Contents

1 SC-400T00: Microsoft Information Protection Administrator

This repository includes lab instructions for the following courses:

- SC-400T00: Microsoft Information Protection Administrator

Download Latest Student Handbook and AllFiles Content

Are you a MCT? - Have a look at our GitHub User Guide for MCTs

Need to manually build the lab instructions? - Instructions are available in the MicrosoftLearning/Docker-Build repository

1.1 What are we doing?

- To support this course, we will need to make frequent updates to the course content to keep it current with the Azure and Microsoft 365 services used in the course. We are publishing the lab instructions and lab files on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the Azure platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Azure changes and you find it first during a live delivery, go ahead and make an enhancement right in the lab source. Help your fellow MCTs.

1.2 How should I use these files relative to the released MOC files?

- The instructor handbook and PowerPoints are still going to be your primary source for teaching the course content.
- These files on GitHub are designed to be used in conjunction with the student handbook, but are in GitHub as a central repository so MCTs and course authors can have a shared source for the latest lab files.
- It will be recommended that for every delivery, trainers check GitHub for any changes that may have been made to support the latest Azure or Microsoft 365 services, and get the latest files for their delivery.

1.3 What about changes to the student handbook?

- We will review the student handbook on a quarterly basis and update through the normal MOC release channels as needed.

1.4 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repro, Microsoft and the course author will triage and include content and lab code changes as needed.
- You can submit bugs, changes, improvement and ideas. Find a new Azure feature before we have? Submit a new demo!

1.5 Notes

1.5.1 Classroom Materials

1.6 It is strongly recommended that MCTs and Partners access these materials and in turn, provide them separately to students. Pointing students directly to GitHub to access Lab steps as part of an ongoing class will require them to access yet another UI as part of the course, contributing to a confusing experience for the student. An explanation to the student regarding why they are receiving separate Lab instructions can highlight the nature of an always-changing cloud-based interface and platform. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only.

1.7 title: Online Hosted Instructions permalink: index.html layout: home

2 Content Directory

Hyperlinks to each of the lab exercises and demos are listed below.

2.1 Labs

{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | | --- | --- | {% for activity in labs %}| {{ activity.lab.module }} | [{{ activity.lab.title }}{% if activity.lab.type %} - {{ activity.lab.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/SC-400T00A-Microsoft-Information-Protection-Administrator/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

{% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/SC-400T00A-Microsoft-Information-Protection-Administrator/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

3 Exercise 1 - Manage Compliance Roles

In your role as Joni Sherman, the newly hired Compliance Administrator for Contoso Ltd. you are tasked to configure the new Microsoft 365 tenant of your organization, to meet the organizations compliance requirements. Contoso Ltd. is a company with a headquarters in the United States and several new subsidiaries in the European Union and your organization needs to make sure the new Microsoft 365 tenant fulfills the legal requirements of different countries and regulatory requirements of your industry sector.

3.0.1 Task 1 – Assign Compliance Roles

In this exercise, you will follow the principal of least privilege and use the default Global Administrator to assign the Compliance Admin role to Joni Sherman, which is required to perform the operations described in this lab.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account. The password should be provided by your lab hosting provider.
2. Open **Microsoft Edge** from the taskbar and when a **Welcome to the new Microsoft Edge** windows is displayed, select **Complete setup**.
3. Select **Confirm** to accept the default browser settings and **Continue without signing in**.
4. In **Microsoft Edge**, navigate to **https://admin.microsoft.com** and log into the Microsoft 365 Admin center as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
5. On the **Stay signed in?** dialog box, select the **Don't show this again** checkbox and then select **No**.
6. Close the password save dialog from the bottom with Never, to not save the default global admins credentials in your browser.

7. If a welcome screen is displayed, close it. If the Office 365 apps notification appears, also close it.
8. If a welcome window is displayed, select Get started and close it.
9. In the left navigation pane, expand **Users** and then select **Active users**.
10. In the **Active users** list, search and select **Joni Sherman**, to open the right-side settings pane.
11. In the settings below the **Account** tab, scroll to **Roles** and select **Manage roles** below.
12. When the **Manage admin roles** pane opens, select **Admin center access**, select **Show all by category** and scroll down to select **Compliance admin** in the Security & Compliance section.
13. Select **Save changes** to apply the role. When the **Admin roles updated** message is displayed on the upper part of the pane, select the arrow pointing to the left.
14. Close the window of Joni Sherman's account with the **X** in the upper right to go back to the **Active users** list.
15. Select the circle with **MA** in the upper right and select **Sign out**.
16. Close the **Microsoft Edge** browser window.

