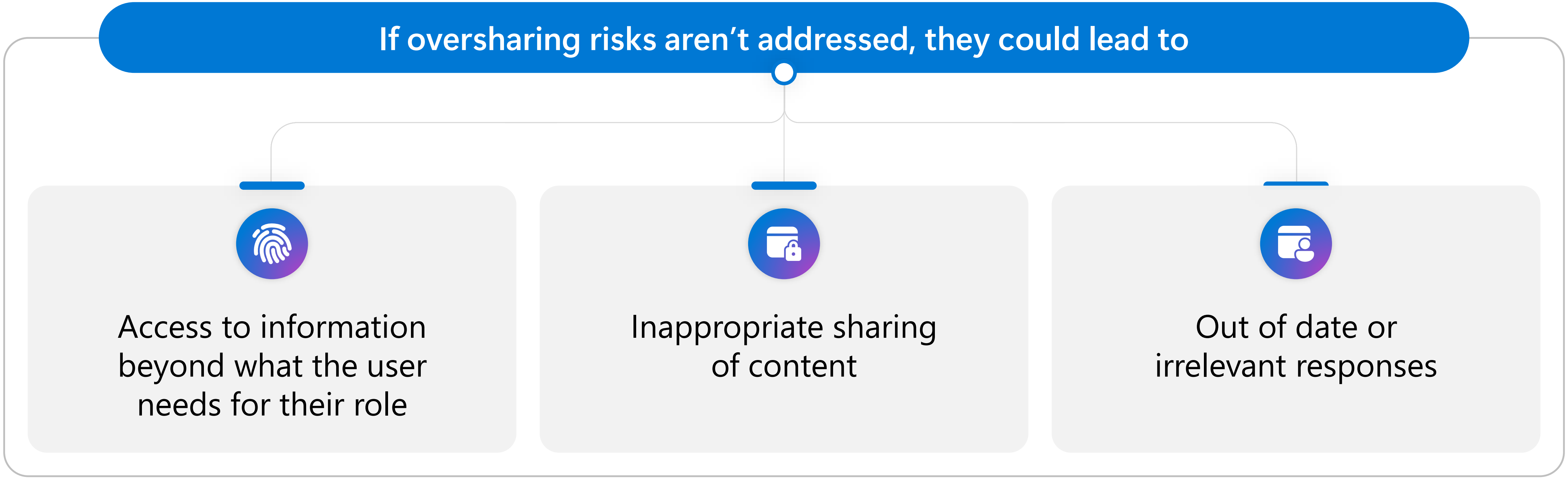
Microsoft

Address oversharing in Microsoft 365 Copilot

Microsoft deployment blueprint

Problem summary

Microsoft 365 Copilot (Copilot)'s ability to leverage information available to employees has raised concerns for organizations about overshared permissions



If oversharing risks aren't addressed, they could lead to

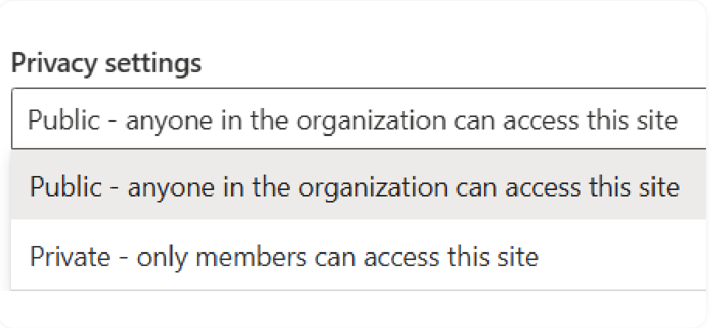
Access to information beyond what the user needs for their role

Inappropriate sharing of content

Out of date or irrelevant responses

By addressing these risks, organizations can ensure that information is shared appropriately and securely

