Advanced Data Governance

Lab Guide

Updated: June 2020

Contents

Lab Overview: Advanced Data Governance

Advanced Data Governance (ADG) is an important part of Office 365's Security and Compliance Center. It allows organizations to create and enforce policies to retain or delete sensitive information.

The two greatest values of uniform data policies are security and compliance. Keeping data longer than necessary increases security risks from inadvertent or purposeful sharing of sensitive information. However, governmental or industry regulations may require that certain records be kept for specific periods of time, such as during legal proceedings.

Advanced data governance enables a company to create policies that help ensure both security and compliance needs of the business are met.

.

Prerequisites

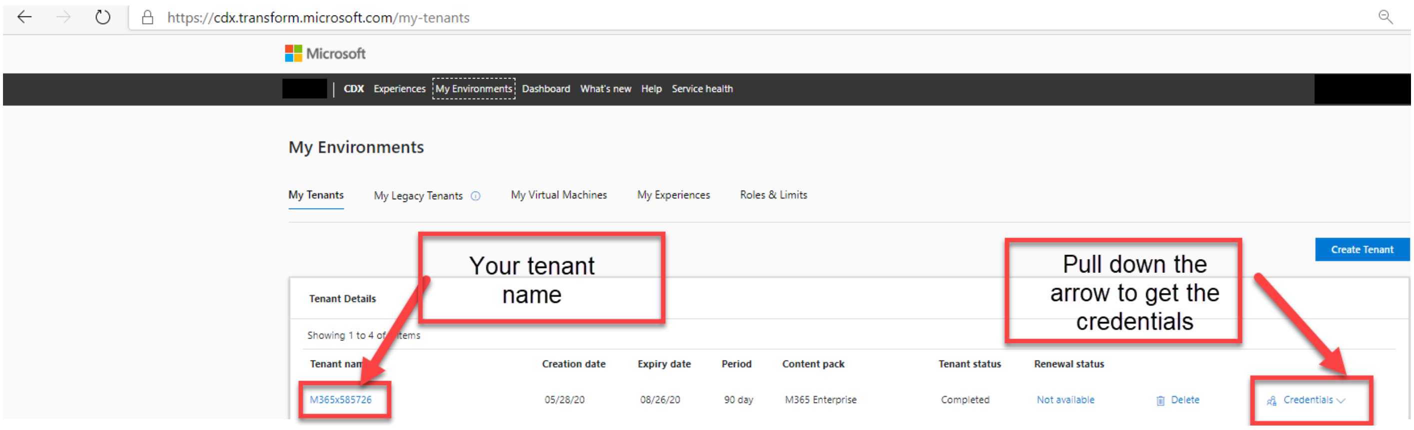
Demo Home Page and Login

1. Please ensure you have access to Partner Center. If you have not got access please follow the "Getting Started Guide" which can be downloaded here https://aka.ms/m365masterclass-Intro
2. If this is the first time completing this lab please go to Appendix: Set up the tenant for this lab

Lab Personnas

The recommended lab personas to use for in this guide, unless otherwise stated, are:

- Administrator scenarios: **admin@<tenant>.onmicrosoft.com or** MeganB@<Tenant>.onmicrosoft.com
- The default password for both users can be found on your tenant information card at https://cdx.transform.microsoft.com (See picture below)



Admin user
admin@M365x585726.onmicrosoft.com Copy

Demo user
meganb@M365x585726.onmicrosoft.com Copy

Password
[redacted] Copy

Configure Labs

Part 2 cannot be completed until Part 1 features are enabled, it takes time for the Part 1 features to propagated and process.

PART 1

Publish a Label

NOTE: This is needed to activate the UI for applying labels or it will not show up.

1. Start a browser session and navigate to your demo tenant.
2. Sign into https://protection.office.com/ as **MeganB**.
3. In the left navigation, click **Classifications**.
4. Click **Labels**.
5. Click **Retention** tab to change labels focus.
6. Click **Product Retired**.
7. Click **Publish label** in label fly-out
8. Click **Next** for **Choose labels to publish** section.
9. Leave set to **All locations** in **Publish to users and groups** section.
10. Click **Next**.
11. In **Name your policy**, select the **Name** field, type **Product Retirement**.
12. Click **Next**.
13. Click **Publish labels**.