You have successfully assigned Joni Sherman the Compliance Administrator role, which is required to perform the different exercises of this lab. Continue with the next task.

3.0.2 Task 2 – Explore the Compliance Center

In this task, you will sign out of the global admin account and sign-in again as Joni Sherman. Because Joni Sherman just got the Compliance admin role assigned, her account will be sufficient for most of this lab's exercises.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com**.
3. When the **Pick an account** window is displayed, select **Use another account**.
4. When the **Sign in** window is displayed, sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
5. When the **Improve your compliance posture** message window opens, read the text and select **Next** twice and then select **Done**.
6. Scroll down and select **... Show all*** from the lower left side to open all menu items of the Microsoft 365 compliance center.
7. Get yourself familiar with the different settings. When you are done, leave the browser window open.

You have successfully switched to Joni Sherman's account and you are now ready to start with the lab.

4 Proceed to Exercise 2

5 Exercise 2 - Manage Office 365 Message Encryption

The first setting Joni Sherman needs to configure and test with her pilot team is the Microsoft 365 built-in Office 365 Message Encryption (OME). For this purpose, she will modify the default template and create a new branding template, that will be assigned to one of the pilot users. The pilot users will then test the OME functionality with their accounts.

5.0.1 Task 1 – Verify Azure RMS functionality

In this task, you will install the Exchange Online PowerShell module and verify the correct Azure RMS functionality of your tenant in context of Joni Sherman, who was assigned the role of the Compliance Administrator in the last exercise.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.

2. Open an elevated PowerShell window by selecting the Windows button with the right mouse button and then right-click **Windows PowerShell** and choose **Run as Administrator**.
3. Confirm the **User Account Control** window with **Yes**.
4. Enter the following cmdlet to install the latest Exchange Online PowerShell module version:

   Install-Module ExchangeOnlineManagement
5. Confirm the NuGet provider security dialog with **Y** for Yes and press **Enter**.
6. Confirm the Untrusted repository security dialog with **Y** for Yes and press **Enter**.
7. Enter the following cmdlet to change your execution policy and press **Enter**

   Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
8. Confirm the Execution Policy Change with **Y** for Yes and press **Enter**.
9. Close the PowerShell window.
10. Open a regular PowerShell window, by selecting the Windows button with the right mouse button and select **Windows PowerShell**.
11. Enter the following cmdlet to use the Exchange Online PowerShell module and connect to your tenant:

    Connect-ExchangeOnline
12. When the **Sign in** window is displayed, sign in as sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
13. Verify Azure RMS and IRM is activated in your tenant by using the following cmdlet:

    Get-IRMConfiguration | fl AzureRMSLicensingEnabled
14. Test the Azure RMS templates used for Office 365 Message Encryption against the other pilot user **Megan Bowen**:

    Test-IRMConfiguration -Sender MeganB@contoso.com
15. Verify all tests are in the status PASS and no errors are shown.
16. Leave the PowerShell window open.

You have successfully installed the Exchange Online PowerShell module, connected to your tenant and verified the correct functionality of Azure RMS.

5.0.2 Task 2 – Modify default OME template

There is a requirement in your organization to restrict trust for foreign identity providers, such as Google or Facebook. Because these social IDs are activated by default for accessing messages protected with OME, you need to deactivate the use of social IDs for all users in your organization.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account and there should still be an open PowerShell window with Exchange Online connected.
2. Run the following cmdlet to view the default OME configuration:

   Get-OMEConfiguration -Identity "OME Configuration" |fl
3. Review the settings and confirm that the SocialIdSignIn parameter is set to True.
4. Run the following cmdlet to restrict the use of social IDs for accessing messages from your tenant protected with OME:

   Set-OMEConfiguration -Identity "OME Configuration" -SocialIdSignIn:$false
5. Confirm the warning message for customizing the default template with **"Y"** for Yes and press **Enter**.
6. Check the default configuration again and validate, the SocialIdSignIn parameter is now set to False.

   Get-OMEConfiguration -Identity "OME Configuration" |fl
7. Leave the PowerShell window and client open.

You have successfully deactivated the usage of foreign identity providers, such as Google and Facebook in Office 365 Message Encryption.

5.0.3 Task 3 – Test default OME template

You must confirm that no social IDs dialog is displayed for external recipients when receiving a message protected with Office 365 Message Encryption from users of your tenant.