Common causes of Copilot oversharing in SharePoint



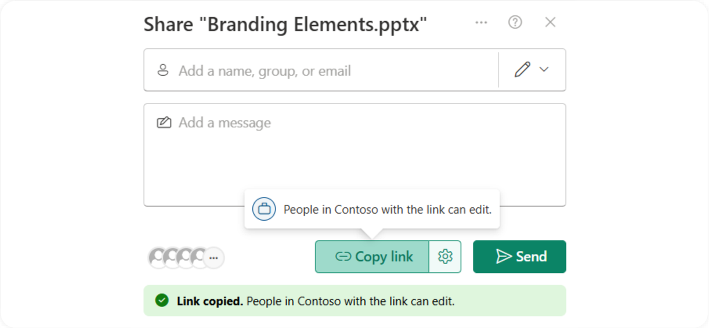
Privacy settings

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"

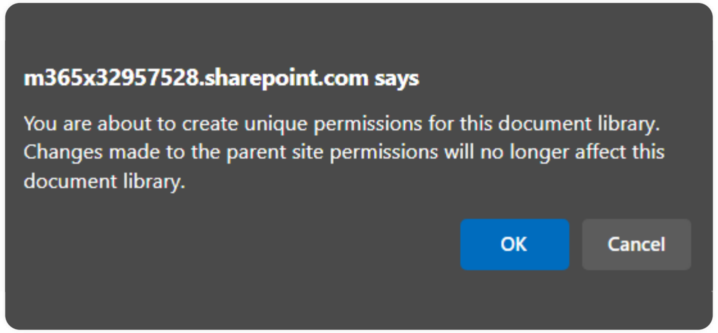
Add a name, group, or email

Add a message

People in Contoso with the link can edit.

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

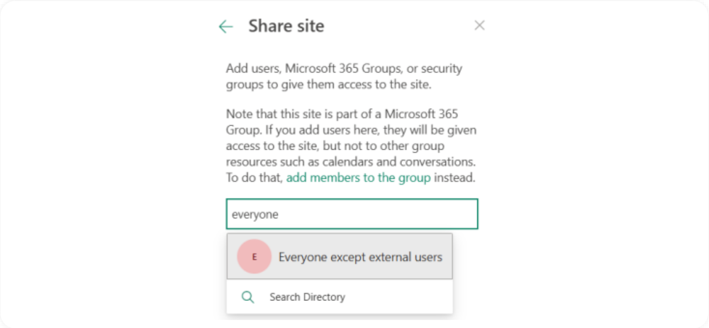
Default sharing option is everyone



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.

Broken permission inheritance



Share site

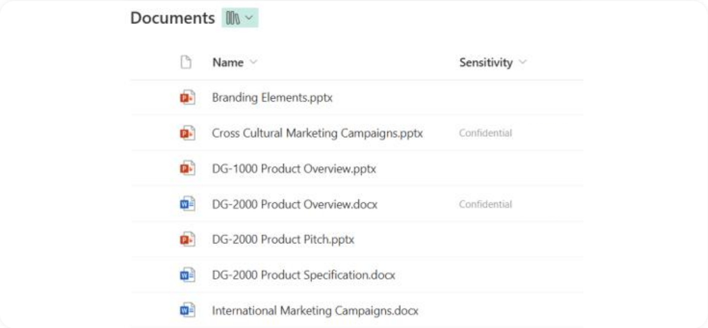
Add users, Microsoft 365 Groups, or security groups to give them access to the site.

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

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	

Sites and files without sensitivity labels

Address internal oversharing concerns for M365 Copilot deployment

	Pilot	Deploy (at scale)	Operate
Activities	• Identify most popular sites & assess oversharing • Grant Copilot access to popular, low risk sites • Turn on proactive audit and protection	• Discover oversharing risks • Restrict sensitive info from Copilot access and/or processing • Increase site privacy	• Further reduce risk and simplify oversight • Further secure sensitive data • Improve Copilot responses
Outcomes	Deploy copilot to sub-set of users with up to 100 sites	Copilot fully deployed in your organization	Continuous improvement of data security practices
Effort*	2–4 days	2–4 weeks	More than one month

*Suggested efforts should be reviewed into timelines based on your tenant size and organizational complexity

Last updated: Oct 24, 2024

Customers with E5 **Optimized**

LEGEND **1** – Copilot and SharePoint Adv. Mgt. **2** – OE3/ME3 **3** – ME5/E5 Compliance

