Microsoft 365 lifecycle management: User's guide

SysKit

Contents

Introduction 4

Retention and sensitivity labels 5

Retention policies Microsoft 365 6

What Microsoft 365 files can be deleted? 7

Inactive mailboxes 8

Deleting a user 9

PST files lifecycle management 10

Ways to import PST files to Microsoft 365 10

Multiple retention policies applied: What takes priority? 12

Storage: SharePoint and OneDrive 14

Storage: Exchange 14

Storage: Teams and Yammer 15

Microsoft Purview 15

Where to create retention labels and policies 16

Want to know more about creating labels and policies? 16

Adaptive or static retention policy? 17

The role of metadata in Microsoft Purview 18

How to view policies that apply to specific locations 18

Preserving incoming, outgoing, and internal data 19

Immutable storage for Azure blob storage 19
Preservation Lock 20
Microsoft 365 lifecycle management with Teams 20
3 typical stages of a Team lifecycle – and what to consider 21
How to set group expiry in Azure 23
Naming policies (Azure) 24
Features available in the group naming policy 25
Managing Microsoft 365 guest users in your Microsoft 365 environment 27
Managing Microsoft 365 guest users 29
Want to know more about managing Microsoft 365 users? 31
Microsoft Power Automate 31
Microsoft Graph API 33
Example HTTP requests 34
Turning lifecycle management from complication to collaboration 34
Syskit Point in action 35
Creation 36
Maintenance 37
Disposal 39

INTRODUCTION

This eBook is for IT managers, admins, and business leaders responsible for managing their organizations' Microsoft 365 data lifecycle.

The exponential rise in cloud-based working means a high increase in M365-related data, activities, and sprawl, along with an ongoing increase in users, groups, teams, sites, and endpoints. Microsoft 365 has a reported 345 million paid seats, while Teams has exceeded 270 million monthly active users.

The result is more digital workplaces than ever before. With greater complexity, evolving governance requirements, plus potential inconsistencies in managing data throughout its life. Of course, these risks are to be balanced and mitigated. After all, a business needs to support collaboration, communication, and transformation.

That is why we will analyze the most important aspects relating to creation, maintenance, and deletion in this eBook. We will explore how you can allow your users to find what they need without getting caught up in cluttered environments. Examine best practices for managing memberships and minimizing attack surfaces – without having to resort to overly restrictive permissions.

And we will also touch upon different scenarios that match different user cases – with topics and themes chosen to help you manage your Microsoft 365 data lifecycle.

RETENTION AND SENSITIVITY LABELS

The shift to remote working has raised many questions about IT teams' infrastructure, security, and operations.

As organizations have adapted and ensured Business as Usual, this has also meant new regulatory and compliance challenges for teams. These have an impact whenever a user adds data to your environment, from uploading documents to posting a message in Teams.

This is where retention policies and labels come in. They're essential tools for data life cycle management because they can help you to:

- **Comply with industry regulations and internal policies**

Set data in your environment to be retained for legally required periods of time.

- **Mitigate risks from threats and potential breaches**

Assign expiry dates and the automatic deletion of sensitive files and data.

- **Share knowledge through a single source of truth**

Keep tenants up to date by making sure users work from the latest and most relevant document versions.

Retention policies Microsoft 365

The main actions you need are:

- **Retain content**

Microsoft 365 information remains available for eDiscovery purposes – forever or for a specified period.

- **Delete content**

Microsoft 365 information is permanently and irreversibly removed after a specified period.

- **Retain and delete content**

You may need to combine elements of retention and deletion. For example, a retention policy that lasts for five years before data is permanently and irreversibly removed.

This involves identifying workloads that require retention policies in Microsoft 365 and the wider tenant. These policies will automatically apply to container-level items.

For specific items that fall outside the retention policy, you can create retention labels for these exceptions. For example, high-value or sensitive documents that are part of a SharePoint site. You can use these to extend, override, or simply ignore existing deletion periods.

Creating retention labels for retention policy exceptions

Your global admin has full permission to create and edit retention labels. Each tenant can have the following:

Item	Maximum number of policies
Retention labels	1,000
Retention policies	10,000 (including policies for DLP; information barriers; holds for eDiscovery, litigation, and in-place; sensitivity labels)
Policies for retention per workload	1,800 for Exchange, 25 recommended and 50 maximum per mailbox
SharePoint or OneDrive	13 when all sites are included
SharePoint or OneDrive	2,600 (specific locations included or excluded)

WHAT MICROSOFT 365 FILES CAN BE DELETED?

For retention settings to apply, SharePoint sites must be indexed. Even if data within the sites is configured not to appear in search results, retention settings will still apply.

Data retention requirements for some common regulations:

- **SEC (Securities and Exchange Commission) Rule 17**

Organizations must use storage tools that can make records restricted, non-rewriteable, and non-erasable. The storage tools must also be able to store records for at least 3-6 years, with a capacity much longer.

- **FINRA**

Rule 4511(c) requires organizations to preserve books and records for at least six years, where there is no specified retention period under applicable FINRA or SEA rules.

- **MiFID II**

Records should be kept for five years or up to seven years when requested by certain authorities.

- **HIPAA**

Records must be kept for at least six years, whether from the creation date or last-effective data.

Inactive mailboxes

A departing employee doesn't just mean ensuring secure offboarding. Your organization is probably required to also retain their emails, data, and other Microsoft 365 assets. For a few months, years (up to seven for the Sarbanes-Oxley Act), or even indefinitely.

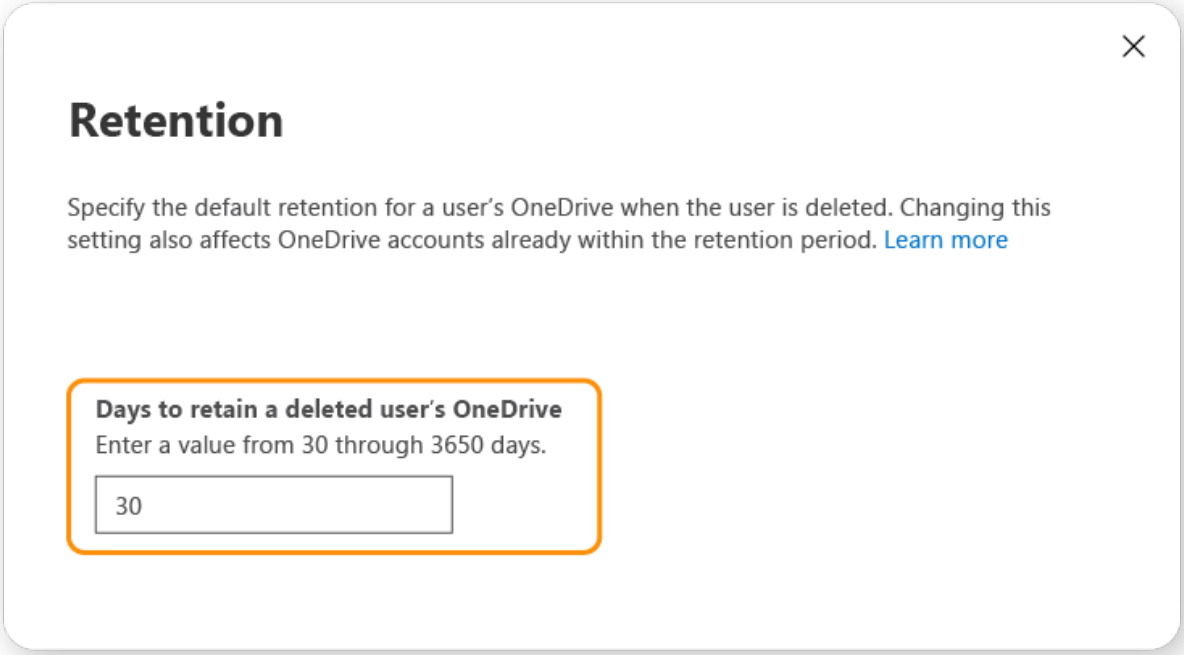
Naturally, this scenario calls for a program of Microsoft 365 lifecycle management. Ultimately, you don't want to keep paying for licenses for departed users. And you also don't want to simply delete their Microsoft account and the data contained within, risking fines for non-compliance.

You can remove the mailbox by using the Remove-Mailbox cmdlet in Exchange Online PowerShell. Although Microsoft states, "The best way to delete a mailbox is to delete the corresponding user account in the Microsoft 365 admin center".

Just bear in mind that Microsoft "strongly recommends that you avoid having an active and inactive mailbox with the same SMTP address." If you need to reuse the SMTP address, recover, or restore the inactive mailbox to an active mailbox instead.

Deleting a user

When you delete a user, their OneDrive account stays available for a set retention period. While the default is 30 days, you can go up to 3650 days. You can change this in the SharePoint admin center, or with the PowerShell cmdlet Set-SPOTenant: SetSPOTenant -OrphanedPersonalSitesRetentionPeriod <int32>



This can be made available to another user who can access and download any files. If you configure automatic access delegation, their manager or the secondary owner is automatically given OneDrive access by default. If this is not configured, check you're not at risk of creating orphaned resources in Microsoft 365.

During the deletion period, any file-sharing access will continue functioning, and the user's OneDrive files will remain discoverable in search. Any content created will also stay online because it's part of SharePoint and is considered a collaborative environment. Their email will be converted to a shared mailbox for access.

Seven days before the retention period expires, a reminder email is sent to the secondary owner. The deleted user's OneDrive is moved to the site collection recycle bin at expiry. It stays there for 93 days, and shared content is no longer accessible.

