Records Management in Microsoft 365

Use the following guide to learn more about the latest records management solution and how to configure these solution elements for your organization. Getting started is easy, and this guide will help you prioritize your first steps in meeting internal policy, reducing risk, and ultimately increase efficiency using Microsoft 365.

Prepared by:
Microsoft 365 Security & Compliance team

Records management in Microsoft 365: Overview

Organizations of all types require a records-management solution to manage regulatory, legal, and business-critical records across their corporate data. Records management in Microsoft 365 helps an organization manage their legal obligations, provides the ability to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be retained, no longer of value, or no longer required for business purposes.

The records-management solution supports the following elements:

- **Label content as a record**. Publish record labels to be applied by end users or auto-apply record labels to items containing specific sensitive information, keywords, or content types.
- **Migrate and manage your retention plan with file plan** and use file plan manager to bring in your existing retention plan, or build new with file descriptors and expanding hierarchies.
- **Establish retention and deletion policies within the record label**. Define retention and disposition periods based on various factors including the date last modified or created.
- **Trigger** event-based retention.
- **Review and validate** disposition.
- **Review disposed items with disposition review** and export a disposition report for further validation and reporting.
- **Set specific permissions** for records manager functions in your organization to have the right access.

At a high level, declaring content as a record means that:

- The item becomes immutable (a record can't be modified or deleted).
- Additional activities about the item are logged.
- Records are disposed of after their stated retention period is past.

Keep the following things in mind about records:

- **Records are immutable.** A retention label that declares content as a record can be applied to content in Exchange, in addition to SharePoint and OneDrive for Business.
- **Records and folders.** You can apply a retention label to a folder in Exchange, SharePoint, and OneDrive.
- **Records can't be deleted**. If a user attempts to delete a record in Exchange, the item is moved to the Recoverable Items folder as described in How a retention policy works with content in place.

- **Records labels can't be removed.** Once a record label has been applied to an item, only the admin of that location (for example, a site collection admin of a SharePoint site) can remove that record label.

Using retention labels to declare records
When you create a retention label, you have the option to use the retention label to classify the content as a record.

***NOTE**: Using a retention label that declares content as a record requires an Office 365 Enterprise E5 license for each user who has permissions to edit the content. Users who simply have read-only access don't require an E5 license.*

Record versioning
An essential part of records management is the ability to declare a document as a record and have that record be immutable. At the same time, record immutability prevents collaboration on the document if people need to create subsequent versions. To use record versioning, the first step is to use the Microsoft 365 compliance center to create and publish retention labels that declare records to all SharePoint sites and/or OneDrive accounts, or publish them to specific SharePoint sites and/or OneDrive accounts.

***NOTE**: Record versioning requires an Office 365 Enterprise E5 license for each user who has permissions to edit content that's been declared as a record in a SharePoint site or OneDrive account. Users who have read-only access don't require a license.*

Record versions
Each time a user unlocks a record, the latest version is copied to the Records folder in the Preservation Hold library, and that version contains the value of **Record** in the **Comments** field of the version history.

Where records are stored
Records are stored in the Records folder in the Preservation Hold library in the top-level site in the site collection. The Preservation Hold library is visible only to site collection admins.

Searching the audit log for record versioning events
The actions of locking and unlocking records are logged in the Office 365 audit log.

For more information about searching for these events, see the "File and page activities" section in Search the audit log in the Security & Compliance Center.

File Plan

Overview of file plan manager

File plan manager provides advanced management capabilities for retention labels, retention label policies, and provides an integrated way to traverse label and label-to-content activity for your entire content lifecycle – from creation, through collaboration, record declaration, retention, and finally disposition.

- From file plan manager, you can bulk import new retention labels, modify existing retention labels, and export the details of all retention labels into a .csv file to assist you in facilitating periodic compliance reviews with data governance stakeholders in your organization.

Accessing file plan manager
There are two requirements to access file plan manager:

- An Office 365 Enterprise E5 subscription.
- The user has been in assigned one of the following roles in the security and compliance center: Retention Manager or View-only Retention Manager.

Navigating your file plan
File plan manager makes it easier see into and across the settings of all your retention labels and policies from one view. Note that retention labels created outside of the file plan will be available in the file plan and vice versa.

Label settings columns

- **Based on** identifies the type of trigger that will start the retention period.
- **Record** identifies if the item will become a declared record when the label is applied.
- **Retention** identifies the retention type.
- **Disposition** identifies what will happen to the content at the end of the retention period.

