



The Two Sides of the Data Coin: *Data Protection vs. Data Retention in Practice*

Anna Bordioug

Protiviti M365 Consultant

Joanne Klein

NexNovus M365 Consultant, Microsoft MVP

Microsoft 365 Security & Compliance User Group | October 29, 2025



Joanne C Klein

NexNovus M365 Consultant

joannecklein.com

<https://www.linkedin.com/in/joannecklein/>



Anna Bordioug

Protiviti M365 Consultant

www.annabordioug.com

<https://www.linkedin.com/in/anna-bordioug/>

Agenda

- Data Classification: An Important Underpinning to Purview
- Data Protection and Data Retention: What They Each Look Like in Purview
- How Does AI Affect Both Data Protection and Data Retention
- Practical Lessons We've Learned from Customers
- Common Questions We Hear from Customers
- Q&A (time permitting)



Leave with our exclusive Top 20 Label Behavior Comparison Chart (at the end of this deck!)

Data Classification

An Important Underpinning to Purview



What is data classification and why is it important?

Core Role of the Data Classification service

To store classification details of your content to reflect the current Purview classifier definitions (match, confidence level, occurrence count). This helps to **identify information** your org finds sensitive in a **scalable, automated** way.



Actionable Compliance Workflows

Classified data enables **policy enforcement, automated labeling**, data loss prevention, and insider risk management **risky activity detection**.

Where do you see classification details for your content?

A lot of places! Some of it is summarized for you in a nice UI format; some of it is raw classification details.
(e.g., Purview Data Explorer)

The screenshot shows the 'Data explorer' interface. On the left, there's a sidebar with a search bar and a dropdown menu for 'Choose a classifier or a label'. Below that is a section for 'Sensitive info types' with a list of items like 'Employee Number', 'All Full Names', etc. On the right, there's a main pane titled 'Microsoft 365' showing a table of results. The columns are 'Data source', 'Sensitive info types', 'Sensitivity labels', 'Trainable classifiers', 'EDM classifiers', 'Retention labels', and 'Items'. The table lists five entries: Copilot, Exchange, OneDrive, SharePoint, and Teams, each with their respective classification details and item counts.

Data source	Sensitive info types	Sensitivity labels	Trainable classifiers	EDM classifiers	Retention labels	Items
Copilot	Employee Number, ...	Finance, IT, Source c...	None			24 >
Exchange	Employee Number, ...	Internal Use, Internal...	None			2707 >
OneDrive	Employee Number, ...	Internal Use, Internal...	Finance, IT, Custome...	None	Lease Agreement, C...	45 >
SharePoint	Employee Number, ...	Internal Use, Internal...	Finance, IT, Source c...	None	Lease Agreement, C...	23316 >
Teams	Employee Number, ...	Finance, IT, Source c...	None			20 >



What is data classification and why is it important?

Alerts > DLP policy match for document 'Part document B.docx' in SharePoint

DLP policy match for document 'Part document B.docx' in SharePoint

Low Active

Overview Events 1 of 14 selected

Event	User	Time detected	Location
<input checked="" type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input checked="" type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint
<input type="checkbox"/> Sensitive info found in 'Part docume... [redacted]	[redacted] Joanne Klein	Oct 22, 2025 6:46 PM	SharePoint

Sensitive info found in 'Part document D.docx'

Source Details Classifiers File activity Metadata

SensitivityLabelIds: []
SensitivityLabelNames: []
SharedBy: [null]
SiteAdmin: []
SiteCollectionGuid: "39d35ad7-590d-4383-bc56-3d2efc952102"
SiteCollectionUrl: "https://[redacted].sharepoint.com/sites/SITClassificationTest"
UniqueId: "4756b626-48f5-4aae-af1b-dd7b67638617"
PolicyMatch: "Block Part Numbers for External"
PolicyId: "1021069f-971e-4eea-ac22-a26c776ab58e"
RuleId: "932b464b-de0b-4d63-9197-f4138ba639c0"
RuleMatch: "Check for part number"
SITDetected: [{"Name": "ABC Corp Part Number", "Confidence": 85, "Count": 2, "Id": "e9f78631-ab3f-4a2b-9236-a40e3a1d5fae", "DetailedClassificationAttributes": [{"Confidence": 65, "Count": 2, "IsMatch": false}, {"Confidence": 75, "Count": 2, "IsMatch": false}, {"Confidence": 85, "Count": 2, "IsMatch": true}], "ClassifierType": "Content"}
TrainableClassifier: []
ActionTaken: "BlockAccess, NotifyUser, GenerateAlert"
UserOverride: "No"
DetectedValuesForSITS: [{"SITName": "ABC Corp Part Number", "MatchedSensitiveContent": "ABC-123", "SurroundingCharacters": "Part ABC-123\\nPart DKJ-444-098\\n", "SITId": "e9f78631-ab3f-4a2b-9236-a40e3a1d5fae"}, {"SITName": "ABC Corp Part Number", "MatchedSensitiveContent": "DKJ-444-098", "SurroundingCharacters": "Part ABC-123-123\\nPart DKJ-444-098\\n", "SITId": "e9f78631-ab3f-4a2b-9236-a40e3a1d5fae"}]
OtherMatchedConditions: []

Actions Update alert status

Sensitive info type

Sensitive info type	High confidence	Medium confidence	Low confidence
ABC Corp Part Number	2	2	2

Sensitive info details

Sensitive info type	Matched cont...	Surrounding context
ABC Corp Part Number	ABC-123-123	Part ABC-123-123 Part DKJ-444-098
ABC Corp Part Number	DKJ-444-098	Part ABC-123-123 Part DKJ-444-098



What is data classification and why is it important?

What triggers data to be classified?

Client-side classification

- Users create/update content
- Exchange/SharePoint/OneDrive

“data in motion”

Re-index SharePoint site

- Initiated via UI or PowerShell
- SharePoint/OneDrive

“data at rest”*

On-demand classification

- Initiated via Purview... UI or PowerShell
- SharePoint/OneDrive/Endpoint

“data at rest”

Downstream effects of having your data classified...

Once data is classified, many other Purview solutions can use the classification details as input. This can reduce the risk of AI tools surfacing unlabeled or unprotected data.

PURVIEW SOLUTION

Information Protection

Data Loss Prevention (DLP)

Insider Risk Management

Records Management

eDiscovery & Audit

Communication Compliance

CLASSIFICATION IMPACT

Auto-labeling based on current classification of content

Policy actions can be triggered by classified content

Flags risky behavior involving sensitive data

Applies retention labels based on current classification of content

Enables targeted search and review of sensitive content in classified content

Detects sensitive or inappropriate communications for classified content



Technical Best Practices

BEST PRACTICE	DESCRIPTION
Start with Built-in Types	Start with predefined sensitive info types for validation for accuracy in your tenant. Don't underestimate the time/effort in this step!
Expand to Custom Classifiers as early as possible	Create organization-specific classifiers for tailored detection. The earlier you can define these in your tenant lifecycle the better.
Testing classifiers	<p>Test via Exchange PowerShell: <code>\$r = Test-DataClassification -ClassificationNames "Canada Physical Addresses" -TextToClassify "value" \$r.ClassificationResults</code></p> <p>Testing via UI: Purview Classifiers... SIT classifiers and EDM classifiers (single file only)</p>
Validating post-classification	Use Data Explorer, Content Explorer, eDiscovery search, Activity Explorer to verify classification coverage. Syntax to search for a SIT:  <code>SensitiveType: "SIT Name", 1..99, 86..100</code> <small>SIT name or GUID Count range Confidence range</small>
Cross-Team Collaboration	Align security, compliance, and governance teams for a unified strategy

Data Protection and Data Retention

What they each look like in Purview



Data Protection in Microsoft Purview

Data Security

Secure data across its lifecycle, wherever it lives.

The screenshot shows the 'Data Security' section of the Microsoft Purview portal. It includes links for Data Loss Prevention, Data Security Posture Management, Data Security Investigations (preview), Information Protection (which is highlighted with a red border), Insider Risk Management, and DSPM for AI. Each service has a brief description and a 'Powered by Copilot' note.

The screenshot shows the 'Information Protection' section under 'Reports'. It displays 'Protection coverage' with a circular progress bar and a bar chart for Microsoft 365 (378 items). Below this is a 'Sensitivity label coverage' section. The left sidebar lists navigation options like Overview, Reports, Recommendations, Sensitivity labels, Policies, Classifiers, Explorers, and Diagnostics.

Information Protection

- Classify, label, and protect sensitive data
- Encrypt files and emails to enforce access controls
- Automatically apply sensitivity labels if sensitive information exists in content
- Apply default sensitivity labels to increase labeling coverage
- Protect SharePoint sites, Microsoft 365 groups, and Teams meetings



Microsoft Purview Information Protection Demo

The screenshot illustrates the Microsoft Purview Information Protection feature within Microsoft Word. The 'Sensitive' label is selected from the sensitivity dropdown menu.