You can restore deleted users and their data for up to 30 days after initial deletion.

PST files lifecycle management

You may have to deal with PST files when removing the user's mailbox. These files present risk when used for email archiving:

- **Lack of visibility**

PST files often end up on workstations and user devices. Outside your standard backup servers and systems.

- **Risk of corruption**

Once a PST file hits 20GB, you will not be able to open it. Obviously, this is an issue for auditing, but this also increases the chances of the file corrupting.

- **Low interoperability**

Without Outlook installed or as an active subscription, users can't open PST files.

Ways to import PST files to Microsoft 365

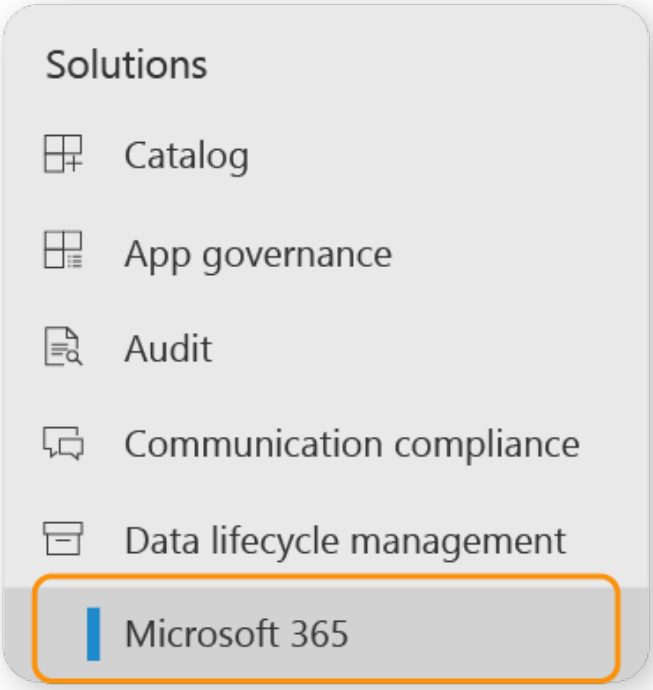
You can move mail from PSTs to Exchange Online via the import service in the Microsoft Purview compliance portal. You can bulk-import using these methods:

- **Network upload (the cloud-based method)**

First, upload your PST files to an Azure blob container. Then use Microsoft 365 Import to move PST data into your organization's mailboxes. After 30 days, the PST files are deleted from the container.

- **Drive shipping (the physical method)**

Copy the PST files to a BitLocker-encrypted hard drive. Send the hard drive to Microsoft (the shipping address appears after you create the import job). Files are uploaded 7–10 working days after the hard drive arrives.



PST files: Good to know

Each PST file you copy should be a maximum of 20GB. Anything above and you could experience reduced performance. To avoid this, you might have to break the PST files into smaller files.

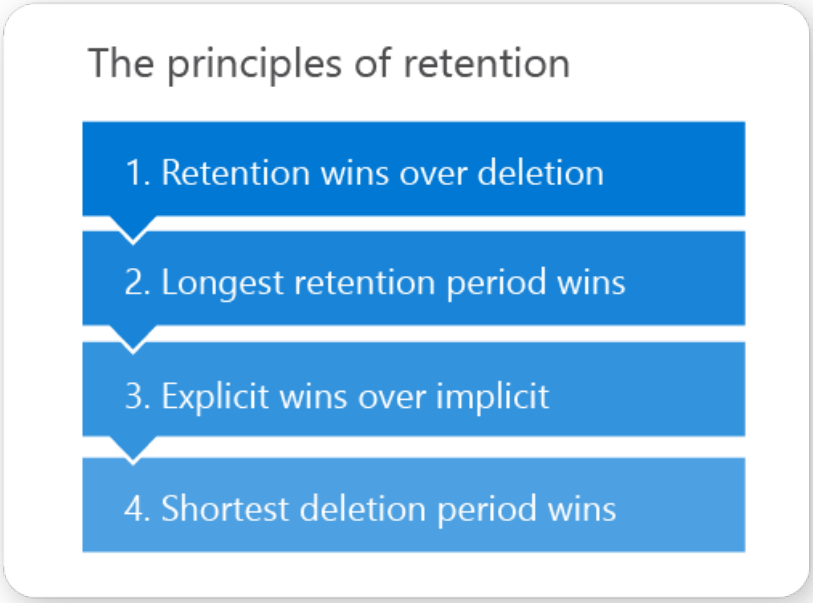
Multiple retention policies applied: What takes priority?

Imagine your retention policies Microsoft 365 are subject to MiFID II. Among the requirements, you have to ensure the following:

"Communication records can be provided to the client involved upon request and shall be kept for a period of five years and when requested by a competent authority this can be extended to a period of **up to seven years**."

Now, imagine you have retention policies applied to the same SharePoint documents within your Microsoft 365 environment. One retains items for five years, and one retains items for seven years. For this scenario, the longest retention period wins.

This outcome is based on the **Microsoft principles of retention:**



Refer to these whenever you find a conflict in retention/deletion actions for items:

1. **Retention always takes priority over permanent deletion**
   Permanent deletion is suspended, so your content is kept for compliance. The content can still be deleted (if initiated by the user or system) from the user's view.

If conflicts still remain...

2. **The longest retention period wins**
   An exception would be if the 7-year period is configured based on when the file is created, and the 5-year period is based on when a file is modified.

If conflicts still remain...

3. **Explicit labels for deletion have priority over implicit policies**
   A retention label is assigned to a specific item, unlike a policy, which is assigned from a container. The added specification from a label gives it prioritization.

If conflicts still remain...

4. **The shortest deletion period wins**
   If the three previous principles haven't resolved the required action, it comes to comparing retention periods.

STORAGE: SHAREPOINT AND ONEDRIVE

The Preservation Hold Library is where SharePoint Online and OneDrive keep information for retention purposes.

Until November 2021, multiple versions of the same file or list item would be stored, even if just one change was made within each file. Microsoft has since changed this, so one version is preserved. However, all retained data here counts toward your overall SharePoint storage quota.

Typically, that's 1TB per organization, 10GB for every Microsoft 365 licensed user in your tenant, plus storage from any purchased Microsoft 365 Extra File Storage add-on. So, you might want to check and increase your storage settings.

Supported list items with document attachments

- **Standard retention label (doesn't declare an item to be a record)**

Document attachment doesn't automatically inherit retention settings of the label but can be labeled independently.

- **Retention label that declares the item a record**

Document attachment automatically inherits the retention settings from the label – if the document isn't already labeled.

STORAGE: EXCHANGE

Data is held in the **Recoverable Items folder.**

STORAGE: TEAMS AND YAMMER

Data is held in the **SubstrateHolds folder** – a subfolder of the Exchange Recoverable Items folder.

Let's go into more detail about applying some of these within Microsoft 365. Here's where to start with ensuring your organization complies with legal and regulatory standards for Microsoft 365 lifecycle management.

MICROSOFT PURVIEW

This gives you a unified and centralized data governance solution. You get data discovery, traceability, and searchability across your entire environment. Lineage can extend from on-premises to cloud.

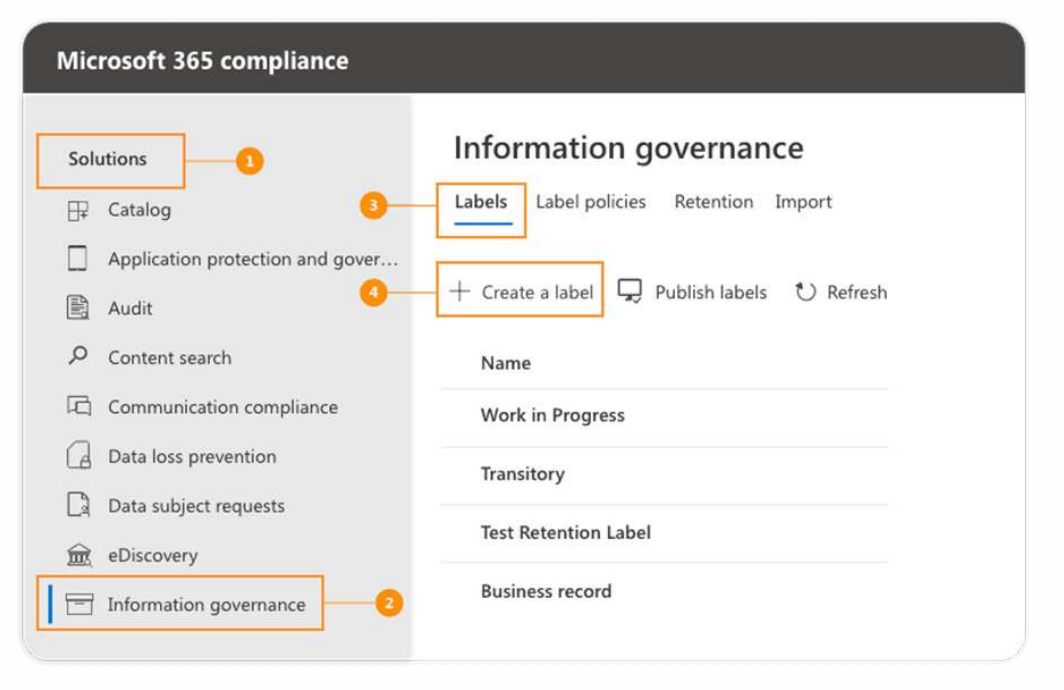
Retention policies can be used at the container level for:

- **Exchange email**
- **Exchange public folder**
- **Microsoft 365 Groups**
- **OneDrive**
- **SharePoint**
- **Skype for Business**
- **Teams channel messages**
- **Teams chat**
- **Yammer community**
- **Yammer private messages**

Where to create retention labels and policies

Permission required: Global admin for your organization.