1. Log into the Client 2 VM (LON-CL2) as the **lon-cl2\admin** account.
2. Open **Microsoft Edge** from the taskbar and when a **Welcome to the new Microsoft Edge** windows is displayed, select **Complete setup** if it appears.
3. Select **Confirm** to accept the default browser settings and **Continue without signing in** if it appears.
4. In **Microsoft Edge**, navigate to **https://outlook.office.com** and log into Outlook on the web as LynneR@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Lynne Robin's password should be provided by your lab hosting provider.
5. On the **Stay signed in?** dialog box, select the **Don't show this again** checkbox and then select **No**.
6. Select **Save** in the **Save password** dialog, to save the pilot users password in your browser.
7. If a **Translate page from...** window is shown, select the arrow down and select **Never translate from...**.
8. Select **New message** from the upper left side part of Outlook on the web.
9. In the **To** line enter your personal or other third-party email address that is not in the tenant domain. Enter **Secret Message** to the subject line and **My super-secret message.** to the body.
10. From the top pane, select **Encrypt** to encrypt the message. Once you've successfully encrypted the message, you should see a notice that says something like "...This message is encrypted."
11. Select **Send** to send the message.
12. Sign in to your personal email account and open the message from Lynne Robbins. If you sent this email to a Microsoft account (like @outlook.com) the encryption may be processed automatically and you will see the message. If you sent the email to another email service (like @google.com), you may have to perform the next steps to process the encryption and read the message.
13. Select **Read the message**.
14. Without having social IDs activated, there is no button to authenticate with your Google account.
15. Select **Sign in with a One-time passcode** to receive a limited time passcode.
16. Go to your personal email portal and open the message with subject **Your one-time passcode to view the message**.
17. Copy the passcode, paste it in to the OME portal and select **Continue**.
18. Review the encrypted message.

You have successfully tested the modified default OME template with deactivated social IDs.

5.0.4 Task 4 – Create custom branding template

Protected messages sent by your organizations finance department require a special branding, including customized introduction and body texts and a Disclaimer link in the footer. The finance messages shall also expire after seven days. In this task, you will create a new custom OME configuration and create a transport rule to apply the OME configuration to all mails sent from the finance department.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account and there should still be an open PowerShell window with Exchange Online connected.
2. Run the following cmdlet to create a new OME configuration:

   New-OMEConfiguration -Identity "Finance Department" -ExternalMailExpiryInDays 7
3. Confirm the warning message for customizing the template with **"Y"** for Yes and press **Enter**.

4. Change the introduction text message with the following cmdlet:

   Set-OMEConfiguration -Identity ”Finance Department” -IntroductionText ” from Contoso Ltd. finance department has sent you a secure message.”

5. Confirm the warning message for customizing the template with **”Y”** for Yes and press **Enter**.

6. Change the body email text of the message with the following cmdlet:

   Set-OMEConfiguration -Identity ”Finance Department” -EmailText ”Encrypted message sent from Contoso Ltd. finance department. Handle the content responsibly.”

7. Confirm the warning message for customizing the template with **”Y”** for Yes and press **Enter**.

8. Change the disclaimer URL to point to Contoso’s privacy statement site:

   Set-OMEConfiguration -Identity ”Finance Department” -PrivacyStatementURL ”https://contoso.com/privacystatemen

9. Confirm the warning message for customizing the template with **”Y”** for Yes and press **Enter**..

10. Use the following cmdlet to create a mail flow rule, which applies the custom OME template to all messages sent from the finance team.

    New-TransportRule -Name ”Encrypt all mails from Finance team” -FromScope InOrganization -FromMemberOf ”Finance Team” -ApplyRightsProtectionCustomizationTemplate ”Finance Department” -ApplyRightsProtectionTemplate Encrypt

11. Leave the PowerShell open.

You have successfully created a new transport rule that applies the custom OME template automatically, when a member of the finance department sends a message to external recipients.

5.0.5 Task 5 – Test the custom branding template

To validate the new custom OME configuration, you need to use the account of Lynne Robbins again, who is a member of the finance team.

1. You should still be logged into your Client 2 VM (LON-CL2) as the **lon-cl2\admin** account, and you should be logged into Microsoft 365 as **Lynne Robbins**.

