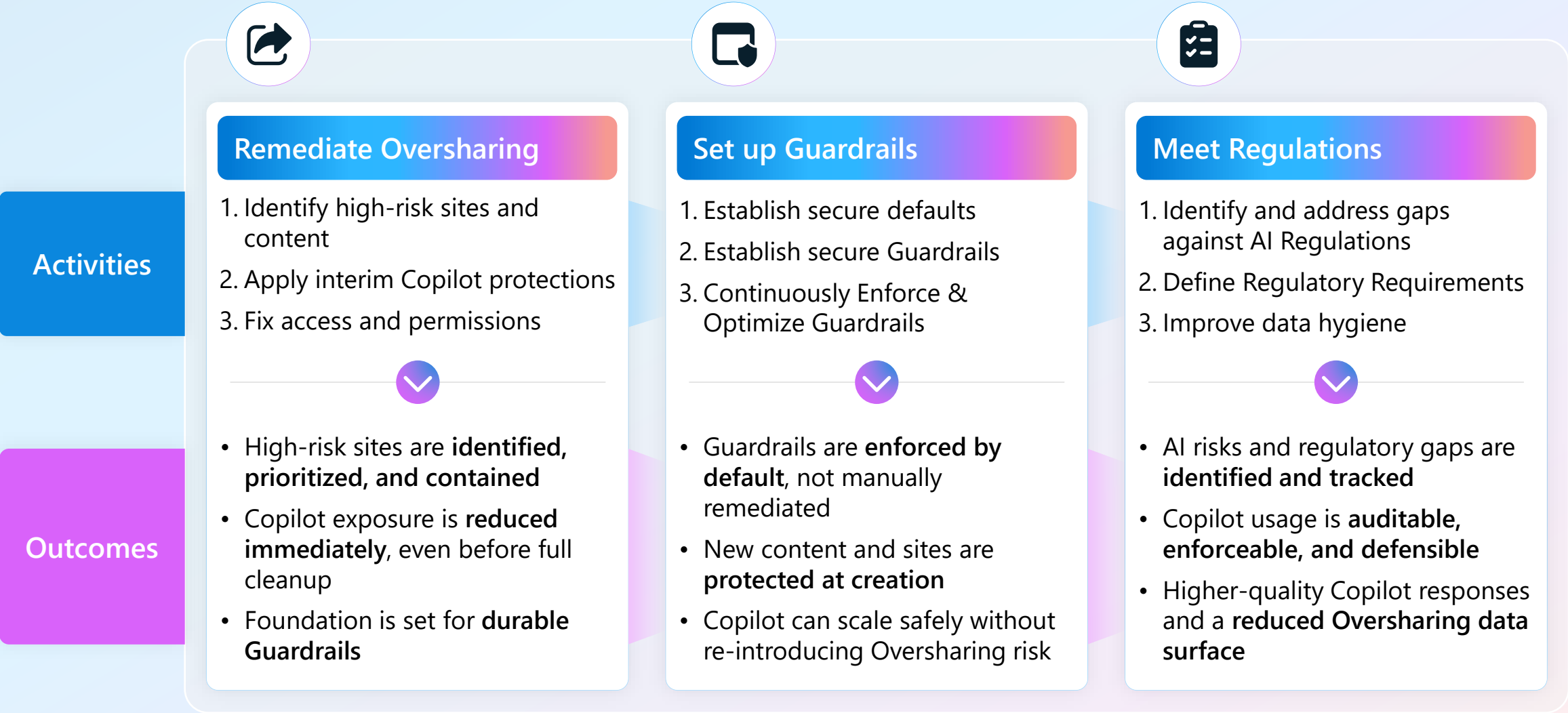
Unauthorized disclosure of confidential information



Out of date or irrelevant responses

By addressing these risks, organizations can ensure that Microsoft 365 Copilot is secured end to end

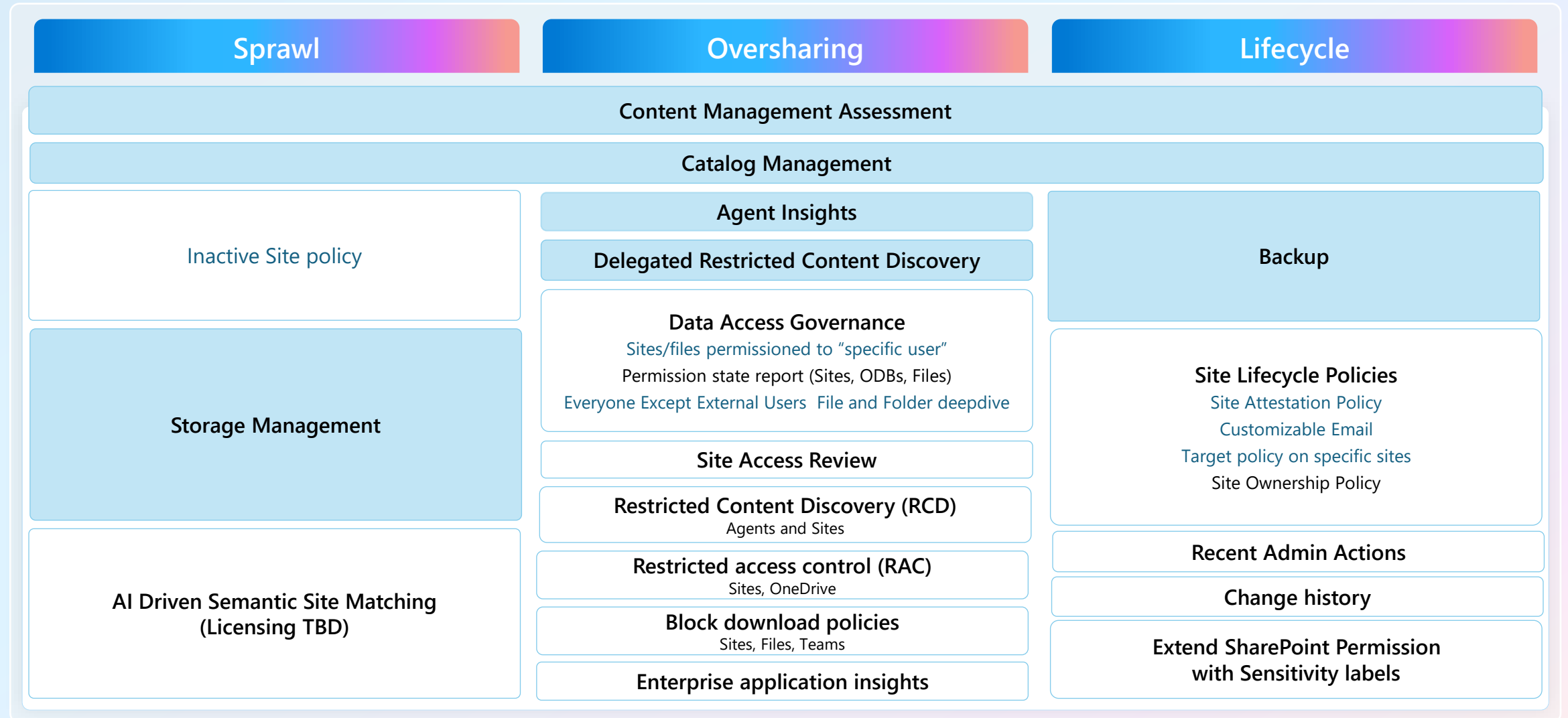
Secure and Govern Microsoft 365 Copilot



SharePoint Advanced Management demo

SAM | SharePoint Advanced Management

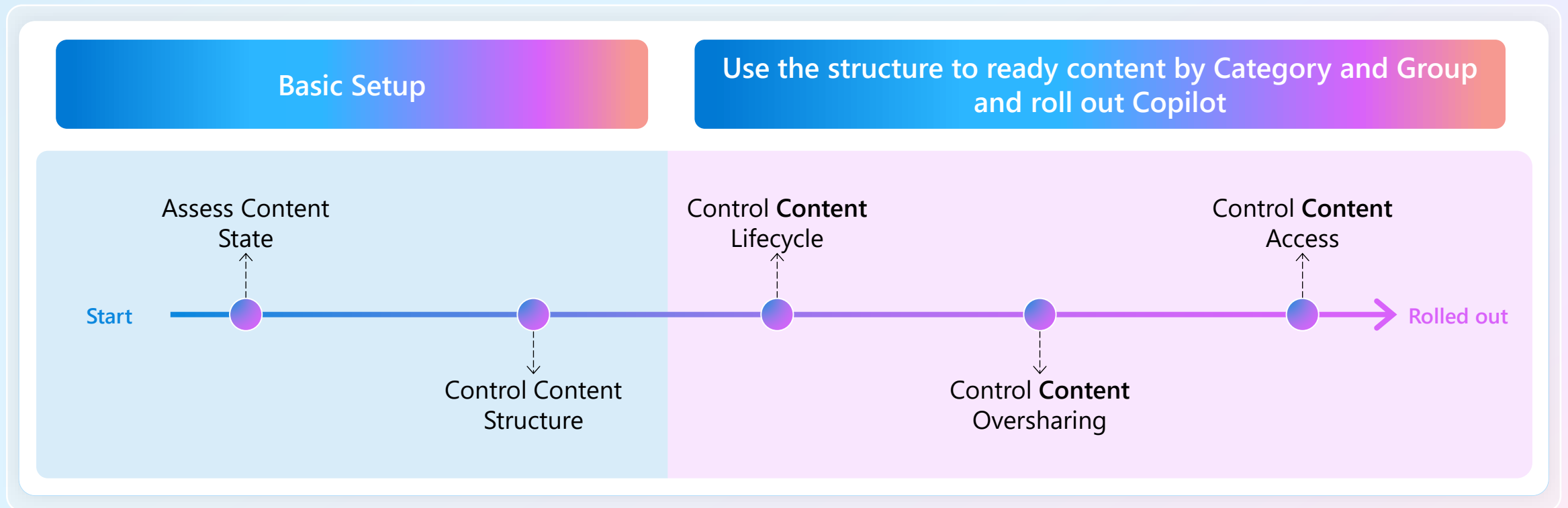
Copilot native governance capabilities



 New Feature Area

Content Readiness Journey

powered by SharePoint Advanced Management (SAM)



Assess Content State

Evaluate your SharePoint and OneDrive estate powered by Content Management Assessment

What does it do?

- A built-in tool to evaluate and improve content management within SharePoint
- Helps identify content risks, ensure compliance, and maintain data integrity

Benefits:

- **Comprehensive Tenant wide Insights**
Provide a detailed report on governance state
- **Actionable Solutions**
Link problem areas to SAM features for quick resolution
- **Boost Efficiency**
Reduce manual assessments and expert involvement
- **Helps Define Copilot Readiness**
Establish a clear governance roadmap for Copilot success

Generally Available

SharePoint admin center

Home > Advanced management

Advanced management

Easily manage your content with policies, reports, and settings that simplify your workflow, strengthen security, and help your organization work better together.
[Learn more about SharePoint Advanced Management](#)

Overview All features

Is your organization ready for Copilot?

Evaluate your Copilot readiness, get actionable insights, and discover ways to simplify implementation with advanced management tools.

[Restart assessment](#)

Content management assessment

Site lifecycle

39,413 sites require attention
39% of sites

Issue type	Number of issues	Recommendations
Site inactivity	8,041	View recommendations
Missing site ownership	31,372	View recommendations

Oversharing

26,422 sites require attention
26% of sites

Issue type	Number of issues	Recommendations
Broken permission inheritance	15,932	View recommendations
Org-wide site permissions	9,147	View recommendations
Organization and anyone sharing links	1,343	View recommendations

- North America
- Home
- Sites
- Policies
- Settings
- Content services
- Migration
- Reports
- Advanced
- More features
- Advanced management **PRO**
- Customize navigation
- Show all

Home > Advanced management

Advanced management

Easily manage your content with policies, reports, and settings that simplify your workflow, strengthen security, and help your organization work better together.

[Learn more about SharePoint Advanced Management](#)

Overview All features

Is your organization ready for Copilot?

Evaluate your Copilot readiness, get actionable insights, and discover ways to simplify implementation with advanced management tools.

[Start assessment](#)



Improve Copilot results across your Microsoft 365 apps

- SharePoint
- Microsoft Teams
- OneDrive
- Power BI
- Viva Engage

Content management assessment

Site lifecycle

Run assessment

0% of sites

Issue type	Number of issues	Recommendations
Site inactivity	—	View recommendations
Missing site ownership	—	View recommendations

Oversharing

Run assessment

0% of sites

Issue type	Number of issues	Recommendations
Broken permission inheritance	—	View recommendations
Org-wide site permissions	—	View recommendations
Sharing links	—	View recommendations

- North America
- Home
- Sites
- Policies
- Settings
- Content services
- Migration
- Reports
- Advanced
- More features
- Advanced management **PRO**
- Customize navigation
- Show all

Advanced management

Easily manage your content with policies, reports, and settings that simplify your workflow, strengthen security, and help your organization work better together.
[Learn more about SharePoint Advanced Management](#)

Overview All features

Is your organization ready for Copilot?

Evaluate your Copilot readiness, get actionable insights, and discover ways to simplify implementation with advanced management tools.

Restart assessment



Improve Copilot results across your Microsoft 365 apps

- SharePoint
- Microsoft Teams
- OneDrive
- Power BI
- Viva Engage

Content management assessment

Site lifecycle

39,413 sites require attention

Issue type	Number of issues	Recommendations
Site inactivity	8,041	View recommendations
Missing site ownership	31,372	View recommendations

Oversharing

26,422 sites require attention

Issue type	Number of issues	Recommendations
Broken permission inheritance	15,932	View recommendations
Org-wide site permissions	9,147	View recommendations
Organization and anyone sharing links	1,343	View recommendations

- North America
- Home
- Sites
- Policies
- Settings
- Content services
- Migration
- Reports
- Advanced
- More features
- Advanced management **PRO**
- Customize navigation
- Show all

Home > Advanced management

Advanced management

Easily manage your content with policies, reports, and settings that simplify your workflow, strengthen security, and help your organization work better together.

[Learn more about SharePoint Advanced Management](#)

Overview All features

Is your organization ready for Copilot?

Evaluate your Copilot readiness, get actionable insights, and discover ways to simplify implementation with advanced management tools.

Assessment in progress



Impr
ShareF
Micros

Content management assessment

Site lifecycle

39,413 sites require attention



Issue type	Number of issues	Recommendations
Site inactivity	8,041	View recommendations
Missing site ownership	31,372	View recommendations

Oversharing

26,422 sites require attention



Issue type	Number of issues
Broken permission inheritance	15,000
Org-wide site permissions	9,000
Organization and anyone sharing links	1,500

Inactivity

Inactive site policy

This report detected sites that haven't been used for a specified period.

[Learn more about managing inactive sites](#)

Inactive sites
8,041

Recommended next steps

- Download the report to identify inactive sites.
- Create an inactive site policy to notify owners or archive sites.

Why do these sites require attention?

Inactive sites can become security risks if they're not regularly monitored or maintained.

How we got this number

The number of inactive sites includes classic sites, communication sites, Microsoft 365 group-connected sites, Teams-connected sites, and non group-connected team sites that have been inactive for at least three months.

Inactive site policy features

- Identify inactive sites.
- Send notifications to site owners or site admins.
- Automatically archive or mark sites as read-only.

[Go to the inactive site policy page](#)

Control Content Structure

Define organizational content clusters for targeted actions

Provides an overview of content distribution across regions, departments, users, info barriers and customer defined custom properties for targeting actions, monitoring and Copilot grounding.