1. Head to the Microsoft Compliance Center: https://compliance.microsoft.com/
2. Click **Solutions > Information governance**
3. Click the Labels tab or Label policies
4. Click Create



Want to know more about creating labels and policies?

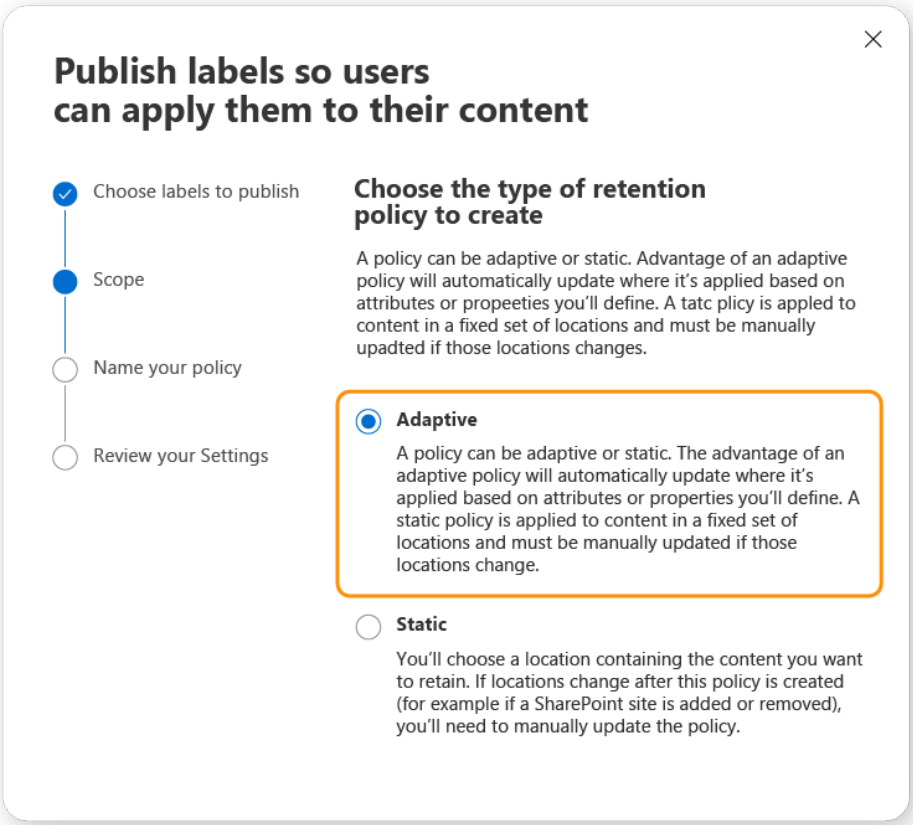
If you want to know more about creating labels and policies, take a look at our in-depth guide on retention policy. The article will guide you from the basics of retention policies and labels all the way to how you can create and apply them.

Adaptive or static retention policy?

Imagine a scenario where you want to create retention policies for C-level executives.

Adaptive means using a specified query dynamically. This is run daily against attributes or properties of the C-level executives. You don't need to add specific emails or OneDrive URLs – the scope will automatically include these.

Static doesn't use queries. It's simply applied to specific instances, using "include/exclude" and "organizational" criteria. For every instance, you would need to add emails and OneDrive URLs of the C-level executives. Over time, as these executives move in, you'll need to configure and update retention policies manually.



THE ROLE OF METADATA IN MICROSOFT PURVIEW

Metadata tags are at the heart of Microsoft Purview capability.

From a discovery perspective, the tags make it possible to surface, tag and map data. From a compliance and lifecycle perspective, you can use the tags to manage and restrict access to sensitive information.

Microsoft Purview can scan your data and extract technical metadata and schema for structured data sources. Classifications on schemas can be applied, along with sensitivity labels, if your Microsoft Purview Data Map is connected to a Microsoft Purview compliance portal. Scan configurations include:

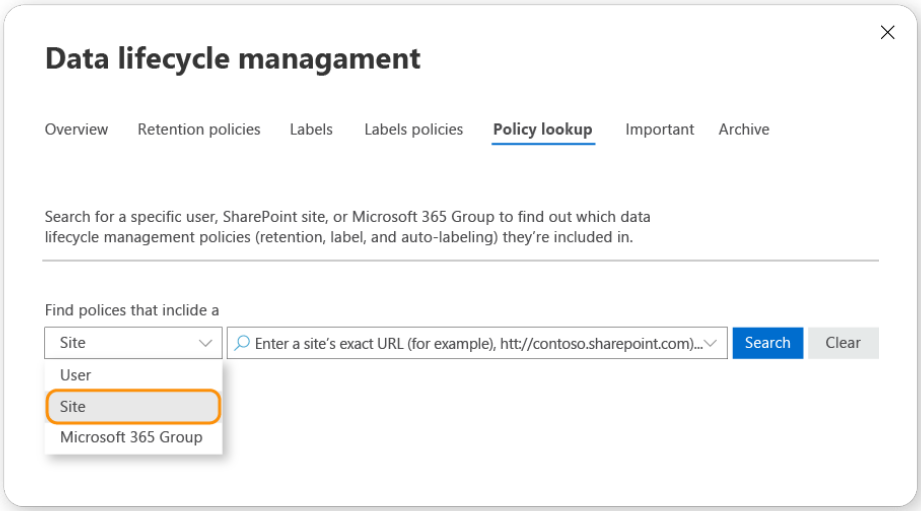
- **Scope and entities** - such as entire databases vs. specific tables.
- **Rules** - what information to look for.
- **Schedules** - weekly for frequently changed and developing data sources or monthly for less frequent updates.

Once this is complete, the identified metadata is sent to Ingestion. This populates the Data Map and lets you discover and organize the resulting assets and schemas.

How to view policies that apply to specific locations

Here's a big time-saver when you want to know what policy applies to specific Microsoft 365 locations.

Policy Lookup lets you search via the site, user, or Microsoft 365 Group. You have to specify the exact parameters, so no partial or broad matches. You'll find Policy Lookup in the **Compliance Center > Data lifecycle management:**



PRESERVING INCOMING, OUTGOING, AND INTERNAL DATA

Imagine a scenario where you have to comply with **Securities and Exchange Commission (SEC) Rule 17a-4.** You need a way to store records to **prevent any alteration or deletion before the retention period expires**. Below are some solutions you can use in Microsoft 365:

Immutable storage for Azure blob storage

This means you can store data in a Write Once Read Many (WORM) state. Authorized users can create and read blobs, but the data can't be erased or modified.

You can request an attestation letter if you have an Azure support plan. The letter contains reassurances from Microsoft relating to SEC Rule 17a-4. Use this to notify your designated examining authority at least 90 days before you employ storage for the data that needs securing.

Preservation Lock

Preservation Lock lets you choose whether to make a policy restrictive. Apply this after creating the retention policy or label. When activated, **not even admins** can overwrite, modify, or delete data during the preservation period.

MICROSOFT 365 LIFECYCLE MANAGEMENT WITH TEAMS

Built on Microsoft 365 groups, Teams automatically comes with an Exchange mailbox, SharePoint site, OneNote notebook, and other Office and Microsoft 365 assets.

The reason for all this provisioning is simple. The goal of Teams is to get employees aligned and projects completed. That's why users get access to all these tools from Day 1. That's also why it's critical to implement lifecycle management and governance simultaneously. To avoid sprawl, for if/when a project scope evolves, and members join or leave.

3 typical stages of a Team lifecycle – and what to consider

Microsoft splits a Teams project into three stages – creation, maintenance, and disposal. Each one calls for different lifecycle-related considerations.

Stage 1: Creation

Here's where you identify the initial members. You'll need to decide who can add new users, whether the team is public or private, and who has permission to create channels and add tabs, bots, or connectors.

We also recommend choosing at least two owners to reduce the risks of orphans in your Microsoft 365 tenant.

Microsoft Teams allows name duplication. So, it's worth setting up a naming policy to maintain consistency. For example, always include the relevant team, project, or region.

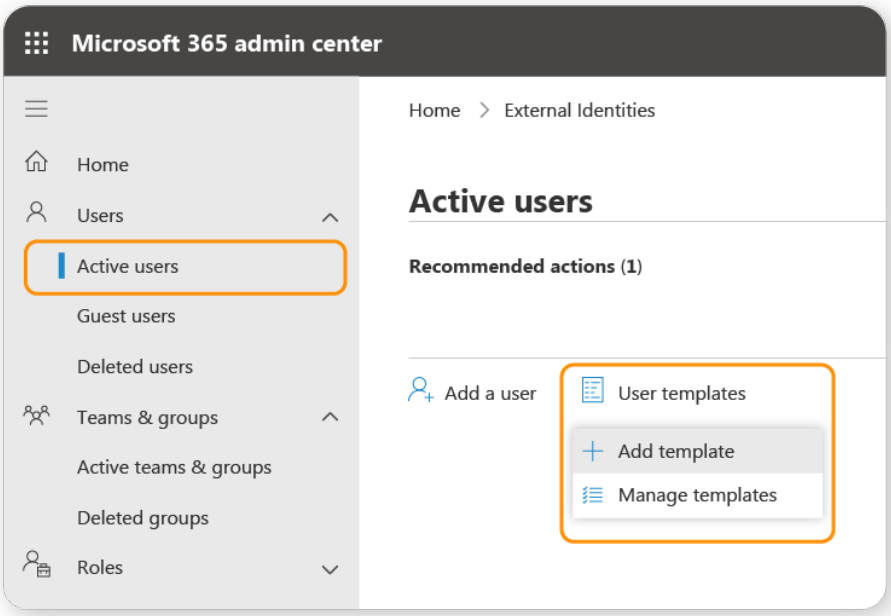
You can also create Teams templates to save time and minimize lifecycle issues further down the line. These can be managed in the Microsoft Teams admin center or with PowerShell. You can choose from two types:

- **Base templates**

  Microsoft offers pre-built industry-specific base templates. These often include proprietary apps not available in the Microsoft Store. Additional capabilities get added with new releases of Teams.