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	**1. Identify the most popular sites & assess oversharing** • Export the top 100 most used sites from SPO admin center • Run SAM permission state report[1] • Run the Purview DSPM for AI Oversharing posture assessment to gain visibility into all data at risk of Copilot access, pivoted on labels and sensitive information types[3] **2. Grant Copilot access to popular, low risk sites** • Cross reference the report results from SAM and Purview DSPM for AI with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery[1,3] • Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified[1] **3. Turn on proactive audit and protection** • Turn Off EEEU (everyone except external users) at the tenant level[2] • Turn on Purview Audit and view Copilot interaction activity reports and charts[1,2,3] • Turn on proactive analysis for sensitive data handling with prompts and responses with Purview Communications Compliance[3] • Turn on audit-mode oversharing SPO Purview DLP policy to detect anyone sharing links for labeled and unlabeled data[2]	**1. Discover oversharing risks** • Use DAG permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)[1] • Identify Copilot agent insights & take actions[1] • Create customized Purview DSPM for AI Oversharing posture assessments to scale out data security actions, pivoted on labels and sensitive information types[3] **2. Restrict sensitive info from Copilot access and/or processing** • Initiate SAM Access Review for all sites that are overshared[1] • Apply SAM restricted access control (RAC) on business-critical sites[1] • Exclude critical sites from Copilot reasoning over them with SAM Restricted Content Discovery (RCD)[1] • Publish sensitivity labels with Purview Information Protection to Office apps, Container/Sites, Outlook for manual data protection by user[2] • Exclude Copilot from summarizing sensitive content via sensitivity labels[3] **3. Increase site privacy** • Use site sensitivity labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members[2] • Apply default site library sensitivity labels to protect new and modified unlabeled documents[3] • Turn on enforce-mode oversharing SPO Purview DLP policy to restrict access to sensitive data exposure & starting remediating them[2] • Disable RSS (if enabled) to allow full Copilot experience[1]	**1. Further reduce risk and simplify oversight** • Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners[1] • Automate SAM permission state report to maintain permissions hygiene[1] – Automate permission reports and actions to maintain permission hygiene[1] – Regularly review oversharing reports and restrict access as needed.[1] – Proactively avoid oversharing by applying RAC at site provisioning.[1] – Periodically review ownerless sites and take necessary action[1] – Control site provisioning by allowing creation for users that complete training[1] – Use change history to identify site changes that may cause oversharing[1] • Routinely run Purview DSPM for AI Oversharing assessment report to scale out data security actions, pivoted on labels and sensitive information types[3] • Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue[2] • View risky user activity in context of oversharing Purview DLP incidents[3] **2. Further secure sensitive data** • Automatically label new documents and prevent them from oversharing with run time auto-labeling policy, starting with client-side policies and extend to service-side policies[3] • Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitive labels and disabling anyone access[2] **3. Improve Copilot responses** • Setup Purview retention/deletion policies for SharePoint to reduce data surface[2] • Identify inactive sites with SAM, then restrict access or delete[1]

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: https://aka.ms/E5PrepareYourDataForCopilot

Customers with E3 Foundational

LEGEND **1** – Copilot and SharePoint Adv. Mgt. **2** – OE3/ME3

Address internal oversharing concerns in Microsoft 365 Copilot

Realize value quickly with Copilot by reviewing potential content sharing risks and optionally enabling Restricted SharePoint Search to address risk to enable full Copilot deployment

Select services are included in your FastTrack benefit. Other critical services are available thru Microsoft Unified or our Partner Ecosystem