Retention label file plan descriptors columns
You can now include more information in the configuration of your retention labels. Inserting file plan descriptors into retention labels will improve the manageability and organization of your file plan.

Retention labels: overview, policies, and use

Overview

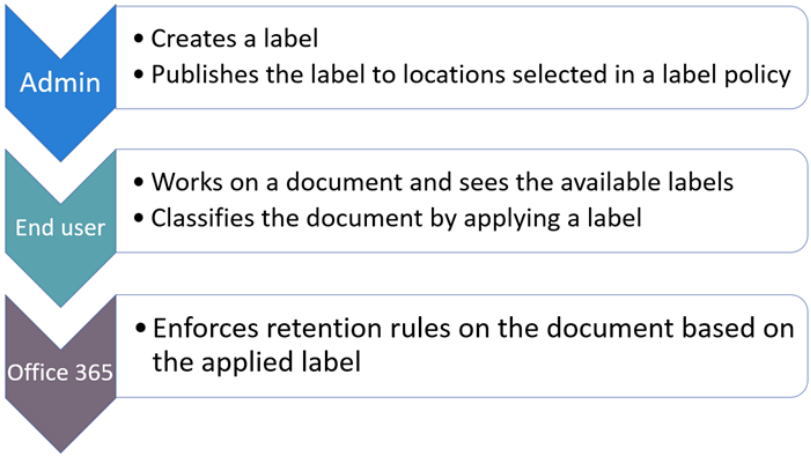
Across your organization, you probably have different types of content that require different actions taken on them in order to comply with industry regulations and internal policies. With retention labels, you can classify data across your organization for governance, and enforce retention rules based on that classification.

With retention labels, you can:

- Enable people in your organization to apply a retention label manually
- Apply retention labels to content automatically
- Implement records management across Office 365
- Apply a default retention label to a document library, folder, or document set

Policies

Making retention labels available to people in your organization so that they can classify content is a two-step process: first you create the retention labels, and then you publish them to the locations you choose. When you publish retention labels, a retention label policy gets created.



The primary purpose of a retention label policy is to group a set of retention labels and specify the locations where you want those labels to appear.

1. When you publish retention labels, they're included in a retention label policy.
2. A single retention label can be included in many retention label policies.
3. A single location can also be included in many retention label policies.
4. Retention label policies specify the locations to publish the retention labels.

Only one retention label at a time

- Content like an email or document can have only a single retention label assigned to it at a time.
    - For retention labels assigned manually by end users, people can remove or change the retention label that's assigned.
    - If content has an auto-apply label assigned, an auto-apply label can be replaced by a retention label assigned manually by an end user.
    - If content has a retention label assigned manually by an end user, an auto-apply label cannot replace the manually assigned retention label.
    - If there are multiple rules that assign an auto-apply label and content meets the conditions of multiple rules, the retention label for the oldest rule is assigned.

How long it takes for retention labels to take effect

- When you publish or auto-apply retention labels, they don't take effect immediately:
    1. First the label policy needs to be synced from the admin center to the locations in the policy.
    2. Then the location may require time to make published retention labels available to end users or time to auto-apply labels to content. How long this takes depends on the location and type of retention label.

Retention label policies and locations

- Different types of retention labels can be published to different locations, depending on what the retention label does:

If the retention label is...	**Then the label policy can be applied to...**
Published to end users	Exchange, SharePoint, OneDrive, Office 365 groups
Auto-applied based on sensitive information types	Exchange (all mailboxes only), SharePoint, OneDrive
Auto-applied based on a query	Exchange, SharePoint, OneDrive, Office 365 groups