How it works:

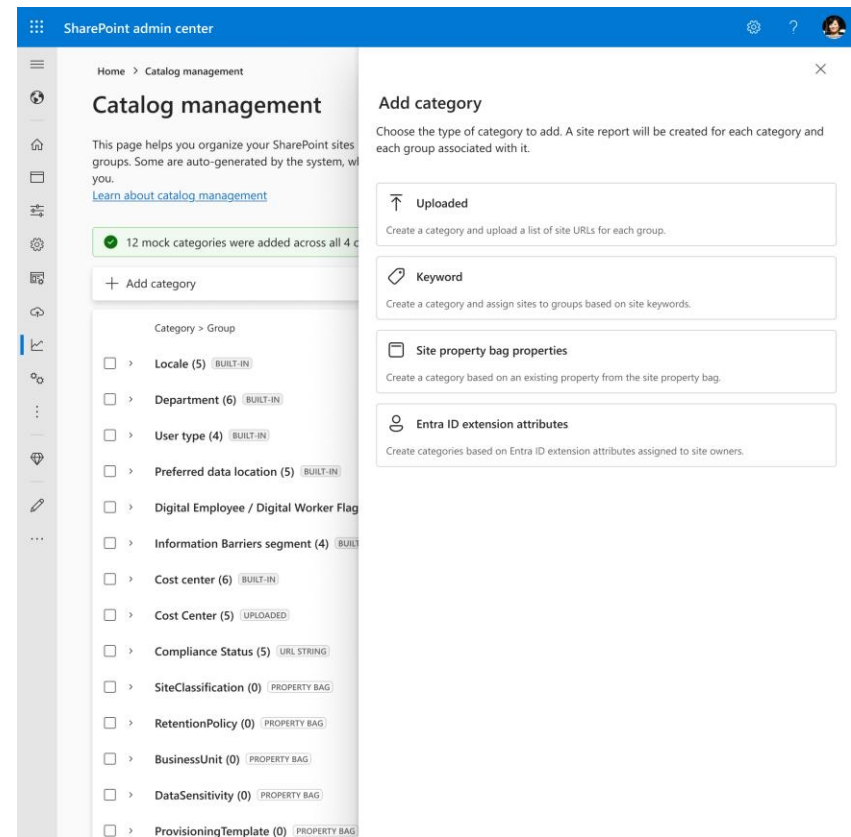
- Uses built-in Microsoft 365 metadata
- Create content categories and groups for targeted management
- Enable surgical billing, policies, reports, and Copilot access on region, department, user type, info barriers segment and more

Impact:

- Consistent governance across the organization
- Reduced admin overhead through automation
- Precision targeting for lifecycle, access reviews, and security baselines

V1 Generally Available

V2 Coming Soon





Home > Catalog management

Catalog management

This page helps you organize your SharePoint sites into categories using catalog properties and groups. Some are auto-generated by the system, while others can be created and customized by you.

[Learn about catalog management](#)

+ Add category

Category > Group	Sites	Site report
<input type="checkbox"/> > Locale (5) BUILT-IN	100,000	Download
<input type="checkbox"/> > Department (6) BUILT-IN	100,000	Download
<input type="checkbox"/> > User type (4) BUILT-IN	100,000	Download
<input type="checkbox"/> > Preferred data location (5) BUILT-IN	100,000	Download
<input type="checkbox"/> > Digital Employee / Digital Worker Flag (2) BUILT-IN	100,000	Download
<input type="checkbox"/> > Information Barriers segment (4) BUILT-IN	100,000	Download
<input type="checkbox"/> > Cost center (6) BUILT-IN	100,000	Download



Add category

Choose the type of category to add. A site report will be created for each category and each group associated with it.

Uploaded

Create a category and upload a list of site URLs for each group.

Keyword

Create a category and assign sites to groups based on site keywords.

Site property bag properties

Create a category based on an existing property from the site property bag.

Entra ID extension attributes

Create categories based on Entra ID extension attributes assigned to site owners.

ies and
nized by

Site report

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)



ies and
nized by

Site report

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)



Upload

Enter a category name and then upload a list of sites for each group you want to create.

Category name *

Description

Groups *

3/20

Upload a single-column CSV file with a list of site URLs for each group you want to create.



CVP Content

194 sites • Permissioned_Users_Count_SharePoint_report_2026-02-19 (1).csv



EVP Content

129 sites • Sites_20251008211703223 (1).csv



Drop file or click to upload

No file uploaded



Catalog management

This page helps you organize your SharePoint sites into categories using catalog properties and groups. Some are auto-generated by the system, while others can be created and customized by you.

[Learn about catalog management](#)

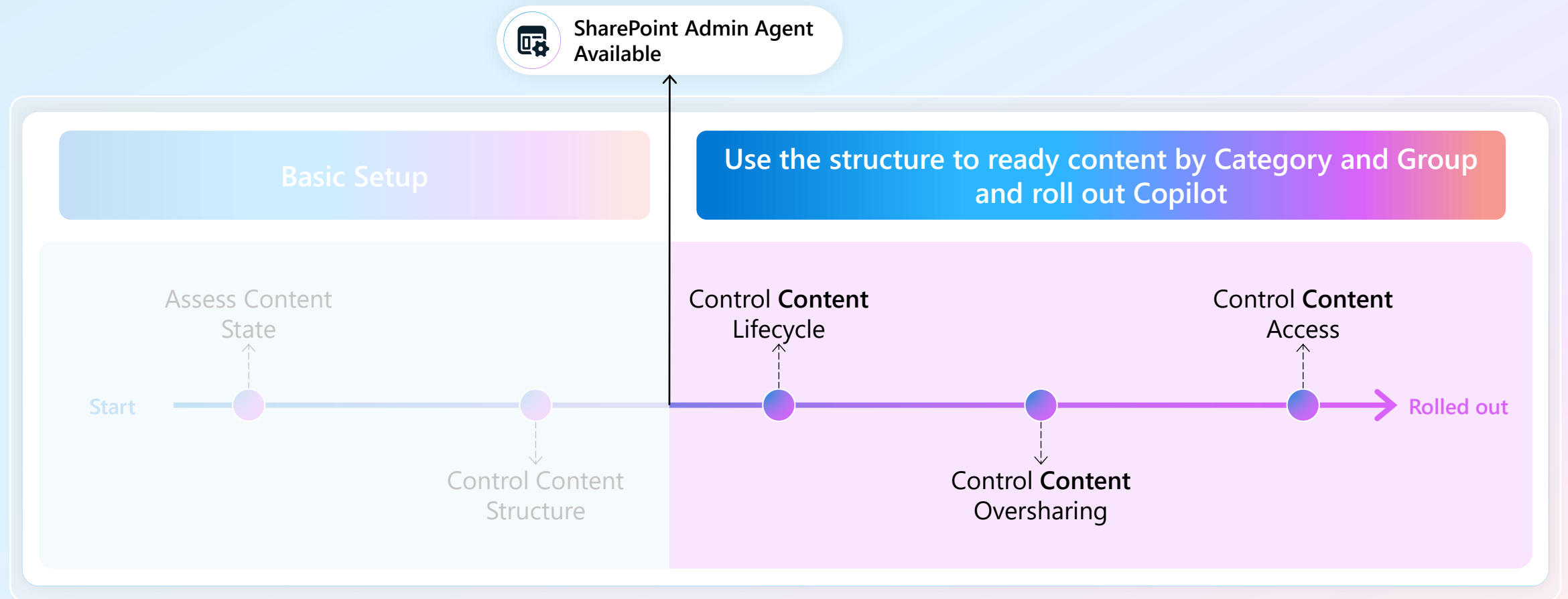
✔ "LT content" was added to your catalog.

+ Add category

	Category > Group	Sites	Site report
<input type="checkbox"/>	> Locale (5) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> Department (6) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> User type (4) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> Preferred data location (5) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> Digital Employee / Digital Worker Flag (2) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> Information Barriers segment (4) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> Cost center (6) <small>BUILT-IN</small>	100,000	Download
<input type="checkbox"/>	> LT content (2) <small>UPLOADED</small>	323	Download

Content Readiness Journey

powered by SharePoint Advanced Management (SAM)



Control Content Lifecycle

Improve AI response quality, reduce management scope at enterprise scale

Identifies stale, outdated and ownerless content to help reduce management surface and improve Copilot response quality.

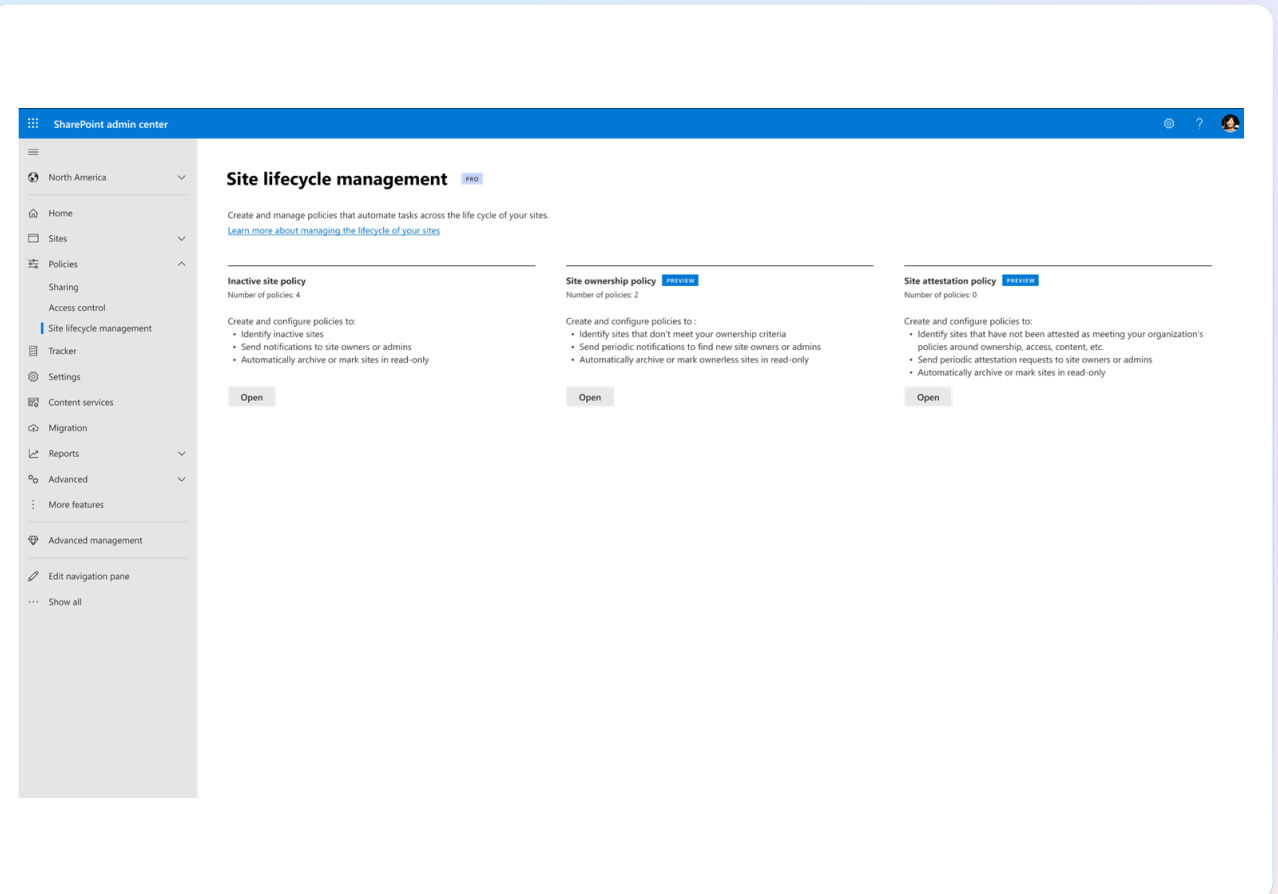
How it works:

- Takes about 5 minutes to set up.
- Admin selects the policy scope and action conditions.
- Tool supports simulation and active modes.
- When activated, tool will automatically detect stale and ownerless content, identify the owners, contact the owners and mitigate the issue. If owners do not respond, content can be archived or placed in a read only state.
- Supports custom scoping and email customization.

Impact:

- Policy creates an admin
- Consistent governance across the organization
- Reduced admin overhead through automation

Generally Available



- Canada
- Home
- Sites
 - Active sites
 - Archived sites
 - Deleted sites
- Applications
- Containers
- Policies
 - Sharing
 - Access control
 - Site lifecycle management**
- Settings
- Content services
- Migration
- Reports
 - Agent insights
 - App insights
 - Catalog management
 - Change history
 - Content events
 - Content policy analytics
 - Content services
 - Data access governance
 - OneDrive accounts
 - Site policy comparison
- Content solutions
- Advanced
- More features

Site lifecycle management PRO

Use this page to create and manage policies that automate tasks across the lifecycle of your sites.
[Learn more about managing the lifecycle of your sites](#)

Inactive site policies

Number of policies: 2

Create and configure policies to:

- Identify inactive sites
- Send notifications to site owners or admins
- Automatically archive or mark sites in read-only

Open

Site ownership policies

Number of policies: 0

Create and configure policies to:

- Identify sites that don't meet organization's ownership criteria
- Send notifications to find new site owners or admins
- Automatically mark sites in read-only

Open

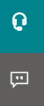
Site attestation policies

Number of policies: 0

Create and configure policies to:

- Identify sites due for attestation of their information
- Send notifications to site owners or admins seeking attestation
- Automatically archive or mark sites in read-only

Open



- Canada
- Home
- Sites
 - Active sites
 - Archived sites
 - Deleted sites
- Applications
- Containers
- Polices
 - Sharing
 - Access control
 - Site lifecycle management**
- Settings
- Content services
- Migration
- Reports
 - Agent insights
 - App insights

Site lifecycle management PRO

Use this page to create and manage policies that automate tasks across the lifecycle of your sites.

[Learn more about managing the lifecycle of your sites](#)

Inactive site policies

Number of policies: 2

Create and configure policies to:

- Identify inactive sites
- Send notifications to site owners or admins
- Automatically archive or mark sites in read-only

Open

Site ownership policies

Number of policies: 0

Create and configure policies to:

- Identify sites that don't meet organization's ownership criteria
- Send notifications to find new site owners or admins
- Automatically mark sites in read-only

Open

Site attestation policies

Number of policies: 0

Create and configure policies to:

- Identify sites that don't meet organization's attestation criteria
- Send notifications to find new site attesters or admins
- Automatically mark sites in read-only

Open

- Canada
- Home
- Sites
 - Active sites
 - Archived sites
 - Deleted sites
- SharePoint Embedded
- Backup
- Policies
 - Sharing
 - Access control
 - Site lifecycle management
- Settings
- Content services
- Migration
- Reports
 - Agent insights
 - App insights

Create an inactive site policy

- Overview
- Scope**
- Configuration
- Finish

Set policy scope

How do you want to select the sites for the policy? *

- Upload a CSV file with a list of up to 10,000 URLs

Create your list using the sample CSV file.

[Download sample CSV file](#)

To create the list:

1. Export the site list from the [SharePoint active sites page](#)
2. Make sure there are no duplicates and save the file as CSV.

Upload CSV file with URLs

Browse

- Select sites at scale

- Overview
- Scope**
- Configuration
- Finish

Set policy scope

How do you want to select the sites for the policy? *

- Upload a CSV file with a list of up to 10,000 URLs
- Select sites at scale

Which sites should be checked for inactivity? *

ⓘ Overlapping scopes across active policies may affect enforcement and notifications
[Learn more about scoping policies](#)

Classic sites, Communication sites, oup connect sites without teams, Teams co... ▾

Filter by sensitivity label

Top secret ▾

Filter by catalog category

Finance department ▾

Filter by site creation source

Include sites with retention policies and retention holds

Exclude sites

Exclude specific sites from this policy

- Overview
- Scope
- Configuration**
- Finish

Configure policy

How long after the last activity should a site be considered inactive?