- **Custom templates**

  You can also build your own from scratch. Include predefined channels, tabs, and apps, and make them accessible through a catalog. Go to the Teams admin center > Users > Active users > User templates > Add template to get started.



Stage 2: Maintenance

The maintenance stage is **the longest** in the lifecycle and is where change is most likely - it will require close lifecycle management. At least initially, so IT admins can identify usage patterns and ensure data governance is being fulfilled.

This will involve regular usage of the Teams admin center to monitor and guide users. You'll need to make sure owners are regularly reminded to check what's still active and what needs archiving or deleting.

You'll also need to review guest and external access procedures. **If guests have been invited to a team**, deleting the team won't remove the guests. They'll still be able to use Microsoft Teams features, such as chat, apps, and voice and video calls.

Stage 3: Disposal

When the lifecycle ends, use group expiration policies to define what happens next. The team goes into a soft-delete state without activity within a specified period. Within Teams, an activity could be related to a user visiting a channel, and this activity can renew group expiration.

For 30 days, you can restore the team. After expiry, services and content not under a retention policy are then purged. This doesn't include emails and files used in Teams – they have separate retention policies.

HOW TO SET GROUP EXPIRY IN AZURE

To set an expiration policy, go to the Azure Active Directory admin center: https://aad.portal.azure.com/, then click Groups > Expiration to choose:

- **Group lifetime in days**

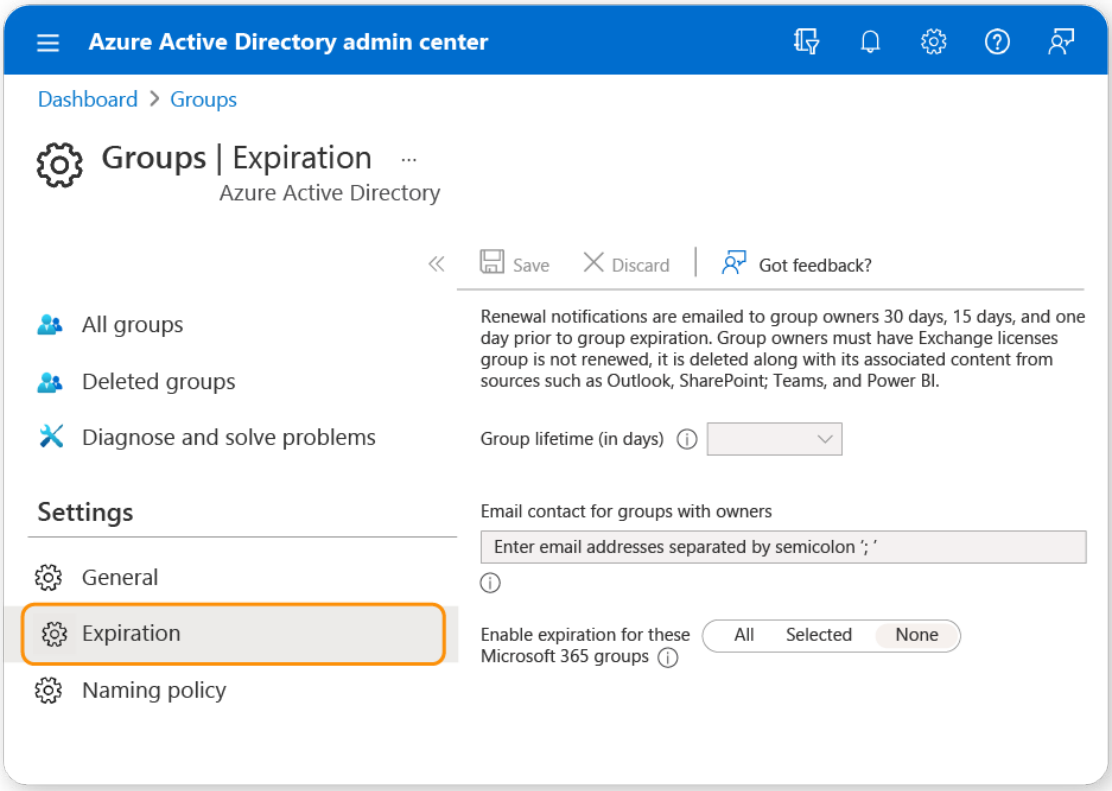
Choose how long the group (or team) can exist before being renewed.

- **Email contact for groups with no owners**

Choose who receives notifications and can manage the lifecycle and deletion.

- **Enable expiration for these Microsoft 365 groups**

Choose the groups the policy applies to.



When deleting groups, you have 30 days to restore them from a soft-delete stage. When that period expires, associated content, services and resources are removed from your Microsoft 365 environment. Apart from:

- **Videos in Stream**
  These remain under the ownership of the video uploader/recorder.

- **Flows in Power Automate**
  These remain under the ownership of the flow creator.

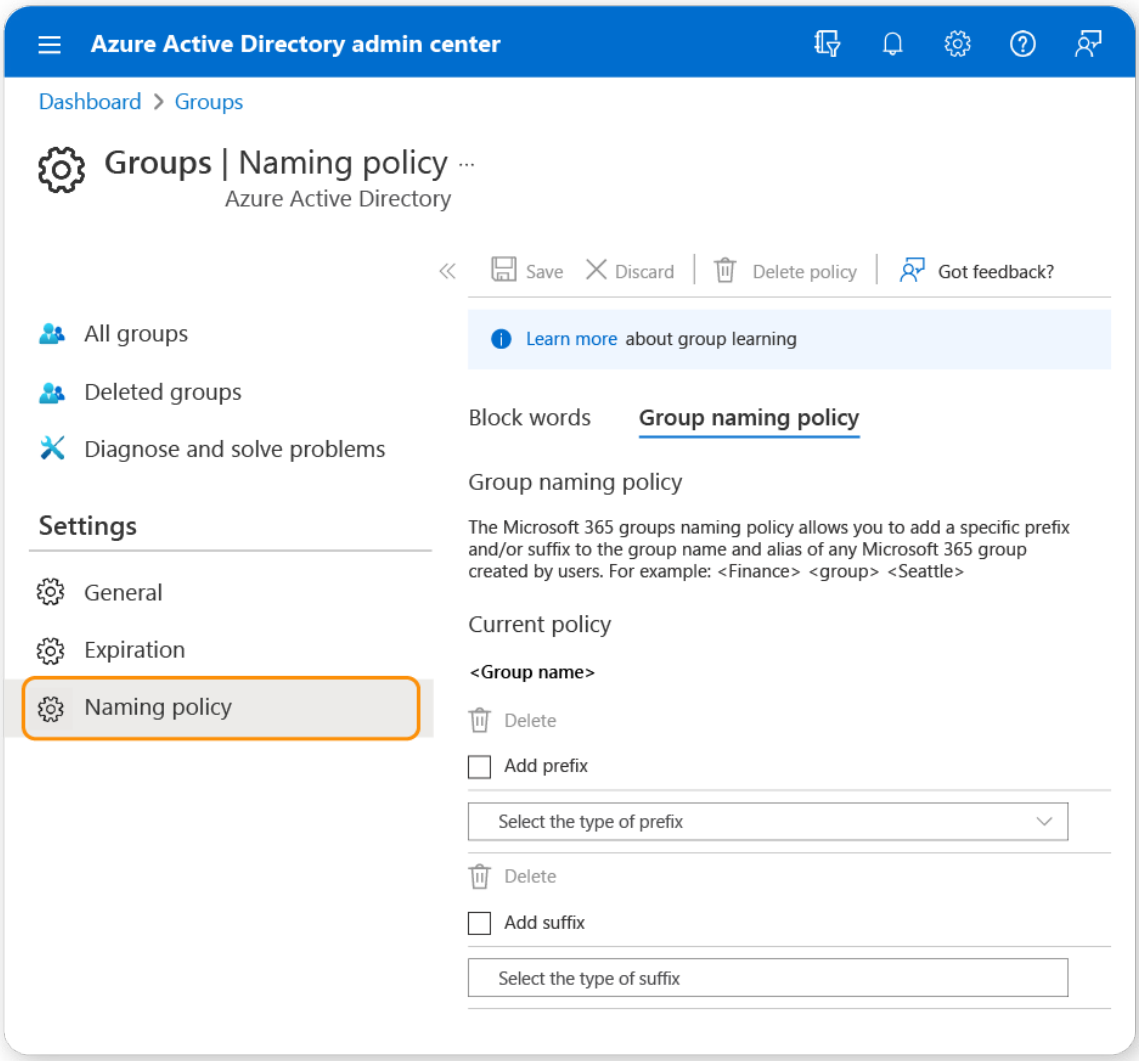
- **Project and roadmap data**
  It remains in the Common Data Service (CDS) and can be restored separately.

NAMING POLICIES (AZURE)

Another way to support your Microsoft 365 Lifecycle Management is the group naming policy functionality.