2. Select the **Outlook** symbol from the left navigation pane.

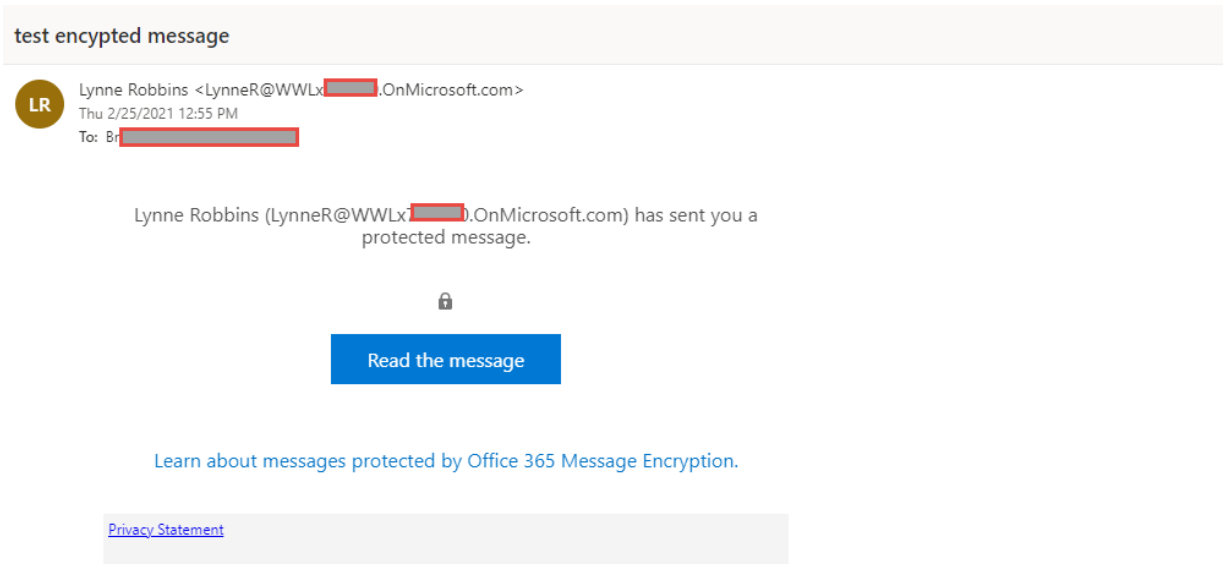
3. Select **New message** from the upper left side part of Outlook on the web.

4. In the **To** line enter your personal or other third-party email address that is not in the tenant domain. Enter *Finance Report* to the subject line and enter *Secret finance information.* to the body.

5. Select **Send** to send the message.

6. Sign in to your personal email account and open the message from Lynne Robbins.

7. You should see a message from Lynne Robbins that looks like the image below. Select **Read the message**.



8. The customized OME configuration gets social IDs activated, because both options are available. Select **Sign in with a One-time passcode** to receive a limited time passcode.
9. Go to your personal email portal and open the message with subject **Your one-time passcode to view the message**.
10. Copy the passcode, paste it in to the OME portal and select **Continue**.
11. Review the encrypted message with custom branding.

You have successfully tested the new customized OME template.

6 Proceed to Exercise 3

7 Exercise 3 - Manage Sensitive Information Types

Contoso Ltd. previously had issues with employees accidentally sending out personal information from customers when working on support tickets in the ticketing solution. To educate users in the future, a custom sensitive information type is required to identify employee IDs in emails and documents, which consist of three uppercase characters and six numbers. To lower the false positive rate, the keywords "Employee" and "IDs" will be used. In this task you will create a new custom sensitive information type, a database for EDM-based classification and a keyword dictionary.

7.0.1 Task 1 – Create Custom Sensitive Information Types

In this exercise, you will use the Security & Compliance Center PowerShell module to create a new custom sensitive information type that recognizes the pattern of employee IDs near the keywords "Employee" and "ID".

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as sign in as sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
3. Select **Data classification** from the left pane.
4. If a **What is data classification?** message is displayed, select **Close** and select **Sensitive info types** from the top pane.
5. Select **(+) Create info type** to open the wizard for a new sensitive information type.
6. On the **Choose a name and description** page, type *Contoso Employee IDs* into **Name**.
7. Type *Pattern for Contoso employee IDs.* to the **Description** field and select **Next**.
8. On the **Requirements for matching** page, select **(+) Add an element**.
9. Select the dropdown field below **Detect content containing** and select **Regular expression**.
10. Enter the following to the input field: *\s[A-Z]{3}[0-9]{6}\s*
11. Below **Supporting elements**, select **+ Add supporting elements** in the drop-down menu select **Contains this keyword list**.
12. Enter the following into the text box below **Keyword list**: *Employee*, *IDs*
13. Decrease the **Character proximity** value to *100* characters.
14. Select **Next**.
15. Finish the wizard by selecting **Finish**.
16. In the **compliance** window, select **Yes** to test the created sensitive type.
17. Select the **Search** box in the upper right-side of the Data classification area, type *Contoso* and press the enter key.
18. Select the newly created sensitive information type *Contoso Employee IDs* to open the right-side pane.
19. Review the configured settings of the sensitive information type.