Includes activity on the site, files, and any connected resources like Microsoft Team

3 months

Who should be notified via email if site has been inactive? *

These users can certify the site to keep it active.

- Site owners
- Site admins

[Customize email to be sent](#)

Exclude site owners or admins from receiving requests ⓘ

Exclude users or groups

How many emails should be sent before enforcement is applied? *

Site owners get an email after every monthly policy run. If they don't act after the c of emails, enforcement will start.

3 emails

Which enforcement action should be applied to inactive sites that aren't certified chosen number of emails are sent? *

ⓘ Enforcement actions cannot be edited after policy creation

- Archive sites after chosen read-only period **RECOMMENDED**
Sites admins and owners can't access archived sites.

Duration of read-only period *

3 months

- Read-only access
Site admins and owners can view the site's content, but can't edit it.

- Days notifications for 3 months

Customize email

Sender

custom@contosoenergyusa40.onmicrosoft.com

Tip: If you want to change the default sender, reconfigure it in [Microsoft admin center](#)

Subject

\$SiteName site is inactive and needs attention

Message

Dear \$UserDisplayName,

You're receiving this email because you're associated with the [\$SiteName](\$SiteUrl) site, which has been inactive for some time. As per your organization's policy, sites should not remain inactive beyond the allowed period.

Tip: Use \$UserDisplayName to insert the user's name and [\$SiteName](\$SiteUrl) to insert the name with the link to the site.

Policy guideline

URL ⓘ

Enter your URL

Display text

Learn more about site inactivity

Email preview



Contoso Team site is inactive and needs attention



Contoso Team
Connected to Teams

Dear John Doe,

You're receiving this email because you're associated with the [Contoso Team](#) site, which has been inactive for some time. As per your organization's policy, sites should not remain inactive beyond the allowed period.

Select **Certify site** to confirm that it's still in use, or consider deleting it if the site is no longer needed.

Certify site

Learn more how to delete site



[Privacy Statement](#)

- Canada
- Home
- Sites
 - Active sites
 - Archived sites
 - Deleted sites
- Applications
- Containers
- Policies
 - Sharing
 - Access control
 - Site lifecycle management**
- Settings
- Content services
- Migration
- Reports
 - Agent insights
 - App insights
 - Catalog management
 - Change history
 - Content events
 - Content policy analytics
 - Content services
 - Data access governance
 - OneDrive accounts
 - Site policy comparison
- Content solutions
- Advanced
- More features

Create an inactive site policy

- Overview
- Scope
- Configuration
- Finish**

Finish

Policy name *

Description

Add a description to help others understand why the policy was created.

Policy mode *

- Simulation
The policy runs once to generate a report. No notifications are sent, and no enforcement takes place.
- Active
The policy will run on a monthly basis, generate the report, notify site owners or site admins and act on inactive sites.

New Message

Delete Archive Move Flag Mark as Unread Sync

- Favorites**
 - Inbox 2
 - Travel 2
 - Robin Counts
 - Contoso Marketing
- All Accounts**
 - Inbox** 2
 - Drafts 2
 - Sent
 - Groups
 - Marketing
 - Engineering
 - Deleted Items

Focused Other 3

Other Emails Northwind Trader, Elvia Atkin, Daisy Phillips

Today

Zava Action needed:Some of your sites n... 09:00 AM Email body

Lydia Bauer Team Pictures 9:22 AM

Yesterday

Colin Ballinger Upcoming Trip Sunday

Elvia Atkin Meet Meet & Greet Sunday

Pat Volunteers Needed Sunday

Henry Brill Back Cover Idea Sunday

Colin Ballinger Hey Katri, I know this is last minutes... Sunday

Robin Counts Thanks, Henry! Looking forward to R... Sunday

Friday

Daisy Phillips Upcoming Workshop 4/11/2021

Mona Kane Virtual Planning 4/11/2021

Lydia Bauer

Action needed: Some of your sites need attention

Zava To: Katri Ahokas



Review inactive sites

Dear Katri Ahokas,

You are receiving this email because you're associated with [ZAVA Team](#), which has been inactive for for some time. As per your organization's policy, sites should not remain inactive beyond the allowed period.

Select **Certify site** to confirm that it is still in use, or consider deleting it is the site is no longer needed.

Total inactivity reviews pending
5

Sites set to read-only in last 30 days
2

Sites archived in last 30 days
3

[Review inactive sites](#)

This email is generated from an unmonitored alias. Please do not reply.

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

Site reviews

View and manage all reviews assigned to you.

- All
- Pending reviews
- Completed reviews
- Archived sites
- Read-only sites

Filters

Site name ↓	Review type	Status	Requested on	Action due by	Required Actions
Contoso Finance Team site	Inactivity	Pending	Apr 2, 2026	May 2, 2026	
Marketing Hub Team site	Inactivity	Pending	Apr 2, 2026	May 2, 2026	
Customer Portal Team site	Inactivity	Completed	Feb 9, 2026	Mar 9, 2026	
Org policies Communication site	Inactivity	Archived	-	-	
Consumer Data Team site	Inactivity	Completed	Feb 3, 2026	Mar 5, 2026	
Sales enablement Team site	Site attestation	Completed	Feb 3, 2026	Mar 5, 2026	
Sales Directory Team site	Inactivity	Archived	-	-	
New Joinee Onboarding Team site	Inactivity	Completed	Jan 18, 2026	Feb 18, 2026	
Org Offsite Team site	Site ownership	Completed	Jan 3, 2026	Feb 3, 2026	

Control Content Oversharing

Gain Control Over Site Permissions and Overshared Content

What does it do?

- Comprehensive permission report for entire tenant (SharePoint sites and OneDrive) – supports ~1M sites
- Detect root causes of oversharing (broken inheritance, sharing links, EEUEs, site privacy and more)
- Focus on critical permissions by user count and large groups
- Filter with sensitivity, privacy, external sharing
- Downloadable report, with insights from AI analytics

Actions:

- Site Access Review for site owners with file level details
- Easily discover files exposed via EEUE, large groups, sharing links and rectify permissions accordingly

Generally Available

Snapshot till March

Review sites with a high number of users across all permission scopes (inherited and broken).
Download a detailed .csv report for up to 10,000 sites.

[Download detailed report](#)

Contoso Finance Home News Team directory Patents Files FAQs Edit Private | Top secret ☆ Follow

All Documents

Site reviews > **Permissions to many users**

The list below details scopes which have the highest number of permissioned users. It also highlights possible sources such as count of sharing links and presence of groups such as Everyone and Everyone Except External Users (EEUE).
Remove permissions where they are no longer required to prevent oversharing.

Name	Scope	Total number of Permissioned users	Total number of groups	Count of 'Anyone' links	Count of 'People in your org' links	Has EEUE	Has Everyone	Action	Final status
Contoso Finance	SharePoint Site	6804	4	-	-	-	-	Manage access	Select
Finance_projections_FY23.xlsx	File	7142	5	2	2	-	-	Manage access	Select
Vendor_bills	Folder	7524	7	1	2	-	-	Manage access	Select
ProfitabilityPlan.pptx	File	7945	6	1	3	Yes	-	Manage access	Select
Flow_map.jpg	File	8580	3	2	1	Yes	-	Manage access	Select
Confidential Q2 CY24 ReOrg	File	9092	4	3	3	Yes	-	Manage access	Select

Broken inheritance, Sharing links, EEUE domain group

Retained all permissions
Modified existing permissions
Removed permissions completely

[Complete review](#) [Save as draft](#) [Cancel](#)

Common causes of Copilot oversharing in SharePoint

Privacy settings

Public - anyone in the organization can access this site

Public - anyone in the organization can access this site

Private - only members can access this site

Site privacy set to public

Share "Branding Elements.pptx"

Add a name, group, or email

Add a message

People in Contoso with the link can edit.

Copy link

Send

Link copied. People in Contoso with the link can edit.

Default sharing option is everyone

m365x32957528.sharepoint.com says

You are about to create unique permissions for this document library. Changes made to the parent site permissions will no longer affect this document library.

OK

Cancel

Broken permission inheritance

Share site

Add users, Microsoft 365 Groups, or security groups to give them access to the site.

Note that this site is part of a Microsoft 365 Group. If you add users here, they will be given access to the site, but not to other group resources such as calendars and conversations. To do that, add members to the group instead.

everyone

Everyone except external users

Search Directory

Use of "everyone except external users" domain group

Documents

Name	Sensitivity
Branding Elements.pptx	
Cross Cultural Marketing Campaigns.pptx	Confidential
DG-1000 Product Overview.pptx	
DG-2000 Product Overview.docx	Confidential
DG-2000 Product Pitch.pptx	
DG-2000 Product Specification.docx	
International Marketing Campaigns.docx	

Use of "everyone except external users" domain group

- Canada
- Home
- Sites
 - Active sites
 - Archived sites
 - Deleted sites
- SharePoint Embedded
- Backup
- Policies
- Settings
- Content services
- Migration
- Reports
 - Agent insights
 - App insights
 - Catalog management
 - Change history
 - Content events
 - Content policy analytics
 - Content services
 - Data access governance**
 - OneDrive accounts
 - Site policy comparison
- Content solutions

Data access governance PRO

Reports All review requests

This page provides reports to help you maintain the security and compliance of your data in SharePoint. [Learn more about data access governance](#)



Get started

We recommend starting with a snapshot report to get a quick overview of permissions for all sites in your organization.

Snapshot reports ⓘ

Site permissions across your organization RECOMMENDED

Check for broad permissions such as Everyone except external users, guest access, sharing links, and unique permissions across all sites in your organization, as of the report generation date.

[View reports](#)

Site permissions for users NEW

Identify all sites a user can access and determine whether they can access the entire site or specific sections, granted directly to the user or indirectly through groups as of the report date.

[View reports](#)

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where stored and the policies applied to these sites, as of the

[View reports](#)

Activity reports ⓘ

Sharing links

Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint sites in the last 28 days.

[View reports](#)

Shared with 'Everyone except external users'

Make sure files, folders, and lists aren't being overshared by reviewing sites that have the most items shared with "Everyone except external users" in the last 28 days.

[View reports](#)

Snapshot till March

As of March 3, 2024

Review sites with a high number of users across all permission scopes (inherited and broken).
Download a detailed .csv report for up to 1M sites.

[Download detailed report](#)

[+ Initiate site access review](#) [View all reviews](#) [Restrict site access](#)

100 items

Filters: Site sensitivity: All External sharing: All

Name	URL	Site access review	Total permissioned users ↓	Files	Sensitive Files ⓘ	Items with unique permissions	EEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
Contoso HR	.../teams/contosohr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
Contoso Marketing	.../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
Contoso Finance	.../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
Contoso Team	.../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
Contoso Vac	.../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
Contoso in house	.../teams/contosoin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
Contoso infra	.../teams/contosoin	-	3998	28187	2890	5	2	21	21	Public	General	On
Contoso leaders	.../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
Contoso design	.../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
Contoso BI	.../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
Contoso HR	.../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
Contoso Give	.../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
Contoso Sesh	.../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
Contoso Sesh	.../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On

Snapshot till March

As of March 3, 2024

high number of users across all permission scopes (inherited and broken).
 .csv report for up to 1M sites.

ailed report

Access review View all reviews Restrict site access

Activity: All ▼ External sharing: All ▼

Search

Files containing sensitive data

Broken permission inheritance

Use of "everyone except external users" domain group

Default sharing option is everyone

Site privacy set to public

URL	Site access review	Total permissioned users ↓	Files	Sensitive Files ①	Items with unique permissions	EEEEU permissions	People in your org links	Anyone links	Site Privacy	Site sensitivity	External sharing
.../teams/contosoehr	-	22334	44869	4821	2	2	312	312	Private	Top secret	On
.../teams/contosoma	-	15698	41839	4213	1	2	298	298	Private	Confidential	On
.../sites/contosofin	-	11237	38286	4200	3	2	167	167	Private	-	On
.../sites/contosoteam	-	10134	35310	3189	6	2	124	124	Private	Confidential	On
.../sites/contosovac	-	8530	31498	3120	2	2	72	72	Public	General	On
.../teams/contosooin	-	6054	30764	3100	1	2	214	214	Public	Confidential	On
.../teams/contosooin	-	3998	28187	2890	5	2	21	21	Public	General	On
.../teams/contosole	-	2804	22396	2340	8	2	12	12	Public	-	On
.../teams/contosoen	-	1890	20189	2310	2	2	9	9	Public	-	On
.../teams/contosoen	-	1890	20189	2231	2	2	9	9	Public	-	On
.../teams/contosoen	-	1890	20189	2213	2	2	9	9	Public	-	On
.../teams/contosoen	-	1890	20189	1313	2	2	9	9	Public	-	On
.../teams/contosoen	-	1890	20189	1110	2	2	9	9	Public	-	On
.../teams/contosoen	-	1890	20189	989	2	2	9	9	Public	-	On



Site reviews > Permissions to many users

The list below details inherited and unique permissions which have the highest number of users and possible contributing factors such as links, groups or Everyone Except External Users (EEEEU) claims. Remove permissions where they are no longer required to prevent oversharing.

Name	Scope	Number of Permissioned users	Sensitivity Info Type	Sensitivity Label	Number of groups	Number of 'Anyone' links	Number of 'People in your org' links	Has EEEU	Action	Final status
Contoso Finance	SharePoint Site	6804	US Passport Number +2	Top secret	4	-	-	-	Manage access	Select
Finance_projections_FY23.xlsx	File	7142	US SSN Number + 4	Confidential	5	2	2	-	Manage access	Select
Vendor_bills	Folder	7524	US SSN Number + 1	Highly confidential	7	1	2	-	Manage access	Select
ProfitabilityPlan.pptx	File	7945	US SSN Number	-	6	1	3	Yes	Manage access	Select
Flow_map.jpg	File	8580	US Passport Number	General	3	2	1	Yes	Manage access	Select
Confidential_Q2_CY24_ReOrg	File	9092	ABA Routing Number	-	4	3	3	Yes	Manage access	Select

Default sharing option is everyone

Site privacy set to public

Broken permission inheritance

Files containing sensitive data

Use of "everyone except external users" domain group

Group name	Alias	Members
Contoso FTE	cfe@contosoenergy.com	4528
Contoso Giving	cgive@contosoenergy.com	198
Contoso Benefits	cbenefits@contosoenerg...	126
Contoso Vendors	conv@contosoenergy.co...	78

ts

help you maintain the security and compliance of your data in SharePoint.
[governance](#)

Starting with a snapshot report to get a quick overview of permissions for all sites in your organization.

organization **RECOMMENDED**

Such as Everyone except external users, guest user permissions across all sites in your organization as of the report generation date.

by monitoring sites where users created new content in the last 28 days.

Site permissions for users **NEW**

Identify all sites a user can access and determine whether they can access the entire site or specific sections, granted directly to the user or indirectly through groups as of the report date.

[View reports](#)

Shared with 'Everyone except external users'

Make sure files, folders, and lists aren't being overshared by reviewing sites that have the most items shared with "Everyone except external users" in the last 28 days.

[View reports](#)

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites, as of the report generation date.

[View reports](#)

Information Barrier (IB) compliance

Use these reports to view sites with incompatible segmentations due to a change in IB policy or segments.

[View reports](#)

User access review report















As of October 1, 2025

Review sites where the given user has direct or indirect permissions to the content of the site. Download a CSV report per user or download all reports for all users as a .zip file. Each file can have up to 1 M sites.