Document Properties:

- Name: Document.docx
- Title: Enter value here
- Department: Enter value here
- Department2: Enter value here
- Sensitivity: Internal
- Apply label: Label H - record (unlocked)
- Record status: Unlocked

Word Document Interface:

- File, Home, Insert, Layout, References, Review, View, Help tabs.
- Search bar: Search for tools, help, and more (Alt + Q).
- Share button: Comments, Catch up, Editing, Share.
- Sensitivity dropdown menu: General, Company Only, Sensitive (selected), Restricted, Learn More.
- Font, size, bold, italic, underline, and other styling tools.
- Normal style button.
- Share pane on the right.



Microsoft Purview Information Protection Demo

The screenshot shows a Microsoft Purview Information Protection interface. On the left, there's a compose email screen with fields for 'To', 'Cc', 'Subject' (labeled 'Add a subject'), and 'Body' (labeled 'Type / to insert files and more'). On the right, a protection level dropdown menu is open, showing five options: 'General' (unselected), 'Company Only' (selected, indicated by a checkmark), 'Sensitive' (unselected), and 'Restricted' (unselected). Below the dropdown are 'Learn more...' and navigation arrows. At the top right of the main window, there are icons for trash, copy, and other actions.

- General
- Company Only
- Sensitive
- Restricted

Learn more... ▶◀▶



Microsoft Purview Information Protection Demo

The screenshot shows the Microsoft Word ribbon interface. The top bar includes the 'File' tab, the current document name 'Document3', and a search bar. Below the ribbon is the toolbar with various icons for font, size, bold, italic, underline, and alignment. A yellow callout box displays a 'POLICY TIP' message: 'Your organization recommends that you change the sensitivity to: Sensitive.' It includes a 'Change now' button and a close 'X' button. In the main content area, there is a placeholder image icon and the text 'Credit Card: 5370-4638-8881-3020'.



Microsoft Purview Information Protection Demo

Your organization recommends that you change the Sensitivity to Sensitive.

[Change sensitivity](#) [Dismiss](#) [X](#)

[Send](#) [Company Only](#)

To: Megan Bowen [X](#)

Bcc:

Cc:

Test Email Containing Test Credit Card Number Draft saved at 11:25 AM

Credit Card: 5370-4638-8881-3020



Data Protection in Microsoft Purview

Data Security

Secure data across its lifecycle, wherever it lives.

Data Loss Prevention
Protect sensitive content as it's used and shared throughout your org - in the cloud, on-premises, and on devices.
Powered by Copilot

Data Security Posture Management
Get insights and recommendations for protecting sensitive data, improving data security posture, and identifying top risks using Security Copilot.
Powered by Copilot

Data Security Investigations (preview)
Leverage AI to identify, analyze, and mitigate risks in response to a data security incident.
Powered by Copilot

Information Protection
Discover, classify, and protect sensitive and business-critical content throughout its lifecycle.

Insider Risk Management
Detect risky user activity to help quickly identify and take action on insider risks and threats.
Powered by Copilot

DSPM for AI
Discover and secure your org's AI data and activity in Microsoft Copilot experiences, agents, and other AI apps in one central location.

Data Loss Prevention

- Overview
- Policies
- Alerts
- Classifiers
- Explorers
- Diagnostics

Related solutions

- Data Security Investigations (preview)
- Information Protection
- Insider Risk Management

Top activities detected
2 activities
2 Exchange
[View all activities](#)

Device health overview
All devices are updated
These devices may not be fully protected until they are correctly configured and policies have synced.
[View affected devices](#)

Adaptive Protection
Automatically mitigate potential risks with Adaptive Protection
Adaptive Protection combines Data Loss Prevention, Conditional Access & Insider Risk Management capabilities to help minimize risky activity early.
• Define which risk activities to detect
[Get started](#)

Extend protection to auto-labeling
2 policies ready to extend
You already have policies protecting sensitive info in email. Extend that protection by quickly setting up auto-labeling policies that apply a sensitivity label to email matching the same conditions as your DLP policies.
[Get started](#)

Data Loss Prevention

- Implement policies to audit and block data loss across Microsoft 365 and other cloud locations
- Monitor user activity and protect data on devices
- Educate users on unapproved information flows
- Protect data on-premises
- Review and escalate realized data security risks tracked by policies



Microsoft Purview Data Loss Prevention Demo

Policy tip: Warning - The content you are sending contains Personal Information. [Show details](#)

The following recipient is outside your organization: Bordioug, Anna (13100). X

Send ▼ Company Only ▼

To Bordioug, Anna (13100) <anna.bordioug@protiviti.com> X Bcc

Cc

External Sensitive Email Draft saved at 11:28 AM

Olivia Wilson Social Insurance Number: 740 486 436|

Send blocked

Your organization won't allow this message to be sent until the sensitive information is removed. Please remove it and try to send the message again.

OK



Data Protection in Microsoft Purview

Data Security

Secure data across its lifecycle, wherever it lives.

The screenshot shows the 'Data Security' section of the Microsoft Purview portal. It includes cards for:

- Data Loss Prevention**: Protect sensitive content as it's used and shared throughout your org - in the cloud, on-premises, and on devices. Powered by Copilot.
- Data Security Posture Management**: Get insights and recommendations for protecting sensitive data, improving data security posture, and identifying top risks using Security Copilot. Powered by Copilot.
- Data Security Investigations (preview)**: Leverage AI to identify, analyze, and mitigate risks in response to a data security incident. Powered by Copilot.
- Information Protection**: Discover, classify, and protect sensitive and business-critical content throughout its lifecycle.
- Insider Risk Management**: Detect risky user activity to help quickly identify and take action on insider risks and threats. This card is highlighted with a red border.
- DSPM for AI**: Discover and secure your org's AI data and activity in Microsoft Copilot experiences, agents, and other AI apps in one central location. Powered by Copilot.

The screenshot shows the 'Insider Risk Management' section of the Microsoft Purview portal. It includes:

- A sidebar menu with options like Overview, Recommendations, Alerts, Cases, Policies, Users, Reports, Forensic Evidence, Notice templates, Audit log, Adaptive Protection, Related solutions, and Communication.
- A main area with a 'Manage reports' button.
- A 'Resources' section titled 'Insider risk management resources'.
- A 'Stay informed about insider risk management' section with a note about updates and links to 'Read the official docs', 'Get the latest news', and 'Become an Insider Risk Ninja'.

Insider Risk Management

- Implement policies to proactively identify insider risks (e.g., exfiltration of data by departing users)
- Tailor policies to industry-specific insights such as misuse of health records
- Dynamically apply security controls based on a user's risk level
- Review and escalate data security risks realized by insiders and tracked by policies



Microsoft Purview Insider Risk Management Demo

≡

Insider Risk Management

- Overview
- Recommendations
- Alerts
- Cases
- Policies**
- Users
- Reports
- Forensic Evidence
- Notice templates
- Adaptive Protection

Related solutions

- Communication Compliance
- Information Barriers
- Data Loss Prevention

Policies

Policy warnings | 11 Policy recommendations | 6 Healthy policies | 0

Review collection policies. Collection policies control what activities can be detected by device indicators. We recommend reviewing your org's collection policies to ensure they're set up to detect the device activities you want to detect in your insider risk policies. [Learn more about collection policies.](#)

[Go to collection policies](#)

7 items						
<input type="checkbox"/> Policy name ↑	Status	Users in scope	Active alerts	Confirmed alerts	Actions taken on alerts	Policy alert effectiveness
<input type="checkbox"/> Colin Data Leak (Cloud-Only)	● 1 warning	0	0	0	0	0%
<input type="checkbox"/> Colin Data Leak (Endpoint-only)	● 1 warning	0	0	0	0	0%
<input type="checkbox"/> datariskcheck-sev-april19	● 2 warnings	0	0	0	0	0%
<input type="checkbox"/> Departing User (Cloud-Only)	● 2 warnings, 2 recommendations	1	0	0	0	0%
<input type="checkbox"/> DSPM for AI - Detect risky AI usage	● 1 warning, 2 recommendations	1	0	0	0	0%
<input type="checkbox"/> DSPM for AI - Detect when users visit AI sites	● 1 warning, 1 recommendation	0	0	0	0	0%
<input type="checkbox"/> tests	● 3 warnings, 1 recommendation	0	0	0	0	0%



Microsoft Purview Insider Risk Management Demo

Microsoft Purview

Search

Copilot

Home

Solutions

Agents

Learn

Settings

Insider Risk Management

- Overview
- Recommendations
- Alerts
- Cases
- Policies
- Users
- Reports
- Forensic Evidence
- Notice templates
- Audit log
- Adaptive Protection

Related solutions

- Communication Compliance
- Information Barriers
- Data Loss Prevention

Alerts

Spotlight 1

Export

2 items Alerts tutorial Search Customize columns

Filter set: Save

Severity: Any Status: Any Time detected (UTC): Any Add filter

ID	Users	Policy	Status	Spotlight	Alert severity	Time detected	Assigned to	Case	Case sta...
24ba8a01	#Anonymized#EAAAAE9wKAO9y/30dR...	Test Data Leak	Needs review	High	a month ago	Unassigned	No case		
f1c9e427	#Anonymized#EAAAADHueHluBmhHhx...	Restricted Sites Monitoring	Needs review	High	4 months ago	Unassigned	No case		