20. Leave the browser window open.

You have successfully created a new sensitive information type to identify employee IDs in the pattern of three uppercase characters, six numbers, and the keywords 'Employee' or 'IDs' within a range of 100 characters.

7.0.2 Task 2 – Create EDM-based classification information type

As an extra search pattern, you will create an EDM-based classification with a database schema of employee data. The database source file will be formatted with the following data fields of employees: Name, Birthdate, StreetAddress, and EmployeeID.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. To create the required Azure AD security group, sign out of Joni Sherman's account by selecting the user image in the upper right corner and select **Sign out**.
3. Close the browser window and open a new browser window.
4. In **Microsoft Edge**, navigate to **https://admin.microsoft.com**.
5. When the **Pick an account** page is displayed, select **Use another account** and sign in as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
6. From the left pane, select **Groups** and select **Active groups**.
7. Select **Add a group** from the top pane.
8. On the **Choose a group type** page, select **Security** and **Next**.
9. On the **Set up the basics**, enter the following to the **Name** field: *EDM_DataUploaders*. In the Description field, enter *people who will upload data for EDM*.
10. Select **Next**.
11. On the **Review and finish adding group** page, review your settings and select **Create group**.
12. When the **New group created** page is shown, select **Close**.
13. Select **Refresh** from the top pane and select the newly created **EDM_DataUploaders** group from the list to open the right side pane.
14. Select the **Members** tab and select **View all and manage members**.
15. In the **Manage group members** screen, select **(+) Add members**.
16. Select **Joni Sherman**, select **Save changes**.
17. Verify **Joni Sherman** is listed below **Group members** and select **Close**.
18. Close the right side pane with **X**.
19. Select the circle with the MOD Administrator initials **MA** and select **Sign out**.
20. Close the browser window and open a new one.
21. Navigate to the Microsoft 365 Compliance Center at https://compliance.microsoft.com.
22. When the **Pick an account** page is displayed, select **Joni Sherman** and sign in.
23. Navigate to **Data classification** and select **Exact data matches** tab from the top pane.
24. Select **(+) Create EDM schema** to create a new schema definition.
25. In the **Name** field, enter *employeedb*.
26. In the **Description** field, enter *Employee Database schema.*.
27. Select **Ignore delimiters and punctuation for all schema fields**.
28. Select **Choose delimiters and punctuation to ignore** and select *Hyphen*, *Period*, *Space*, *Open parenthesis* and *Close parenthesis*.
29. In the first **Schema field name**, enter *Name* and select **Field is searchable**.

30. Select **(+) Add schema data field**.
31. In **Schema field name**, below **Schema field #2**, enter *Birthdate*.
32. Select **(+) Add schema data field**.
33. In **Schema field name**, below **Schema field #3**, enter *StreetAddress*.
34. Select **(+) Add schema data field**.
35. In **Schema field name**, below **Schema field #4**, enter *EmployeeID*.
36. Select **Field is searchable**.
37. Select **Save**.
38. Select **EDM sensitive info types** from the left pane.
39. Select **(+) Create EDM sensitive info type** to open the **EDM rule package** wizard.
40. On the **Define data store schema** page, select **Choose an existing EDM schema**.
41. Select **employeedb** and select **Add**.
42. Review the data store schema and select **Next**.
43. On the **Define patterns for this EDM sensitive info type** page, select **(+) Create pattern**.
44. On the **New pattern** right-side pane, in the Primary element field, select *EmployeeID*.
45. Below **Choose primary element's sensitive info type**, select **Choose sensitive info type**.
46. In the **Search** bar, enter *Contoso* and press the enter key.
47. Select **Contoso Employee IDs** and select **Done**.
48. Select **Done**.
49. Select **Next**.
50. In the **Character proximity** field, enter *100*.
51. Select **Next**.
52. In the **Name** field, enter *Contoso Employee EDM*.
53. In the **Description for admins** field, enter *EDM-based sensitive information type for employee personal information.*.
54. Select **Next**, review the settings and select **Submit**.
55. On the **Your EDM sensitive info type was created** page, select **Done**.
56. Leave the browser open with the Microsoft 365 Compliance Center.