Download report for all users

6 Users	Download report for Brenda Thomas									Top 100 sites
Search user	Filters: Site sensitivity: All External sharing: All Template: All Privacy: All									
BT Brenda Thomas	Site name	URL	Files in site	Site shared ⓘ	Direct access items ⓘ	Indirect access items ⓘ	Site privacy	Site sensitivity	External sharing	Primary admin
CS Chris Smith	Contoso HR	.../teams/contosohr	44869	No	20671	9987	Public	General	On	Mona Kane
JB Jack Becker	Contoso Marketing	.../teams/contosoma	41839	Yes	0	0	-	-	On	Contoso HR
JW Jesse Wallin	Contoso Finance	.../sites/contosofin	38286	Yes	0	0	Private	Top secret	Off	Mona Kane
SV Shikha Verma	Contoso Team	.../sites/contosoteam	35310	Yes	0	0	-	Confidential	Off	Contoso Marketing
VS Venkateshwaran S	Contoso Vac	.../sites/contosovac	31498	No	23	3120	Private	General	Off	Adam Grant
	Contoso in house	.../teams/contosoin	30764	No	6782	3100	Private	Confidential	On	Clay Wallin
	Contoso infra	.../teams/contosoin	28187	Yes	0	0	Public	General	Off	Contoso HR
	Contoso leaders	.../teams/contosole	22396	Yes	0	0	-	-	On	Adam Grant
	Contoso design	.../teams/contosoen	20189	No	2310	23	Public	General	Off	Contoso Marketing
	Contoso BI	.../teams/contosoen	20189	Yes	0	0	Privat	General	Off	Contoso Admin
	Contoso HR	.../teams/contosoen	20189	No	12	2213	-	Confidential	On	SPAC_owners
	Contoso Give	.../teams/contosoen	20189	No	2472	1313	Privat	Confidential	On	Contoso Admin
	Contoso Sesh	.../teams/contosoen	20189	No	12	1110	Publi	-	On	Mona Kane
	Contoso Sesh	.../teams/contosoen	20189	No	23	989	Public	General	Off	Adam Grant

Site sensitivity: All External sharing: All Template: All Privacy: All

Site name	URL	Files in site	Site shared (i)	Direct access items (i)	Indirect access items (i)	Site privacy	Site sensitivity	External sharing	Primary admin
Contoso HR	.../teams/contosohr	44869	No	20671	9987	Public	General	On	 Mona Ka
Contoso Marketing	.../teams/contosoma	41839	Yes	0	0	-	-	On	 Contoso
Contoso Finance	.../sites/contosofin	38286	Yes	0	0	Private	Top secret	Off	 Mona Ka
Contoso Team	.../sites/contosoteam	35310	Yes	0	0	-	Confidential	Off	 Contoso
Contoso Vac	.../sites/contosovac	31498	No	23	3120	Private	General	Off	 Adam Gr
Contoso in house	.../teams/contosoin	30764	No	6782	3100	Private	Confidential	On	 Clay Wall
Contoso infra	.../teams/contosoin	28187	Yes	0	0	Public	General	Off	 Contoso
Contoso leaders	.../teams/contosole	22396	Yes	0	0	-	-	On	 Adam Gr
Contoso design	.../teams/contosoen	20189	No	2310	23	Public	General	Off	 Contoso
Contoso BI	.../teams/contosoen	20189	Yes	0	0	Privat	General	Off	 Contoso
Contoso HR	.../teams/contosoen	20189	No	12	2213	-	Confidential	On	 SPAC_ow
Contoso Give	.../teams/contosoen	20189	No	2472	1313	Privat	Confidential	On	 Contoso
Contoso Sesh	.../teams/contosoen	20189	No	12	1110	Publi	-	On	 Mona Ka
Contoso Sesh	.../teams/contosoen	20189	No	23	989	Public	General	Off	 Adam Gr

Restricted Content Discovery (RCD) + Delegation

Advanced discoverability control to exclude sites from Copilot and Agents

What does it do?

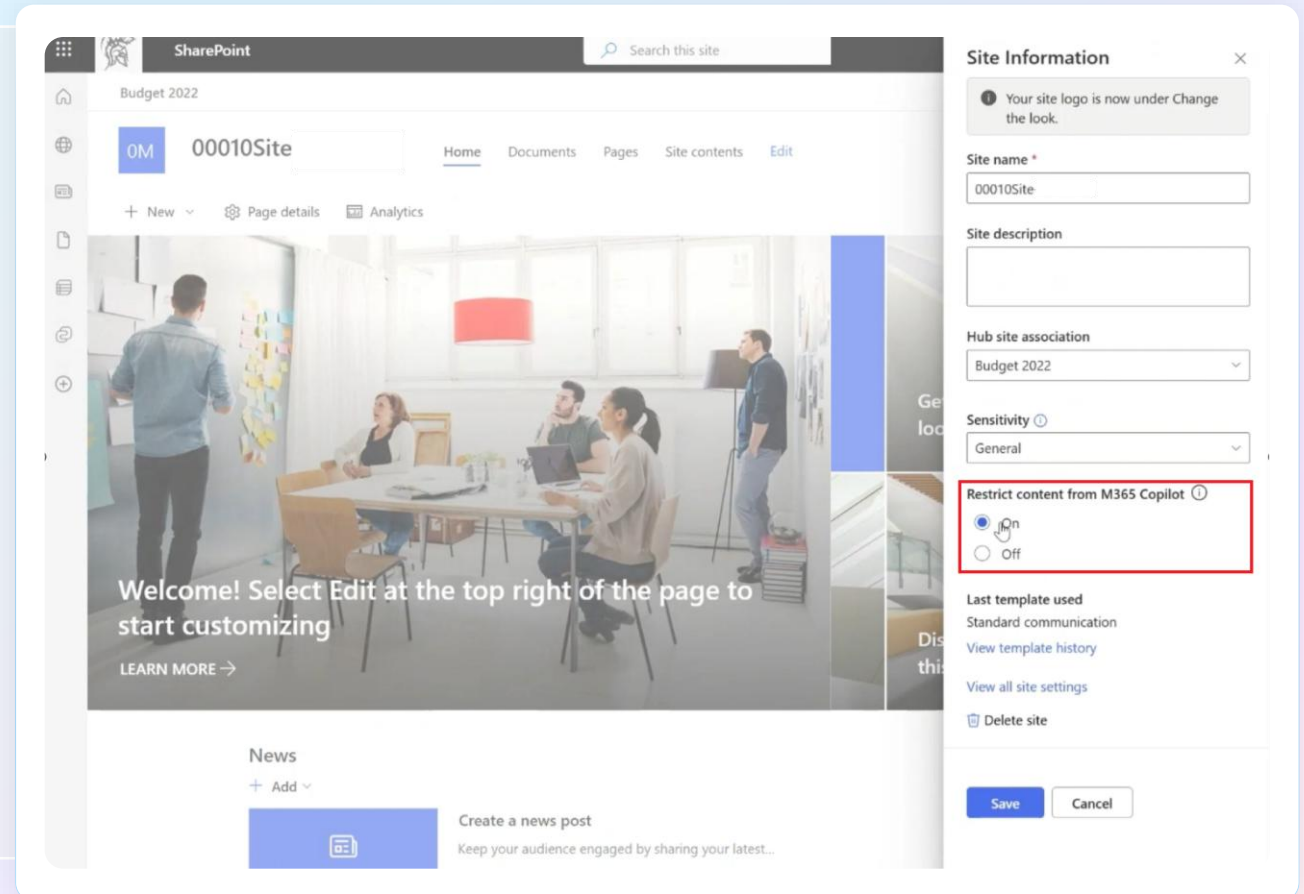
Limit SharePoint sites to be discoverable by Copilot and Agents.

What's New

1. Restricted Content Discovery for SPO admins (v1)
2. SPO admins can delegate RCD management to Site Admins! *

V1 Generally Available

In Private Preview



The screenshot displays the SharePoint interface for a site named '00010Site' under the 'Budget 2022' hub. The 'Site Information' panel on the right is open, showing various site settings. A red box highlights the 'Restrict content from M365 Copilot' toggle, which is currently set to 'On'. Other visible settings include 'Site name' (00010Site), 'Site description', 'Hub site association' (Budget 2022), and 'Sensitivity' (General). The main content area shows a welcome message and a 'News' section with a 'Create a news post' button.

Restricted Access Control (RAC) Policy: SharePoint & OneDrive

Restrict site or ODB access to a specific group

What does it do?

RAC (Restricted access control) policy can be set at the site level.

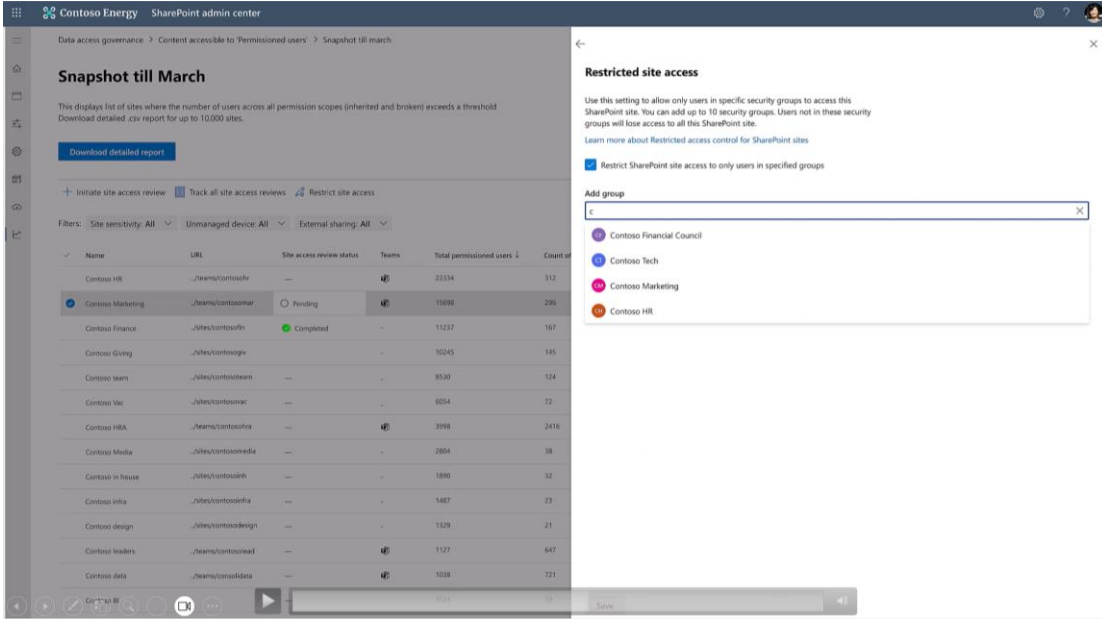
Even if individual files/folders have broken inheritance and over-shared, only RAC allowed users can access.

Copilot honors RAC policy !

Includes:

Microsoft 365 group-connected sites, Non-group SharePoint sites, Teams sites, Shared channel sites, OneDrive sites.

Generally Available



The screenshot displays the SharePoint admin center interface. The main pane shows a 'Snapshot till March' report for 'Content accessible to Permissioned users'. A table lists various sites with columns for Name, URL, Site access review status, Teams, Total permissioned users, and Count of users. The 'Content Marketing' site is highlighted. A 'Restricted site access' dialog box is open on the right, showing the option to 'Restrict SharePoint site access to only users in specified groups' which is checked. Below this, there is an 'Add group' search box with a list of groups including 'Contoso Financial Council', 'Contoso Tech', 'Contoso Marketing', and 'Contoso HR'.

Learn more:
aka.ms/RACPolicyForSites

Microsoft Purview Demo

Secure & Govern Microsoft 365 Copilot

With Microsoft Purview

Secure defaults & guardrails
from day one

Ongoing remediations
to reduce risk and improve compliance

Ensure auditability
of all Copilot
interactions

Establish secure
grounding for
responses

Address gaps against
AI regulations

Prevent data loss and
oversharing of sensitive
information

Remediate oversharing
of high-risk sites and
content

Reduce data exposure
and increase Copilot
response accuracy

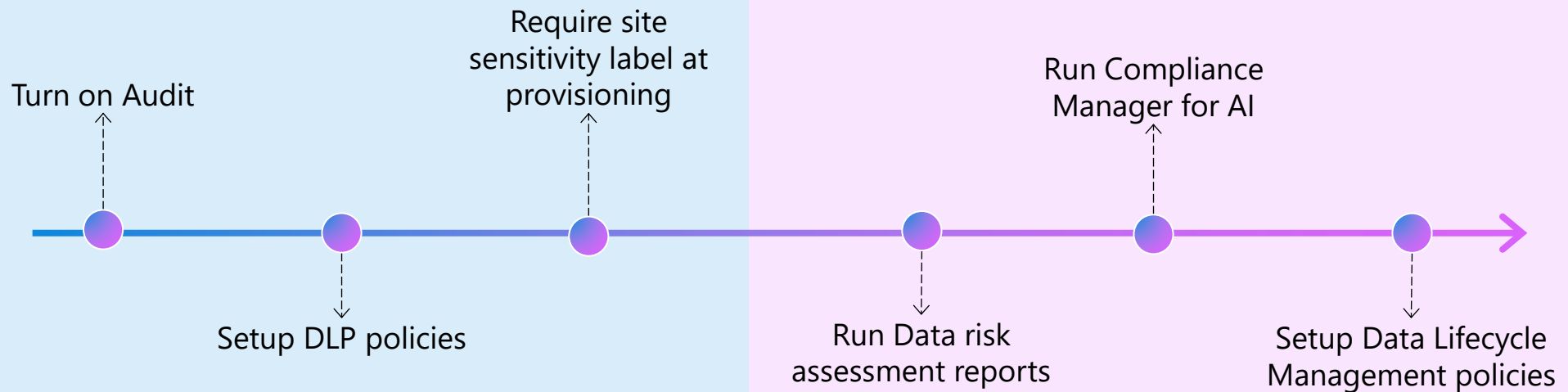


Secure & Govern Microsoft 365 Copilot

With Microsoft Purview

Secure defaults & guardrails
from day one

Ongoing remediations
to reduce risk and improve compliance



Secure defaults from Day One

- Home
- Copilot
 - Overview
 - Connectors
 - Search
 - Billing & usage
 - Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup
- Customize navigation
- Show all

Home

Enable Dark mode

Copilot Control System

- Overview
- Security**
- Usage
- Health
- Discover

Protected by Microsoft Purview

Microsoft 365 Copilot already includes built-in security controls powered by Microsoft Purview. Review the Copilot security information on this page for insights and to further protect your data. [Learn about data protection in Copilot](#)

Discover and assess end-to-end AI and agent risk across Purview, Microsoft Defender, and Microsoft Entra. [Go to Microsoft Security Dashboard for AI](#)

Prevent data leaks

Default protections in place

- Policy running: Protect sensitive Microsoft 365 Copilot interactions
 - All Copilot interactions are scanned for sensitive info.
 - Sensitive info monitored for all users.

Policy is monitoring only

Prevent data leakage in Copilot interactions

We've detected the following sensitive info types in your org. Turn on a policy to prevent sensitive info from being used in Copilot.

