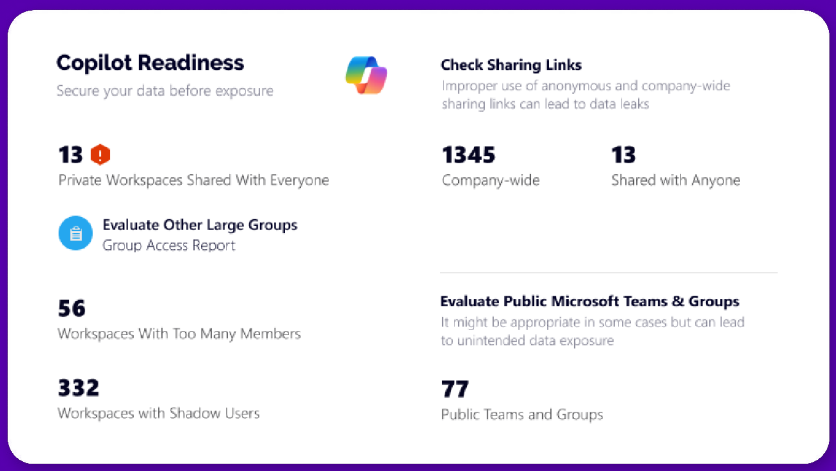
Syskit Point

SECURE AND GOVERN MICROSOFT COPILOT WITH SYSKIT POINT

Microsoft Copilot will help end-users create new content quickly, but it will also have a great impact on IT admins when considering security and governance. **Syskit Point** can help you assess, prepare, and protect your tenant to ensure your environment aligns with Microsoft Copilot's operational demands.



CHALLENGE: Information governance and control of GenAI

Microsoft Copilot improves productivity and helps unleash creativity. Yet, it is essential to remember that it operates on the principle of retrieving **all the information** that a user explicitly has access to.

Using **Microsoft Copilot can expose content and sensitive data** in your organization, both internally and externally. Information that is unprotected and overshared can be easily accessed through Copilot and can pose a serious security threat.

The **drivers behind a Copilot rollout are often the business users,** not IT teams, who are tasked with implementing it. IT teams understand how Copilot works and that **it will drastically expose the existing security risks organizations have in their environments.** Risks businesses are often unaware of.

Data sprawl and **poor information management can reduce the value of Microsoft Copilot** by providing old or incorrect results. Many organizations do not have proper content lifecycle management procedures in place to deal with stale and redundant content.

Overshared and exposed data

Copilot can have access to old and redundant data and can present that information as fact. This creates misleading and inaccurate content.

Permission Management

IT teams should review user permissions before they assign a Microsoft Copilot license to ensure users have access to the right content.

Stale and redundant data

Copilot can have access to old and redundant data and can present that information as fact. This creates misleading and inaccurate content.

The Syskit Point advantage

With Syskit Point in your toolbelt, you can **prepare your tenant for Microsoft Copilot** and keep it secure as users increasingly utilize the power of AI.

Syskit Point's robust reporting, permissions management, and governance features helps **minimize the risks of oversharing and outdated content on a large scale.**

Prepare your environment

Prepare your tenant

Ensure that **Microsoft 365 Copilot** has access to the right data. With Syskit Point, you can minimize oversharing and widely accessible content. You can evaluate existing sharing links and set up alerts for sharing activities and privacy changes.

Check user permissions

Before you assign any **Microsoft Copilot** licenses, you should review all user permissions. Syskit Point lets you easily detect which users, groups, and external collaborators have access to your data, down to the file level.

Manage sharing links

As Copilot operates on the principle of retrieving all the information that a user explicitly has access to, you should revise and manage **sharing links** in your organization.

Prevent oversharing and protect data

Automations and policies

Use **Syskit Point** as a continuous monitoring solution that uses policies to enforce correct workspace setup, sharing settings, provides real-time alerts, automatically removes dubious oversharing and identifies inactive content and workspaces.

Continuous access review

IT teams should include workspace owners to ensure that access to content is regularly re-certified. With **Syskit Point** you can establish regular access reviews and set up rules to ensure new workspaces are being reviewed.