File plan descriptors

PII Retention Policy

1. In the left navigation under **Data Governance**, click **File plan**.
2. Click **PII Retention Policy** in the existing named entries.
3. Click **Edit label** in the fly-out.
4. Click **File plan descriptors** section.
5. Click drop-down for **Reference Id**.
6. Click **+Add a new file plan descriptor reference Id**.

7. In the **Reference Id** edit field, type **Legal-2019**.
8. Click **Add**.
9. Click **Business function/department** drop-down and choose **Legal**.
10. Click **Category** drop-down, at the bottom choose **+Add a new file plan descriptor category**.
11. In the **Category** edit field, type **Commercial transactions**.
12. Click **Add**.
13. Click **Authority type** drop-down and select **Legal**.
14. Click **Save**.
15. Click **Close**.

Product Retired

1. Click **Product Retired** in the existing named entries.
2. Click **Edit label** in the fly-out.
3. Click **File plan descriptors**.
4. Click drop-down for **Reference Id**.
5. Click **Add a new file plan descriptor reference Id**.
6. In the **Reference Id** edit field, type **SAL1300**.
7. Click **Add**.
8. Click **Business function/department** drop-down and at the bottom select **+Add a new file plan descriptor business function/department**.
9. In the **Business function/department** edit field, type **Sales and Marketing**.
10. Click **Add**.
11. Click **Category** drop-down and select **Add a new file plan descriptor category**.
12. In the **Category** edit field, type **Sales / Marketing**.
13. Click **Add**.
14. Click **Authority type** drop-down and select **Business**.
15. Click **Save**.
16. Click **Close**.

Private

1. Click **Private** in the existing named entries.
2. Click **Edit label** in the fly-out.
3. Click **File plan descriptors**.
4. Click drop-down for **Reference Id**.
5. Click **Add a new file plan descriptor reference Id**.
6. In the **Reference Id** edit field, type **Private101**.
7. Click **Add**.

8. Click **Business function/department** drop-down, at the bottom choose **+Add a new file plan descriptor business function/department**.
9. In the **Business function/department** edit field, type **Strategy development research**.
10. Click **Add**.
11. Click **Category** drop-down and choose **Add a new file plan descriptor category**.
12. In the **Category** edit field, type **Business**.
13. Click **Add**.
14. Click **Authority type** drop-down and select **Business**.
15. Click **Save**.
16. Click **Close**.
17. **OPTIONAL:** - For the remaining labels, repeat Steps 3-15 above, personalizing your own descriptors for each.

Create an Event

NOTE: Complete this to make sure the event UI options are live when you do the demo.

1. In the left navigation under **Data Governance**, click **Events**.
2. Click **+Create**.
3. In the **Name** field, type **Mark8**.
4. Click **Next**.
5. Select **Use existing labels**.
6. Click **Choose labels**.
7. Click **+Add**.
8. Choose **Product Retired**.
9. Click **Add**.
10. Click **Done**.
11. Click **Next**.
12. In the **Asset IDs for items in SharePoint and OneDrive** text box, type **Mark8**.
13. Set **Date** to any date in the future.
14. Click **Next**.
15. Click **Create this event**.
16. Click **Close** at the bottom of the fly-out.

Enable Label Explorer

NOTE: This process can take several hours to complete once started.

1. In **Office 365 Security & Compliance**, click **Data Governance**.
2. Click **Label activity explorer**.
3. Click **Get started with Office 365 Analytics**.