Groups created by users have to follow your naming strategy – so if you keep things consistent and minimize duplication, search results will stay streamlined.

Go to the **Azure Active Directory admin center** (https://aad.portal.azure.com), and click **Groups > Naming policy:**



Features available in the group naming policy

Want to use an Azure AD naming policy for Microsoft 365 Groups? You'll need to have – not necessarily assign – an Azure Active Directory Premium P1 license or the Azure AD Basic EDU license for every unique user that's a member of one or more groups.

You can then make use of features such as:

Custom blocked words

Upload a set (maximum 5,000) of words that can't be used in groups. An exact match is required to trigger, although blocked words aren't case-sensitive.

Prefix-suffix naming policy

These define the naming convention of your groups. You have a choice of:

- **Fixed string**
  Use to differentiate groups in the GAL and navigation bars, often with group names.

- **Attributes**
  Use to identify features about the group, such as who created the group, where and when.

About prefixes and suffixes:

- **You have a maximum of 53 characters.**

- **The names can contain special characters that are supported in group names and group aliases.**

- **Periods and hyphens are allowed, apart from at the beginning or end.**

You can apply a group naming policy **across group workloads**, including Outlook, Teams, SharePoint, and Yammer.

An exception is distribution groups created in **Exchange Online**. To apply a policy to them, you must create policies in the Exchange Online admin center.

MANAGING MICROSOFT 365 GUEST USERS IN YOUR MICROSOFT 365 ENVIRONMENT

Part of lifecycle management involves reviewing your guests. Clients, suppliers, stakeholders – external users without a work or school account with your organization.

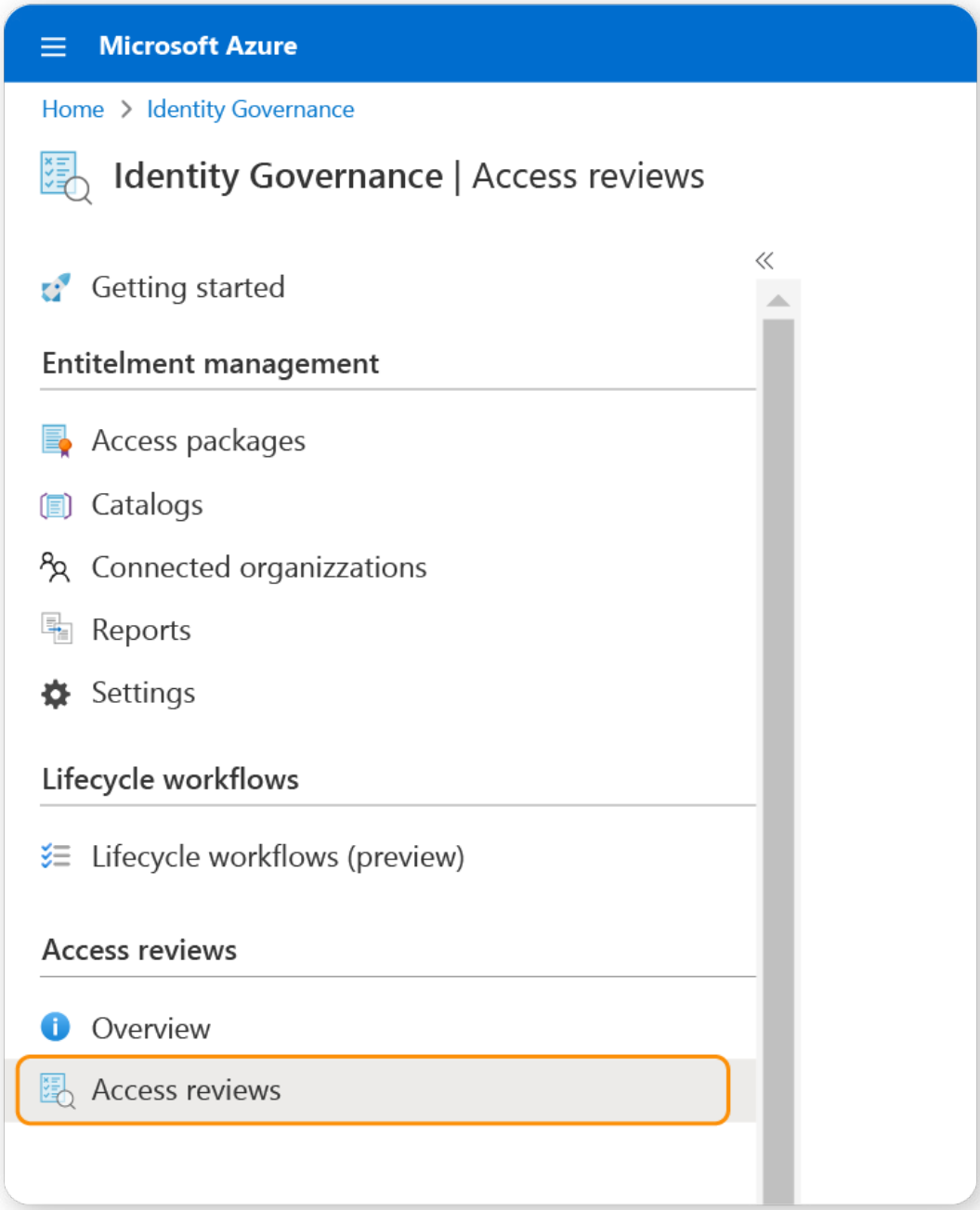
Naturally, this supports the principle of least privilege, alongside meeting compliance and regulatory requirements. For example, PCI DSS requirement 12 states that related reviews should take place "at least annually."

You can complete access reviews using Azure Active Directory (Azure AD) for:

- Groups in Azure AD containing one or more guest members
- Applications connected to Azure AD with one or more guest members assigned

Access reviews

A license EMS E5 or P2 is required. To check, go to Azure (https://portal.azure.com/) **> Identity Governance > Access reviews:**



From there, you can create the following:

- **Single-stage access reviews**
  All nominated reviewers have the same time period to decide. The last reviewer has the final decision. This relatively linear model is commonly used for simple configurations.

- **Multi-stage access reviews**
  Instead of the burden falling on the final reviewer, responsibility can be shared more equally. You can even hide previous review results from later review stages.

You can specify how many days the review should be, whether it's recurring, the start date, and who the reviewers can be:

- Group owners
- Selected users or groups
- Users reviewing their own access
- Managers of users

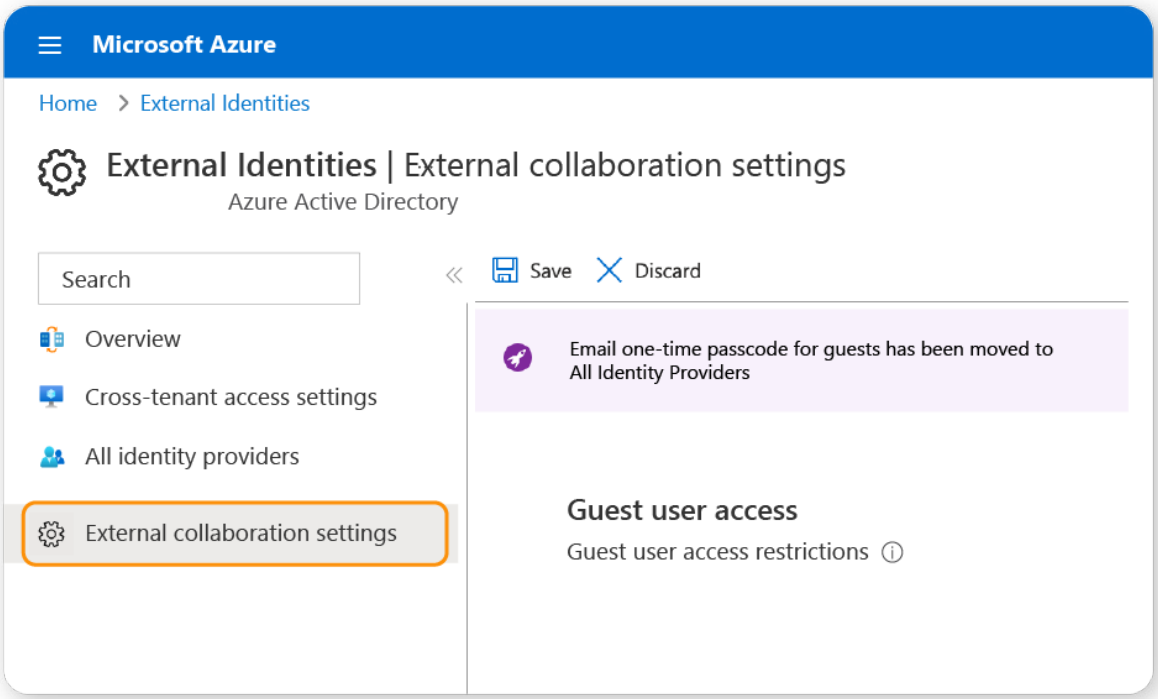
If there's no response to an access review request, choose a default action:

- No change
- Remove access
- Approve access
- Take the system's recommendations for denying or approving user access

Managing Microsoft 365 guest users

By default, Azure AD lets users invite guests from any external organization. That's great for collaboration in Microsoft 365 but not so great for control. Here's how to add extra layers of protection:

Navigate to https://portal.azure.com, and click External Identities > External collaboration settings:



You can now define different levels of restrictions:

- **Guest user access**

You can go from giving Microsoft 365 guest users the same access as members to restricting their access to their directory objects only.