How retention labels enforce retention

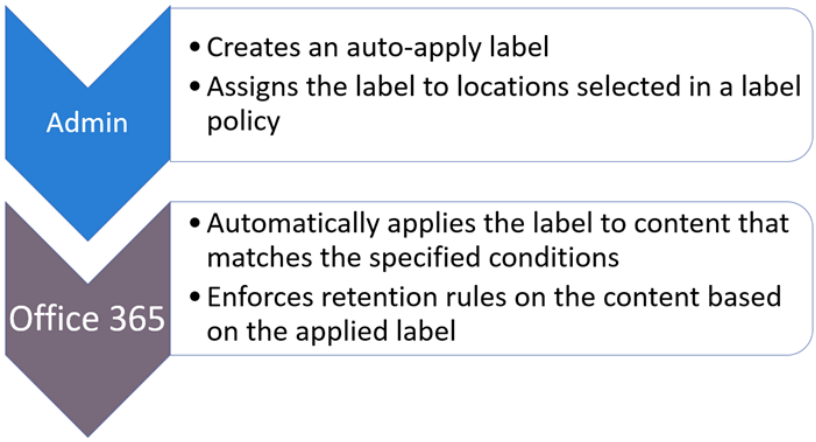
- Retention labels can enforce the same retention actions that a retention policy can. You can use retention labels to implement a sophisticated content plan (or file plan).
- In addition, a retention label has two retention options that are available only in a retention label and not in a retention policy. With a retention label, you can:
    - Trigger a disposition review at the end of the retention period, so that SharePoint and OneDrive documents must be reviewed before they can be deleted
    - Start the retention period from when the content was labeled, instead of the age of the content or when it was last modified

Where published retention labels can appear to end users

- If your retention label will be assigned to content by end users, you can publish it to: Outlook on the web, Outlook 2010 and later, OneDrive, SharePoint, and Office 365 groups.
- View more details on labeling in each app here.

Applying a retention label automatically based on conditions

- One of the most powerful features of retention labels is the ability to apply them automatically to content that matches certain conditions. In this case, people in your organization don't need to apply the retention labels. Office 365 does the work for them:



- Auto-apply retention labels are powerful because:
    - You don't need to train your users on all of your classifications.
    - You don't need to rely on users to classify all content correctly.
    - Users no longer need to know about data governance policies - they can focus on their work.

- You can choose to apply retention labels to content automatically when that content contains:
    - Specific types of sensitive information.
    - Specific keywords that match a query you create.

Applying a default retention label to all content in a SharePoint library, folder, or document set

- In addition to enabling people to apply a retention label to individual documents, you can also apply a default retention label to a SharePoint library, folder, or document set, so that all documents in that location get the default retention label.
- If you apply a default retention label to existing items in the library, folder, or document set:
    - All items in the library, folder, or document set automatically get the same retention label, **except** for items that have had a retention label applied explicitly to them. Explicitly labeled items keep their existing label.
- If you change or remove the default retention label for a library, folder, or document set, the retention labels also changed or removed for all items in the library, folder, or document set, **except** items with explicit retention labels.
- If you move an item with a default retention label from one library, folder, or document set to another library, folder, or document set, the item keeps its existing default retention label, even if the new location has a different default retention label.

Applying a retention label to email by using rules

- In Outlook 2010 or later, you can create rules to apply a retention label or retention policy. For example, you can create a rule that applies a specific retention label to all messages sent to or from a specific distribution group.

Classifying content without applying any actions

- When you create a retention label, you can do so without turning on any retention or other actions, as shown below. In this case, you can use a retention label simply as a text label, without enforcing any actions.
- For example, you can create a retention label named "Review later" with no actions, and then auto-apply that retention label to content with sensitive information types or queried content.

Monitor retention labels

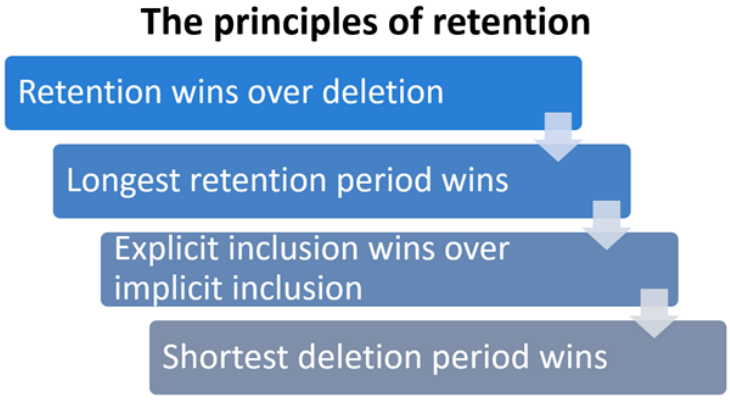
- After you publish or auto-apply your retention labels, you'll want to verify that they're being applied to content as you intended. To monitor your retention labels, you can use the:
    - Label Activity Explorer
    - Label analytics page
    - Data governance reports

Using Content Search to find all content with a specific retention label applied to it

- After retention labels are assigned to content, either by users or auto-applied, you can use content search to find all content that's classified with a specific retention label.
- For more information, see Keyword queries and search conditions for Content Search.