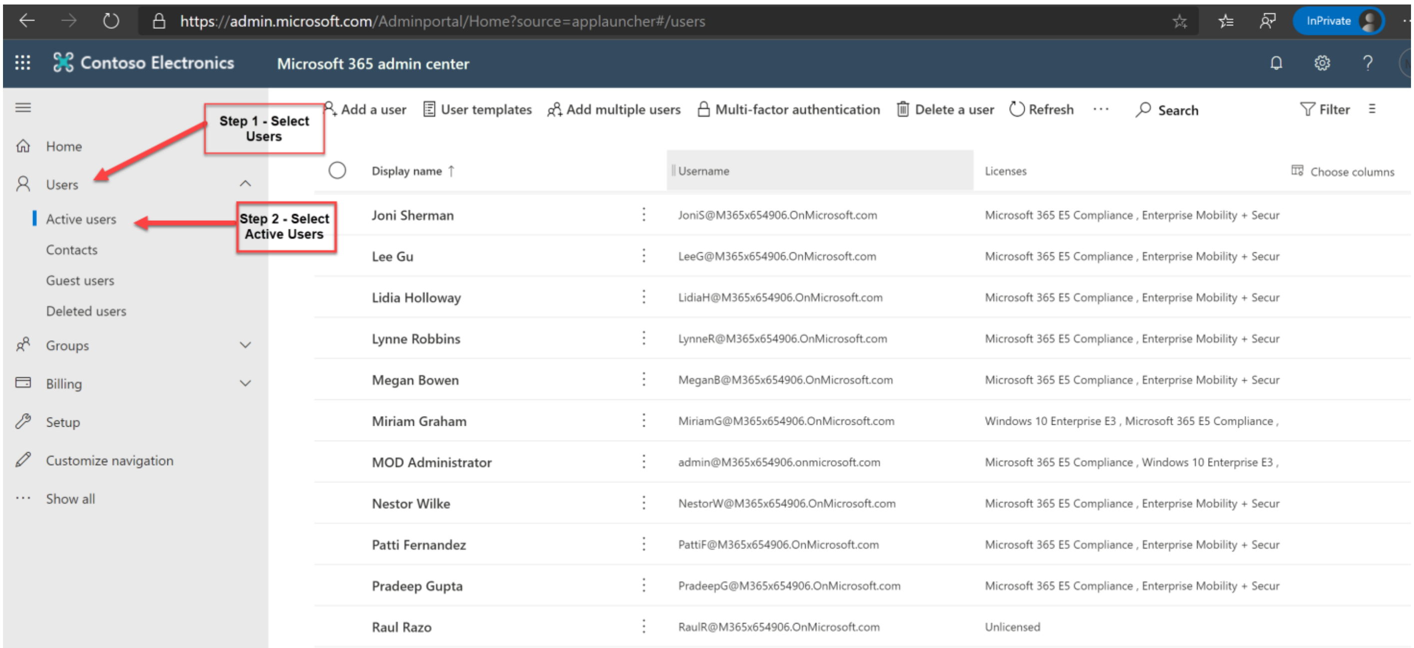
4. Click **Next**.
5. Click **Next**.
6. Click **Enable Office 365 Analytics**.

STEP 5:

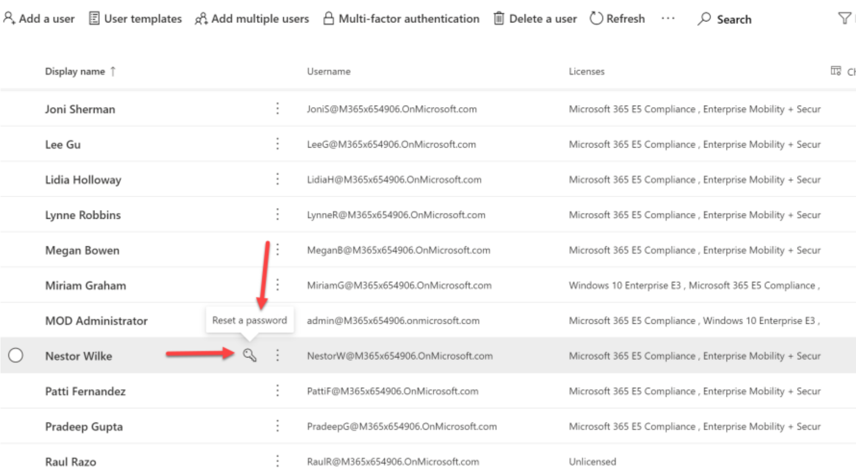
1. Sign in to Office.com <u>with each of these accounts</u> (Global Admin's) and follow steps 2-9 below to label documents:

   NOTE: The password should be the same for each, remember to sign out of the previous account before signing in with a new one.