You have successfully created a new EDM-based classification sensitive information type for identifying employee data from a database file source.

7.0.3 Task 3 – Create EDM-based classification data source

To associate the EDM-based classification with a database containing sensitive data, hashing and uploading the actual data for the sensitive information type via the EDM Upload Agent tool is required next.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, navigate to **https://go.microsoft.com/fwlink/?linkid=2088639** to access the EDM download agent.
3. Select **Run** to download and install the tool.
4. When the setup wizard opens in the background, select the installer from the taskbar.
5. In the **Microsoft Exact Data Match Upload Agent Setup**, select **Next**.
6. Select **I accept the terms in the License Agreement** and select **Next**.
7. Do not change the default **Destination Folder** path and select **Next**.

8. Select **Install** to perform the installation.
9. When the **User Account Control** window opens, select **Yes**.
10. When the installation finishes, select **Finish**.
11. Select the Windows symbol in the lower left to open the start menu, enter **Notepad** and select **Notepad** from the start menu.
12. Enter the following text to the first line in the notepad window:

    Name,Birthdate,StreetAddress,EmployeeID
13. Use enter and add the following text to the second line in the notepad window:

    Joni Sherman,01.06.1980,1 Main Street,CSO123456
14. Use enter and add the following text to the third line in the notepad window:

    Lynne Robbins,31.01.1985,2 Secondary Street,CSO654321
15. Select **File** and **Save As** to save the file.
16. Select **Documents** from the left side pane and enter the following in the **File name** field: *Employee-Data.csv*
17. Select the dropdown at **Save as type:** and select **All Files (.)**.
18. Select the dropdown at **Encoding:** and select **UTF-8** and select **Save**.
19. Close the Notepad window.
20. Select the windows symbol in the taskbar with the right mouse button and select **PowerShell** and run as administrator.
21. When the **User Account Control** window opens, select **Yes**.
22. Navigate to the EDM Upload Agent directory:

    cd "C:\Program Files\Microsoft\EdmUploadAgent"
23. Authorize with your Account to upload the database to your tenant by running the following:

    .\EdmUploadAgent.exe /Authorize
24. When the **Pick an account** window is displayed, sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
25. Download the database schema definition of the EDM-based classification sensitive information type by running the following script in PowerShell:

    .\EdmUploadAgent.exe /SaveSchema /DataStoreName employeedb /OutputDir "C:\Users\Admin\Documents"

    Note: If the last command fails, it possibly takes more time until the **EDM_DataUploaders** group membership is applied. It can take up to one hour until it is possible to download the schema file.
26. Hash the database file and upload it to the EDM-based classification sensitive information type by running the following script in PowerShell:

    .\EdmUploadAgent.exe /UploadData /DataStoreName employeedb /DataFile "C:\Users\Admin\Documents\Employee
    /HashLocation "C:\Users\Admin\Documents" /Schema "C:\Users\Admin\Documents\employeedb.xml"
27. Check the upload progress until the state changes to completed then run the following PowerShell command:

    .\EdmUploadAgent.exe /GetSession /DataStoreName employeedb
28. Close the PowerShell window.

You have successfully hashed and uploaded a database file for a EDM-based classification sensitive information type.

7.0.4 Task 4 – Create Keyword Dictionary

Several violations of personal information leakage happened when users sent out emails after colleagues reported on sick leave. When that happened the reason or disease was sent out.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. Select **Data classification** from the left-side pane and **Sensitive info types** from the top pane.
4. Select **(+) Create info type** to open the wizard for a new sensitive information type.
5. On the **Choose a name and description** page, enter *Contoso Diseases List* into **Name**.
6. Enter *List of possible diseases of employees.* to the **Description** field and select **Next**.
7. On the **Requirements for matching** page, select **(+) Add an element**.
8. Select the dropdown field below **Detect content containing** and select **Dictionary (Large keywords)**.
9. Select **(+) Add a dictionary** and **Create new keyword dictionaries** to open the Keyword dictionary pane.
10. Below **Choose a name for your keyword dictionary**, enter *Diseases Dictionary.*
11. Below **Enter the keywords, with each keyword on a separate line.**, enter the following keywords, each into a separate line:
    - *flu*
    - *influenza*
    - *cold*
    - *bronchitis*
    - *otitis.*
12. Select **Save**.
13. Below **Keyword dictionaries**. select **Diseases Dictionary** and select **Add**.
14. Below **Supporting elements**, select **Add supporting elements** and **Contains this keyword list** to add additional support for the keyword dictionary.
15. To the text box below **Keyword list**, enter the following keywords: *employee,absence,reason*
16. Increase the **Minimum Count** value to *2.*
17. Select **Next**, review the configuration and select **Finish**.
18. When the **compliance** window appears, select **No**.
19. Leave the browser window in the Microsoft 365 Compliance center open.