Phase	Pilot	Deploy	Operate
Effort	2–4 days	2–4 weeks	1+ months
Deployment steps	**1. Identify the most popular sites & assess oversharing** • Export the top 100 most used sites from SPO admin center • Run SAM permission state report[1] • Use Purview Content Explorer to view which sites contain sensitive information types (SITs)[2] **2. Grant Copilot access to popular, low risk sites** • Cross reference the report results from SAM and Content Explorer with the top 100 used sites to identify up to 100 sites to be allowed for Copilot discovery[1,2] • Optionally enable Restricted SharePoint Search (RSS) for up to 100 sites identified[1] **3. Turn on proactive audit and protection** • Turn Off EEEU (everyone except external users) at the tenant level[2] • Turn on Audit and view Copilot interaction activity reports and charts[1,2] • Turn on audit-mode oversharing SPO DLP policy to detect anyone sharing links for labeled and unlabeled data[2]	**1. Discover oversharing risks** • Use permission state report with SITs to flag sites and files that are potentially overshared (Includes: EEEU, company shared links)[1] • Identify Copilot agent insights & take actions[1] **2. Restrict sensitive info from Copilot access and/or processing** • Initiate Access Review for all sites that are overshared[1] • Apply restricted access control (RAC) on business-critical sites[1] • Exclude critical sites from Copilot reasoning over them[1] **3. Increase site privacy** • Publish labels to Office apps, Container/Sites, Outlook for manual data protection by user[2] • Use site labels to limit access to org-wide sharing by marking sites as 'Private' and giving access only to site members[2] • Turn on enforce-mode oversharing SPO DLP policy to restrict access to sensitive data exposure & starting remediating them[2] • Disable RSS (if enabled) to allow full Copilot experience[1]	**1. Further reduce risk and simplify oversight** • Routinely run the SAM site lifecycle management policy's site ownership policy and review the ownerless sites and assign owners[1] • Automate SAM permission state report to maintain permissions hygiene[1] – Automate permission reports and actions to maintain permission hygiene[1] – Regularly review oversharing reports and restrict access as needed[1] – Proactively avoid oversharing by applying RAC at site provisioning[1] – Periodically review inactive sites and take necessary action[1] – Control site provisioning by allowing creation for users that complete training[1] – Use change history to identify site changes that may cause oversharing[1] • Continuously manage all your oversharing DLP alerts via the Microsoft Purview Portal[2] **2. Further secure sensitive data** • Reduce risk by remediating alerts for overshared documents from the SPO DLP policy and applying sensitive labels[2] **3. Improve Copilot responses** • Setup retention/deletion policies for SharePoint to reduce data surface[2] • Identify inactive sites, then restrict access or delete[1]

Guidance assumes Copilot technical prerequisites in place: Technical enablement of core services (Teams, SharePoint, Exchange), Office Applications deployed (modern Outlook recommended) and on current or monthly update channel

Learn how to use the features in the blueprint and how these features impact Microsoft 365 Copilot: https://aka.ms/E3PrepareYourDataForCopilot

Pilot

1. Identify most popular sites & assess oversharing
2. Grant Copilot access to popular, low risk sites
3. Turn on proactive audit and protection

Outcome

Deploy Copilot to sub-set of users and limit access to only low-risk content

Identify the most popular sites & assess oversharing

1. In SharePoint admin center, under active sites, sort sites descending by "page visits" to find the most used sites in your organization. Export the results to a CSV. You will use this later to cross reference with following reports.
2. Run and export the SharePoint Advanced Management (SAM) Data Access Governance Permission state report, which will give you a list of all sites in your organization, and show:
   - Number of people that have permissions to the site
   - Which Purview Information Protection sensitivity label is applied to site
   - The privacy setting of the site
3. Run the Purview Data Security Posture Management for AI (DSPM for AI) Oversharing assessment report scoped to the sub-set of pilot users to gain visibility into all data at risk of Copilot access. This report will include:
   - The sites the user has access to, the total number of users that have accessed the site, the amount of sensitive data on those sites, the sensitivity labels applied, and the quantity of dark data (data that has not been scanned for Sensitive Information Types).

Pilot

1 Identify most popular sites & assess oversharing

2 Grant Copilot access to popular, low risk sites

3 Turn on proactive audit and protection

Outcome

Deploy Copilot to sub-set of users and limit access to only low-risk content

Grant Copilot access to popular, low risk sites

1. Cross reference the report results from SAM and Purview DSPM for AI with the top 100 used sites. Identify up to 100 sites that should be allowed for Copilot discovery by your Pilot group of users. For sites that are highly used and not showing signs of risk for oversharing, we would suggest including these in Copilot access for the best results. Admins will likely leverage their organizational knowledge to determine which sites to include as well
2. Optionally enable Restricted SharePoint Search (RSS) temporarily for up to 100 sites that are determined to be included in Copilot access during the Pilot phase

Pilot

1. Identify most popular sites & assess oversharing
2. Grant Copilot access to popular, low risk sites
3. Turn on proactive audit and protection