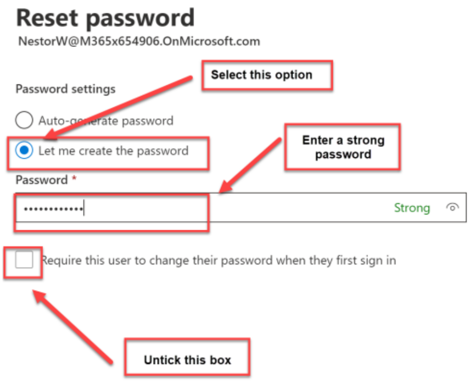
   - MeganB@<tenant>.onmicrosoft.com
   - NestorW@<tenant>.onmicrosoft.com (You will need to rest this password yourself as its not in the default credentials)
   - To complete password reset for NestorW – logon as MeganB@<tenant>.onmicrosoft.com to https://admin.microsoft.com/Adminportal/
     - On the right hand tab **select users > Active Users**



Hover over Nestor Wilke name and you will see a **Reset a password** – Select the key to reset the password.



Save the credentials so that you can logon as him in the later stages of this lab.



Document Labeling Steps for each account

1. Go to the account's **OneDrive** folder.
2. Select a file, right click and choose **Details** (no need to right click and choose **Details** if fly-out is already open).

   (For Megan DO NOT choose **Annual Financial Report(DRAFT…**, it is used later in the demo.)
3. In the right fly-out panel, click **Choose a label** under **Apply retention label** and from those listed choose any label.
4. De-select, selected file.
5. Repeat **Steps 3-5** two more times.
6. Select a file that you have applied a label to already.
7. Right-click the file.
8. Click **Details**.
9. Click **Choose a label** under **Apply retention label** and change the label to a new one or clear it.

Set up browser tabs for Megan Bowen

1. Start an InPrivate Edge browser and navigate to **Office 365 Security and Compliance** (https://protection.office.com/).
2. Sign in as **Megan Bowen** (alias **MeganB**) using the credentials above.
3. Click **App Launcher** ().
4. Right click **OneDrive** select **Open in new tab**.
5. Click **App Launcher** ().
6. Right click **SharePoint** select **Open in new tab**.
7. Click the **X1050 Launch Team** site.
8. Close the **SharePoint** tab. *(You should now have three (3) browser tabs open.)*
9. Click the **Home – Security and Compliance** browser tab to change focus.
10. The **Office 365 Security and Compliance** center (https://protection.office.com/) is the starting point for this lab.

Lab Steps

Speaker Script	Click Steps
Office 365 Advanced Data Governance (ADG) is an important part of Office 365's Security and Compliance Center. It allows organizations to create and enforce policies to retain or delete sensitive information. The two greatest values of uniform data policies are security and compliance. Keeping data longer than necessary increases security risks from inadvertent or purposeful sharing of sensitive information. However, governmental or industry regulations may require keeping certain records for specific periods of time, such as during legal proceedings. Advanced data governance enables a company to create policies to ensure meeting the company's security and compliance needs. Today we will follow Megan Bowen as she manages parts of Contoso's data governance policies.	No click steps.

Introduction

Data Governance Dashboard

Speaker Script	Click Steps
The Data Governance Dashboard shows Megan a quick visualization of the current data situation across Contoso. She can now make intelligent decisions about what information to retain and what to discard. Several widgets provide snapshots of data status and quick links to common tools.	1. In **Office 365 Security & Compliance** left navigation, click **Data governance**, and then click **Dashboard**.
The **Data governance toolbox** offers fast access to the most common tasks in creating good data management policies. Megan sees two common ways to move external data into Office 365. **Import data** into Office 365 brings in user email boxes and data from other systems using automation and filters to reduce importing outdated information. Megan has already set up data to import later.	2. On the **Data governance toolbox** widget, click **Open the data governance toolbox**.