You have successfully created a new sensitive information type based on a keyword dictionary and added more keywords to decrease the false positive rate. Proceed with the next task.

7.0.5 Task 5 – Work with custom Sensitive Information Types

Custom Sensitive Information Types should always be tested before using them in policies otherwise data loss or leakage may occur due to a malfunctioning custom search pattern.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. Select the Windows symbol in the lower left to open the start menu, enter **Notepad** and select **Notepad** from the start menu.
3. Enter the following text to the notepad window:

   Employee Joni Sherman EMP123456 is on absence because of the flu/influenza.
4. Select **File** and **Save As**.
5. Select Documents in on the left-side pane.

6. In the **File name** field, enter *SickTestData* and select **Save**.
7. Close the Notepad window.
8. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
9. In the left navigation pane select **Data classification**, then select the **Sensitive info types** tab.
10. Select **Search** from the upper left side and enter *Contoso*.
11. Select **Contoso Employee IDs** to open the right side pane.
12. Select **Test type** from the right side pane.
13. On the **Upload file to test** page, select **Click to Browse**.
14. Select **Documents** from the left pane, select the file with the name *SickTestData* and select **Open**.
15. Select **Test** to start the analysis.
16. On the **Match results** page, review the found match.
17. Select **Finish** to close the test page.
18. Back on the **Data classification** page, select the Sensitive Information Type with the name **Contoso Diseases List**.
19. In the right side pane, select **Test type**.
20. On the **Upload file to test** page, select **Click to Browse**.
21. Select **Documents** from the left pane, select the file with the name *SickTestData* and select **Open**.
22. Select **Test** to start the analysis.
23. On the **Match results** page, review the found match.

You have successfully tested the two custom sensitive information types and validated the search pattern recognizes the desired patterns. You have finished the creation of sensitive information types and can proceed with the next exercise.

8 Proceed to Exercise 4

9 Exercise 4 - Manage Trainable Classifiers

The Contoso Ltd. tenant contains a SharePoint site collection with the name "Sales and Marketing" that will be used in the future to store several financial related documents and reports. Because of the nature of these documents, you need to create a trainable classifier to recognize and label these files. For this purpose, you will activate custom trainable classifiers and create a new one.

Important!: After activating trainable classifiers in a tenant, it takes between **7 and 14 days** before any custom trainable classifiers can be created. The button to create a new trainable classifier will not be available until the whole activation process is finished. Therefore, **you will only be able to perform task 1 now** and will need to wait until the trainable classifiers are available later within your tenant. These lab instructions are available online and your tenant should still be active.

9.0.1 Task 1 – Activate trainable classifiers

Before you can create custom trainable classifiers, you need to activate the feature in a tenant. To activate the Global Admin permissions are required, you will sign out of Joni Sherman's account and use the MOD Administrator to activate the feature first.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. Sign out of Joni Sherman's account by selecting the image in the upper right corner and select **Sign out**.
3. Close the browser window and open a new browser window.
4. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com**.

5. When the **Pick an account** page is displayed, select **Use another account** and sign in as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
6. Navigate to **Data Classification** from the left side navigation pane.
7. Select **Trainable classifiers** from the top pane.
8. When you see the **Get started with trainable classifiers** window, select **Start scanning process**.
9. Refresh the browser window.
10. Read the banner at the top part of the window with the message **To set you up for creating trainable classifiers, we're currently scanning your content locations to generate analytics that will help us learn what type of content is in your organization. This process will take 7 to 14 days to complete**
11. Leave the client open.

You have successfully activated trainable classifiers in your tenant. You will now need to wait between 7 and 14 days until the **Create trainable classifiers** button becomes available. If you are in a classroom setting and do not have 7 to 14 days to wait for Trainable Classifiers to complete processing, you may perform the remainder of the tasks in this exercise by logging into the tenant you were provided later when the Trainable Classifiers processing is complete. Your tenant should still be active.