Microsoft Purview Insider Risk Management Demo

Microsoft Purview

Search

Alerts > Test Data Leak

(24ba8a01) Test Data Leak

High severity Risk score: 75/100 Alert created on Jun 8, 2025 (UTC)

Activity that generated this alert Reduce alerts for this activity

Data access: Sensitive SharePoint files accessed
75/100 High severity | Jun 24, 2025 (UTC)
3 events: Sensitive files accessed from 1 SharePoint site
3 events: Files containing sensitive info, including: All Full Names, Diseases, All Medical Terms And Conditions
3 events: Files that have labels applied, including: Public
3 events: Sites that have labels applied, including:
Factors that impacted risk score:
Includes priority content (3 events)

Note: 95 other activities have the same risk score of 75/100
[View all activity](#)

[All risk factors](#) [Activity explorer](#) [User activity](#)

Triggering event Jun 7, 2025 (UTC)
Downloading content from SharePoint

User details
#Anonymized#EAAAALg5YP3VKxrHYmkC2xSNVEZTv/4o+NCKmsSoemnFv9IW3vmfxm00XrSqw+QP OV2wha2YRe8NXH/6owOhIAjTV/IKk/7f48aQdsO 6ljxmwWa
[View all details](#)

User alert history
Last 30 days: No alert history
[View full user history](#)

[Assign](#) [Needs review](#) [Confirm all alerts & create case](#) [Dismiss alert](#)

What will these actions do?

All risk factors for this user's activity

Top exfiltration activities Cumulative exfiltration activities Sequence of activity Unusual activity for this user

Insider Risk Management... Home Solutions Agents Learn Cases Policies Users Reports Forensic Evidence Notice templates Audit log Adaptive Protection Data Lifecycle Managem... Records Managem... Information Protection Data Loss Prevention Communication Compliance Information Barriers

Data Lifecycle Management in Microsoft Purview

Data Governance

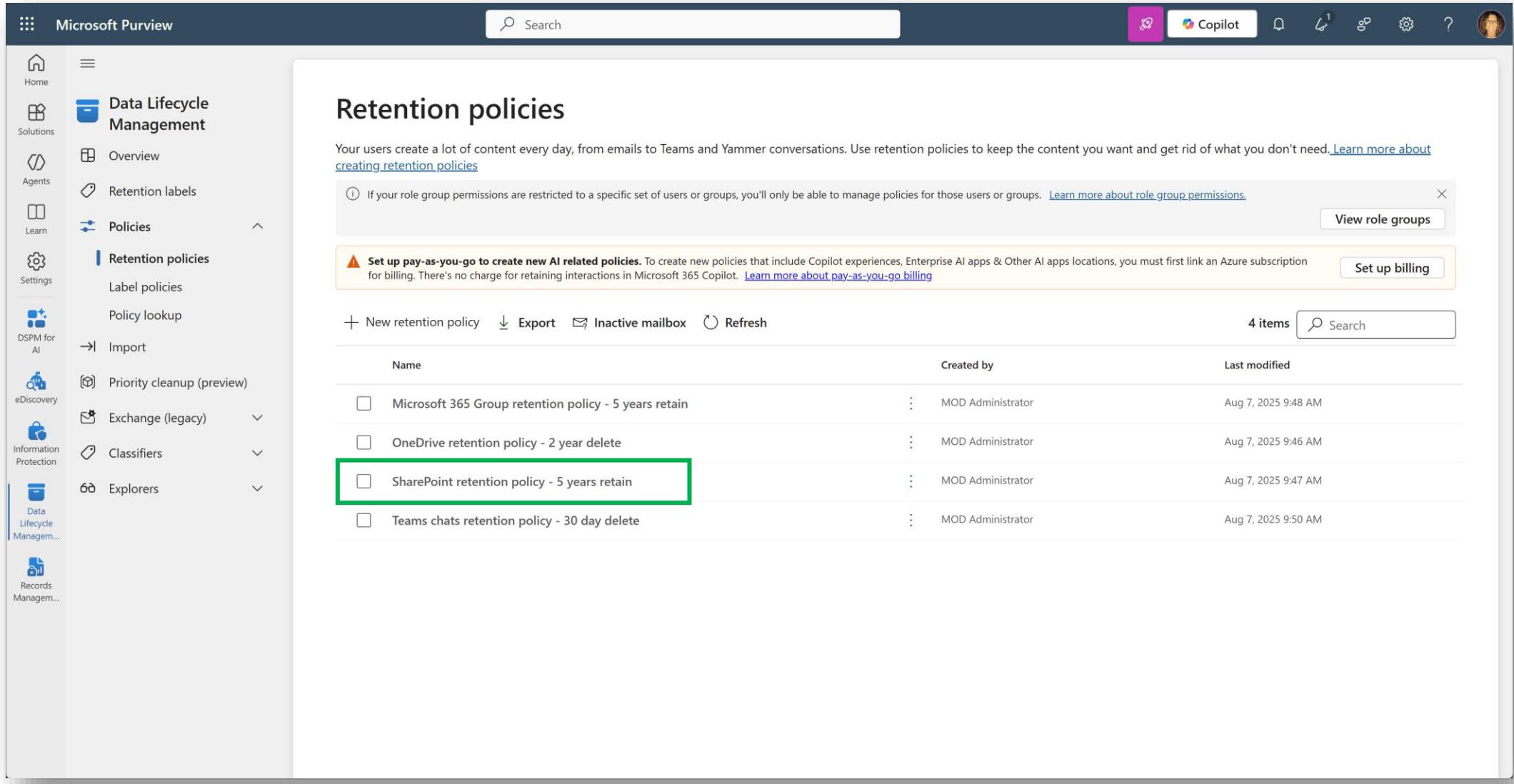
Govern data seamlessly to empower your organization.

The screenshot shows the Microsoft Purview Data Governance interface. On the left, there's a sidebar with a tree view of data management tools: Data Catalog, Data Lifecycle Management (selected), Retention labels, Policies, Import, Priority cleanup (preview), Exchange (legacy), Classifiers, and Explorers. The main area has two cards. The first card, 'Data Catalog', says 'Find and curate data across your org with this searchable inventory of data assets and metadata.' The second card, 'Data Lifecycle Management', says 'Manage your content lifecycle so you can keep what you need and delete what you don't.' A red box highlights the 'Data Lifecycle Management' card. Below these cards is the 'Overview' page for Data Lifecycle Management. It features a sidebar with 'Most used retention labels' (Administrative Convenience Copy, Permanent, External Reference Material, Corporate Enterprise Document) and 'Data lifecycle management resources' (Read the official docs, Get the latest news, Watch recent videos, Learn what's new in Microsoft Purview). The main content area includes a 'Recommendation' section with a button to 'View Recommendation' and a note about adaptive scopes.

Data Lifecycle Management

- Implement retention policies to automatically retain and/or delete content (e.g., retain all executive's emails for 10 years, delete all Teams chats after 30 days)
- Tailor controls to government and industry-specific regulations such as CCPA, GDPR
- Dynamically apply retention policies based on a user's role
- Preserve content due to inadvertent or malicious deletes based on elevated user risk level

Microsoft Purview Data Lifecycle Management



The screenshot shows the Microsoft Purview Data Lifecycle Management interface. The left sidebar navigation includes Home, Solutions (with Data Lifecycle Management selected), Agents, Learn, Settings, DSPM for AI, eDiscovery, Information Protection (with Explorers selected), and Records Management. The main content area is titled "Retention policies". It displays a message about users creating content daily and using retention policies to manage it. A note says if role group permissions are restricted, only those users can manage policies. A warning about pay-as-you-go billing is present. Below is a table of retention policies:

Name	Created by	Last modified
<input type="checkbox"/> Microsoft 365 Group retention policy - 5 years retain	MOD Administrator	Aug 7, 2025 9:48 AM
<input type="checkbox"/> OneDrive retention policy - 2 year delete	MOD Administrator	Aug 7, 2025 9:46 AM
<input checked="" type="checkbox"/> SharePoint retention policy - 5 years retain	MOD Administrator	Aug 7, 2025 9:47 AM
<input type="checkbox"/> Teams chats retention policy - 30 day delete	MOD Administrator	Aug 7, 2025 9:50 AM

Microsoft Purview Data Lifecycle Management

The screenshot shows a SharePoint document library titled "Retention Policy DEMO site". The library interface includes a top navigation bar with "Contoso Electronics" and "SharePoint" links, a search bar, and various management icons. Below the navigation is a ribbon menu with "Home", "Documents" (selected), "Pages", "Site contents", and "Edit" buttons. The main content area displays a grid of documents. The columns are "Name", "Modified", "Modified By", and "Retention label". A "New" button is available for creating new documents. The "Retention label" column shows that all documents are assigned to "MOD Administrator".