Speaker Script	Click Steps
Increase mailbox storage enables automatic archiving of older email. This will reduce unexpected issues when importing large mailboxes from other sources. In the toolbox Megan has access to commonly used wizards for classifying data and applying policies from one location.	3. Under **Prepare**, point to, *but do not click*, **Import data** and **Increase mailbox storage**.
On the main dashboard, widgets give Megan insights into data usage and provide useful links, such as an overview of where data is stored and how it is growing over time. **Suggestions Widget** Office 365 ADG uses cloud intelligence to proactively recommend policies for Contoso. Recommended policies are visible in the Data Governance Dashboard, based on the types of documents in use by Contoso and the profiles of similar organizations. For example, ADG provides a widget titled **Recommended for you**, containing Data Governance policy suggestions. Megan can appropriately manage documents by reviewing the suggestions and implementing what makes sense for Contoso. As Contoso's ADG use grows, widgets in the dashboard are enriched by ADG's cloud intelligence. Because this is a demo installation, some of these widgets may not show data, as they would in a production environment. **Retention** shows how many users' files are being retained and provides a way to turn on retention for everyone and add refined policies. **Online archive mailbox** shows what percentage of Contoso users have enabled archive mailboxes. **Your content at a glance** shows a snapshot of how much and which types of data are being stored. **Your content over time** shows how data has accumulated over the years based on the date created.	4. Scroll down if needed and point to the **Govern** section in the toolbox. 5. Below **Govern**, point to the wizard links regarding *label and policy management tools*. 6. Scroll down if needed and point to the **Monitor & Respond** section in the toolbox. 7. Below **Monitor & Respond**, point to the wizard links *regarding label and alert policies tools*. 8. In the bottom left of the toolbox, click **Close**. 9. Scroll down the page to show additional widgets. 10. Point to the **Recommended for you** items. **NOTE:**(this widget area is dynamic and may show different suggestions in your tenant). 11. Skip over the **Classify your data** section because it often has no data in a demo environment. 12. Scroll down to **Govern and stay compliant**. 13. Point to **How much content is being retained**. **NOTE**: This may just show: *We're getting your info*. 14. Point to **Retention**. 15. Point to **Online archive mailbox**. 16. Point to **Your content at a glance**. 17. Point to **Your content over time**.

Speaker Script	Click Steps
	NOTE: This may not show data.

Retention

Speaker Script	Click Steps
Keeping data longer than needed or required, imposes significant costs and risks for Contoso. For example, it's costly to store unneeded data from users who have left the organization. In addition, the more data that's stored, the greater the risk of a security breach. On the other hand, Contoso must keep some historical data for business reasons and to comply with policies and government regulations. Powerful tools to manage retention and policy-based deletion are needed to balance these needs in a uniform way. **Office 365 offers two approaches to applying Retention policies, Retention policies and Label policies.** Contoso's data governance managers control **Retention** policies. They apply the policies across an organization or to specific locations. Retention policies use basic data age-based rules to determine how long to ensure retention and/or to trigger deletion. **Label** policies can be applied automatically or by users. Users can update data labels, using their insight to refine which data is protected. Label based retention policies add more choices for policy timing. They can also trigger a formal review of the content at the end of the retention period vs. automatically moving data towards removal.	No click steps.

Retention Policies

Speaker Script	Click Steps
Retention Policies by Data Location Contoso decided to retain all the Teams chats and channel messages for 3 years and then delete them, unless they fall under another retention policy. Megan does this using unified retention management controls in Advanced Data Governance. From one location, she can administer retention policies for Exchange, SharePoint, OneDrive, Skype, and Teams. She will create a policy that retains data for 3 years and then deletes the data automatically. Megan sets unique **Locations** to focus this policy on, specifically the new types of data they are now using in Teams messages and chats. She could also apply these policies to other locations like Exchange, SharePoint, OneDrive, and Skype for Business. But this policy is just for Teams message and chats, so she deselects all other locations. When a policy includes automatic deletion, creating the policy will trigger the permanent removal of all data that matches policy rules.	1. In the left navigation, under **Data governance**, click **Retention**. 2. Click **+Create**. 3. In the **Name** text box, type **Teams Retention**. Optionally, type a description. 4. Click **Next**. 5. Click **Yes, I want to retain it.** 6. Change the length setting to **3 years.** 7. Under **Do you want us to delete it after this time?** click **Yes**. 8. Click **Next**. 9. Point to, but do not click, options under **Include** and **Exclude** for **Exchange email**, **SharePoint sites**, **OneDrive accounts**, and **Office 365 groups**, showing how these can narrow the focus and set exclusions. 10. Use the slider to turn off, the top 4 locations. 11. Use the slider to turn on, **Teams channel messages** and **Teams chat**. 12. To the right, point out the targeting options, **Exclude teams** for **Team channel messages** and **Exclude users** for **Teams chats.** Do not make any changes. 13. Click **Next**. 14. In **Review your settings**, point out the alert at the top: ⚠ **It will take up to 7 days to apply the retention policy to the locations you chose**. 15. Click **Create this policy**. 16. Click **Close**.