Lifecycle Management

Prevent Microsoft Copilot in misleading end users by confidently providing information it has access to. With Syskit Point, you can archive or delete **inactive workspaces** with ease.

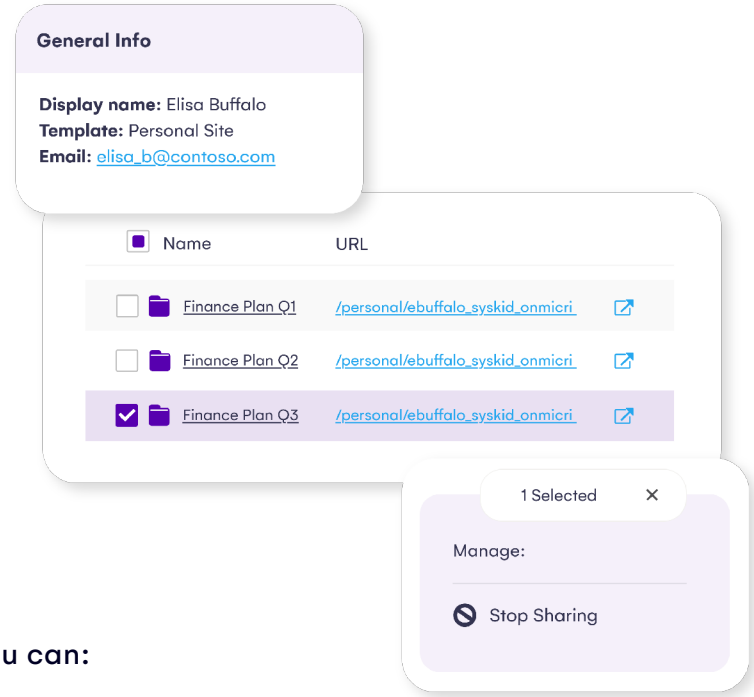
SOLUTION: Prepare for Copilot rollout - review access and sharing links

To raise awareness about potential oversharing, IT teams need the ability to understand if some content is shared beyond the necessary audience and easily report this to stakeholders. To do this properly, IT teams must have deep visibility to understand who has access to what.

Prevent sensitive data exposure - manage sharing links

Quickly assess all sharing links across your environment. Including company wide and anonymous links.

Syskit Point gives you the ability to easily manage sharing links, limiting content oversharing, and ensuring sensitive **data is shared appropriately** and Copilot uses only the content it's supposed to.



With **Syskit Point**, you can:

- Remove multiple sharing links, including anonymous links and company wide shared links.
- Prevent specific users from using **external links**.
- Stop internal and external file sharing from OneDrive.
- Remove group, site, or team guest users.

Syskit Point gives you a tenant-wide view or you can choose individual workspaces to report on. You can instantly generate and export the reports you need, and perform management actions in bulk straight from the reports.

Preform a detailed analysis - generate access and workspace reports

Group Access Report

The Group Access report is essential for managing and minimizing the risk of oversharing information and helps prepare your environment for Copilot by enabling IT Teams to quickly assess and mitigate any potential oversharing with large groups.

This report:

- Provides insight into where particular group's have access to across the entire environment.
- Helps identify where oversharing might be occurring.
- Enables immediate interventions from the report and remove access in bulk.

User Access Report

The User Access Report is a vital tool for ensuring that users have the appropriate access levels before being granted Copilot licenses.

Using the User Access report, IT teams can:

- Perform in-depth analysis of user permissions and memberships, identifying potential oversharing risks.
- Get up-to-date information on user permissions.
- Understand details whether permissions are given directly or through groups, offering a full view of access levels.
- Immediately remove user access for one or multiple workspaces in bulk, directly from the report.

Sharing Links Report

The Sharing Links Report is crucial for preparing environments for Copilot by offering real-time insights and direct actions to remove risky sharing links, such as anonymous and company-wide links, in bulk.