Outcome

Deploy Copilot to sub-set of users and limit access to only low-risk content

Turn on proactive audit and protection

1. Turn off EEEU (everyone except external users) at the tenant level. If content is shared using this type of user group, it is likely overshared and should be reviewed. Therefore, such sites should be excluded from the pilot phase and included in Copilot access only after the review. This will be a quick change, and it will immediately stop some of the oversharing in your organization
2. Turn on Microsoft Purview Audit to see user activity. Once Copilot is activated for the pilot users, proceed to review the users' Copilot interactions with activity reports and charts in Purview DSPM for AI
3. Turn on proactive analysis with Microsoft Purview Communication Compliance to monitor sensitive data in Copilot prompts and responses
4. Turn on an audit-mode oversharing SharePoint (SPO) Purview DLP policy to detect when anyone sharing links are used with labeled or unlabeled data. This policy allows you to identify potential oversharing incidents without immediately blocking the sharing action

Deploy (at scale)

1 Discover oversharing risks

2 Restrict sensitive info from Copilot access and/or processing

3 Increase site privacy

Outcome

Copilot is fully deployed in your organization

Discover oversharing risk

1. To flag sites and files that are potentially overshared, use the SAM Data Access Governance (DAG) Permission state report. You can use the report you ran during the pilot phase, so rerunning it might not be necessary. In the report's output, examine the sensitivity of the information and identify where EEEU groups and company-wide shared links are utilized. Later, we will leverage some Purview capabilities to act and secure the sensitive information
2. Run DSPM for AI Oversharing assessment report to gain additional insights into data sensitivity and access. These assessments help identify files and sites that are potentially overshared by examining permissions and the sensitivity of the information. The assessment also provides remediation actions to mitigate risks. In the next step of the deployment stage, we will start implementing protection measures to secure the identified sensitive information

Deploy (at scale)

1. Discover oversharing risks
2. Restrict sensitive info from Copilot access and/or processing
3. Increase site privacy

Outcome

Copilot is fully deployed in your organization

Restrict sensitive info from Copilot access and/or processing

1. Initiate access review for all sites identified as overshared in the SAM and DSPM for AI oversharing assessment report. During the access review process, site owners and admin can examine permissions on their sites and files. This helps identify any oversharing or inappropriate access that needs to be addressed
2. While sites are in Access Review, optionally lock down content with SAM Restricted access control (RAC). RAC ensures that only authorized users have access to sensitive information. Site admin should review existing RAC policies and configure new ones as needed. This includes defining which users or groups should have access to specific sites, libraries, or documents
3. To restrict overshared sites from Copilot access and/or processing, optionally use Restricted Content Discovery (RCD). This will restrict copilot from discovering these sites
4. If not already done, publish sensitivity labels with Purview Information Protection to Office apps, containers/sites, and Outlook for manual data protection by users. By publishing sensitivity labels during a Copilot deployment, users will become accustomed to seeing and using these labels, which helps to jump-start data protection improvements that we will discuss in the Optimize phase
5. If sensitivity labeling is in place, you can optionally create a Data Loss Prevention policy to exclude files with specific sensitivity labels from Copilot processing. This will allow you to scope out sensitivity labels such as a label for mergers & acquisitions while you are working through restrictions at the site level

Deploy (at scale)

1 Discover oversharing risks

2 Restrict sensitive info from Copilot access and/or processing

3 Increase site privacy

Outcome

Copilot is fully deployed in your organization

Increase site privacy

1. We recommend applying a Purview Information Protection container sensitivity label to sites to define the sensitivity and enforce privacy settings. Setting the site to 'Private' will limit the site's content access to people with explicit access to the site. Access to sites with certain sensitivity labels or within private SharePoint (SPO) sites will be restricted based on the assigned sensitivity label or privacy settings
2. You can also increase site privacy without sensitivity labels by setting the default site privacy setting to 'Private', which will lower the internal oversharing of sites. However, using sensitivity labels allow you to leverage other optional settings now or in the future, such as external user access settings
3. After applying container sensitivity labels, it's important to set up default library labels to ensure that all new and modified documents within those containers are automatically labeled. This helps maintain consistent data protection and prevents oversharing by applying the appropriate sensitivity labels to all content
4. Turn on enforce-mode oversharing SPO DLP policies to restrict users access to sensitive data
5. Turn off RSS, if enabled, to allow for broader search capabilities, enabling users to access a wider range of information and resources. This will enhance productivity and collaboration by ensuring that all relevant content is searchable and accessible to authorized users