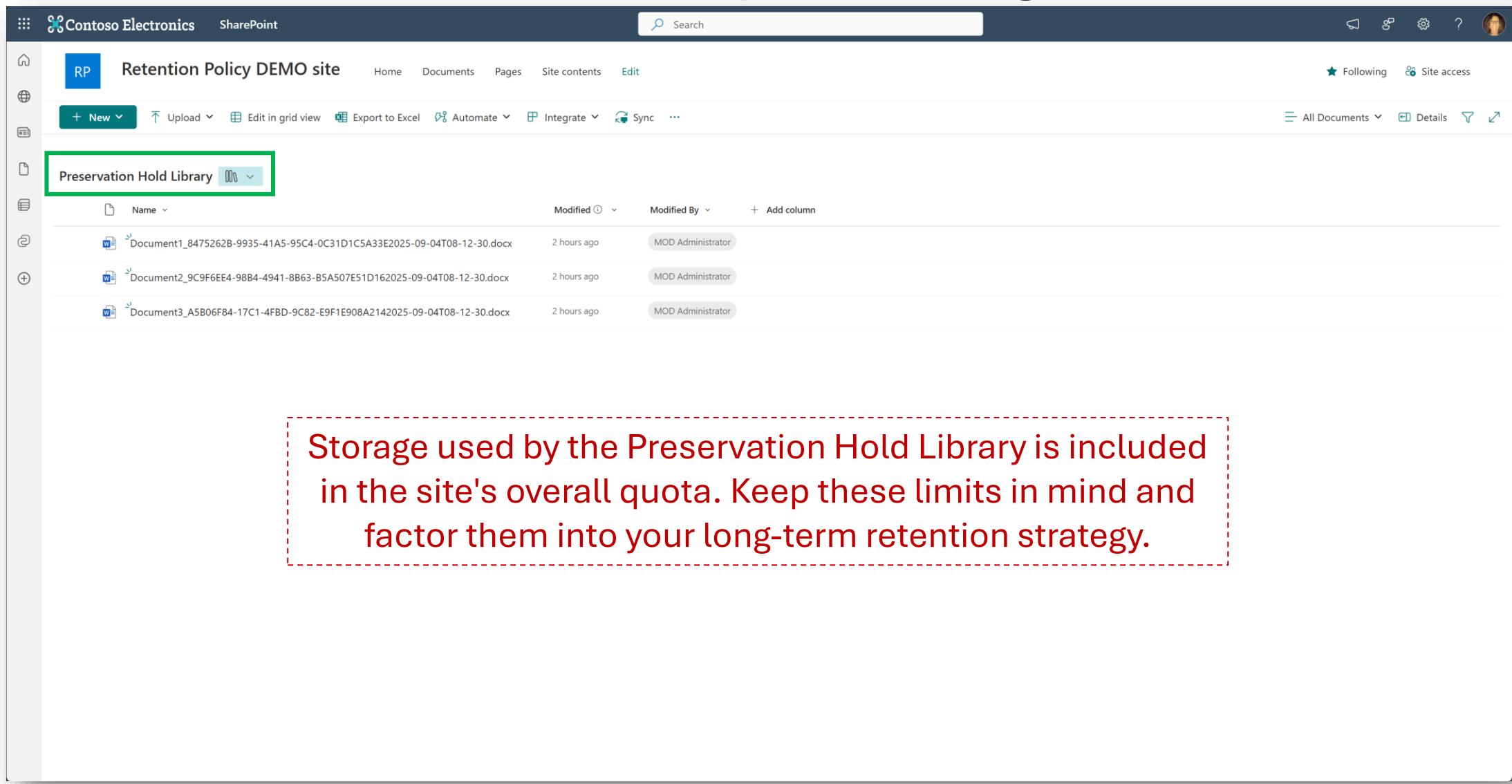
Name	Modified	Modified By	Retention label
Document1.docx	About a minute ago	MOD Administrator	
Document2.docx	About a minute ago	MOD Administrator	
Document3.docx	About a minute ago	MOD Administrator	
Document4.docx	About a minute ago	MOD Administrator	
Document5.docx	About a minute ago	MOD Administrator	
Document6.docx	About a minute ago	MOD Administrator	
Document7.docx	About a minute ago	MOD Administrator	
Mapping Retention Schedules into a Purview File Plan.pdf	About a minute ago	MOD Administrator	

Microsoft Purview Data Lifecycle Management

The screenshot shows a SharePoint document library interface titled "Retention Policy DEMO site". The library contains several documents, all of which have been modified "About a minute ago" by "MOD Administrator". A yellow circle highlights the "Delete" button in the top navigation bar, indicating it is the focus of the demonstration.

Name	Modified	Modified By	Retention label
Document1.docx	About a minute ago	MOD Administrator	
Document2.docx	About a minute ago	MOD Administrator	
Document3.docx	About a minute ago	MOD Administrator	
Document4.docx	About a minute ago	MOD Administrator	
Document5.docx	About a minute ago	MOD Administrator	
Document6.docx	About a minute ago	MOD Administrator	
Document7.docx	About a minute ago	MOD Administrator	
Mapping Retention Schedules into a Purview File Plan.pdf	About a minute ago	MOD Administrator	

Microsoft Purview Data Lifecycle Management



The screenshot shows a Microsoft SharePoint site titled "Retention Policy DEMO site". The left navigation bar includes icons for Home, Documents, Pages, Site contents, and Edit. The top navigation bar shows "Contoso Electronics" and "SharePoint" with a search bar. The main content area displays a "Preservation Hold Library" containing three documents:

Name	Modified	Modified By
Document1_8475262B-9935-41A5-95C4-0C31D1C5A33E2025-09-04T08-12-30.docx	2 hours ago	MOD Administrator
Document2_9C9F6EE4-98B4-4941-8B63-B5A507E51D162025-09-04T08-12-30.docx	2 hours ago	MOD Administrator
Document3_A5B06F84-17C1-4FB0-9C82-E9F1E908A2142025-09-04T08-12-30.docx	2 hours ago	MOD Administrator

A red callout box highlights the "Preservation Hold Library" heading. A red dashed box surrounds the following text:

Storage used by the Preservation Hold Library is included in the site's overall quota. Keep these limits in mind and factor them into your long-term retention strategy.

Microsoft Purview Data Lifecycle Management

Microsoft Purview

Search

Copilot

Notifications

Profile

Data lifecycle management > Create retention policy

Name

Administrative Units

Type

Locations

Retention settings

Finish

Locations you can apply a Retention policy to

Choose where to apply this policy

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

ⓘ You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

⚠ Set up pay-as-you-go to create new AI related policies. To create new policies that include Copilot experiences, Enterprise AI apps & Other AI apps locations, you must first link an Azure subscription for billing. There's no charge for retaining interactions in Microsoft 365 Copilot. [Learn more about pay-as-you-go billing](#)

Set up billing

Status	Location	Applicable Content	Included	Excluded
<input type="radio"/> Off	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. More details		
<input type="radio"/> Off	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). More details		
<input type="radio"/> Off	OneDrive accounts	All files in users' OneDrive accounts. More details		
<input type="radio"/> Off	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. More details		

Back

Next

Cancel

Microsoft Purview Data Lifecycle Management

The screenshot shows the Microsoft Purview Data Lifecycle Management interface. On the left, a vertical navigation pane lists steps: Name (checked), Administrative Units (checked), Type (checked), Locations, Retention settings, and Finish. The 'Type' step is currently selected. To the right, a list of locations is shown with toggle switches:

Location Type	Description	Action	Action
Skype for Business	Skype conversations for the users you choose.	Off	
Exchange public folders	Items from all Exchange public folders in your organization.	Off	
Teams channel messages	Messages from channel conversations and channel meetings. Doesn't apply to Teams private channel messages. More details	Off	
Teams chats	Messages from individual chats, group chats, meeting chats, bot chats. More details	Off	
Teams private channel messages	Messages from Teams private channels. More details	Off	
Yammer community messages	Messages from Yammer community discussions. More details	Off	
Yammer user messages	Private messages and community message notifications. More details	Off	
Microsoft Copilot experiences	Built-in and custom Copilot experiences. More details	On	All users Edit
Enterprise AI apps	Non-Copilot AI apps that are onboarded or connected to your org using methods like Entra registration and data connectors. More details	Off	
Other AI apps	AI Apps users interact with through a browser. These apps are categorized as "Generative AI" in the Defender for Cloud Apps catalog. More details	Off	

A red dashed box highlights the 'Locations' section, and a red arrow points from it to the 'Locations' step in the navigation pane. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Microsoft Purview Data Lifecycle Management

The screenshot shows the Microsoft Purview Data Lifecycle Management interface for creating a retention policy. The top navigation bar includes the Microsoft Purview logo, a search bar, and various icons for Copilot, notifications, and user profile.

The current step is "Decide if you want to retain content, delete it, or both".