Top sensitive info types found in interactions **4015**

IP Address V4 IP Address + 3 more

Current status

Prompts with sensitive info types **234**

Total prompts **234**

Manage policy

Manage data oversharing

Default protections in place

Not started



- Home
- Copilot
- Overview
- Connectors
- Search
- Billing & usage
- Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup
- Customize navigation
- Show all

Home

Copilot Control System

Overview **Security** Usage Health Discover

Protected by Microsoft Purview

Microsoft 365 Copilot already includes built-in security controls powered by Microsoft Purview. Review the Copilot security information. [Learn about data protection in Copilot](#)

Discover and assess end-to-end AI and agent risk across Purview, Microsoft Defender, and Microsoft Entra. [Go to Microsoft Security Dashboard for AI](#)

Prevent data leaks

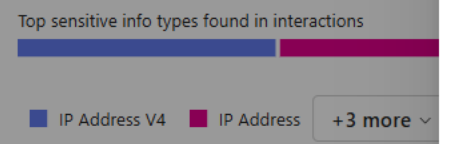
Default protections in place

- Policy running: Protect sensitive Microsoft 365 Copilot interactions
 - All Copilot interactions are scanned for sensitive info.
 - Sensitive info monitored for all users.

Policy is monitoring only

Prevent data leakage in Copilot interactions

We've detected the following sensitive info types in Copilot interactions. Turn on a policy to prevent sensitive info from being used in Copilot.



Manage policy

Manage data oversharing

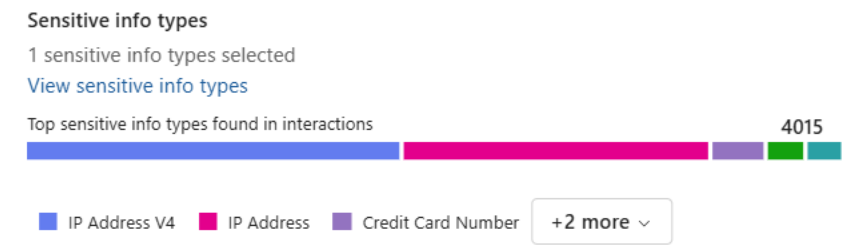
Default protections in place

Not started

Prevent data leakage in Copilot interactions

Turn on a policy to prevent Copilot from processing prompts that include sensitive info. [Learn more about Microsoft Purview Data Loss Prevention policies](#)

Policy name
Protect sensitive Microsoft 365 Copilot interactions



Users and groups
All users and groups selected
[Select users and groups](#)

Locations
Microsoft 365 Copilot
Copilot chat

- Actions**
- Prevent Copilot from processing user prompts that include sensitive info.

- What to expect**
- When a policy is turned on, it takes up to 24 hours for the policy to go into effect.
 - The policy can be customized further with Microsoft Purview Data Loss Prevention.

Turn on policy Cancel

- Home
- Copilot
- Overview
- Connectors
- Search
- Billing & usage
- Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup
- Customize navigation
- Show all

Home

Copilot Control System

Overview Security Usage Health Discover

Protected by Microsoft Purview

Microsoft 365 Copilot already includes built-in security controls powered by Microsoft Purview. Review the Copilot security information. [Learn about data protection in Copilot](#)

Discover and assess end-to-end AI and agent risk across Purview, Microsoft Defender, and Microsoft Entra. [Go to Microsoft Security Dashboard for AI](#)

Prevent data leaks

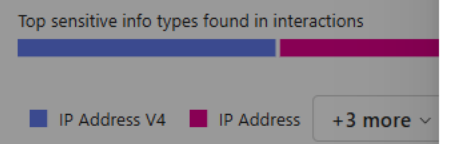
Default protections in place

- Policy running: Protect sensitive Microsoft 365 Copilot interactions
 - All Copilot interactions are scanned for sensitive info.
 - Sensitive info monitored for all users.

Policy is monitoring only

Prevent data leakage in Copilot interactions

We've detected the following sensitive info types used in Copilot.



Manage policy

Manage data oversharing

Default protections in place

Not started

Select users and groups

- All users and groups
- Specific users and groups

No users selected
No groups selected

Select users and groups

Confirm

Cancel

Search

Chat

Agents

Analyst

Researcher

Interview Questions Assist...

Quiz Tutor

Learning Coach

All agents

Create agent

Conversations

Pages

Notebooks

Create

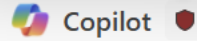
Apps

Admin

Today

Mergers and Acquisitions

Anything related to mergers & acquisitions.



Summarize Fabrikam Merger Status - May 26 2025.docx

The document titled [Fabrikam Merger Status - May 26 2025](#) is restricted due to your organization's security policies, so I'm unable to access or summarize its contents.

If you have specific questions about the document or need help with a particular section, feel free to paste the text here or let me know how else I can assist!



Summarize the key points of the document

Provide an overview of the merger status



Message Copilot

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Compliance Manager
- Overview
- Policies
- Recommendations
- Alerts
- Classifiers
- Explorers
- Diagnostics
- Pay-as-you-go usage report
- Posture reports
- Related solutions
- Data Security Investigations
- Information Protection
- Insider Risk Management

Policy not enforced

Safeguard sensitive data in Microsoft 365 Copilot interactions

Purview now offers granular Copilot controls, allowing admins to block all processing or allow internal knowledge access while blocking when sensitive data is detected. The default DLP policy is currently in simulation mode and can be turned on to restrict Copilot from prompts or performing web searches.

Top sensitive info types in Copilot interactions



Enforce policy

Create policy Export policies Refresh Copilot

Name	Priority	Mode	Triage agent
<input type="checkbox"/> Restrict Copilot for M365 access to content by label	0	On	Lim
<input type="checkbox"/> Restrict Copilot processing of sensitive prompts	1	On	Lim
<input type="checkbox"/> Block sharing sensitive information in Teams	2	On	Eligi
<input type="checkbox"/> Devices: File Too Large	3	On	Lim
<input type="checkbox"/> Service: HR Data	4	On	Eligi
<input type="checkbox"/> Devices: HR Data	5	On	Lim
<input type="checkbox"/> Project Obsidian Endpoint Policy	6	On	Eligi
<input type="checkbox"/> Prevent sharing sensitive information externally	7	On	Eligi
<input type="checkbox"/> Prevent emailing sensitive information externally	8	On	Lim
<input type="checkbox"/> Prevent sharing sensitive information with Gen AI sites	9	On	Lim
<input type="checkbox"/> Prevent sharing of sensitive info with external collab sites	10	In simulation with notifications	

Data security

Safeguard sensitive data in Microsoft 365 Copilot interactions

Customize the policy by choosing from the sections below. For advanced configuration, edit the policy in DLP solution.

Users and groups

Sensitive Information Types

Select the sensitive information type you want to protect with your DLP policy.

Content contains: Any of these

Sensitive info types: 2 selected (view)

- All Medical Terms And Conditions
- All Credential Types

+ Add

Actions

Use actions to protect content when the conditions are met

Restrict Copilot from processing content

Choose how content that matches your conditions should be restricted during the following Copilot activities. Learn more about these actions

- Restrict user prompts from being processed
- Restrict web searches

Enforce policy

Cancel



Search

Chat

Agents

Analyst

Researcher

Interview Questions Assist...

Quiz Tutor

Learning Coach

All agents

Create agent

Conversations

Pages

Notebooks

Create

Apps

Admin

Today

Please summarize Project Wingtip



This request can't be completed because your organization has blocked Copilot from responding to some types of content.

Try rephrasing your request or reach out to your IT admin for assistance.



Message Copilot

Microsoft 365 Copilot interface sidebar:

- New chat
- Search
- Library
- Create
- Frontier
- Agents
 - Researcher
 - Analyst
 - Idea Coach
 - Prompt Coach
 - New agent
 - All agents
- Notebooks
 - All notebooks
- Chats
 - Fabrikam's Wingtip Toys Acqui...
 - Vendor Bank Details Verification...
 - Latest Update on Contoso Mer...
- Apps

Yesterday

Can you share more detail about Fabrikam's acquisition of Wingtip Toys, aka "Project Falcon"

Copilot

Your request cannot use web search because it includes content restricted by your organization's security policy. Here's a grounded, internal-data-based view of **Fabrikam's acquisition of Wingtip Toys**, which is internally referred to as **Project Falcon**, based on the latest files and communications in our Microsoft 365 environment.

Overview of Project Falcon (Wingtip Toys Acquisition)

Project Falcon is the internal codename used for **Fabrikam's acquisition of Wingtip Toys**, a strategic move aimed at expanding product offerings and capturing operational and cost synergies. The acquisition has progressed through all major transactional milestones and is currently in the integration phase.

Create wingtip ac... +1

Transaction Timeline & Key Milestones

The following milestones are explicitly documented in the acquisition status materials and email updates:

Message Copilot

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Compliance Manager

- Posture
- Objectives
- AI observability
- Discover
- Apps and agents
- Activity explorer
- Asset explorer
- Data risk assessments**
- Tasks and actions
- Reports

Data risk assessment results

Review results to identify potential oversharing risks in your organization and apply fixes, such as limiting access to sensitive data and evaluating access to S

Export selected item Scoped assessment


<input type="checkbox"/>	Site name	Source type	Sensitivity label	Total items	Total items accessed	Times users accessed items
<input type="checkbox"/>	Data Security Sample Data	SharePoint / Standard	Confidential/All em...	8,621	8,625	13,460
<input type="checkbox"/>	DSI 40MB	SharePoint	None	1,487	1,487	1,962
<input checked="" type="checkbox"/>	Mark 8 Project Team	SharePoint / Standard	None	60	118	357
<input type="checkbox"/>	Project Obsidian v2	SharePoint / Standard	None	111	111	319
<input type="checkbox"/>	Data Security Demos	SharePoint / Standard	None	84	80	242
<input type="checkbox"/>	Project Obsidian	SharePoint / Standard	None	15	17	153
<input type="checkbox"/>	Microsoft Security Labs for C...	SharePoint	General	26	29	145
<input type="checkbox"/>	Engineering	SharePoint	Confidential/All em...	69	69	115
<input type="checkbox"/>	Sales and Marketing	SharePoint / Standard	None	21	47	111
<input type="checkbox"/>	Project Rho (Restricted conte...	SharePoint / Standard	Highly Confidential/...	12	12	93
<input type="checkbox"/>	ZavaCore v-Team	SharePoint / Standard	None	81	59	88
<input type="checkbox"/>	Contoso Digital's Headquarters	SharePoint	General	39	39	78
<input type="checkbox"/>	TinUStudio	SharePoint	None	36	38	77
<input type="checkbox"/>	Finanzas	SharePoint	Highly Confidential/...	33	37	74
<input type="checkbox"/>	Proseware Merger	SharePoint / Standard	None	10	10	58
<input type="checkbox"/>	Communication site	SharePoint	None	13	16	42
<input type="checkbox"/>	Gerald's Demos	SharePoint	Confidential/All em...	41	41	41

Mark 8 Project Team

Other labeling policies


Default sensitivity label for SharePoint document library

When a default sensitivity label is created, the label will only apply to new items added to the site. Select a sensitivity label in the SharePoint site.

 **Create default sensitivity label for SharePoint document library**
 Microsoft SharePoint location

Default labels


Label all new items by default using sensitivity labels. The admin can define labels with protection and labels with no protection. Assign default labels when creating a label policy.

 **Assign default sensitivity label**
 Microsoft Purview Information Protection


Sensitive information auto-labeling policy

Files with sensitive info types
34
[View items](#)


Use auto-labeling policies based on sensitive content or keywords.

 **Create auto-labeling policy for sensitive information**
 Microsoft Purview Information Protection

SharePoint site sensitivity label

 This label will only apply to the site and not the contents of the site.

Apply a sensitivity container label to the site.

 **Edit SharePoint site sensitivity container label**
 Microsoft SharePoint location

Review unused files

Remediate Oversharing

- Home
- Copilot
 - Overview
 - Connectors
 - Search
 - Billing & usage
 - Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup
- Customize navigation
- Show all

Copilot Control System

- Overview
- Security**
- Usage
- Health
- Discover

Protected by Microsoft Purview

Microsoft 365 Copilot already includes built-in security controls powered by Microsoft Purview. Review the Copilot security information on this page for insights and to further protect your data. [Learn about data protection in Copilot](#)

Discover and assess end-to-end AI and agent risk across Purview, Microsoft Defender, and Microsoft Entra. [Go to Microsoft Security Dashboard for AI](#)

Prevent data leaks

Default protections in place

- Policy running: Protect sensitive Microsoft 365 Copilot interactions
 - All Copilot interactions are scanned for sensitive info.
 - Sensitive info monitored for all users.

Policy is monitoring only

Prevent data leakage in Copilot interactions

We've detected the following sensitive info types in your org. Turn on a policy to prevent sensitive info from being used in Copilot.

Top sensitive info types found in interactions 4008

■ IP Address V4 ■ IP Address + 3 more

[Manage policy](#)

Current status

Prompts with sensitive info types **234**

Total prompts **234**

Manage data oversharing

Default protections in place

Not started

- Home
- Copilot
- Overview
- Connectors
- Search
- Billing & usage
- Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup

- Customize navigation
- Show all

Manage data oversharing

Default protections in place

- Copilot honors sensitivity labels and permissions for files, preventing potential oversharing.
- Specific SharePoint sites can be restricted from being used in Copilot.

Not started

Reduce oversharing risks

Apply sensitivity labels and tighten permissions to limit access to sensitive files and sites in Copilot.

What we found

Sharepoint sites referenced	Files referenced
20	43

Improve permissions

Sensitive data prevented from oversharing

File referenced with labeling protection
31 of 43

Strengthen data compliance

Default protections in place

- Copilot is checked against Microsoft recommended AI compliance standards.
- Essential actions are enforced to keep Copilot interactions secure.
- Compliance scores are monitored in real time and logged in audit-ready reports for continuous tracking.

In progress

Enhance compliance for Copilot interactions

Complete the suggested actions to meet Microsoft recommended AI compliance standards and keep Copilot interactions secure.

Completed by Microsoft	Completed by your organization
96	3/80

Breakdown of recommended actions

Protect Copilot when it is deployed	66
Manage, govern, and ensure transparency on data	141
Proactively identify, manage and reduce risks	128

Completed By Microsoft +2 more

View details



- Home
- Copilot
 - Overview
 - Connectors
 - Search
 - Billing & usage
 - Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup
- Customize navigation
- Show all

Manage data oversharing

Default protections in place

- Copilot honors sensitivity labels and permissions for files, preventing potential oversharing.
- Specific SharePoint sites can be restricted from being used in Copilot.

Not started

Reduce oversharing risks

Apply sensitivity labels and tighten permissions to restrict access to sensitive files and sites in Copilot.

What we found

Sharepoint sites referenced	Files referenced
20	43

Improve permissions

Strengthen data compliance

Default protections in place

- Copilot is checked against Microsoft recommended AI compliance standards.
- Essential actions are enforced to keep Copilot interactions secure.
- Compliance scores are monitored in real time and logged in audit-ready reports for continuous tracking.

In progress

Enhance compliance for Copilot interactions

Complete the suggested actions to meet Microsoft recommended AI compliance standards and keep Copilot interactions secure.

Completed by Microsoft	Completed by your organization
96	3/80

View details

Reduce oversharing risks

Learn how to address oversharing concerns in Copilot

In the [Microsoft 365 Copilot deployment blueprint](#) learn more about a recommended, staged approach to address oversharing concerns during a Copilot deployment.

Work with your data security admins on reviewing sensitivity labeling

- Create [sensitivity labels](#) to limit file access. Copilot only shows files to users with the right label or permission.
- When you create a sensitivity label, you can [automatically assign](#) it to Microsoft 365 items such as files and emails.

[Learn more about Microsoft Purview controls for Copilot](#)

Work with your SharePoint admins on reviewing site and file permissions

- Restrict specific [SharePoint sites](#) from being used in Copilot.
- Update [link sharing defaults for your organization](#) from organization-wide sharing to specific people links.
- Initiate a [Site Access Review](#) for site owners to evaluate permissions and user access on sites.