Advanced Retention Policies

Speaker Script	Click Steps
Contoso uses organizational retention policies for specific types of data covered by regulations or legal concerns.	Talk track only.
Contoso is concerned that employees are still storing email information covered under the new General Data Protection Regulation (GDPR) even after it has been filed into the proper locations. Megan creates a new retention policy, **GDPR Email Removal**. She knows that retention rules supersede deletion, so this rule will only affect detected data that doesn't fall under other retention policies. Megan will add **advanced retention settings** to delete any email with GDPR-covered data after 6 months unless retained by another policy. **Advanced retention settings** can detect words or phrases the policy creator specifies or organizations can use a set of predefined templates to apply policies to data covered by regulations in their region. Megan uses a Microsoft provided template for GDPR data formats. Organizations can also create custom mappings, giving granular control over what kind of information is protected. After choosing the pattern to detect, Megan sets the deletion rules for this policy. She could also refine the rules in this template to meet Contoso's unique needs. This rule is not looking for large lists of data, but emails with small amounts that could miss other reviews. This template looks for emails containing between 1 and 9 occurrences of the covered information. Megan sets the location to cover as **Exchange**.	1. Under **Data Governance** click **Retention**. 2. Click **+Create**. 3. Click **Name** and type **GDPR Email Removal**. 4. In **Description** type **Remove data with GDPR covered ID patterns, not covered under other retention policies**. 5. Click **Next**. 6. Under **Need more options?** click **Use advanced retention settings**. 7. In the drop-down menu, click **Detect content that contains sensitive info**. 8. Click **Next**. 9. Next to **Show options for**, click **European Union**. 10. Click **Privacy**. 11. Click **General Data Protection Regulation (GDPR)**. 12. In the right column, point to the types of information it will detect in your data. 13. Click **Next**. 14. Note that **Advanced Retention** defaults to **Keep content for 7 years.** 15. Click **Edit**. 16. Scroll down to **Retain the content**. 17. Set period to **6 months**. 18. Under **Do you want to delete it after this time?** click **Yes**. 19. Scroll up to show that the administrator can adjust the provided template if needed. Point to the counts and accuracy ratings that control this template.

Speaker Script	Click Steps
During policy creation, ADG alerts Megan to how long this policy may take to apply to the whole organization.	20. At the bottom, click **Next**. 21. Click **Let me choose specific locations**. 22. Set toggle to **off** for **SharePoint sites** and **OneDrive accounts**. 23. Click **Next**. 24. In **Review your settings**, point to the alert at the top: ⚠ **It will take up to 7 days to apply the retention policy to the locations you chose**. 25. Click **Create this policy**. 26. Click **Close.**

Summary of Retention Policies

Speaker Script	Click Steps
Retention policies created in **Data Governance,** are best for broad policies that are almost always true and don't change with adjustments to organizational structures or strategies. They work in the background, with no actions required or changes possible from members of your organization. They may be applied to Exchange email and public folders, SharePoint sites, OneDrive accounts, Skype for Business, and Teams. They may be applied using high-level rules related to the user and the location. If needed, advanced policies that detect sensitive information can be applied. Retention policies offer high-level automation, flexibility, and control over how and when different types of data are stored or discarded.	No click steps.