On the left, a vertical progress bar shows the following steps:

- Name (checkmark)
- Administrative Units (checkmark)
- Type (checkmark)
- Retention settings** (blue circle, currently selected)
- Finish (radio button)

The main content area contains the following options:

Decide if you want to retain content, delete it, or both

Retain items for a specific period
Items will be retained for the period you choose.

Retain items forever
Items will be retained forever, even if users delete them.

Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Delete items older than

of years months days

Delete content based on

At the bottom of the page are buttons for Back, Next, and Cancel.

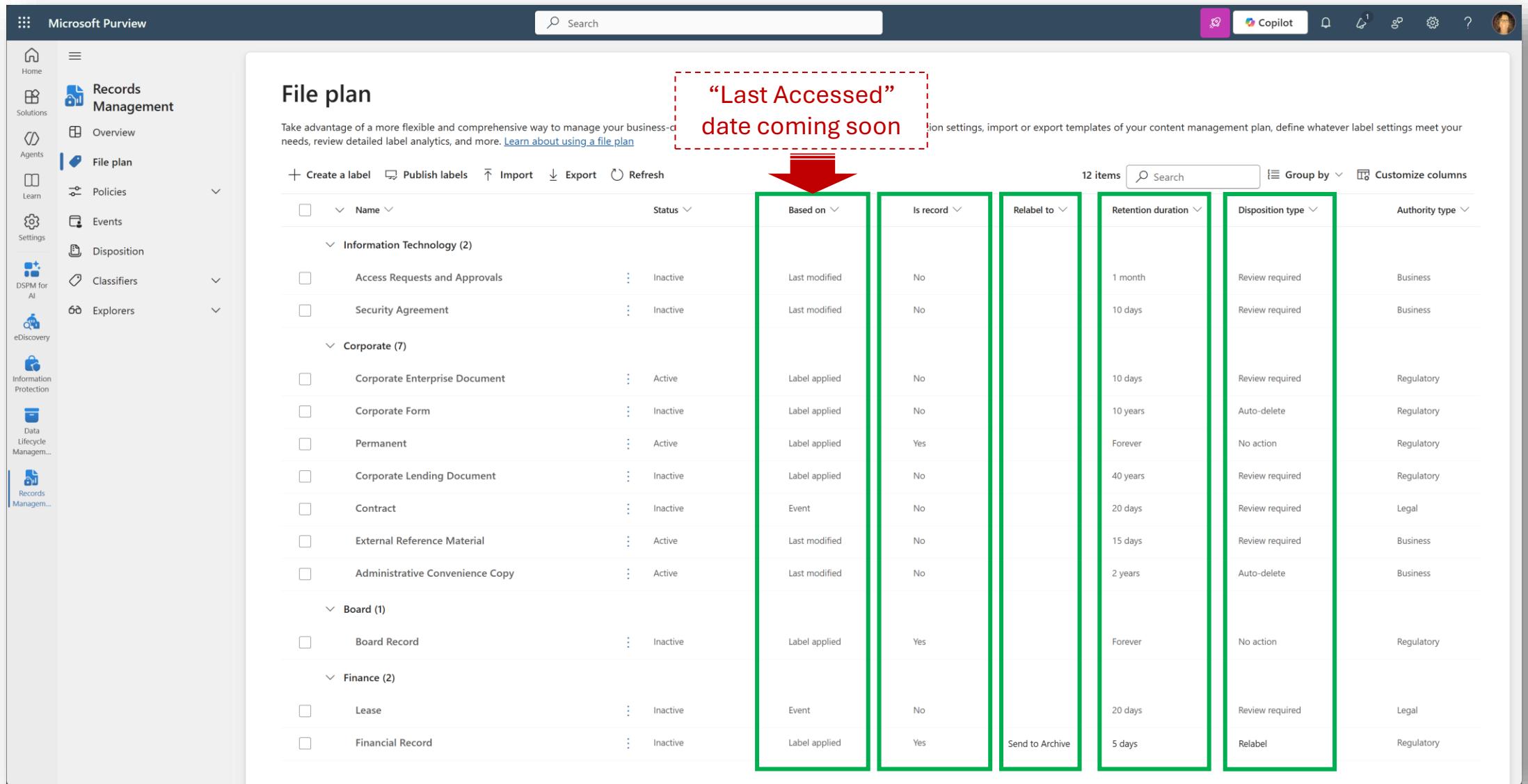
Records Management in Microsoft Purview

The screenshot shows the Microsoft Purview Risk & Compliance interface. On the left, there's a sidebar with a navigation menu for 'Records Management' which includes 'Overview', 'File plan', 'Policies', 'Events', 'Disposition', 'Classifiers', and 'Explorers'. The main area is titled 'Risk & Compliance' with the sub-section 'Manage critical risks and regulatory requirements.' Below this are four cards: 'Communication Compliance' (capture inappropriate messages), 'Compliance Manager' (get insight into compliance posture), 'eDiscovery' (identify, preserve, and export data in response to legal discovery requests), and 'Records Management' (automate and simplify retention schedules). The 'Records Management' card is highlighted with a red box. The bottom half of the screen shows an 'Overview' section with a chart titled 'Label application activity' showing the number of items over time (07/30 to 08/06) for 'Manually applied' (blue line) and 'Automatically applied' (pink line) labels. The chart shows a peak in manually applied labels around August 4th.

Records Management

- Implement retention labels in a file plan to identify business records (e.g., contracts, budgets, maintenance records, board meeting minutes)
- Labels provide regulatory-grade control such as immutability and defensible disposition
- Automatically apply labels based on location, metadata, or Purview classifiers

Microsoft Purview Records Management



The screenshot shows the Microsoft Purview Records Management interface. On the left, there's a navigation sidebar with various options like Home, Solutions, Agents, Learn, Settings, and several under the Records Management section. The main area is titled 'File plan' and contains a table of records. A red callout box with the text 'Last Accessed date coming soon' is positioned over the 'Based on' column header. A red arrow points from this callout to the 'Based on' column itself. The table has columns for Name, Status, Based on, Is record, Relabel to, Retention duration, Disposition type, and Authority type. The 'Based on' column values include 'Last modified', 'Label applied', 'Event', and 'Last modified'. The 'Is record' column values include 'No', 'No', 'Yes', 'No', 'Yes', 'Yes', 'No', 'Yes', and 'Send to Archive'. The 'Retention duration' column includes values like '1 month', '10 days', '10 years', 'Forever', '40 years', '20 days', '15 days', '2 years', 'Forever', '20 days', '5 days', and 'Relabel'. The 'Disposition type' and 'Authority type' columns show various compliance requirements.

Name	Status	Based on	Is record	Relabel to	Retention duration	Disposition type	Authority type
Access Requests and Approvals	Inactive	Last modified	No		1 month	Review required	Business
Security Agreement	Inactive	Last modified	No		10 days	Review required	Business
Corporate Enterprise Document	Active	Label applied	No		10 days	Review required	Regulatory
Corporate Form	Inactive	Label applied	No		10 years	Auto-delete	Regulatory
Permanent	Active	Label applied	Yes		Forever	No action	Regulatory
Corporate Lending Document	Inactive	Label applied	No		40 years	Review required	Regulatory
Contract	Inactive	Event	No		20 days	Review required	Legal
External Reference Material	Active	Last modified	No		15 days	Review required	Business
Administrative Convenience Copy	Active	Last modified	No		2 years	Auto-delete	Business
Board Record	Inactive	Label applied	Yes		Forever	No action	Regulatory
Lease	Inactive	Event	No		20 days	Review required	Legal
Financial Record	Inactive	Label applied	Yes	Send to Archive	5 days	Relabel	Regulatory

Microsoft Purview Records Management

Choose what happens during the retention period

These settings control what users can do to retained items.

During the retention period

Retain items even if users delete

Users will be able to edit items and change or remove the label. If they delete items location. [Learn more](#)

Mark items as a record

Users won't be able to edit or delete items, and only admins will be able to change or OneDrive files, actions are blocked or allowed based on whether the item's record. [more about records](#)

Unlock this record by default

Choose this option if you want to allow users to edit items before locking the record items across OneDrive accounts or SharePoint document libraries while the record is locked.

Choose what happens after the retention period

These settings determine what happens to items when the retention period ends.

Delete items automatically

We'll permanently remove labeled items from wherever they're stored.

Start a disposition review

Let the disposition reviewers you assign in the next step decide if items can be safely deleted or whether other actions (such as changing the retention period) should be taken. [Learn more](#)

Stage 1

Edit stages, reviewers, and settings

Change the label

You can extend the period by choosing an existing label to replace this one with. [Learn more about relabeling items](#)

Run a Power Automate flow

Customize what happens to labeled items with a Power Automate flow. You can run a flow to meet a specific business need, such as moving labeled items to a certain location or sending email notifications.

[Learn more about running a Power Automate flow](#)

Deactivate retention settings

Labeled items won't be retained or deleted when their retention settings are deactivated. You'll have to manually remove any items that you want deleted.