- **Guest invite settings**

You have four options for restricting invitations – from allowing anyone in your organization to allowing nobody.

- **External user leave settings**

You can allow external users to remove themselves from your organization, which can help manage membership lifecycles.

- **Collaboration restrictions**

Choose whether invitations can be sent to any domain, denied to specified domains, or restrict invitations to specific domains.

Want to know more about managing Microsoft 365 users?

We've got you covered. Take a look at our lifecycle-focused instructions for managing Microsoft 365. The article will show you how you can manage and detect guest user access and much more.

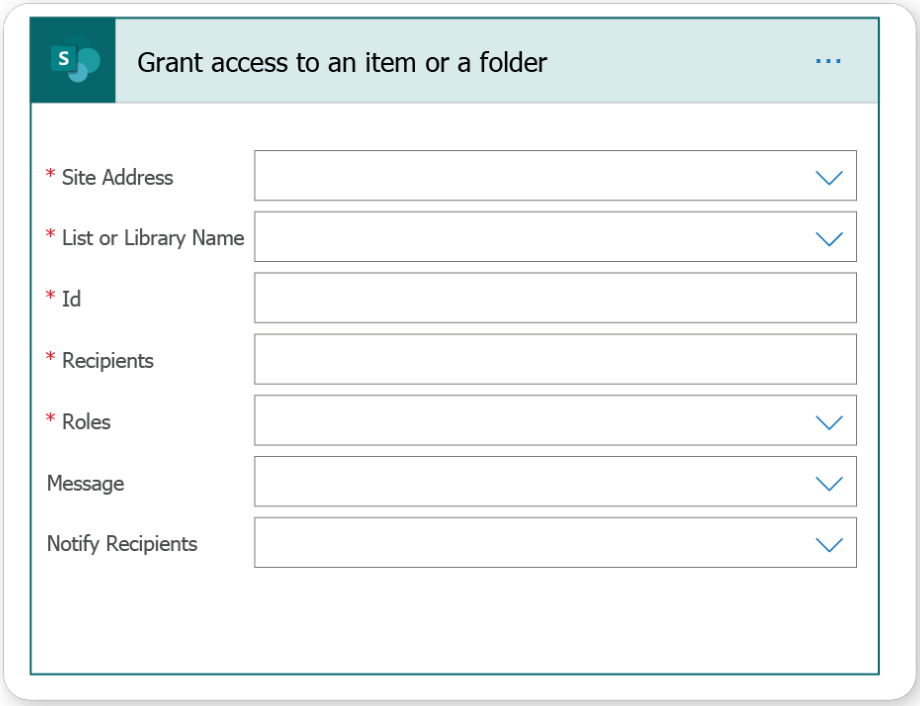
Prefer something more automated? Continue reading.

Microsoft Power Automate

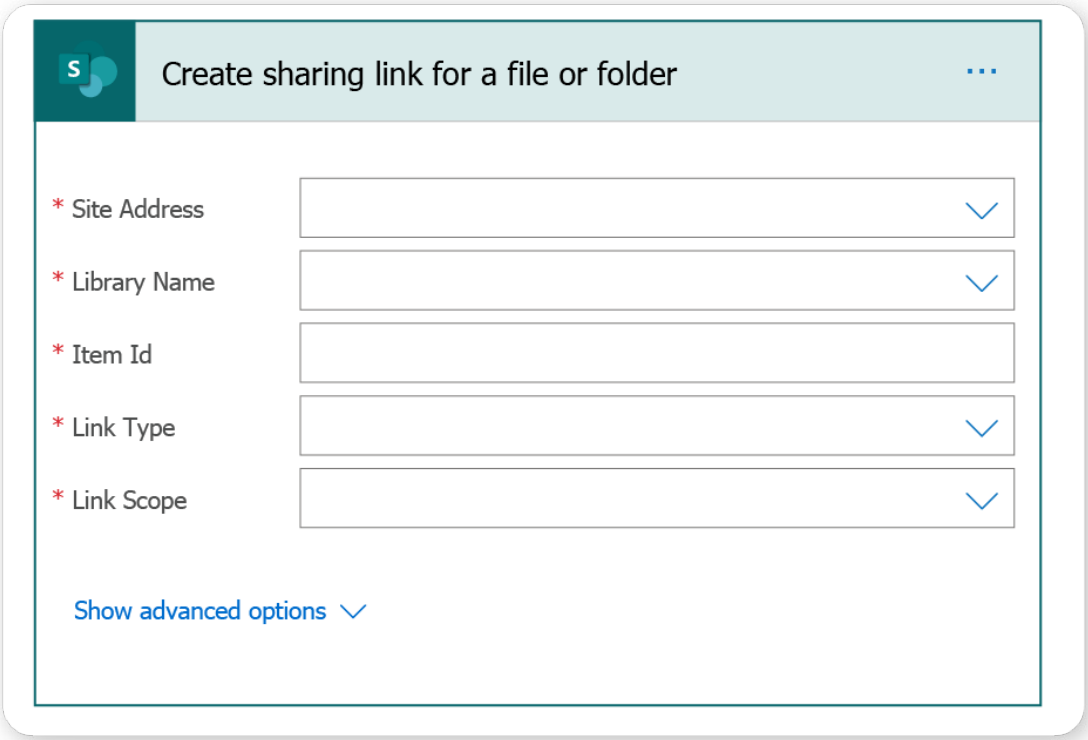
You can use automation to help manage your lifecycle through triggers and actions

What's more, Power Automate offers some built-in 'Security Actions' to help you get started quickly. For example, the SharePoint connector in Power Automate lets you:

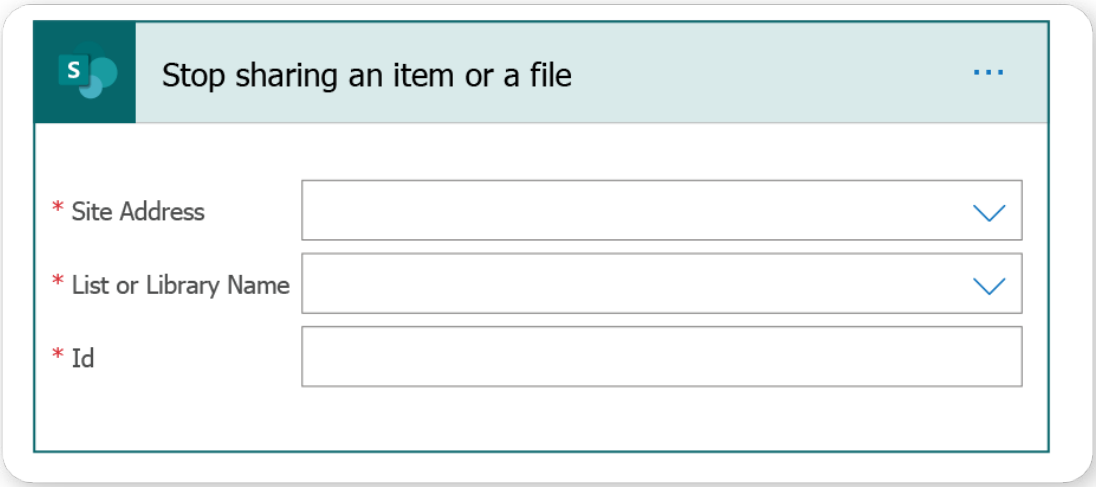
- Grant access to items and folders.



- Create shareable links for files and folders in a document library (list items aren't supported yet).



- Stop sharing items and files.



Microsoft Graph API

Developers can use Microsoft Graph to manage group members **dynamically** – if your tenant has an Azure AD Premium P1 license or greater.

Using the Create group API means you can create, manage, and delete groups throughout the lifecycle of a collaboration.

Groups can then be made available across multiple Microsoft 365 applications. **Access is synchronized by Microsoft Graph, giving all members group access.** For lifecycle management, this synchronization makes it possible to:

- Add and remove members from existing groups.
- Get lists of group owners and members (useful for approvals, renewals, and lifecycle admin).
- Remove owners.
- Enforce naming policies.
- Renew groups.
- Restore deleted groups.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	Group.ReadWrite.All, Directory.readWrite.All
Delegated (personal Microsoft account)	Not supported.
Application	Group.Create, Group.ReadWrite.All, Directory.ReadWrite.All

Example HTTP requests

This example HTTP request uses the Microsoft Graph API to activate group dynamic membership and set membership criteria:

PATCH https://graph.microsoft.com/v1.0/groups/{id}

```
{
  "groupTypes": ["Unified", "DynamicMembership"],
  "membershipRule": "user.department -eq 'Marketing'",
  "membershipRuleProcessingState": "on"
}
```

This HTTP Get request (to the /groups endpoint) can be used to get a list of all groups in an organization:

GET https://graph.microsoft.com/v1.0/groups

TURNING LIFECYCLE MANAGEMENT FROM COMPLICATION TO COLLABORATION

As we've seen in this eBook, Microsoft 365 offers multiple functions that support lifecycle management.

However, as data volumes grow and workforces become more distributed, IT admins need new methods to secure environments, endpoints, and users. Manual processes, especially at scale, are no longer enough.

That's why many organizations are turning to automation. Gartner has forecasted that:

"By 2026, applying automated trust metrics across internal and external data ecosystems will replace most outside intermediaries, reducing data sharing risk by half."

SYSKIT POINT IN ACTION

You can explore how to apply automation within your Microsoft 365 environment very easily. At least, it's easy with SysKit Point, which lets you manage the entire end-to-end workspace lifecycle across multiple stages **- from workspace creation to its end of life.**

With SysKit Point, you get a platform that lets IT teams shift away from doing governance tasks on a day-to-day basis and **become enablers of governance** within their organizations.