Labels

Speaker Script	Click Steps
Contoso has many types of content and records they need to manage in different ways. Office 365 Advanced Data Governance labels allow members of an organization to contribute to the precision of the data retention policies. They also allow for business events to trigger retention policies. Events like employees leaving and product end-of-life often have organizational rules attached to them. Labels empower managers to automatically implement data retention aligned with those policies.	No click steps.
One of the added features of using labels is the option to trigger a disposition review when the content has reached the end of its retention period. **NOTE:** *If the customer asks, the* ***GDPR email removal rule*** *is listed here because Advanced Retention policies use this label system to mark content using that rule.* Megan needs to **create a label** to enable retention policies on **Sales Data** content that needs a disposition review by the legal team before it is deleted or archived. She wants to enhance the ability of her new label by adding additional Metadata options in **File plan descriptors.** Megan adds a new unique **Reference Id** and sets the **Business function/department** drop-down to *Sales and Marketing*. She selects *Sales / Marketing* from the **Category** drop-down and finishes up by setting the **Authority type** to *Business*. Megan turns on retention and configures the settings. First, she will use the default setting to **Retain for 7 years**. Next, she will **Trigger a disposition review** when staff will review items that have reached the end of their retention period to decide whether they can safely delete that data. Next, Megan specifies which reviewers will receive an email notification when items reach the end of the retention period. In this case the legal team, lead attorney Alex Wilber, and the sales	1. In the **Security & Compliance** left navigation, click **Classifications** and click **Labels**. 2. Point to the **Sensitivity** and **Retention** tabs at the top. 3. Click the **Retention** tab. **NOTE**: **GDPR Email Removal** label is listed here even though we didn't explicitly create a label. 4. Click **+Create a label**. 5. Click the **Name** field and type **Sales Data**. Leave the **Description** field blank. 6. Click **Next**. 7. Click **Reference ID** drop-down, add a unique entry that make sense for the business function, such as **SAL1300 for sales**. 8. Click the **Business function/department** drop-down and select **Sales and Marketing**. 9. Click the **Category** drop-down and select **Sales / Marketing**. 10. Click the **Authority type** drop-down and select **Business.** 11. Click **Next**. 12. Toggle **Retention** to **On**.

Speaker Script	Click Steps
team will be notified that a review is needed. They can then go to disposition page to review items.	13. Confirm setting to **Retain the content for 7 years**. 14. Click **Trigger a disposition Review**.
As with Retention policies, Megan has the choice to start the retention policy based on when the data **was created** or **when it was last modified**. She can also set the retention date to when the **label was applied**. She can also base the retention period on a business **event** like an employee exiting or retiring a product. For this label, a data's last modified date triggers the policy. **RECORD Classification** If a label has the classification "Record" that label can never be deleted and once the label is applied that data cannot be edited or changed and will be retained or deleted based on the rule for that label. Once created, Megan can publish the retention policy label so members of the organization can apply it to data, or she can set up rules to auto-apply the labels. Megan publishes this label to all locations for users to apply as needed.	15. Below **Notify these people when there are items ready to review**, click the text box and type: **Alex**. In the drop-down, click **Alex Wilber**. 16. Next to **Alex Wilber**, type **Sales.** In the drop-down click **Sales Team.** 17. Next to **Sales Team**, type **Legal.** In the drop-down click **Legal Team.** 18. Click the **Retain or delete the content based on** drop-down. 19. *Point to,* these options: **when it was created**, **when it was labeled** and **an event**. **20.** Select from the list **when it was last modified.** **NOTE**: *You cannot delete a label having a **Record** classification*. It will be there even after you reset the tenant for a new demo. 21. Point to, do not click, the setting for **Label classification**.
Here we see an example of the power of unified labeling. One label and policy applied across several services. And the manager can still target the usage to specific sites or users.	22. Click **Next**. 23. Click **Create this label**. **NOTE**: This can take several seconds - If you encounter issues, move to the extra ADG tab you opened for the next section and skip publishing. 24. In the right fly-out, click **Publish label**, and then click **Next**. 25. Click **Let me choose specific locations.**

Speaker Script	Click Steps
	26. Point to all the locations this label can be applied to. 27. Click the **All locations. Includes…** option. 28. Click **Next**. 29. Name the policy **Sales Data**. Skip **Description.** 30. Click **Next.** 31. Click **Publish labels**. 32. Click **Close** if needed.

Applying an Existing Label

Speaker Script	Click Steps
Once a label is published there will be a time period for tenant propagation, before the users can apply the label. Megan has already published some labels and can apply them in places like her OneDrive and Outlook Inbox. With a couple of clicks in OneDrive, Megan's copy of the Annual Report is now protected by the new retention policy. Megan can find and apply the same label to an email in Outlook.	1. Click the **OneDrive** browser tab. 2. Right-click **Annual Financial Report (Draft)** and select **Details**. 3. In the fly-out panel, point to **Apply retention label**. 4. Click **Choose a label** and select **Confidential**. **NOTE**: each label summarizes the retention policy (5 years, 7 years, etc.). 5. Click **App Launcher** and select **Outlook**. 6. Right-click any email in the **Inbox**. 7. Click **Assign Policy**. 8. Point to **Confidential** now listed with Outlook's time-based retention labels. 9. Click **Confidential**.
By giving users the ability to tag their own content, Contoso better ensures the right policies are applied across their organization.	No click steps.