Microsoft Purview Records Management

DR DEMO Retention Site A Home Documents Pages LibraryA Site contents Edit

General ★ Following 🔍 Site access

+ New Upload Edit in grid view Add shortcut to OneDrive Create an agent Classify and extract Translate Pin to Quick access Export to Excel Automate Integrate Sync ... All Documents* Details

LibraryA

Name	Modified	Modified By	Retention label	Retention label Applied	Label applied by	Item is a Record	Sensitivity
Document for custom sit #1 - medium confidence.docx	August 15	Joanne Klein				No	General
Document for custom sit #2 - medium confidence.docx	August 15	Joanne Klein				No	General
Document for custom sit #3 - medium confidence.docx	August 15	Joanne Klein				No	General
Sample Notebook for Auto-apply to pages	Monday at 8:18 AM	Joanne Klein				No	General
Small # of CC numbers in doc.docx	August 15	Joanne Klein				No	General
Retention label: Financial Record (4)							
Financial docs	Yesterday at 9:50 AM	Joanne Klein	Financial Record	9/5/2025 6:14 AM	Joanne Klein	Yes	General
Finance Document 1.docx	Yesterday at 9:48 AM	Joanne Klein	Financial Record	9/5/2025 6:21 AM	Joanne Klein	Yes	Highly Confidential
Finance Document 2.docx	Yesterday at 9:49 AM	Joanne Klein	Financial Record	9/5/2025 6:21 AM	Joanne Klein	Yes	Highly Confidential
Finance Document 3.docx	Yesterday at 9:49 AM	Joanne Klein	Financial Record	9/5/2025 6:21 AM	Joanne Klein	Yes	Public
Retention label: Legal Matter TEST (4)							
Another HC Cno document for testing.docx	Sunday at 10:11 AM	Joanne Klein	Legal Matter TEST	9/3/2025 7:55 AM	System Account	No	General
Document for custom sit #1 - high confidence.docx	August 15	Joanne Klein	Legal Matter TEST	8/15/2025 4:42 PM	System Account	No	Confidential \ NexNovus Internal Only
Document for custom sit #2 - high confidence.docx	August 15	Joanne Klein	Legal Matter TEST	8/15/2025 4:42 PM	System Account	No	General
Document for custom sit #3 - high confidence.docx	August 15	Joanne Klein	Legal Matter TEST	8/15/2025 4:42 PM	System Account	No	Confidential \ NexNovus Internal Only
Retention label: Retain3Days (3)							
OCR document sample 3.jpg	A few seconds ago	Joanne Klein	Retain3Days	9/5/2025 6:30 AM	Joanne Klein	No	
OCR document sample 4.png	A few seconds ago	Joanne Klein	Retain3Days	9/5/2025 6:30 AM	Joanne Klein	No	
Sample Notebook for auto-deletion	Sunday at 4:25 PM	Joanne Klein	Retain3Days	9/1/2025 7:26 AM	Joanne Klein	No	
Retention label: Test Review Label (1)							
Sample Notebook for Retention Test	August 19	Joanne Klein	Test Review Label	8/31/2025 11:20 AM	Joanne Klein	No	

Microsoft Purview Records Management

DEMO Retention Site A

General ★ Following 🔍 Site access

+ New Edit grid view Delete Favorite Download Create an agent Classify and extract Move to Copy to Translate Automate ...

All Documents* 3 selected Details

LibraryA

Name Modified Modified By Retention label Retention label Applied Label applied by Item is a Record Sensitivity

Retention label: Unassigned (5)

- Document for custom sit #1 - medium confidence.docx August 15 Joanne Klein No General
- Document for custom sit #2 - medium confidence.docx August 15 Joanne Klein No General
- Document for custom sit #3 - medium confidence.docx August 15 Joanne Klein No General
- Sample Notebook for Auto-apply to pages Monday at 8:18 AM Joanne Klein No
- Small # of CC numbers in doc.docx August 15 Joanne Klein No General

Retention label: Financial Record (4)

- Financial docs Yesterday at 9:50 AM Joanne Klein Financial Record 9/5/2025 6:14 AM Joanne Klein Yes
- Finance Document 1.docx Yesterday at 9:48 AM Joanne Klein Financial Record 9/5/2025 6:21 AM Joanne Klein Yes Highly Confidential
- Finance Document 2.docx Yesterday at 9:49 AM Joanne Klein Financial Record 9/5/2025 6:21 AM Joanne Klein Yes Highly Confidential
- Finance Document 3.docx Yesterday at 9:49 AM Joanne Klein Financial Record 9/5/2025 6:21 AM Joanne Klein Yes Public

Retention label: Legal Matter TEST (4)

- Another HC Cno document for testing.docx Sunday at 10:11 AM Joanne Klein Legal Matter TEST 9/3/2025 7:55 AM System Account No General
- Document for custom sit #1 - high confidence.docx August 15 Joanne Klein Legal Matter TEST 8/15/2025 4:42 PM System Account No Confidential \ NexNovus Internal Only
- Document for custom sit #2 - high confidence.docx August 15 Joanne Klein Legal Matter TEST 8/15/2025 4:42 PM System Account No General
- Document for custom sit #3 - high confidence.docx August 15 Joanne Klein Legal Matter TEST 8/15/2025 4:42 PM System Account No Confidential \ NexNovus Internal Only

Retention label: Retain3Days (3)

- OCR document sample 3.jpg A few seconds ago Joanne Klein Retain3Days 9/5/2025 6:30 AM Joanne Klein No
- OCR document sample 4.png A few seconds ago Joanne Klein Retain3Days 9/5/2025 6:30 AM Joanne Klein No
- Sample Notebook for auto-deletion Sunday at 4:25 PM Joanne Klein Retain3Days 9/1/2025 7:26 AM Joanne Klein No

Retention label: Test Review Label (1)

- Sample Notebook for Retention Test August 19 Joanne Klein Test Review Label 8/31/2025 11:20 AM Joanne Klein No

Bulk edit properties

Image Tags Add tag

Field created by MediaTA

Apply label None

Save

None Clear the label

Contract Retain for 2 years

DEMO - Label Flow Trigger Retain for 2 days

Financial Info Retain for 2 years

Financial Record Retain for 7 years

Marketing Sample Label Retain for 5 days

Permanent Retain forever

Project Artifact Retain for 5 years

Record3Days Retain for 3 days

Retain3Days Retain for 3 days

Statement of Work Retain for 10 years

Test Review Label Retain for 2 days

Microsoft Purview Records Management

The screenshot shows the Microsoft Purview Records Management interface. On the left, there's a navigation sidebar with various options like Home, Solutions, Agents, Learn, Events, and Settings. Under the 'Records Management' section, 'Disposition' is highlighted with a green border. The main area is titled 'Legal Matter TEST' and shows a list of 'Pending dispositions'. There are two tabs: 'Pending dispositions' (which is selected) and 'Disposed items'. Below the tabs are filters for 'Source: SharePoint and OneDrive', 'Expiration date', 'Name', 'Location', 'Created by', and 'Label applied by'. The results table has columns for Name, Location, Author, Applied by, Applied date, Expiry date, and Stage Name. The table lists 60 items, including various documents and screenshots, all assigned to Joanne Klein or John Brown, with expiry dates ranging from Aug 15, 2025 to Jul 17, 2025.

Name	Location	Author	Applied by	Applied date	Expiry date	Stage Name
Document for custom sit #1 - high confidence.docx	https://.sharepoint.com/sites/DEMO...	Joanne Klein		Aug 15, 2025 4:42 PM	Aug 20, 2025 4:42 PM	Legal Team Reviewers
Document for custom sit #3 - high confidence.docx	https://.sharepoint.com/sites/DEMO...	Joanne Klein		Aug 15, 2025 4:42 PM	Aug 20, 2025 4:42 PM	Legal Team Reviewers
Document for custom sit #2 - high confidence.docx	https://.sharepoint.com/sites/DEMO...	Joanne Klein		Aug 15, 2025 4:42 PM	Aug 20, 2025 4:42 PM	Legal Team Reviewers
Balatro The Card Game V2.docx	https://-my.sharepoint.com/personal...	John Brown		Aug 8, 2025 4:58 PM	Aug 13, 2025 4:58 PM	Legal Team Reviewers
mc-template2.jpg	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Mastercard image 1.jpg	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
bus_gold_chip_338x211.png	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Mastercard sample.jpg	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
R.jpg	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Screenshot 2020-05-05 at 16.33.29.png	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Screenshot 2020-05-05 at 16.31.53.png	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Screenshot 2020-05-05 at 16.15.47.png	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Screenshot 2020-05-05 at 16.22.32.png	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers
Screenshot 2020-05-05 at 16.21.29.png	https://-my.sharepoint.com/personal...	John Brown		Jul 12, 2025 12:36 AM	Jul 17, 2025 12:36 AM	Legal Team Reviewers

Microsoft Purview Records Management

The screenshot shows the Microsoft Purview Records Management interface. On the left, the navigation menu includes Home, Solutions, Agents, Learn, Events, Disposition, Classifiers, Explorers, Data Lifecycle Management, Data Security Posture Management, Information Protection, and eDiscovery. The 'Records Management' section is selected. The main area displays a list titled 'Legal Matter TEST' under the 'Pending dispositions' tab. The list includes items such as 'Document for custom sit #1 - high confidence.docx', 'Document for custom sit #3 - high confidence.docx', 'Document for custom sit #2 - high confidence.docx', 'Balatro The Card Game V2.docx' (selected), 'mc-template2.jpg', 'Mastercard image 1.jpg', 'bus_gold_chip_338x211.png', 'Mastercard sample.jpg', 'R.jpg', 'Screenshot 2020-05-05 at 16.33.29.png', 'Screenshot 2020-05-05 at 16.31.53.png', 'Screenshot 2020-05-05 at 16.15.47.png', 'Screenshot 2020-05-05 at 16.22.32.png', and 'Screenshot 2020-05-05 at 16.21.29.png'. A detailed view of the 'Balatro The Card Game V2.docx' item is shown on the right, including its source (https://-my.sharepoint.com/personal/...), details (A Journey into Strategy and Chance), and history. Action buttons for Approve disposal, Relabel, Extend, and Add reviewers are available at the bottom.

