

# Part 2 – Collaboration Overview

(Modern Work & Purview)

## Contents

|   |                                     |
|---|-------------------------------------|
| Disclaimer.....                             | 2                                   |
| Target Audience .....                       | 2                                   |
| Document Scope .....                        | 2                                   |
| Out-of-Scope .....                          | 2                                   |
| Notes.....                                  | 3                                   |
| SharePoint Sharing and Access Controls..... | 3                                   |
| Sharing .....                               | 3                                   |
| Access Controls .....                       | 5                                   |
| Mapping Purview to Collaboration.....       | 7                                   |
| Create (data) .....                         | 7                                   |
| Use & Retain (data).....                    | 10                                  |
| Destroy (data) .....                        | 11                                  |
| Next Steps .....                            | 13                                  |
| Appendix and Links .....                    | 14                                  |
| Blog Labels .....                           | <b>Error! Bookmark not defined.</b> |

Before we start, please note that if you want to see a table of contents for all the sections of this blog, you can locate them at the following URL:

[Microsoft Purview and Modern Work \(Part 1\) - Overview](#)

## Disclaimer

This document is not meant to replace any official documentation, including those found at docs.microsoft.com. Those documents are continually updated and maintained by Microsoft Corporation. If there is a discrepancy between this document and what you find in the Compliance User Interface (UI) or inside of a reference in docs.microsoft.com, you should always defer to that official documentation and contact your Microsoft Account team as needed. Links to the docs.microsoft.com data will be referenced both in the document steps as well as in the appendix.

All of the following steps should be done with test data, and where possible, testing should be performed in a test environment. Testing should never be performed against production data.

## Target Audience

The Information Life Cycle Management section of this blog series is aimed at Security and Compliance and Modern Work officers who need to properly label data, encrypt it where needed.

## Document Scope

This blog and document are meant to help an IT administrator who is looking to secure their data throughout the lifecycle of the data.

It is presumed that you already have a basic understanding of the Purview tools and the Modern Work tools (including Exchange, Teams, SharePoint and OneDrive).

## Out-of-Scope

This document does not cover configuring any of the below, ie. Holding your hand through the process of configuration”, as that is covered via other blogs, official Microsoft documents, or through the aid of Microsoft implementation teams or Microsoft partners:


- Audit
- Communications Compliance
- Compliance Manager
- Data Classification (Sensitive Information Types)
- Data Classification (Exact Data Matching)
- Data Classification (Trainable Classifiers)
- Data Lifecycle Management (retention and disposal)
- Data Protection Loss (DLP) for Exchange, OneDrive, Devices, etc
- Information Barriers
- Information Protection (labeling, encrypting, watermarking, etc of files)
- Insider Risk Management
- Microsoft Defender for Cloud Apps (MDCA)


- Privacy Management (Priva)
- Records Management (retention and disposal)
- Standard or Premium eDiscovery


This blog entry is only addressing Collaboration (creation, usage, sharing of files and SharePoint/Teams Sites), not Communication (emails, teams chats, etc).

## Notes

After each section of this blog, I will make a note of which of the 3 parts of the CIA Triad that Microsoft tool will help you meet. Here are a few examples.

Example #1 –  CIA component – Integrity & Availability

Example #2 –  CIA component – Confidentiality & Availability

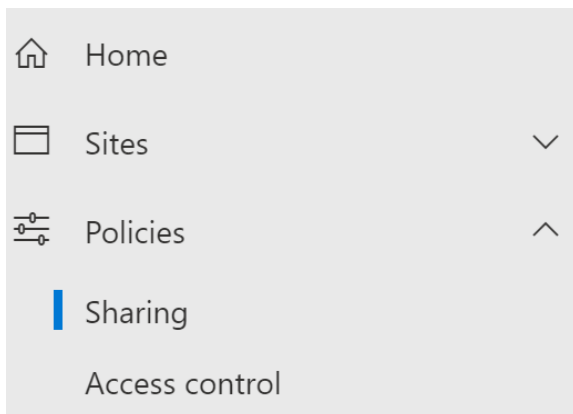
Example #3 –  CIA component – Integrity

## SharePoint Sharing and Access Controls

First, when it comes to protected data, we need to take a moment to make sure that SharePoint specific data controls are enabled. Although we will not go into use cases or configuration on these, you should be aware that where to find these controls.