That means that IT teams focus on defining policies that are later automatically applied to all the workspaces. At the same time, SysKit Point takes care of notifying end users and taking care of what needs to be done and when - ensuring workspaces are in line with the predefined policies.

This makes end-to-end lifecycle management very intuitive for the end users because, from the very moment they request a new workspace, the appropriate policies are applied to it without them needing to worry about it.

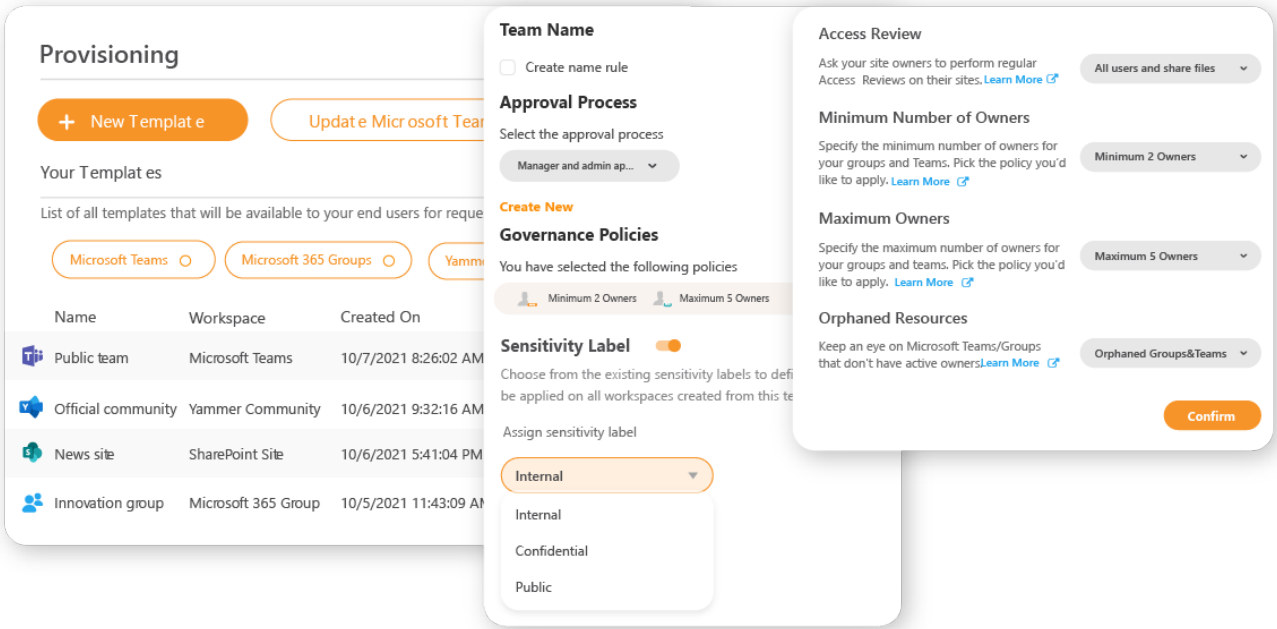
During the entire workspace lifecycle, end users get notified if they need to do something to ensure that their workspace complies with company policies and governance best practices.

Also, SysKit Point takes care that those workspaces are being utilized, so when it detects an inactive workspace, SysKit Point notifies the owners and lets them decide if they wish to keep, archive, or delete the data.

This is how SysKit Point looks in action:

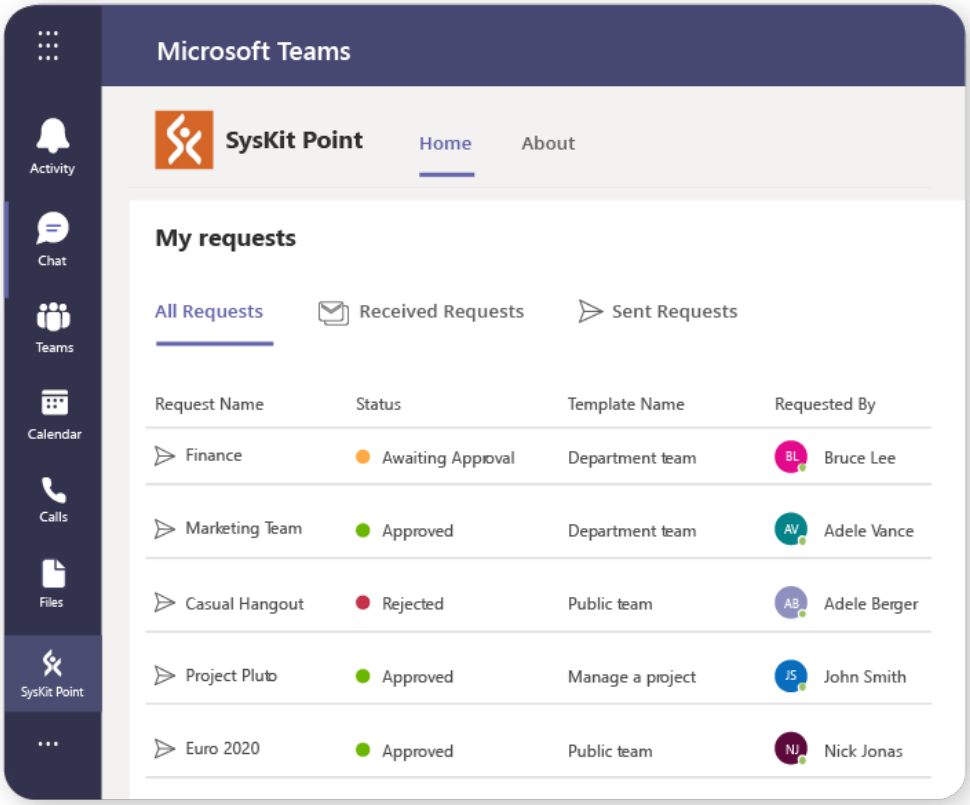
CREATION

You can start by defining governance policies and activating lifecycle management automation. By linking those policies and best practices to provisioning templates for workspace creation, you will ensure all newly created workspaces are **secured from the very moment they are created.**



Setting up provisioning templates enables your end users with an intuitive and easy-to-use interface for workspace creation and approvals using SysKit Point's Teams app.

Once set up, end users can use those templates to request new workspaces **directly from their Teams app**, so there is no need for them to remember where to go to request a new workspace.