IT teams can:

- Locate all files and folders shared via links in real-time, providing a comprehensive view of all shared content.
- Utilize filters and search to target specific types of workspaces, link types, or specific sites.
- Remove specific or multiple sharing links in bulk from within the report, enhancing efficiency and security.

Workspaces with Stale Content

Stale content accumulates slowly, people upload everything and anything, never use it, or it simply becomes old. Copilot can have access to old and redundant data and can present that information as fact. This creates misleading and inaccurate content.

IT teams can:

- Detect and list out all Microsoft 365 workspaces with old and unused content.
- Drill down to workspace and see content modified by date to decide if you need to take action.

Ensure users have appropriate access

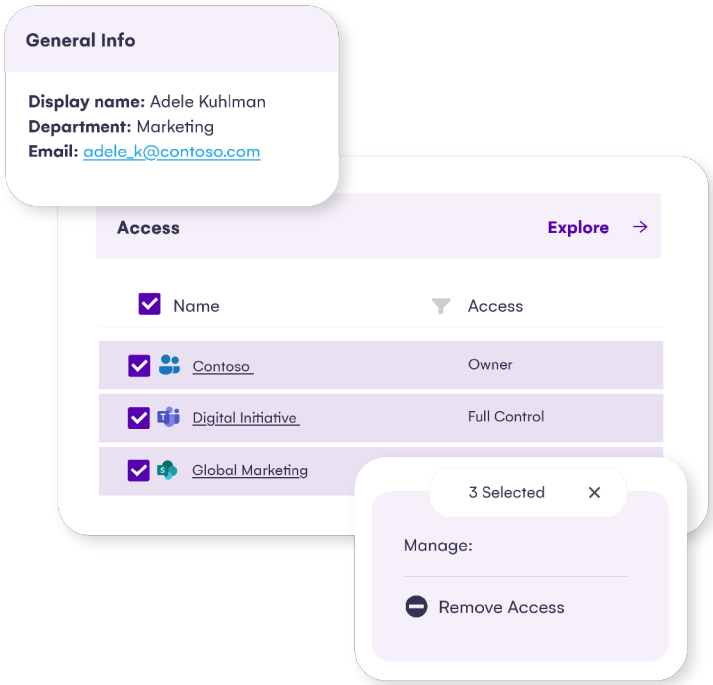
Manage user access - control who has access to what

Syskit Point lets you view and manage memberships and permissions across Microsoft 365 – all from a **single platform.**

Save time when applying a Copilot license by acting in real-time when you need to make access changes due to oversharing.

Syskit Point lets you easily:

- Grant, remove, copy, transfer, or edit user access.
- Add and remove admins and owners in bulk.
- Change admin access.
- Manage and detect content with unique permissions.
- Find and manage guests and external users



SOLUTION: Prevent oversharing and govern Copilot with policy automation, access reviews, and lifecycle management

It is crucial to have a continuous monitoring solution that enforces correct workspace setup and sharing settings, provides real-time alerts, automatically removes obvious oversharing risks, and identifies inactive workspaces.

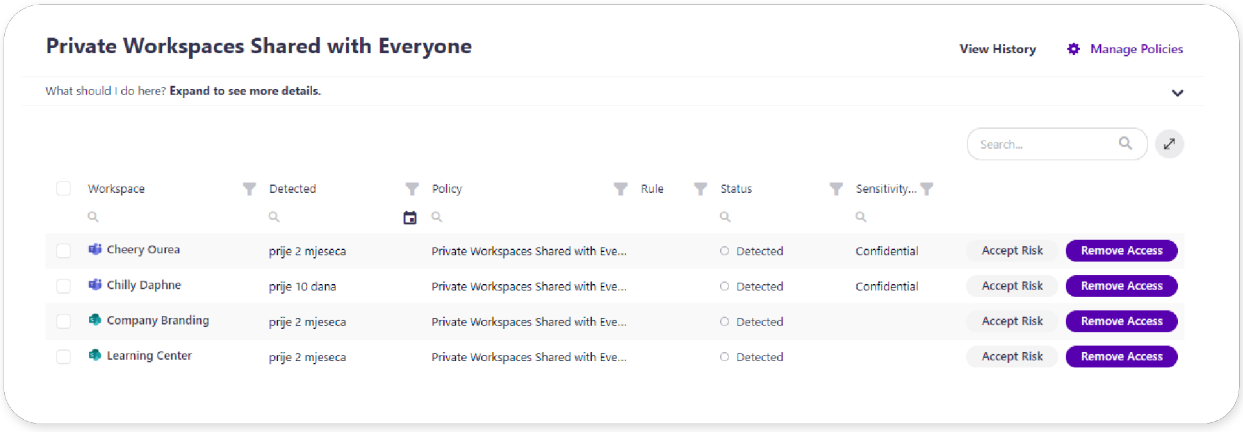
Also, it is vital to be able to delegate guided access management and workspace disposal tasks to their owners. They know if some piece of content or the entire workspace is still needed and who should have access to it.