[Learn more about SharePoint Advanced Management controls for Copilot](#)

Mark as completed Cancel

- Home
- Solutions
 - DSPM (preview)
 - Posture
 - Objectives
 - AI observability
 - Discover
 - Tasks and actions
 - Reports
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Compliance Manager

Key posture metrics

Review key data security posture metrics for your organization's data sources from the last 30 days. This includes data in Microsoft 365 and non-Microsoft 365 sources.

<p>D Data discovery</p> <p>Classified and labeled assets</p> <p>0.59% ↘ 0.11% in 27 days</p>	<p>P Data protection</p> <p>Activities covered by Data Loss Prevention</p> <p>42% ↗ 42% in 30 days</p>	<p>I Data investigation</p> <p>Data protection alerts triaged</p> <p>42% ↘ 20% in 30 days</p>
---	---	--

Featured insights

New tools to help you secure your data, improve your posture, and identify new risks.

Key agent insights

Total agents in your org	65
Agents with sensitive interactions	2
High risk agents	0

Gain visibility into AI agents across your organization

AI observability lets you see how sensitive data flows through AI agents, so you can discover risks early and enforce the right policies with confidence.

[View AI observability](#)

Assess end-to-end AI and agent risk with Security Dashboard for AI

See how AI apps and agents improve your security posture.

Top objectives to protect sensitive data

Focusing on these objectives helps you monitor key areas of your data security posture to prevent risks to sensitive data. Review and complete remediation plans for each objective to improve your posture and protect sensitive data. [Learn more](#)

[View all objectives](#)

<p>P Data protection</p> <p>Prevent data exposure in Microsoft 365 Copilot and Microsoft Copilot interactions</p> <p>Copilot interactions with sensitive data</p> <p>2K → +0% in last 29 days</p> <p>2,006 Microsoft 365 Copilot and Microsoft Copilot interactions with sensitive data were detected from your organization in the last 30 days, a decrease of 0%. This could indicate emerging patterns of data exposure.</p>	<p>P Data protection</p> <p>Prevent oversharing of sensitive data</p> <p>Overshared items</p> <p>9.7K → +0% in last 30 days</p> <p>9,711 items containing sensitive data from Microsoft 365 Copilot and Microsoft Copilot are unlabeled and contain sensitive data, in the last 30 days, an increase of 0%. This could indicate emerging patterns of oversharing sensitive data.</p>
---	--

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Compliance Manager

- DSPM (preview)
- Posture
- Objectives**
- AI observability
- Discover
- Tasks and actions
- Reports

Data security objectives


View and track data security objectives for your organization. Each objective highlights key risks to address, actions to take, and progress over time. This helps your organization stay aligned with your overall data security posture.

- Data protection
- Data discovery


Data protection

Prevent data exposure in Microsoft 365 Copilot and Microsoft Copilot interactions

2,006 Microsoft 365 Copilot and Microsoft Copilot interactions with sensitive data were detected from your organization in the last 30 days, a decrease of 0%. This could indicate emerging patterns of data exposure.



2K interactions

 → +0% in last 29 days

2K → +0% in last 0 days User prompts	9 → +0% in last 0 days Copilot responses	9.7K ↘ -0.37% in last 29 days Files overshared
--	--	--

Take action to reduce risk


Taking action could reduce sensitive interactions from 2006 to 0, which is about a 100% decrease.

[View remediation plan](#) [Copilot prompts](#) [View objective →](#)


Data protection

Prevent oversharing of sensitive data

9,711 items containing sensitive data from Microsoft 365 Copilot and Microsoft Copilot are unlabeled and contain sensitive data, in the last 30 days, an increase of 0%. This could indicate emerging patterns of oversharing sensitive data.



9.7K items at risk

 → +0% in last 30 days

0 → +0% Total unscanned items	11.3K ↗ +1% Total unlabeled items	11.5K ↗ +1% Total items
---	---	-----------------------------------

[View remediation plan](#) [Copilot prompts](#) [View objective →](#)

Data protection

Prevent files and documents from being shared

- Home
 - Solutions
 - Agents
 - Learn
 - Usage center (preview)
 - Settings
 - Data Loss Prevention
 - DSPM (preview)
 - DSPM for AI (classic)
 - eDiscovery
 - Compliance Manager
- DSPM (preview)
 - Posture
 - Objectives
 - AI observability
 - Discover
 - Apps and agents
 - Activity explorer
 - Asset explorer
 - Data risk assessments
 - Tasks and actions
 - Reports

Data security objectives > Prevent oversharing of sensitive data

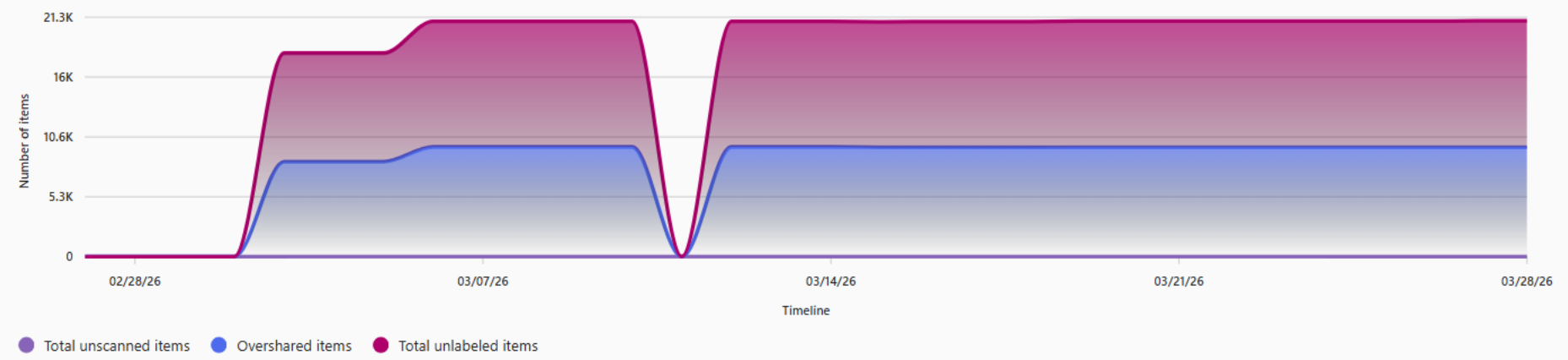
Objective: Prevent oversharing of sensitive data

View prompts

Prevent users in your organization from sharing access to items that are unlabeled and contain sensitive information, beyond what is necessary or appropriate.

Data oversharing trends

Analyze the volume of sensitive data overshared in your organization.



Remediation plan to prevent oversharing (5 actions)
 Reduce oversharing of sensitive data within your organization.

View remediation plan

Key oversharing metrics

Overshared items	9.7K	Total unscanned items	0	Total unlabeled items	11.2K	Total items	11.4K
	↑ +100% in last 30 days		→ +0%		↑ +100%		↑ +100%

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Compliance Manager

- Posture
- Objectives**
- AI observability
- Discover
- Tasks and actions
- Reports

Remediation plan: Prevent oversharing of sensitive data

Increased risks detected in the last 30 days
Unlabeled and sensitive data are at risk of being overshared beyond intended audiences.

Remediation plan
Complete the following actions to reduce oversharing and improve data protection across your organization.

Data risk assessments

Protect your data from potential oversharing risks in Microsoft 365

Data assessments provide you with insights on potential oversharing risks in your organization along with remediation actions to clean up your permissions on data.

[View details](#) [View Microsoft 365 default assessment results](#)

Data risk assessments

Protect your data from potential oversharing risks in Microsoft Fabric

Start the default assessment for Microsoft Fabric to view insights on potential oversharing risks in your Fabric workspaces along with remediation actions to adjust permissions and user access.

[View details](#) [Configure Fabric default assessment](#)

Information Protection

> Hide details

Protect your data from potential oversharing risks in Microsoft 365

The Microsoft 365 default assessment provides you with insights on potential oversharing risks in your organization, along with actions to limit access to sensitive data on your top accessed data sources in Microsoft 365.

Steps at a glance

To view the latest scan results for the default oversharing assessment:

1. Select View Microsoft 365 default assessment.
2. Select a data source to view actions you can take.
3. Complete actions to protect your data.

What to expect

- The default data assessment runs weekly.

[View Microsoft 365 default assessment results](#)

View prompts

04/04/26

[View remediation plan](#)

11.5K

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM**
- Information protection
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

- DSPM (preview)
- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments**
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment | Contoso merger assessment

Contoso merger assessment

Overview Potentially overshared items New

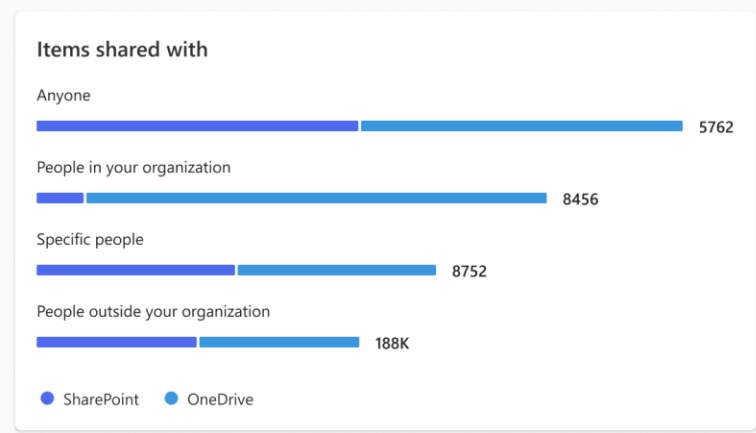
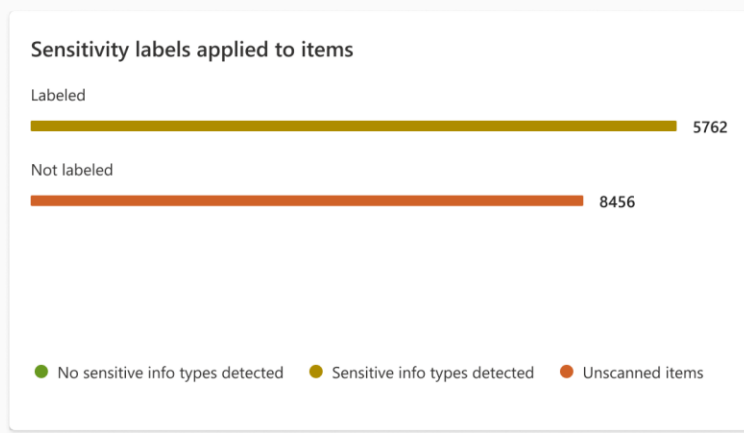
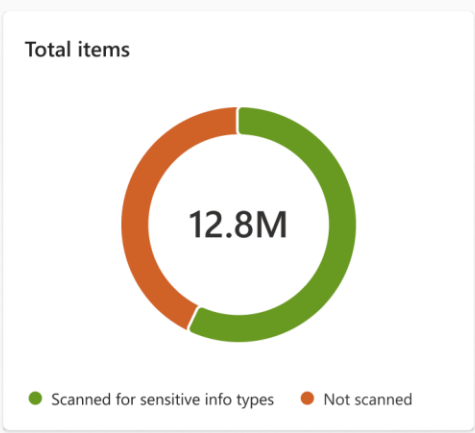
136 potentially overshared items detected

136 items are potentially overshared in your scoped data sources. An item is identified as potentially overshared if it has a sharing link that's accessible to external or anonymous users. View detected items and remediate as needed.

[View items](#)

Assessment details

Sources included 64	Potentially overshared items 136	Status Completed	Completed on March 17, 2025
------------------------	-------------------------------------	---------------------	--------------------------------



Data assessment results

Review potential oversharing risks in your org and take action, such as limiting access to sensitive data and evaluating access to SharePoint sites.

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- ...
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

- DSPM (preview)
- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment | Contoso merger assessment

Contoso merger assessment

Overview Potentially overshared items New

✓ Resolve  Notify More actions ▾

10 items

<input type="checkbox"/>	> Name	Sharing link type	Sensitivity label	Owner	Last modified date	Last Action	Remediation status
<input type="checkbox"/>	▼ https://zava.sharepoint.com/sites/contoso						--
<input type="checkbox"/>	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	Contoso merger strategy.pptx	Anyone	General	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	System_Admin_Credentials_2.text (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	Pending
<input type="checkbox"/>	▼ /sites/operationsdepartment (1)						--
<input type="checkbox"/>	System_setup_instructions.docx	Anyone	Confidential	Robine Kline	10/13/2025	--	Pending

Assessments result in a list of potentially overshared items, security teams can take action

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

DSPM (preview)

- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment Contoso merger assessment

Contoso merger assessment

Overview Potentially overshared items New

✓ Resolve ✉ Notify ⌵ More actions

<input type="checkbox"/>	> Name	Sharing link type	Sensitivity label	Owner
<input type="checkbox"/>	↳ https://zava.sharepoint.com/sites/contoso			
<input checked="" type="checkbox"/>	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
<input checked="" type="checkbox"/>	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
<input checked="" type="checkbox"/>	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Contoso merger strategy.pptx	Anyone	General	Robine Kline
<input type="checkbox"/>	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	↳ /sites/operationsdepartment (1)			
<input type="checkbox"/>	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

Resolve 3 items

Items to resolve
 Contoso status.docx (1), Contoso passwords.txt (2), System_Admin_Credentials_Contoso

Resolving these items mean you've determine they're not overshared. They'll be flagged as "Remediated in the status column"

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

DSPM (preview)

- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment | Contoso merger assessment

Contoso merger assessment

Overview **Potentially overshared items** New

✓ Resolve ✉ Notify **More actions** ▾ 10 items

<input type="checkbox"/>	Name	Sharing link type	Sensitivity label	Owner	Last modified date	Last Action	Remediation status
<input type="checkbox"/>	> https://zava.sharepoi...						--
<input type="checkbox"/>	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline	10/13/2025	Resolved	✓ Remediated
<input type="checkbox"/>	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline	10/13/2025	Resolved	✓ Remediated
<input type="checkbox"/>	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline	10/13/2025	Resolved	✓ Remediated
<input type="checkbox"/>	Contoso merger strategy.pptx	Anyone	General	Robine Kline	10/13/2025	Notified	✓ Remediated
<input checked="" type="checkbox"/>	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	⌛ Pending
<input type="checkbox"/>	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending
<input type="checkbox"/>	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending
<input type="checkbox"/>	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline	10/13/2025	--	⌛ Pending
<input type="checkbox"/>	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending
<input type="checkbox"/>	> /sites/operationsdepartment (1)						--
<input type="checkbox"/>	System_setup_instructions.docx	Anyone	Confidential	Robine Kline	10/13/2025	--	⌛ Pending

Remove sharing link

Apply sensitivity label

Remediation status

- ✓ Remediated
- ✓ Remediated
- ✓ Remediated
- ✓ Remediated
- ⌛ Pending
- ⌛ Pending
- ⌛ Pending
- ⌛ Pending
- ⌛ Pending

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

DSPM (preview)

- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment Contoso merger assessment

Contoso merger assessment


Overview Potentially overshared items New


Resolve
 Notify

<input type="checkbox"/>	Name	Sharing link type	Sensitivity label	Owner
<input type="checkbox"/>	https://zava.sharepoi...			
<input type="checkbox"/>	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Contoso merger strategy.pptx	Anyone	General	Robine Kline
<input checked="" type="checkbox"/>	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	/sites/operationsdepartment (1)			
<input type="checkbox"/>	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