The principles of retention, or what takes precedence?

- It's possible or even likely that content might have several retention policies applied to it, each with a different action (retain, delete, or both) and retention period. What takes precedence? At the highest level, rest assured that content being retained by one policy can't be permanently deleted by another policy.



- The principles of retention work as a tie-breaking flow from top to bottom: If the rules applied by all policies or labels are the same at one level, the flow moves down to the next level to determine precedence for which rule is applied.

Use retention labels instead of these features

- Retention labels can easily be made available to an entire organization and its content across Office 365, including Exchange, SharePoint, OneDrive, and Office 365 groups. If you need to classify content or manage records anywhere in Office 365, we recommend that you use retention labels.

- There are several other features that have previously been used to classify content or manage records in Office 365:
    - Exchange Online
        - Retention tags and retention policies, also known as messaging records management (MRM) (Deletion only)
    - SharePoint Online and OneDrive for Business
        - Configuring in place records management (Retention)
        - Introduction to the Records Center (Retention)
        - Information management policies (Deletion only)

Permissions

- Members of your compliance team who will create retention labels need permissions to the Security & Compliance Center. By default, your tenant admin has access to this location and can give compliance officers and other people access to the Security & Compliance Center, without giving them all of the permissions of a tenant admin.
- These permissions are required only to create and apply retention labels and a label policy. Policy enforcement does not require access to the content.
- For more information, see Give users access to the Office 365 Security & Compliance Center.

Bulk create and publish retention labels by using PowerShell

In Office 365, you can use retention labels to implement a retention schedule for your organization. As a record manager or compliance officer, you might have hundreds of retention labels to create and publish. You can do this through the UI in the Security & Compliance Center, but creating retention labels one at a time is time-consuming and inefficient.

By using the script and .csv files provided here, you can bulk create retention labels and publish retention label policies. For more information about retention labels, see Overview of labels.

View label usage with label analytics

After you create your retention labels and sensitivity labels, you'll want to see how they're being used across your tenant. With label analytics in the Microsoft 365 compliance center and Microsoft 365 security center, you can quickly see which labels are used the most and where they're being applied.

For example, with label analytics, you can view the:

- Total number of retention labels and sensitivity labels applied to content.
- Top labels and the count of how many times each label was applied.
- Locations where labels are applied and the count for each location.
- Count for how many files and folders had their retention label changed or removed.

Sensitivity label usage

The data on sensitivity label usage is pulled from the reports for Azure Information Protection – for more information, see Central reporting for Azure Information Protection.

For sensitivity label usage:

- There is no latency in the data. This is a real-time report.
- To see the count for each top label, point to the bar graph and read the tool tip that appears.
- The report shows where sensitivity labels are applied per app (whereas retention labels are shown per location).

Retention label usage

This report shows a quick view of what the top labels are and where they're applied. For more detailed information on how content in SharePoint and OneDrive is labeled, see View label activity for documents.

For retention label usage:

- Data is aggregated weekly.
- To see the count for each top label, point to the bar graph and read the tool tip that appears.
- The report shows where retention labels are applied per location (whereas sensitivity labels are shown per app).
- For retention labels, this is a summary of the all-time data in your tenant; it's not filtered to a specific date range. By contrast, the Label Activity Explorer shows data from only the past 30 days.

Permissions

To view label analytics, you must be assigned one of the following roles in Azure Active Directory: global administrator, compliance administrator, security administrator, or security reader.

View label activity for documents

After you create your labels, you'll want to verify that they're being applied to content as you intended. With the Label Activity Explorer in the Office 365 Security & Compliance Center, you can quickly search and view label activity for all content across SharePoint and OneDrive for Business over the past 30 days. This is real-time data that gives you a clear view into what's happening in your tenant.

For example, with the Label Activity Explorer, you can:

- View how many times each label was applied on each day (up to 30 days).
- See who labeled exactly which file on which date, along with a link to the site where that file resides.
- View which files had labels changed or removed, what the old and new labels are, and who made the change.
- Filter the data to see all the label activity for a specific label, file, or user. You can also filter label activity by location (SharePoint or OneDrive for Business) and whether the label was applied manually or auto-applied.
- View label activity for folders as well as individual documents. Coming soon is the ability to show how many files inside that folder got labeled as a result of the folder getting labeled.