Operate

1 Further reduce risk and simplify oversight

2 Further secure sensitive data

3 Improve Copilot responses

Outcome

Continuous improvement of data security practices

Further reduce risk and simplify oversight

1. Routinely run the SAM site lifecycle management's site ownership policy, review the ownerless sites, and assign owners. This ensures that site permissions can be reviewed by the designated owners when needed
2. Automate the running of the SAM Permission state report, which allows admin to review sites that have a high potential for oversharing and maintain permission hygiene. Once reviewed, take remediation actions to fine tune your protection. Remediation actions include:
   - Admin functions:
     - Set Restricted access control (RAC): Limit site access to a specific group of users. This helps eliminate concerns about oversharing or permissions sprawl by ensuring that access is only granted to a designated group of users set by the admin
     - Optionally use Restricted Content Discovery (RCD) To restrict overshared sites from Copilot access and/or processing, which will restrict copilot from discovering these sites
   - Site owner functions:
     - Clean Up Permissions and Links: The site owners can review and clean up permissions and links in OneDrive and SharePoint (OD and SPO). This involves ensuring that only the appropriate users have access to specific files and removing any unnecessary or overly permissive sharing links
     - Group Membership Cleanup: Review and clean up the membership of groups in Entra. This ensures that only the necessary users are part of specific groups, reducing the risk of oversharing

Operate

1. Further reduce risk and simplify oversight
2. Further secure sensitive data
3. Improve Copilot responses

Outcome

Continuous improvement of data security practices

Further reduce risk and simplify oversight

3. Routinely run the Purview DSPM for AI Oversharing assessment report for users in specific departments or locations to understand the potential risk of oversharing for sites they have access to. Once ran, take remediation actions to fine tune your protection. Remediation actions include:

   - Create a Purview DLP policy to exclude files with specific sensitivity labels from Copilot processing
   - Setup auto-labeling of Purview sensitivity labels to ensure files are labeled automatically based on sensitive content or keywords to define the sensitivity of the file
   - Setup default sensitivity labels for document libraries to automatically label files
   - Run SAM DAG reports to review oversharing of sites and have owners run access reviews
   - Use SAM Restricted Content Discovery (RCD) to exclude sensitive sites from Copilot access

Operate

1. Further reduce risk and simplify oversight
2. Further secure sensitive data
3. Improve Copilot responses

Outcome

Continuous improvement of data security practices

Further reduce risk and simplify oversight

4. Continuously manage all your oversharing Purview DLP alerts via incidents with Microsoft Defender XDR incident queue. When you receive a DLP alert indicating oversharing, immediately investigate the alert using the Microsoft Defender XDR portal. Take necessary actions such as revoking access or applying sensitivity labels to mitigate risks. Document and track the incident to maintain an audit trail and ensure all steps are followed.

5. View risky user activity in context of oversharing Purview DLP incidents. Monitor the involved users' recent actions and access patterns for any anomalies. Additionally, leverage eDiscovery to search for and preserve relevant content, including deleted items, to ensure a comprehensive investigation. Based on these insights, update DLP policies, provide additional training, or implement stricter access controls to prevent future incidents

Operate

1. Further reduce risk and simplify oversight
2. Further secure sensitive data
3. Improve Copilot responses

Outcome

Continuous improvement of data security practices

Further secure sensitive data

1. Automatically label new documents and prevent them from oversharing with run time auto-labeling policies, starting with client-side policies and extending to service-side policies
2. Reduce risk by remediating alerts for overshared documents from the SPO Purview DLP policy by applying sensitivity labels and disabling anyone access

Improve Copilot responses

1. Reduce obsolete files and sites to reduce oversharing surface and improve Copilot response accuracy
   - Run SAM Site lifecycle management's inactive sites policy to identify inactive sites, and then restrict or delete those sites
   - Create Purview Data Lifecycle Management deletion policies based on last modified or created date to reduce obsolete files

Microsoft

Thank you

Microsoft Deployment models

Read the detailed guide for this model at aka.ms/Copilot/OversharingBlueprintLearn