### Sharing


Go to [sharepoint.com](https://sharepoint.com). Click on **Policies - Sharing**




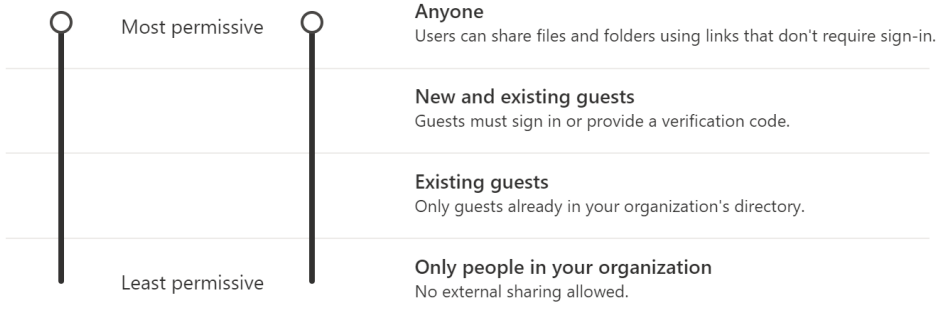
On the right side, you will see sliders that control content sharing.

## External sharing

Content can be shared with:

 SharePoint


 OneDrive




You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings 

Below that you will see **More External Sharing Settings**.

More external sharing settings 

- Limit external sharing by domain
- Allow only users in specific security groups to share externally
- Guests must sign in using the same account to which sharing invitations are sent
- Allow guests to share items they don't own
- Guest access to a site or OneDrive will expire automatically after this many days
- People who use a verification code must reauthenticate after this many days [Learn more](#) 

Below that, you will see controls around Link Sharing and other settings.

## File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

- Specific people (only the people the user specifies)
- Only people in your organization
- Anyone with the link

Choose the permission that's selected by default for sharing links.

- View
- Edit

Choose expiration and permissions options for Anyone links.

These links must expire within this many days

These links can give these permissions:

Files:

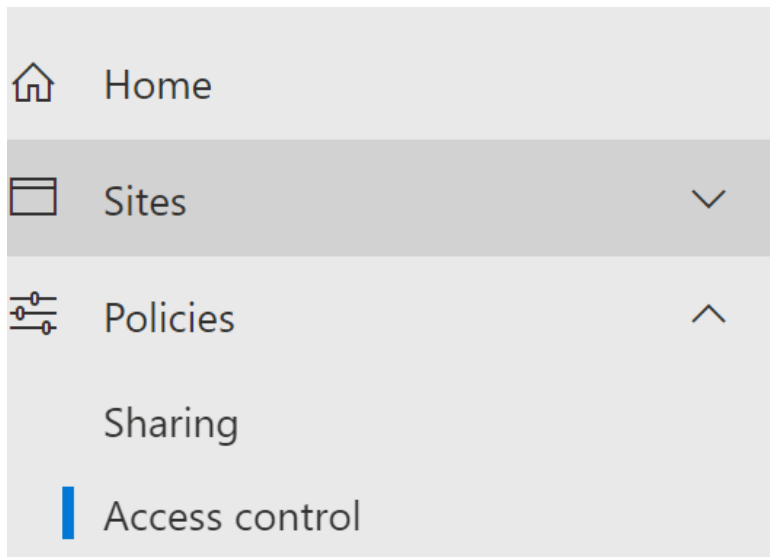
Folders:

## Other settings

- Show owners the names of people who viewed their files in OneDrive
- Let site owners choose to display the names of people who viewed files or pages in SharePoint
- Use short links for sharing files and folders

## Access Controls

Go to [sharepoint.com](https://sharepoint.com). Click on **Policies – Access Controls**



On the right side, you will see various options for controlling access to your SharePoint data. Navigate these controls and investigate what options are available to your organization.

## Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

---

### Unmanaged devices

Restrict access from devices that aren't compliant or joined to a domain.

---

### Idle session sign-out

Automatically sign out users from inactive browser sessions.

---

### Network location

Allow access only from specific IP addresses.

---

### Apps that don't use modern authentication

Block access from Office 2010 and other apps that can't enforce device-based restrictions.