Legal Matter TEST

Pending dispositions Disposed items

Filter Reset Filters

Source: SharePoint and OneDrive Expiration date: Any Name: Any Location: Any Created by: Any Label applied by: Any

Approve disposal Relabel Extend Add reviewers Refresh Export 1 of 60 selected Balatro The Card Game V2.docx

Name	Location
Document for custom sit #1 - high confidence.docx	https://-my.sharepoint.com/sites/DEMC...
Document for custom sit #3 - high confidence.docx	https://-my.sharepoint.com/sites/DEMC...
Document for custom sit #2 - high confidence.docx	https://-my.sharepoint.com/sites/DEMC...
<input checked="" type="checkbox"/> Balatro The Card Game V2.docx	https://-my.sharepoint.com/personal/...
mc-template2.jpg	https://-my.sharepoint.com/personal/...
Mastercard image 1.jpg	https://-my.sharepoint.com/personal/...
bus_gold_chip_338x211.png	https://-my.sharepoint.com/personal/...
Mastercard sample.jpg	https://-my.sharepoint.com/personal/...
R.jpg	https://-my.sharepoint.com/personal/...
Screenshot 2020-05-05 at 16.33.29.png	https://-my.sharepoint.com/personal/...
Screenshot 2020-05-05 at 16.31.53.png	https://-my.sharepoint.com/personal/...
Screenshot 2020-05-05 at 16.15.47.png	https://-my.sharepoint.com/personal/...
Screenshot 2020-05-05 at 16.22.32.png	https://-my.sharepoint.com/personal/...
Screenshot 2020-05-05 at 16.21.29.png	https://-my.sharepoint.com/personal/...

Balatro: The Card Game V2

A Journey into Strategy and Chance

Balatro, a captivating card game, seamlessly blends strategy and chance, inviting players into a world of tactical maneuvers and unpredictable outcomes. Originating from ancient traditions, Balatro has evolved into a modern favorite among card enthusiasts. The game is played with a standard deck of 52 cards and can be enjoyed by two to six players, each vying to outwit their opponents through a series of calculated decisions and clever plays. The objective is to accumulate the highest score by the end of a predetermined number of rounds, with each player attempting to leverage their hand to their best advantage.

What sets Balatro apart from other card games is its unique blend of luck and skill. Players must carefully consider their moves, balancing the cards they hold with the potential plays of their opponents. The game rewards foresight, adaptability, and a keen understanding of probability, making each session a dynamic and engaging experience. Whether you're a seasoned card player or a newcomer to the world of Balatro, the game offers endless opportunities for strategic depth and thrilling competition. As a testament to its enduring appeal, Balatro continues to captivate players, drawing them into its intricate dance of chance and strategy.

Approve disposal Relabel Extend Add reviewers

Data Protection and Data Retention

How Does AI Affect Each of these?



AI and Data Protection ... why it matters



Reason #1: Protect Sensitive Data from Unauthorized Access

Data Protection controls can prevent unauthorized users from accessing, rapidly replicating, and oversharing sensitive data using AI, whether maliciously or inadvertently.

- Classify, label, and protect sensitive data
E.g., “Prevent Microsoft 365 Copilot from accessing data labeled **Restricted**.”
- Implement policies to audit and block data loss
E.g., “Block pasting of sensitive information into third-party AI applications.”

SENSITIVITY Due to content created by Copilot, your organization automatically applied the sensitivity label: Internal Only

Actions

Use actions to protect content when the conditions are met.

Prevent Copilot from processing content

Content that matches your conditions won't be used by Copilot to generate responses. This action is supported for specific content that's processed across various Copilot experiences. [Learn more about this action](#)

DSPM for AI - Block sensitive info from AI sites

Uses Adaptive Protection to give a warn-with-override to elevated risk users attempting to paste or upload sensitive information to other AI assistants in Edge, Chrome, and Firefox. This policy covers all users and groups in your org in test mode.

Policy details

Status: Testing

Admin units: None

Locations: Devices All accounts

Policy settings: Block with override for elevated risk users



AI and Data Protection ... why it matters



Reason #2: Monitor and Audit AI interactions to proactively identify data security risks

Monitoring and auditing AI interactions will help security administrators to proactively identify data protection policy gaps and remediate data security risks before a breach or leak takes place.

- Identify, investigate, and remediate risky AI interactions

E.g., Identify a departing user entering prompts containing sensitive information in Copilot.

- Scan the environment for risks of data oversharing

E.g., Leverage DSPM for AI data risk assessments, SharePoint Advanced Management data governance access reports, SharePoint site permissions and sharing report, or Microsoft Graph Data Connect for SharePoint.

Potential risky AI usage (preview)

10% of users were involved in potentially risky AI usage

Activity from 500 users scanned

Recommendation: Set up a 'Risky AI usage' policy

Detects and alerts you of potentially risky or sensitive content in Microsoft Copilot experiences and web versions of other generative AI apps.

[View details](#)

4% of users received sensitive responses from Copilot
3% of users entered risky prompts in Copilot

Default assessment

Assess oversharing of sensitive data for the top 100 SharePoint sites based on how many times the sites are accessed. Results are derived from data collected over the last 30 days.

Results

Total items
222

Sensitive data detected
55

Links sharing data with anyone
0

Last updated
Aug 1, 2025

Next update
Aug 8, 2025

Frequency
Weekly

[View details](#)

AI and Retention... why it matters



Reason #1: AI Prompts and Responses can be a compliance and discovery risk

You may want to apply retention controls for compliance or risk reasons and to remain compliant with AI regulations. If they exist, they're discoverable!

E.g., “Automatically **delete** Copilot prompts and responses after 7 days with a **retention policy**”

Choose where to apply this policy

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

ⓘ You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Set up now](#)

⚠ Turn on pay-as-you-go to create new AI-related policies: Pay-as-you-go billing is currently turned off for this solution. To create new policies that include Copilot experiences, Enterprise AI apps, and other AI app locations, which are billed under the pay-as-you-go model, turn on pay-as-you-go billing.

Status	Location	Applicable Content	Included	Excluded
On	Microsoft Copilot experiences	Built-in and custom Copilot experiences. More details	All users Edit	None Edit
Off	Enterprise AI apps	Non-Copilot AI apps that are onboarded or connected to your org using methods like Entra registration and data connectors. More details		
Off	Other AI apps	AI Apps users interact with through a browser. These apps are categorized as "Generative AI" in the Defender for Cloud Apps catalog. More details		

Decide if you want to retain content, delete it, or both

Retain items for a specific period
Items will be retained for the period you choose.

Retain items forever
Items will be retained forever, even if users delete them.

Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Delete items older than

of years months days

Custom

Delete content based on

When items were created

AI and Retention... why it matters



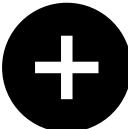
Reason #2: Retention and Deletion controls can improve Data Quality

Retention controls can improve the quality of your data, so AI tools have better information to work with.

Combining these 2 retention controls can help with this:

- **Retention policies**

- Deleting ROT (Redundant, Obsolete, Trivial) content across your Microsoft 365 digital landscape with **retention policies**
- Purview's Data Security Posture Management for AI (DSPM for AI) solution will suggest you create a retention policy for this very reason



- **Retention labels**

- Ensuring you are retaining your records of legal, historical and business value with **retention labels** ... “Keep the gold, delete the rest”

Data Security Posture Management for AI (DSPM for AI)

DSPM for AI

- Overview
- Recommendations**
- Reports
- Apps and agents Preview
- Policies
- Activity explorer
- Data risk assessments

Recommendations

Not Started | 12 Dismissed | 0 Completed | 2

Refresh

Recommendation	Type
Not Started (12)	
Fortify your data security	Data security
Detect unethical behavior in AI apps	Insight into communications
Guided assistance to AI regulations	AI regulations
Protect sensitive data referenced in Copilot and agent responses	Data security
Discover and govern interactions with ChatGPT Enterprise AI (preview)	Data discovery
Protect items with sensitivity labels from Microsoft 365 Copilot and agent pro...	Data security
Protect your data from potential oversharing risks	Data security
Use Copilot and agents to improve your data security posture	Data security
Secure interactions in Microsoft Copilot experiences	Data security
Secure interactions from enterprise AI apps	Data security
Extend insights into sensitive data in AI app interactions	Data security
Secure data in Azure AI apps and agents	Data security
Completed (2)	

DSPM for AI

- Overview
- Recommendations
- Reports
- Apps and agents** Preview
- Policies
- Activity explorer
- Data risk assessments

Apps and agents (preview)

Understand the depth and breadth of Microsoft Purview protection for AI applications and agents in the last 30 days.