View the data governance reports

After you create your labels, you'll want to verify that they're being applied to content as you intended. With the data governance reports in the Office 365 Security & Compliance Center, you can quickly view:

- **Top 5 labels**
- **Manual vs Auto apply**
- **Records tagging**
- **Labels trend over the past 90 days**

All these reports show labeled content from Exchange, SharePoint, and OneDrive for Business.

Events

Overview of event-driven retention

When you retain content, the retention period is often based on the age of the content - for example, you might retain documents for seven years after they're created and then delete them. But with retention labels in Office 365, you can also base a retention period on when a specific type of event occurs. The event triggers the start of the retention period, and all content with a retention label applied for that type of event get the label's retention actions enforced on them.

For example, you can use labels with event-driven retention for:

- **Employees leaving the organization**
- **Contract expiration**
- **Product lifetime**

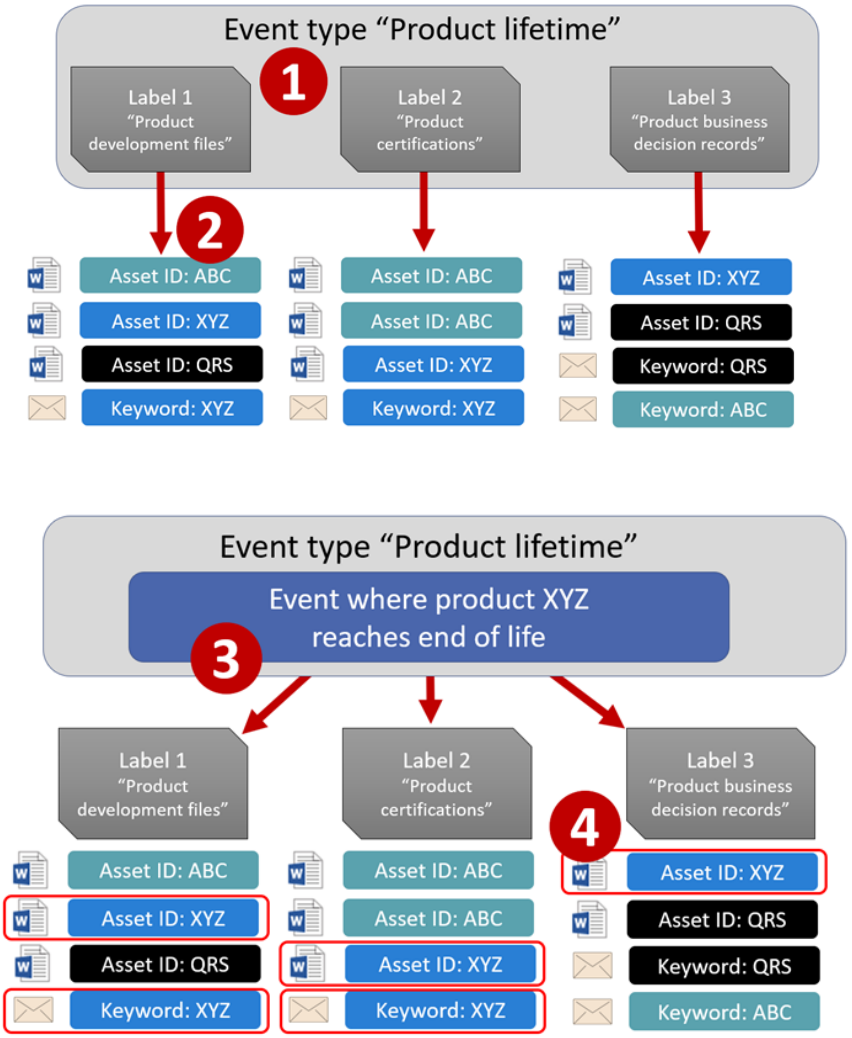
Event-driven retention is typically used as part of a records-management process. This means that:

- Labels based on events also usually classify content as a record. For more information, see Using Content Search to find all content with a specific retention label applied to it.
- A document that's been declared as a record but whose event trigger has not yet happened is retained indefinitely (records can't be permanently deleted), until an event triggers that document's retention period.
- Labels based on events usually trigger a disposition review at the end of the retention period, so that a records manager can manually review and dispose the content. For more information, see Overview of disposition reviews.