---

### Limit OneDrive access

Limit access to OneDrive by security group.

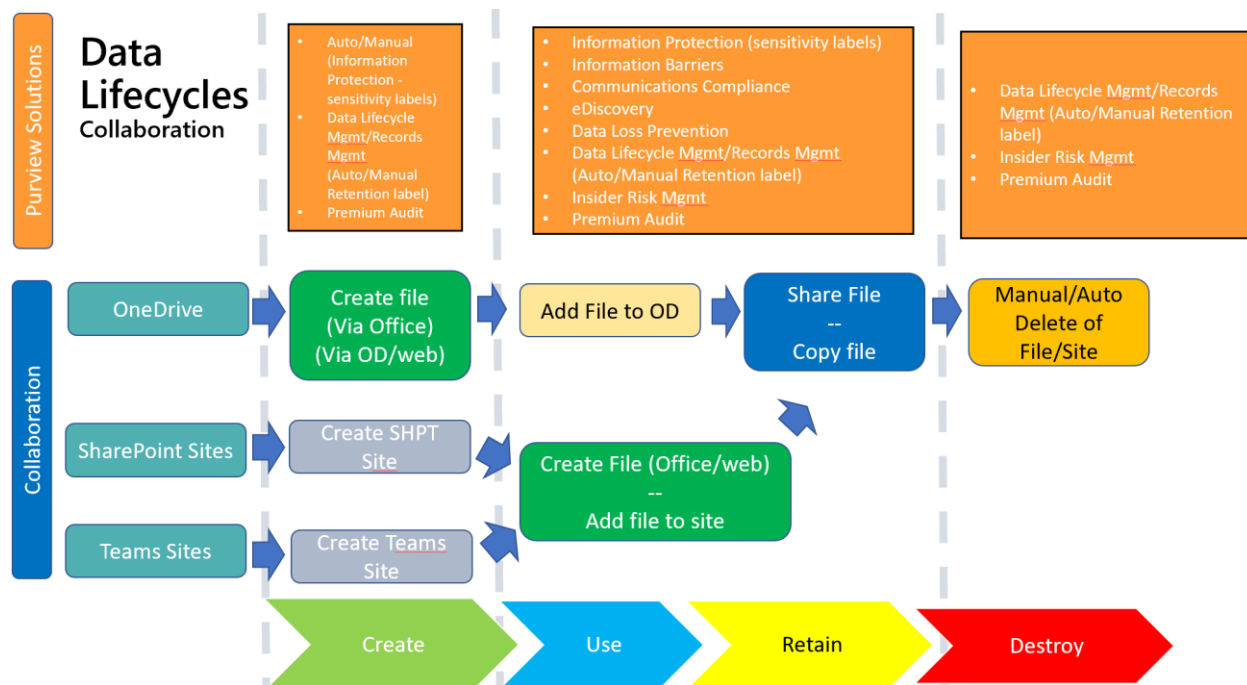
---

Move to the next section where we will address the Purview Specific workloads with your SharePoint, Teams, and OneDrive platform.

## Mapping Purview to Collaboration

Here we will map the Lifecycle of the data (Create -> Use -> Retain -> Delete) of files and data to OneDrive, SharePoint Sites and Team Sites.

When looking at the Information Lifecycle, it is important to understand which Purview tools map to which collaboration activities within that Information Lifecycle. Here is a high-level map.



As this is a bit of an eye chart, we will look at each stage of the Information Lifecycle individually.

Please note that Use & Retain are placed together as these tend to be interchangeable.

### Create (data)

In the Create phase of ILM, here are the recommended Purview Tools.

- Auto/Manual (Information Protection - sensitivity labels)
- Data Lifecycle Mgmt/Records Mgmt (Auto/Manual Retention label)

- Premium Audit

In the Create phase of ILM, here are the SharePoint-based workloads.