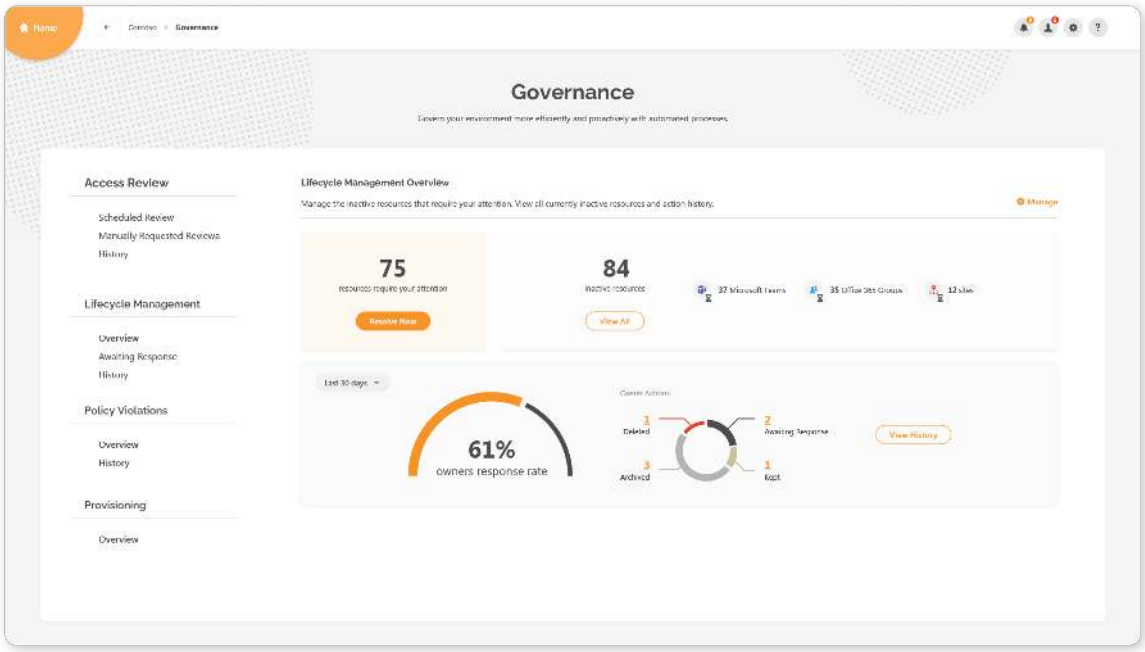


MAINTENANCE

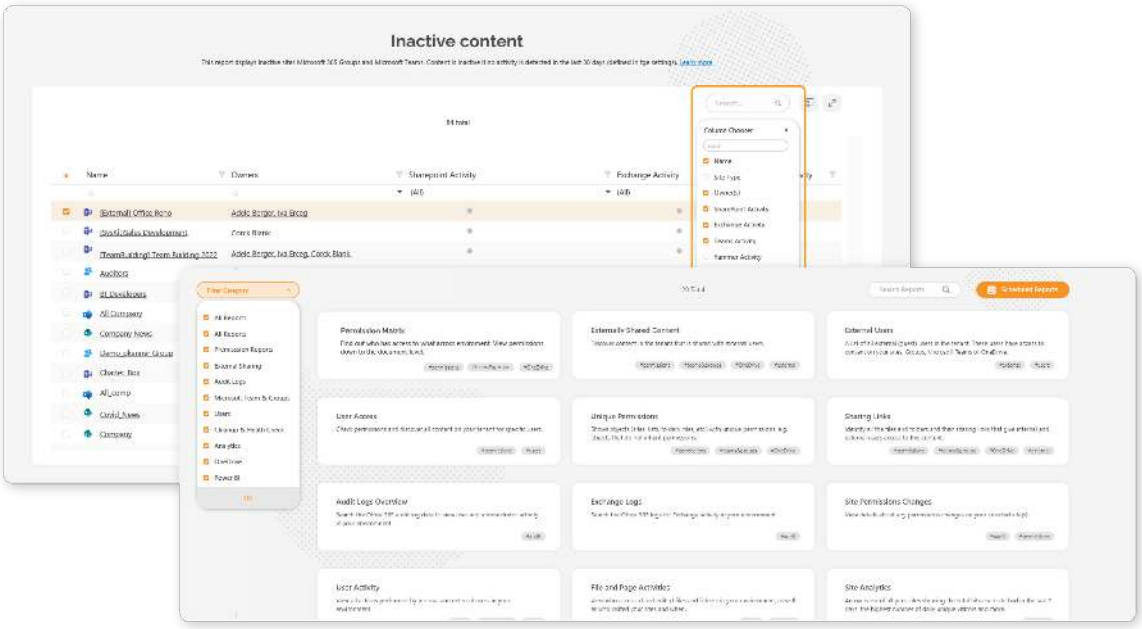
During the maintenance phase, SysKit Point gives IT teams 360 visibility through the SysKit Point governance screen and powerful reporting.

At the same time, SysKit Point triggers automated policies to help and support workspace owners with governance best practices.

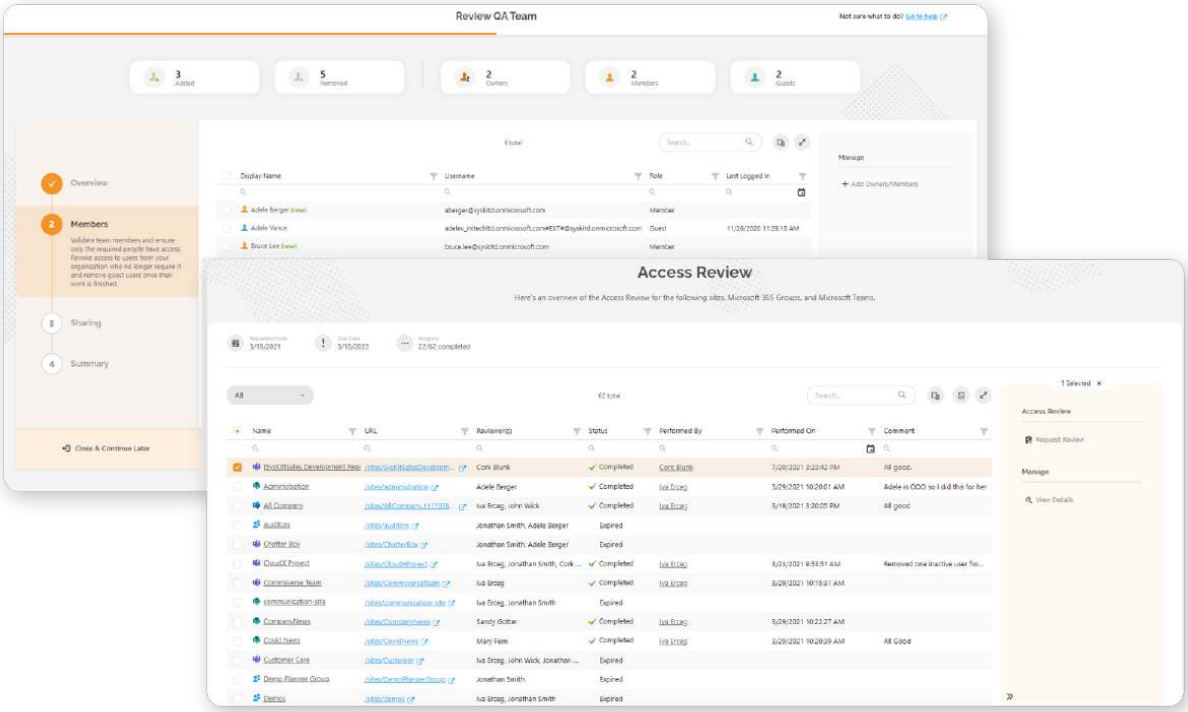
The governance screen gives IT teams quick insight into workspaces that require attention or are inactive. It also provides information about **owner actions, response rates**, and **lifecycle management task history.**



On top of that, IT teams can leverage SysKit Point's extensive reporting and management capabilities to dive deeper into the details.

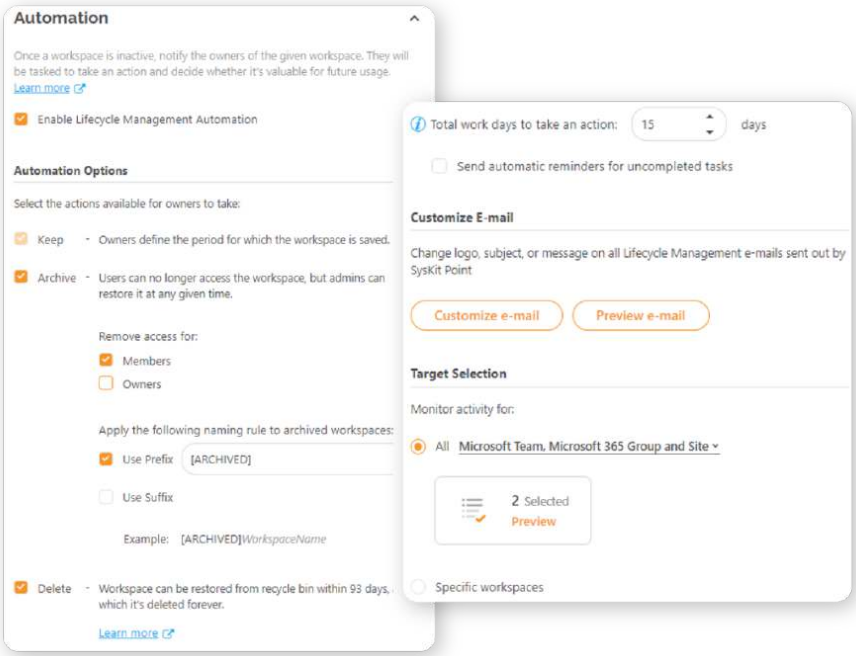


We strongly recommend that you implement regular access reviews to help enforce compliance. Access reviews will ensure that the workspace owners have validated that only the right people can access the right data - giving IT teams a “written” trace that can be useful in an audit.

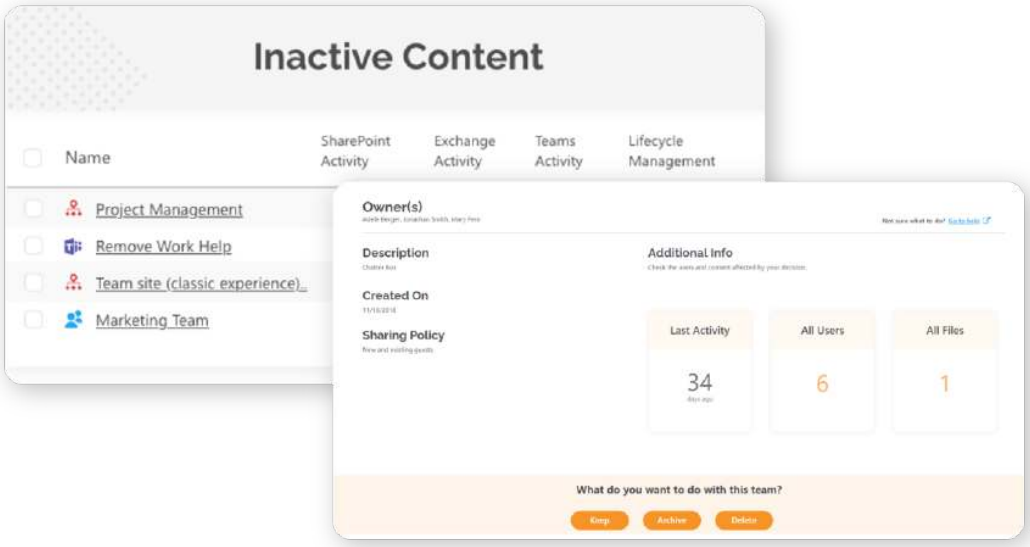


DISPOSAL

For those workspaces that are no longer needed and are not being used, you can also let your owners decide if they wish to **keep, archive, or delete them.**



Once configured, SysKit Point **automatically detects inactive workspaces**, notifies the owner through an email, and supports them in making the right decision through an intuitive interface.



These are just some examples of how SysKit Point can help you with lifecycle management. But SysKit Point is much more. It is an all-in-one management platform for Microsoft 365 that helps you centralize your entire inventory across multiple Microsoft 365 workloads – transforming complex environments into easy-to-manage ones.

Save time and take control of your Microsoft 365 environment today

Start my free trial

SysKit
Krste Pavletića 1
10000 Zagreb, Croatia
+44 (0) 20 3322-2034
+1 (631) 406-4900
+1 (855) 855-5071
sales@syskit.com
www.syskit.com

SysKit