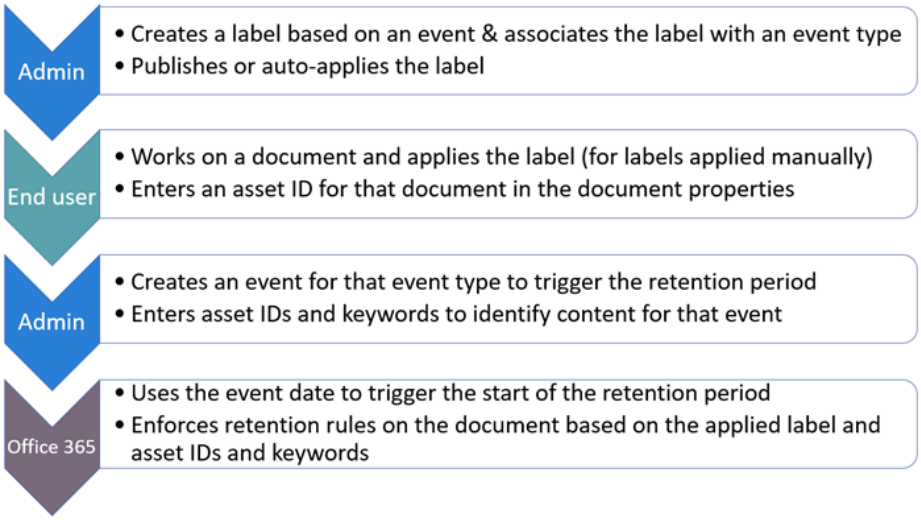
A label based on an event has the same capabilities as any label in Office 365. To learn more, see Overview of labels.

Understanding the relationship between event types, labels, events, and asset IDs

To successfully use event-driven retention, it's important to understand the relationship between event types, labels, events, and asset IDs as illustrated in the following diagram:



Below is the high-level workflow for event-driven retention:



***TIP**: See Manage the lifecycle of SharePoint documents with retention labels for a detailed scenario about using managed properties in SharePoint to auto-apply retention labels and implement event-driven retention.*

Use Content Search to find all content with a specific label or asset ID
After labels are assigned to content, you can use content search to find all content that's classified with a specific label or that contains a specific asset ID. For more information, see Keyword queries and search conditions for Content Search.

Permissions
To get access to the **Events** page, reviewers must be members of a role group with the **Disposition Management** role and the **View-Only Audit Logs** role. We recommend creating a new role group called Disposition Reviewers, adding these two roles to that role group, and then adding members to the role group.

For more information, see Give users access to the Office 365 Security & Compliance Center.

Automate events by using PowerShell
In the admin center, you can only create events manually; it's not possible to automatically trigger an event when it occurs. However, you can use a Rest API to trigger events automatically; for more information, see Automate event-based retention.

Automate event-based retention

The explosion of content in organizations and how it can become ROT (redundant, obsolete, trivial) is serious business. To continue to meet legal, business, and regulatory compliance challenges, businesses must be able to keep and protect important information and quickly find what's relevant. Retaining only important, pertinent information is key to a business's success.

Retention can be triggered by using retention labels. A retention label has the option to base the retention period on a specific event. In order to ensure compliant disposal of content, it is imperative to know when an event takes place. With the volume of content increasing rapidly, it is becoming challenging to retain and dispose content in a timely and compliant manner.

Event-based retention solves this problem. This topic explains how to set up your business process flows to automate retention through events by using the Microsoft 365 REST API.

The period of retention for content can be a known date such as the date the content was created, last modified or labeled. For example, you might retain documents for seven years after they're created and then delete them.

The period of retention of content can also be an unknown date. For example, with retention labels, you can also base a retention period on when a specific type of event occurs, such as an employee leaving the organization.

Disposition Reviews

When content reaches the end of its retention period, there are several reasons why you might want to review that content to decide whether it can be safely deleted ("disposed"). For example, you might need to:

- Suspend the deletion ("disposition") of relevant content in the event of litigation or an audit.
- Remove content from the disposition list to store in an archive, if that content has research or historical value.
- Assign a different retention period to the content, if the original policy was a temporary or provisional solution.
- Return the content to clients or transfer it to another organization.

This is the basic workflow for setting up a disposition review. Note that this flow shows a retention label being published and then manually applied by a user; alternatively, a retention label that triggers a disposition review can be auto-applied to content.