- One Drive -> Create File via Office, OneDrive or Web client
- SharePoint -> Create SharePoint Site
- Teams Site ->Create Teams Site

- Auto/Manual (Information Protection - sensitivity labels)
- Data Lifecycle Mgmt/Records Mgmt (Auto/Manual Retention label)
- Premium Audit

Create file  
(Via Office)  
(Via OD/web)

Create SHPT  
Site

Create Teams  
Site

Create

## Use & Retain (data)

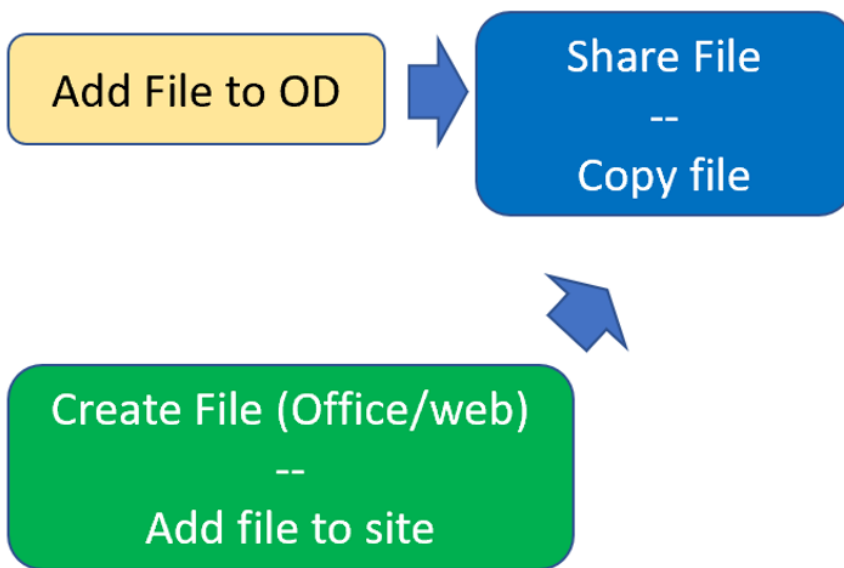
In the Use & Create phase of ILM, here are the recommended Purview Tools.

- Information Protection (sensitivity labels)
- Information Barriers
- Communications Compliance
- eDiscovery
- Data Loss Prevention
- Data Lifecycle Mgmt/Records Mgmt (Auto/Manual Retention label)
- Insider Risk Mgmt
- Premium Audit

In the Use & Create phase of ILM, here are the SharePoint-based workloads.

- One Drive -> Add File to OneDrive -> Share File / Copy File
- SharePoint -> Create File (Office/Web) / Add File to Site SharePoint Site -> Share File/Copy File
- Teams Site -> Create File (Office/Web) / Add File to Site SharePoint Site -> Share File/Copy File

- Information Protection (sensitivity labels)
- Information Barriers
- Communications Compliance
- eDiscovery
- Data Loss Prevention
- Data Lifecycle Mgmt/Records Mgmt (Auto/Manual Retention label)
- Insider Risk Mgmt
- Premium Audit



Destroy (data)

In the Delete phase of ILM, here are the recommended Purview Tools.

- Data Lifecycle Mgmt/Records Mgmt (Auto/Manual Retention label)
- Insider Risk Mgmt
- Premium Audit

In the Delete phase of ILM, here are the SharePoint-based workloads.

- One Drive -> Manual / Auto delete of File / Site
- SharePoint -> Manual / Auto delete of File / Site
- Teams Site -> Manual / Auto delete of File / Site

- Data Lifecycle Mgmt/Records Mgmt (Auto/Manual Retention label)
- Insider Risk Mgmt
- Premium Audit

Manual/Auto  
Delete of  
File/Site

Destroy

## Next Steps

We will now move to look at SharePoint Sites and specific Purview workloads that can be mapped to data within that platform.

## Appendix and Links

- [Microsoft Purview compliance documentation - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview risk and compliance solutions - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview Data Lifecycle Management | Microsoft Security](#)
- [Use Microsoft Teams for collaboration - Microsoft 365 Business Premium | Microsoft Learn](#)
- [What is OneDrive? \(work or school\) - Microsoft Support](#)
- [How to use the Microsoft data classification dashboard - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about insider risk management - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about communication compliance - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about data loss prevention - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview Compliance Manager - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview eDiscovery solutions - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Microsoft Purview Audit \(Premium\) - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about Microsoft Purview Data Lifecycle Management - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Records management for documents and emails in Microsoft 365 - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about information barriers - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about sensitivity labels - Microsoft Purview \(compliance\) | Microsoft Learn](#)
- [Learn about Microsoft Priva - Microsoft Priva | Microsoft Learn](#)