Control oversharing with policies and automations

Syskit Point comes with a set of governance policies to help you **prevent oversharing and protect your digital environment.** Use various automations and cleanup options to solve detected vulnerabilities which you can easily find in a central place – on our **Security and Compliance dashboard.**

Private Workspaces Shared with Everyone policy – detects sharing of private workspaces with large groups which is extremely delicate as it may lead to issues such as security breaches, administrative complexity and uncontrolled access. You can **set up Point to solve these issues for you automatically!**

- Workspaces with **Too Many Members** policy
- **Shadow Users** policy

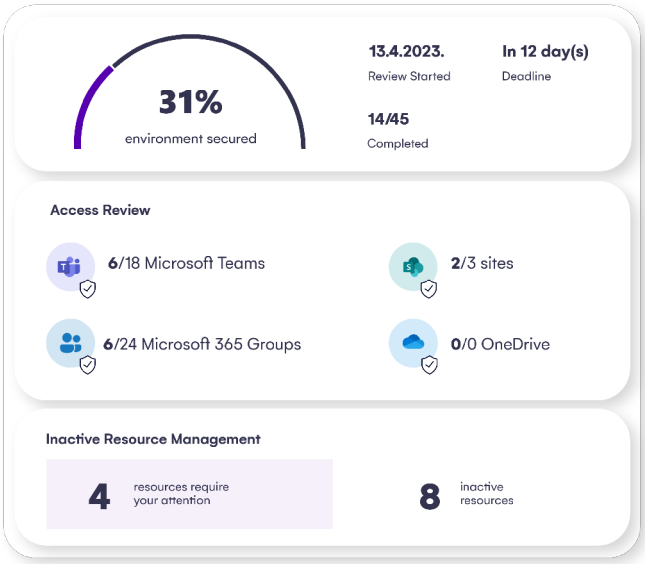


Schedule automated access reviews for workspace owners

Eliminate day to day monitoring and strengthen your Microsoft 365 governance by making team, group, and site owners reliable governance partners.

Customize and schedule periodical access reviews and lifecycle management with Syskit Point. This allows owners to regularly review user access to their workspaces and archive or delete the inactive ones, minimizing the risks of oversharing and outdated content on a large scale.

The entire process takes just a few steps:



- An admin starts the task: what resources need to be governed and how often.
- Owners receive an automated email request to perform an action.
- Any owner of a particular resource does the task in Syskit Point's easy-to-use interface.
- An admin sees the progress of each active task and gets a detailed report on all review task activity.
- Owners receive reminders to complete their tasks.

Regular cleanup: Inactive workspace detection and disposal

Obviously, the fewer unnecessary workspaces you have, the lower the risk of oversharing. **Inactive workspaces** can be a source of oversharing vulnerabilities, but also a source of information for Copilot to confidently provide wrong answers with outdated information to your end users. So, automating the detection and disposal of inactive workspaces has more than one benefit, including minimizing the footprint for potential oversharing.

Prepare and protect your tenant with Syskit Point and manage Microsoft Copilot at scale

Ensure your environment aligns with the operational demands of Microsoft Copilot.

Try Syskit Point for free with our 21-day free trial. **syskit.com**