Apply sensitivity label

Choose a sensitivity label

Choose a sensitivity label 

Changes will apply to all selected items 

Items to update

Contoso FY25 financials.xlsx (2)

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

DSPM (preview)

- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment Contoso merger assessment

Contoso merger assessment

Overview **Potentially overshared items** New

✓ Resolve ✉ Notify **More actions** ▾

<input type="checkbox"/>	> Name	Sharing link type	Sensitivity label	Owner
<input type="checkbox"/>	https://zava.sharepoint.com			
<input type="checkbox"/>	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Contoso merger strategy.pptx	Anyone	General	Robine Kline
<input checked="" type="checkbox"/>	Contoso FY25 financials.xlsx (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	> /sites/operationsdepartment (1)			
<input type="checkbox"/>	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

Apply sensitivity label

Choose a sensitivity label

- Choose a sensitivity label ▾
- Public
- General
- Confidential
- Highly Confidential

- Home
- Solutions
- Agents
- Learn
- Settings
- DSPM
- Information protection
- Tasks and actions
- Setup tasks
- Remediation actions
- Reports

DSPM (preview)

- Posture
- Objectives
- AI observability (preview)
- Discover
- Apps and agents
- Data risk assessments
- Activity explorer
- Asset explorer

← Back to Data Risk Assessment Contoso merger assessment

Contoso merger assessment

Overview Potentially overshared items New

✓ Resolve ✉ Notify **More actions** ▾

<input type="checkbox"/>	> Name	Sharing link type	Sensitivity label	Owner
<input type="checkbox"/>	https://zava.sharepoint...			
<input type="checkbox"/>	Contoso status.docx (1)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso passwords.txt (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_Contoso	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Contoso merger strategy.pptx	Anyone	General	Robine Kline
<input type="checkbox"/>	Contoso FY25 financials.xlsx (2)	Anyone	General	Robine Kline
<input checked="" type="checkbox"/>	Contoso employee info.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	Due diligence report.docx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	System_Admin_Credentials_2.txt (2)	Anyone	Unlabeled	Robine Kline
<input type="checkbox"/>	Contoso FY24 financials.xlsx (2)	Anyone	Confidential	Robine Kline
<input type="checkbox"/>	> /sites/operationsdepartment (1)			
<input type="checkbox"/>	System_setup_instructions.docx	Anyone	Confidential	Robine Kline

- Remove sharing link
- Apply sensitivity label

Remove sharing link

Items to remove sharing link

Name	Access link type
Contoso employee info.xlsx (2)	Anonymous

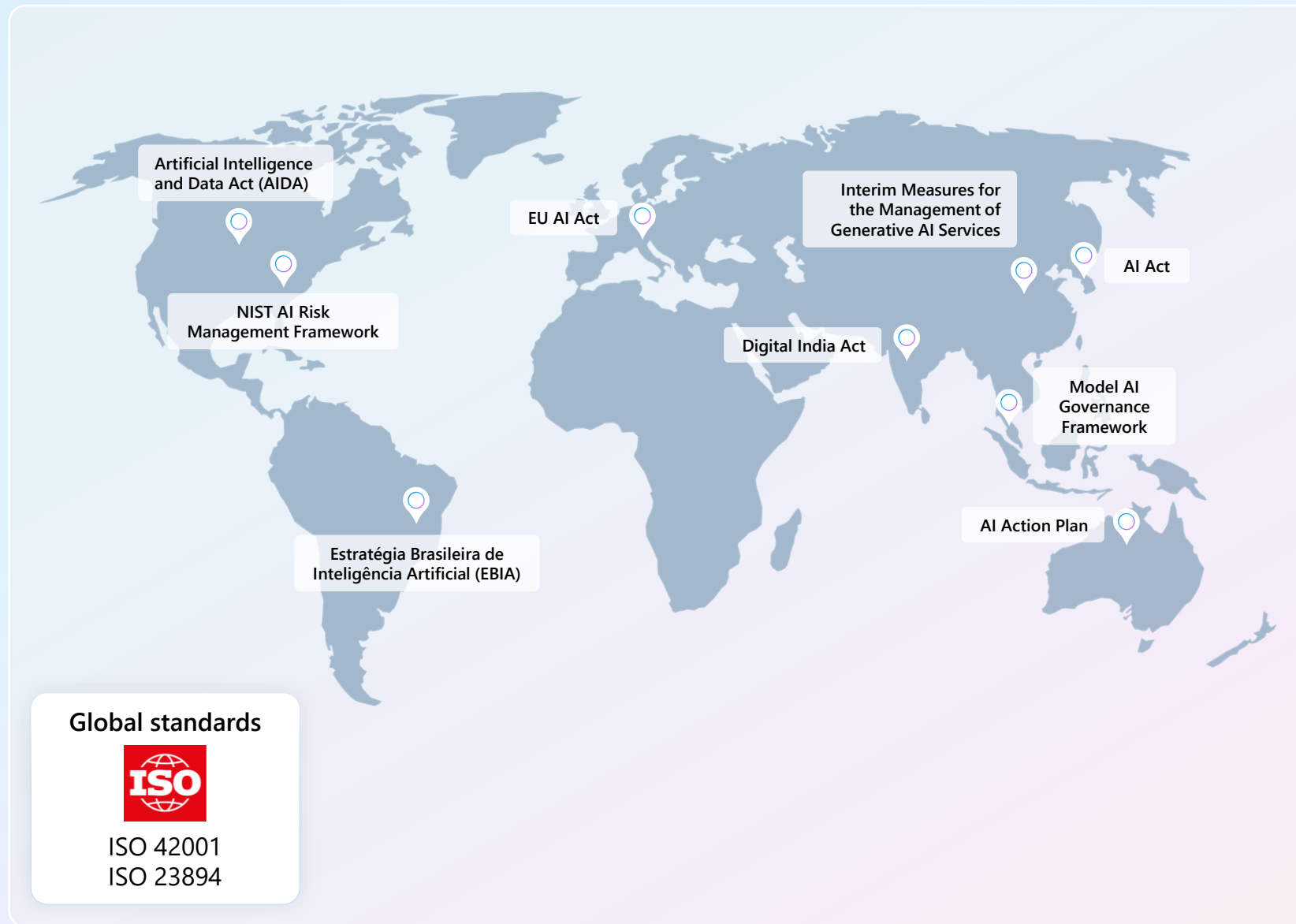
Meet Regulations

AI regulations are emerging across all regions

AI laws expanding across 50+ countries and regions

Organizations must prove AI safety, security, and transparency

Compliance has become the foundation of trust and resilience



Microsoft's view: AI innovation and regulation aren't opposites — they must advance together.

- Home
- Copilot
- Overview
- Connectors
- Search
- Billing & usage
- Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup

- Customize navigation
- Show all

Manage data oversharing

Default protections in place

- Copilot honors sensitivity labels and permissions for files, preventing potential oversharing.
- Specific SharePoint sites can be restricted from being used in Copilot.

Not started

Reduce oversharing risks

Apply sensitivity labels and tighten permissions to limit access to sensitive files and sites in Copilot.

What we found

Sharepoint sites referenced	Files referenced
20	43

Improve permissions

Sensitive data prevented from oversharing

File referenced with labeling protection
31 of 43

Strengthen data compliance

Default protections in place

- Copilot is checked against Microsoft recommended AI compliance standards.
- Essential actions are enforced to keep Copilot interactions secure.
- Compliance scores are monitored in real time and logged in audit-ready reports for continuous tracking.

In progress

Enhance compliance for Copilot interactions

Complete the suggested actions to meet Microsoft recommended AI compliance standards and keep Copilot interactions secure.

Completed by Microsoft	Completed by your organization
96	3/80

View details

Breakdown of recommended actions

Protect Copilot when it is deployed	66
Manage, govern, and ensure transparency on data	141
Proactively identify, manage and reduce risks	128

Completed By Microsoft +2 more



- Home
- Copilot
- Overview
- Connectors
- Search
- Billing & usage
- Settings
- Agents
- Users
- Devices
- Teams & groups
- Billing
- Setup
- Customize navigation
- Show all

Manage data oversharing

Default protections in place

- Copilot honors sensitivity labels and permissions for files, preventing potential oversharing.
- Specific SharePoint sites can be restricted from being used in Copilot.

Not started

Reduce oversharing risks

Apply sensitivity labels and tighten permission access to sensitive files and sites in Copilot.

What we found

Sharepoint sites referenced	Files referenced
20	43

Improve permissions

Strengthen data compliance

Default protections in place

- Copilot is checked against Microsoft recommended AI compliance standards.
- Essential actions are enforced to keep Copilot interactions secure.
- Compliance scores are monitored in real time and logged in audit-ready reports for continuous tracking.

In progress

Enhance compliance for Copilot interactions

Complete the suggested actions to meet Microsoft recommended AI compliance standards and keep Copilot interactions secure.

Completed by Microsoft	Completed by your org
96	3/80

View details

Enhance your protection and compliance

Microsoft has created a set of AI safety and compliance recommendations based on global AI regulations. It contains actions you can take to improve the safety of interactions with Copilot. [Learn more about AI baseline assessment.](#)

What is compliance and why is it important?

Compliance is about following the rules set by laws, regulations, and organization standards on how data is handled. It is crucial because it protects sensitive information, builds trust, reduces risk, improves operational efficiency, and helps prevent legal consequences.

What Microsoft has already completed for you

Actions completed by Microsoft

96

- To protect Copilot when it is deployed
 - Copilot comes with checks to ensure protection and continuous monitoring during deployment and runtime.
- To manage, govern and ensure transparency on data
 - Everything Copilot does- risks, controls, and decisions is clearly logged. This makes it easy for admins to track actions, check compliance, and solve issues.
- To proactively identify, manage and reduce risks
 - Ensure that threats are anticipated, so you take actions to reduce risks and your environment remains secure and compliant.

What you can do to improve your protection

Recommended actions to be completed by your org

3/80

Work with your data security and compliance admin to complete additional recommended actions in Microsoft Purview Compliance Manager. [Learn more about Compliance Manager](#)

View recommendations in Microsoft Purview

Cancel



Microsoft Purview
Compliance Manager

What's new

AI-powered regulatory templates



Helps CISOs, Risk, Legal,
Compliance, and IT leaders.



Turns overwhelming
regulation into clear,
actionable priorities



Applies across
Microsoft Foundry and other
services to access agent
compliance posture

Home Solutions Agents Learn Usage center (preview) Settings Data Loss Prevention DSPM (preview) DSPM for AI (classic) eDiscovery Compliance Manager

Compliance Manager

Overview Improvement actions Solutions Assessments **Regulations** Policies Alerts Reports

Related solutions

Data Security Investigations Data Lifecycle Management Data Loss Prevention

Create new template Customize regulation Delete Draft 391 items Search Group

Filters: Service: Any Role type: Any Created by: Any Activation: Any Availability: Any Status: Any

Regulation Status Availability Created by Last updated d... Overarching re... Created date Activation Services

Sub-Service Compliance Readiness (4)

<input type="checkbox"/>	PCI DSS v4.0	Ready to use	Pre-Deployment	7/10/2023	PCI DSS	2/27/2023	Active	Azure
<input type="checkbox"/>	System and Organization Contro...	Ready to use	Pre-Deployment	7/10/2023	System and Organiza...	2/27/2023	Active	Azure
<input type="checkbox"/>	ISO/IEC 27001:2013	Ready to use	Pre-Deployment	7/10/2023	ISO/IEC 27001:2013	2/27/2023	Active	Azure
<input type="checkbox"/>	NIST 800-53 rev.4	Ready to use	Pre-Deployment	7/10/2023	NIST 800-53	2/28/2023	Active	Azure

Included templates (2)

<input type="checkbox"/>	Data Protection Baseline	Ready to use	Included	7/10/2023	Data protection basel...	7/10/2023	Active	Salesforce, Zoom, M
<input type="checkbox"/>	AI Baseline	Ready to use	Included	11/12/2025	AI Baseline	10/10/2025	Active	Azure AI Foundry, Ui

Premium AI templates (4)

<input type="checkbox"/>	NIST AI Risk Management Frame...	Ready to use	Premium AI	10/3/2025	NIST AI Risk Manage...	3/27/2024	Active	fdxc, myOwnService,
<input type="checkbox"/>	ISO/IEC 23894:2023	Ready to use	Premium AI	10/3/2025	ISO/IEC 23894:2023	4/25/2024	Active	Universal, Microsoft
<input type="checkbox"/>	ISO/IEC 42001:2023	Ready to use	Premium AI	10/3/2025	ISO/IEC 42001:2023	3/29/2024	Active	Universal, Microsoft
<input type="checkbox"/>	EU Artificial Intelligence Act	Ready to use	Premium AI	10/3/2025	EU Artificial Intelligen...	4/17/2024	Active	Universal, Microsoft

Premium templates (381)

<input type="checkbox"/>	Standardized Information Gather...	Ready to use	Premium	10/14/2021	SIG	10/14/2021	Inactive	Microsoft 365, Unive
<input type="checkbox"/>	ISO IEC 80001-1:2010	Ready to use	Premium	5/23/2022	ISO IEC 80001-1:2010	5/23/2022	Inactive	Microsoft 365, Unive
<input type="checkbox"/>	EU - Directive 2006/24/EC	Ready to use	Premium	7/15/2022	EU Dir 2006/24/EC	5/23/2022	Inactive	Universal, Microsoft

Home Solutions Agents Learn Usage center (preview) Settings Data Loss Prevention Related solutions

Compliance Manager

- Overview
- Improvement actions
- Solutions
- Assessments
- Regulations**
- Policies
- Alerts
- Reports
- Data Security Investigations
- Data Lifecycle Management
- Data Loss Prevention

Create new template Customize regulation Delete Draft

Filters: Service: Any Role type: Any Created by: Any Activation: Any Availability: Any Status: Any

	Regulation	Status	Availability	Created by	Last updated
Sub-Service Compliance Readiness (4)					
<input type="checkbox"/>	PCI DSS v4.0	Ready to use	Pre-Deployment		7/10/2023
<input type="checkbox"/>	System and Organization Contro...	Ready to use	Pre-Deployment		7/10/2023
<input type="checkbox"/>	ISO/IEC 27001:2013	Ready to use	Pre-Deployment		7/10/2023
<input type="checkbox"/>	NIST 800-53 rev.4	Ready to use	Pre-Deployment		7/10/2023
Included templates (2)					
<input type="checkbox"/>	Data Protection Baseline	Ready to use	Included		7/10/2023
<input type="checkbox"/>	AI Baseline	Ready to use	Included		11/12/2025
Premium AI templates (4)					
<input type="checkbox"/>	NIST AI Risk Management Frame...	Ready to use	Premium AI		10/3/2025
<input type="checkbox"/>	ISO/IEC 23894:2023	Ready to use	Premium AI		10/3/2025
<input type="checkbox"/>	ISO/IEC 42001:2023	Ready to use	Premium AI		10/3/2025
<input type="checkbox"/>	EU Artificial Intelligence Act	Ready to use	Premium AI		10/3/2025
Premium templates (381)					
<input type="checkbox"/>	Standardized Information Gather...	Ready to use	Premium		10/14/2021
<input type="checkbox"/>	ISO IEC 80001-1:2010	Ready to use	Premium		5/23/2022
<input type="checkbox"/>	EU - Directive 2006/24/EC	Ready to use	Premium		7/15/2022

Create new template (preview)

Create custom templates quickly by uploading your own regulation document or by starting fresh with a blank template. [Learn more](#)

Use your own document

Your file will go through three steps: Scan for malware > Extract controls > Map controls to existing improvement actions. This process may take several minutes depending on file size.

[Upload PDF document](#)

Start from blank template

Begin with a blank template and define your controls manually.