Apps Agents

Refresh Export 5 items Search Group list

AI app	Protection status	User trend	Prompts trend	Response trend	Data protect
Microsoft Copilot Studio (1)	Monitored	No data available	No data available	No data available	0 Policies
Copilot experiences & agents (3)	Monitored	No data available	No data available	No data available	0 Policies
Microsoft 365 Copilot	Monitored	No data available	No data available	No data available	0 Policies
Copilot in Fabric	Monitored	No data available	No data available	No data available	0 Policies
Security Copilot	Monitored	No data available	No data available	No data available	0 Policies

DSPM for AI

- Overview
- Recommendations
- Reports
- Apps and agents Preview
- Policies
- Activity explorer
- Data risk assessments

Data risk assessments

Assess and prevent oversharing

① Identify
Review assessment results for users accessing sensitive items. You can review the weekly results from the default assessment or create custom assessments to review specific data sources and users.

② Protect
Limit Microsoft Copilot and agents access to sensitive data and apply label and retention policies to SharePoint sites and data.

Default assessment

Assess oversharing of sensitive data for the top 100 SharePoint sites based on how many times the sites are accessed. Results are derived from data collected over the last 30 days.

Results

Total items	223	Sensitive data detected	56	Links sharing data with anyone	10
-------------	-----	-------------------------	----	--------------------------------	----

Last updated Sep 12, 2025 Next update Sep 19, 2025 Frequency Weekly

Data Protection and Data Retention

Practical Lessons We've Learned with Customers



Practical Lessons We've Learned About Data Protection

1. Make it easy for your users to label content

- Minimize the number of sensitivity labels available for users to select
- Follow a clear naming convention that aligns with the sensitivity of the data
- Couple end-user facing changes with strong change management efforts

2. Follow a phased rollout approach, especially with blocking policies

- Do not block actions until a detailed understanding of business case exceptions is gained
- Allow for users to request required business case exceptions

3. Ensure alert volume remains manageable

- A higher volume of alerts does not mean a more effective data protection program
- Fine tune policies and automate alert response where possible to support analysts in focusing on high priority alerts

Practical Lessons We've Learned About Data Retention

1. Keep your Purview file plan as simple as your regulation will allow
 - Everything in your retention schedule doesn't need to become a Purview retention label!!
 - There are both technical and practical limits to the number of retention labels – be careful here
2. Have a well-governed SharePoint/Teams setup to reduce complexity
 - Good governance around provisioning, site ownership, content organization will make this easier as it gives Purview something to “automate against”
 - Most retention projects **also** end up being a “SharePoint cleanup” project because of this!
3. Perfection is the enemy of good (enough)
 - The (messy) reality of the Microsoft 365 collaborative environment is often at odds with records managers' expectations. Have mitigating controls in place (DLP, Audit, Adaptive protection) to alert/prevent premature deletion of data in case you don't have the right retention controls in place.
 - Defaulting retention labels as much as possible removes the burden on the end-user to apply a label or set a piece of metadata to trigger retention (**the new SharePoint Knowledge Agent** can help with automatic extraction and generation of metadata... and then apply a retention label based on it)

Data Protection and Data Retention

Common Questions we hear from Customers



Common questions we hear from customers

1. Is it best to do data protection or data retention first?
2. Can you do them at the same time?
3. What are the most challenging parts of each?

Closing Thoughts and Q&A

Thank you for joining us today!



Joanne C Klein

NexNovus M365 Consultant

joannecklein.com

<https://www.linkedin.com/in/joannecklein/>



Anna Bordioug

Protiviti M365 Consultant

www.annabordioug.com

<https://www.linkedin.com/in/anna-bordioug/>

Data Protection and Data Retention

Sensitivity Labels vs Retention Labels

Labels, Policies, and Label Policies



Data Protection

Sensitivity Labels

- Label files, emails, meetings, groups, and sites according to sensitivity.
- Enforce granular protection controls.
- Automatically label data in use.

Label Publishing Policies

- Publish sensitivity labels to users and groups.
- Require labeling, justification, and specify default label.

Auto-Labeling Policies

- Automatically label data at rest and data in transit based on the content of the item.



Data Retention

Retention Labels

- Apply retention controls to **files and emails**.
- Manage item-level retention, deletion, and disposition actions.

Retention Policies

- Apply retention controls to **containers**.
- Manage retention and deletion automatically.

Retention Label Policies

- Publish retention labels OR auto-apply a retention label to locations across Microsoft 365 (e.g., SharePoint, OneDrive, Exchange).

Contrast and Comparison of Label Behaviours (1 thru 10)

PURVIEW LABEL TYPE COMPARISON			
FUNCTIONALITY		SENSITIVITY LABEL ¹ <small>Purpose: applies data handling and protection controls</small>	RETENTION LABEL <small>Purpose: enforces retention and disposition controls to meet regulatory/legal/business requirements</small>
1	TYPICAL VOLUME OF LABELS	Sensitivity labels are created based on your data classification schema and are typically under ~10.	Retention labels are created from your retention schedule and can number in the tens and hundreds.
2	CAN CHANGE THE LABEL NAME	Yes. The display name can be changed after creation.	No
3	CAN HAVE MULTILINGUAL LABEL NAMES	Yes. Requires PowerShell.	No
4	CAN MANUALLY APPLY THE LABEL	Yes (only 1 file at a time)	Yes (1 at a time and bulk)
5	CAN DEFAULT A LABEL FOR A USER	Yes (Different defaults can be set for files, emails, meetings, fabric, power bi)	No
6	CAN DEFAULT A LABEL ON A DOCUMENT LIBRARY	Yes (Applies only to new/edited office files and pdfs based on label priority) ** <i>change 485732 coming soon</i>	Yes (Applies to all unlabeled items regardless of filetype . Can apply to either all items or only new/edited based on a setting)
7	CAN DEFAULT A LABEL ON A SPECIFIC FOLDER	No	Yes
8	CAN RECOMMEND A LABEL TO A USER	Yes	No
9	CAN AUTO-APPLY A LABEL ON CLIENT-SIDE	Yes	No
10	CAN AUTO-APPLY A LABEL ON SERVICE-SIDE	Yes (via auto-labeling policy; does NOT apply to Exchange)	Yes (via auto-apply label policy)

Contrast and Comparison of Label Behaviours (11 thru 20)

PURVIEW LABEL TYPE COMPARISON			
FUNCTIONALITY		SENSITIVITY LABEL ¹ <small>Purpose: applies data handling and protection controls</small>	RETENTION LABEL <small>Purpose: enforces retention and disposition controls to meet regulatory/legal/business requirements</small>
11	CAN MAKE THE LABEL MANDATORY	Yes	No
12	CAN REQUIRE JUSTIFICATION TO CHANGE THE LABEL	Yes	No
13	CAN AUTOMATICALLY OVERWRITE A LABEL THAT'S ALREADY APPLIED	Yes <small>(There are rules based on taxonomy priority)</small>	No with 1 exception <small>(Only by changing 1 default label to another default label)</small>
14	CAN ASSIGN A LABEL PRIORITY	Yes <small>(Priority defined in label taxonomy; manual always wins)</small>	No <small>(First label to be applied to an item wins; manual always wins)</small>
15	LABEL REMAINS WITH CONTENT EVEN OUTSIDE OF TENANT	Yes	No
16	CAN SUPPORT A LABEL HIERARCHY END-USERS SEE	Yes (label groups and sublabels)	No
17	CAN DELETE A LABELED ITEM	Yes (assuming you have the usage rights in the label)	Yes (depends on label type (standard/record), user permission and tenant setting to allow for deletion)
18	WHERE LABELS CAN BE PUBLISHED TO	Users, groups (distribution groups, mail-enabled security groups, Microsoft 365 groups)	Locations <small>(exchange mailboxes, SharePoint sites, OneDrive accounts, Microsoft 365 group mailboxes and sites)</small>
19	COPilot INTEGRATION	Encrypting label without the EXTRACT and VIEW usage rights will prevent Copilot from summarizing the data.	Copilot interactions cannot be individually targeted for retention/deletion with a retention label – a retention policy is needed. Use labels to keep your records of value for Copilot to use.
20	CAN LEVERAGE ADMINISTRATIVE UNITS	YES	YES