Event-Driven Label Policies

Speaker Script	Click Steps
Content retention periods are often based on the age of the content. However, Contoso needs to base some retention on when a specific type of event occurs, regardless of the data's age. The time since the event occurred? is what drives the policy. The first stage is creating a consistent label and policy for a type of event like product retirement. Megan already has a **Product Retired** label and policy in place.	No click steps.
Contoso has scheduled the X1050 product to retire at the end of the year. All the data assets for that project will fall under the retention rules for a product's end of life. The label for this policy already exists. Megan now needs to add an event for December 31st of this year that works with that label to apply the policy. Megan could have created the event with **Use event types** to enable identifying content related to the event, but without a label-based policy. Megan can use **Key Words** rules to identify data this event applies to in **SharePoint**, **OneDrive**, and **Exchange**. For this rule, Megan is only concerned with data in SharePoint and OneDrive with an Asset ID of X1050. This is added like a label to a file. She can set the event date in the past or the future, which is the starting point of that retention policy. Any piece of data that has BOTH the label "Product Retirement" and Asset ID of X1050 will time its retention from the retirement date of December 31st.	1. Return to the **Security and Compliance** tab. 2. In the **Security & Compliance** left navigation, click **Data governance** and select **Events**. 3. Click **Create**. 4. In the **Name** field, type **X1050**. Leave the description blank. 5. Click **Next**. 6. Click **Use existing labels**. 7. Click **Choose Labels**. 8. Click **Add**. 9. Click to select **Product Retired**. 10. Click +**Add**. 11. Click **Done**. 12. Click **Next**. 13. In the **Asset IDs for items in SharePoint and OneDrive** text box, type **X1050**. 14. Set the **date** to **Dec 31st** of this year . 15. Click **Next**. 16. Click **Create this event**. 17. Click **Close**.

Speaker Script	Click Steps
Megan can now test this by applying a label and Asset ID to a document.	18. Go to **SharePoint**. 19. Choose the **X1050 Launch Team** site. 20. In the left navigation, click **Documents**. 21. Click the **Design** folder. 22. Right-click **marketing-initiatives-FY17** and select **Details**.
When an event-driven label is used and an event is created, an extra setting is offered to set the Asset ID. In this case, Megan uses the Asset ID in the event we just created.	23. In the right fly-out panel, under **Apply retention label**, click **Choose a label**. 24. In the drop-down list, click **Product Retired**. 25. Wait a few seconds for the **Asset ID** option to appear below. 26. For **Asset ID**, type **X1050**. 27. Return to **Security and Compliance**.

Auto Apply Labels

Speaker Script	Click Steps
After an Event-driven? label is created, Megan can publish it like she did with the previous labels or set to auto-apply the label. This process is very similar to how the Advanced Retention policy was created, with access to the same templates.	1. In the left navigation, click **Classifications**. 2. Click **Labels**. 3. Click the **Retention** tab. 4. Select **PII Retention Policy**.
Megan needs to create a label for content containing common US financial ID information that users can apply and allow ADG to automatically detect and label the data. Megan goes to the labels list and chooses to Auto-apply.	5. On the right, click **Auto-apply a label**. 6. Click **Next**. 7. Click **Apply label to content that contains sensitive info**. 8. Click **Next**. 9. In the first column, click **Financial**.
This will cover any data with personal financial data that is not under another retention policy.	10. Scroll down and select **U.S. Financial Data**. 11. Click **Next**. 12. Click **Next**. 13. In the **Name** field, type **Auto US Financial.** Leave the description blank. 14. Click **Next**.

Speaker Script	Click Steps
She then selects the label and sets the location to all OneDrive locations. This will find all personal data that users should not store long-term in OneDrive. For the demo, we will not complete applying this label.	15. Click **Let me choose specific locations**. 16. Toggle off all locations except **OneDrive accounts**. 17. Click **Next**. 18. Point to, but ***DO NOT CLICK*** **Auto-apply**. 19. Click **Cancel**. 20. In the dialog, click **Yes**.

Conclusion

Speaker Script	Click Steps
In a few minutes, Megan improved how her organization manages data from a unified administration interface. With these capabilities, Contoso can improve security and compliance needed in today's connected and regulated world.	No click steps.