[Create blank template](#)

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- Related solutions
 - DSPM (preview)
 - DSPM for AI (classic)
 - eDiscovery
 - Compliance Manager

Compliance Manager

- Overview
- Improvement actions
- Solutions
- Assessments
- Regulations**
- Policies
- Alerts
- Reports

Create new template Customize regulation Delete Draft

Filters: Service: Any Role type: Any Created by: Any Activation: Any Availability: Any Status: Any

	Regulation	Status	Availability	Created by	Last updated
Sub-Service Compliance Readiness (4)					
<input type="checkbox"/>	PCI DSS v4.0	Ready to use	Pre-Deployment		7/10/2023
<input type="checkbox"/>	System and Organization Contro...	Ready to use	Pre-Deployment		7/10/2023
<input type="checkbox"/>	ISO/IEC 27001:2013	Ready to use	Pre-Deployment		7/10/2023
<input type="checkbox"/>	NIST 800-53 rev.4	Ready to use	Pre-Deployment		7/10/2023
Included templates (2)					
<input type="checkbox"/>	Data Protection Baseline	Ready to use	Included		7/10/2023
<input type="checkbox"/>	AI Baseline	Ready to use	Included		11/12/2025
Premium AI templates (4)					
<input type="checkbox"/>	NIST AI Risk Management Frame...	Ready to use	Premium AI		10/3/2025
<input type="checkbox"/>	ISO/IEC 23894:2023	Ready to use	Premium AI		10/3/2025
<input type="checkbox"/>	ISO/IEC 42001:2023	Ready to use	Premium AI		10/3/2025
<input type="checkbox"/>	EU Artificial Intelligence Act	Ready to use	Premium AI		10/3/2025
Premium templates (381)					
<input type="checkbox"/>	Standardized Information Gather...	Ready to use	Premium		10/14/2021
<input type="checkbox"/>	ISO IEC 80001-1:2010	Ready to use	Premium		5/23/2022
<input type="checkbox"/>	EU - Directive 2006/24/EC	Ready to use	Premium		7/15/2022

Create new template

AI ACT REGULATION (EU) 2024 1689.pdf Change document

Template name *
AI ACT REGULATION (EU) 2024 1689

Overarching regulation ⓘ
AI ACT REGULATION (EU) 2024 1689

Services *
Azure AI Foundry

What will happen with the document?
Your selected file would go through the following steps. This may take up to several minutes depending on the file size. [Know more](#)

- Scan for malware**
Document will be checked for compatibility and malware.
- Extract controls**
It will be analyzed to identify & extract controls.
- Map controls to existing improvement actions**
The extracted controls will be mapped to existing improvement actions.

Scan and extract Back

- Home
- Solutions
 - Compliance Manager
- Learn
- Settings
- Compliance Manager
 - Overview
 - Improvement actions
 - Solutions
 - Assessments
 - Regulations
 - Policies
 - Alerts
 - Reports
- Related Solutions
 - Data Lifecycle Management
 - Data Loss Prevention

Service

Azure AI Foundry

AI ACT Regulation (EU) 2024/1689

Controls Your improvement actions Microsoft actions

Search Group by

Control family: Any

Control Name	Control ID	Achievable points	Improvement actions	Microsoft actions
> CHAPTER II PROHIBITED AI PRACTICES (2)				
> CHAPTER III HIGH-RISK AI SYSTEMS Section 2 Requirements for high-risk AI systems (35)				
> CHAPTER III HIGH-RISK AI SYSTEMS Section 1 Obligations of providers and deployers of high-risk AI systems and other parties (54)				
> CHAPTER III HIGH-RISK AI SYSTEMS Section 6 Notifying authorities and notified bodies (22)				
> CHAPTER III HIGH-RISK AI SYSTEMS Section 5 Standards, conformity assessment, certification, registration (35)				
> CHAPTER III HIGH-RISK AI SYSTEMS Section 1 Classification of AI systems as high risk (4)				
> CHAPTER IV TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS (7)				
> CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 1 Post-market monitoring (3)				
> CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 2 Sharing of information on serious incidents (9)				
> CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 3 Enforcement (42)				
> CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 4 Remedies (4)				
> CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE Section 5 Supervision, investigation, enforcement and monitoring in respect of providers of general-p...				
> CHAPTER V GENERAL-PURPOSE AI MODELS Section 1 Identification rules (5)				

- Home
- Compliance Manager**
- Solutions
 - Overview
 - Improvement actions
 - Solutions
 - Assessments
 - Regulations
 - Policies
 - Alerts
 - Reports
- Learn
- Settings
- Compliance Manager
- Related Solutions
 - Data Lifecycle Management
 - Data Loss Prevention

Risk management system

Overview

Details

Control ID	Achievable points
Article 9.8	45

Control family
CHAPTER III HIGH-RISK AI SYSTEMS
Section 2 Requirements for high-risk AI systems

Description

The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against predefined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

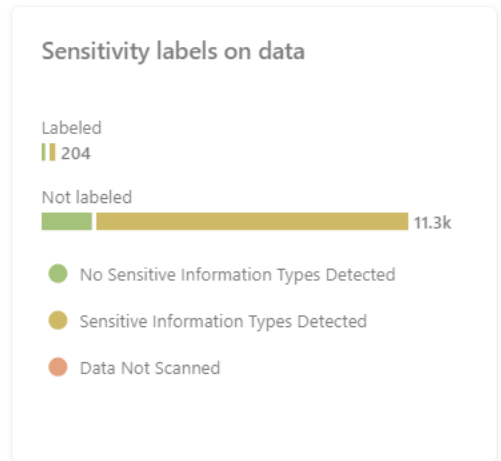
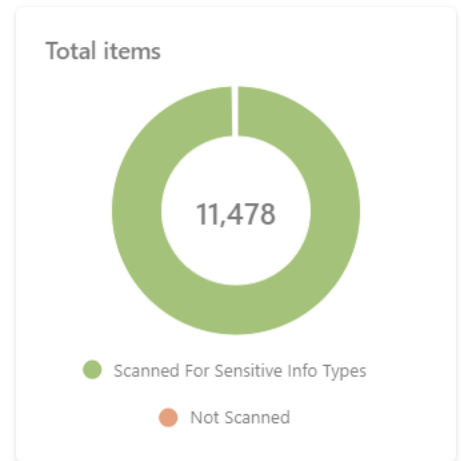
Feedback

Improvement actions Microsoft actions

Improvement action	Products	Achievable points
Enhance AI safety and compliance with Prompt Shields	Azure AI Foundry	9
Ensure compliance and safety for hateful & unfair content in generative AI with Azure AI Foundry	Azure AI Foundry	9
Ensure compliance and safety for ROUGE score in generative AI with Azure AI Foundry	Azure AI Foundry	9
Ensure compliance and safety for self-harm-related content in generative AI with Azure AI Foundry	Azure AI Foundry	9
Ensure compliance and safety for violent content in generative AI with Azure AI Foundry	Azure AI Foundry	9

- Home
- Solutions
- Agents
- Learn
- Usage center (preview)
- Settings
- Data Loss Prevention
- DSPM (preview)
- DSPM for AI (classic)
- eDiscovery
- Compliance Manager

- DSPM (preview)
- Posture
- Objectives
- AI observability
- Discover
 - Apps and agents
 - Activity explorer
 - Asset explorer
- Data risk assessments
 - Tasks and actions
 - Reports



Sharing links

Data risk assessment results

Review results to identify potential oversharing risks in your organization and apply fixes, such as limiting access to sensitive data.

Export selected item Scoped assessment

<input type="checkbox"/>	Site name	Source type	Sensitivity label	Total items	Total items accessed
<input type="checkbox"/>	Data Security Sample Data	SharePoint / Standard	Confidential/All em...	8,621	8,625
<input type="checkbox"/>	DSI 40MB	SharePoint	None	1,487	1,487
<input type="checkbox"/>	Data Security Demos	SharePoint / Standard	None	84	80
<input type="checkbox"/>	Project Management	SharePoint	Highly Confidential/...	48	57
<input type="checkbox"/>	ZavaCore v-Team	SharePoint / Standard	None	81	81
<input checked="" type="checkbox"/>	Mark 8 Project Team	SharePoint / Standard	None	62	121
<input type="checkbox"/>	Microsoft Security Labs for C...	SharePoint	General	26	29

Mark 8 Project Team

Default labels

Label all new items by default using sensitivity labels. The admin can define labels with protection and labels with no protection. Assign default labels when creating a label policy.

Assign default sensitivity label
Microsoft Purview Information Protection

Sensitive information auto-labeling policy

Files with sensitive info types
34

[View items](#)

Use auto-labeling policies based on sensitive content or keywords.

Create auto-labeling policy for sensitive information
Microsoft Purview Information Protection

SharePoint site sensitivity label

This label will only apply to the site and not the contents of the site.

Apply a sensitivity container label to the site.

Edit SharePoint site sensitivity container label
Microsoft SharePoint location

Review unused files

Items older than 3 years
0

Protect sensitive data from oversharing with retention policies.

Create retention policies
Microsoft Purview Data Lifecycle Management

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

Choose where to apply this policy

The policy will apply to content that's stored in the locations you choose.

Status	Location	Applicable Content	Included	Excluded
<input type="checkbox"/> Off	Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. More details		
<input type="checkbox"/> Off	Teams chats	Messages from individual chats, group chats, meeting chats, bot chats. More details		
<input type="checkbox"/> Off	Teams private channel messages	Messages from Teams private channels. More details		
<input type="checkbox"/> Off	Yammer community messages	Messages from Yammer community discussions. More details		
<input type="checkbox"/> Off	Yammer user messages	Private messages and community message notifications. More details		
<input checked="" type="checkbox"/> On	Microsoft Copilot experiences (Preview)	Built-in and custom Copilot experiences. Learn more	All users Edit	None Edit
<input type="checkbox"/> Off	Enterprise AI apps (Preview)	Non-Copilot AI apps that are onboarded or connected to your org using methods like Entra registration and data connectors. Learn more		
<input type="checkbox"/> Off	Other AI apps (Preview)	AI Apps users interact with through a browser. These apps are categorized as "Generative AI" in the Defender for Cloud		

Secure and Govern Microsoft 365 Copilot

A Foundational Deployment Guide



Remediate Oversharing

Identify high-risk sites
and content

Apply interim Copilot
protections

Fix access and permissions

Set up Guardrails

Establish secure defaults

Establish secure guardrails

Continuously enforce &
optimize guardrails

Meet Regulations

Identify and address gaps
against AI Regulations

Define Regulatory
Requirements

Improve data hygiene

Download the blueprint at
aka.ms/Copilot/SecureGovern

**We have an
exciting future ahead.**

Expertise and tools for your journey



Technical expertise via
our FastTrack partners

aka.ms/Microsoft/FastTrack



Tools, resources & training
on our Adoption Hub

adoption.microsoft.com



Events and real-world
knowledge in our
community

aka.ms/TechCommunity

News & community content



Microsoft Community Learning aka.ms/Community/LearningChannel

Community led expert content on all your favorite Microsoft services.



Start your week with live news and event updates aka.ms/MondaysatMicrosoft
Watch live or on-demand & share our blog.

Home / Microsoft 365 Copilot

Microsoft 365 Copilot

Deliver value and employee satisfaction with our tools for Microsoft 365 Copilot deployment and adoption. This powerful technology combines the power of large language models (LLMs) with your organization's data – all in the flow of work – to turn your words into one of the most powerful productivity tools on the planet.

Microsoft 365 Copilot Chat and in-app experiences provide real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills.

[Looking for Copilot resources for Small and Medium Businesses? >](#)

Copilot Success Kit

Our Success Kit empowers you to achieve rapid value with Copilot while enabling your progressive skilling journey with AI tools.

[Download here >](#)

Copilot Chat and agent starter kit

This new kit includes guidance on IT controls, setup, and resources to help prepare your tenant and enable your users to create and use agents.

[Explore the kit >](#)

Join the Copilot community

The Microsoft 365 Copilot community is your hub for the official blog, latest news, and discussions.

[Join now >](#)

Microsoft 365 Copilot

Welcome to the Microsoft 365 Copilot community. Your hub for the latest news, live events, and discussions on Microsoft 365 Copilot. For help & learning (how-to articles and training resources), please visit [Microsoft 365 Copilot Adoption hub](#).

Search this community

[Unfollow](#)

#M365Con

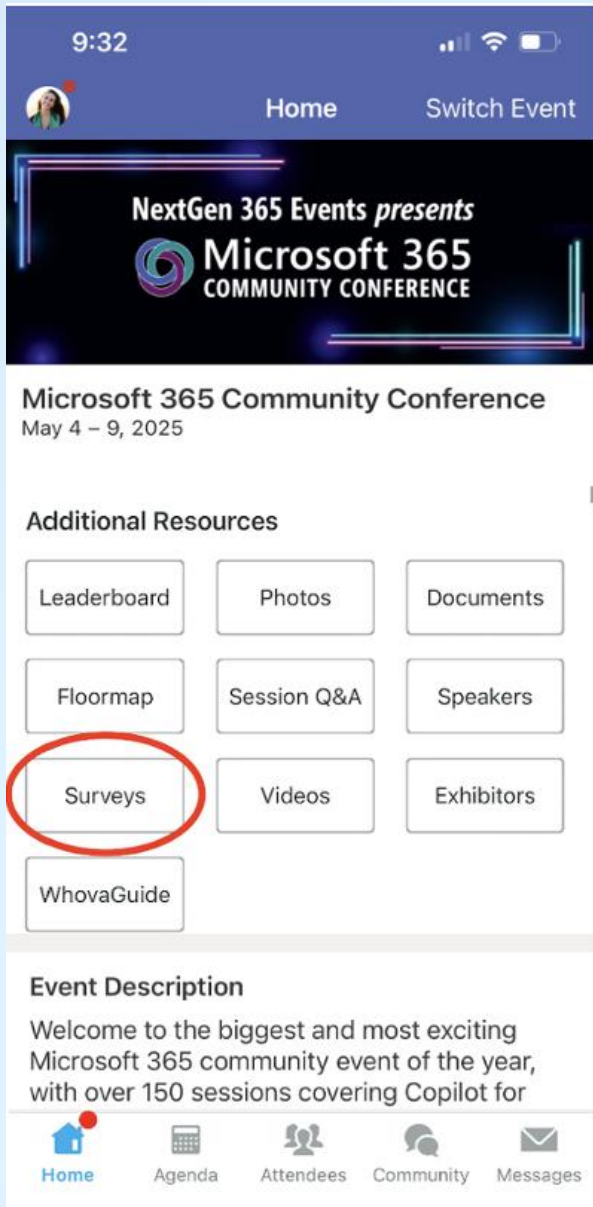
Microsoft 365 COMMUNITY CONFERENCE

May 6-8 Las Vegas

The ultimate Microsoft 365 community event

Learn directly from the experts and redefine what's possible at work—join us at the Microsoft 365 Community Conference.

[Learn more!](#)



Session feedback surveys

We want to hear from YOU!

Share your feedback to make next years conference even better!

Here's how –

- Simply go to the Whova App on your smartphone.
- Scroll down on the M365 Community Conference Homepage to 'Additional Resources' to click "Surveys".
- Click Session Feedback.
- Scroll down to find this session title.
- Complete the session feedback survey.
- Finally, click 'Submit'.

It's just that easy!

Uhova

The official event app for the
Microsoft 365 Community Conference

Event invitation code: Orlando2026



Join the event app to access:

- ➔ Event announcements
- ➔ Personalized agenda, session details
- ➔ Speaker & attendee profiles
- ➔ Networking, meet-ups, messages
- ➔ Event documents