9.0.2 Task 2 – Create a trainable classifier

After trainable classifiers have been activated successfully, the **Create trainable classifiers** button becomes available and it is possible to create a new custom classifier. In this task, Joni will create a new trainable classifier and select different SharePoint sites for identifying typical data created and stored by Contoso Ltd.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **MOD Administrator**.
2. Sign out of the MOD Administrator account by selecting the MA in the upper right corner and select **Sign out**.
3. Close the browser window and open a new browser window.
4. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com**.
5. When the **Pick an account** page is displayed, select **Use another account** and sign in as **Joni Sherman**. JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
6. Navigate to **Data Classification** from the left side navigation pane.
7. Select **Trainable classifiers** from the top pane.
8. Select **+ Create trainable classifier** to create a new classifier.
9. Enter the following information on the **Name and describe your trainable classifier** page:
   - **Name**: Contoso Company Data
   - **Description**: Trainable classifier for company data produced and stored by Contoso Ltd.
10. Select **Next**.
11. Select **Choose sites** to open the right side pane.
12. Select the following SharePoint sites:
    - **Communication site**
    - **News @ Contoso**
    - **Contoso Web 1**
    - **Brand**
    - **Digital Initiative Public Relations**
    - **Work @ Contoso**
    - **Sales and Marketing**
    - **Contoso Landings**
    - **Mark 8 Project Team**

- **HR**
- **Operations**
- **Retail**
- **PointPublishing Hub Site**
- **Team Site**
- **Leadership Team**
- **Community**
- **Give @ Contoso**
- **Benefits @ Contoso**
- **Learn @ Contoso**
- **Campaigns - Events**

13. Wait until the chosen site is shown in the list and select **Next**.
14. Review the settings and select **Create trainable classifier**.
15. When the message **Your trainable classifier was created** is shown, select **Done**.
16. Now you have to wait between 1 hour up to 24 hours to proceed forward. Leave the browser open.

The documents and files in the chosen SharePoint site are now being analyzed, which can take up to 24 hours.

9.0.3 Task 3 – Publish a trainable classifier

After the new trainable classifier was created and the initial analysis of the documents and files is done, the manual training process needs to be performed. In this task, Joni will start the calibration of the classifier to achieve the required accuracy for publishing.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In your browser window, you are in the Microsoft 365 compliance center at **Data classification** in the **Trainable classifiers** tab.
3. Select the trainable classifier with the name **Contoso Company Data** of the type **Custom** to open the detailed settings.
4. Review the **Details** tab on the right side, including the source site for the classifier, the number of processed items and the **Status**, which is in **Need test items**.
5. To add items for training the classifier, select **Add items to test** to open the right side selection pane.
6. In the **Choose sites with items to test** pane, select **+ Choose sites**.
7. Select the following SharePoint sites:
    - **Communication site**
    - **News @ Contoso**
    - **Contoso Web 1**
    - **Brand**
    - **Digital Initiative Public Relations**
    - **Work @ Contoso**
    - **Sales and Marketing**
    - **Contoso Landings**
    - **Mark 8 Project Team**
    - **HR**
    - **Operations**
    - **Retail**
    - **PointPublishing Hub Site**
    - **Team Site**
    - **Leadership Team**
    - **Community**
    - **Give @ Contoso**
    - **Benefits @ Contoso**
    - **Learn @ Contoso**
    - **Campaigns - Events**
8. Select **Add**.

9. Wait until the sites are shown in the list and select **Add**.
10. When the **Overview** section is updated, a new tab is shown in the top of the window.
11. Select **Tested items to review** from the top pane.
12. It will take between 15 to 30 minutes until first results are ready for review. Refresh the browser window if no files are shown in the list, until data is available.
13. Select the name of the first file from the list to open the preview window.
14. When the **Prediction** row is equal to **Match**, the file was identified as a match for the classifier. Below the preview window, a message **We predict this item "matched" this classifier.** is shown. Select **Match** to approve the automatic classification.
15. When the **Prediction** row is equal to **Not a match**, the file was identified not as a match for the classifier. Below the preview window, a message **We predict this item "does not match" this classifier.** is shown. Select **Not a match** to approve the automatic classification.
16. Proceed with all items in the list and approve the automatic classification. After all items have been reviewed, select **Overview** from the top pane and **Tested items to review** again, to load the next set of items for review.
17. For each 30 reviewed items an **Auto-retrain performed** window is shown. Select **OK** and proceed with the previous steps, until no items for review are left.
18. After sufficient items are reviewed, the **Publish** button in the upper right gets available. Select it as soon it is available.
19. In the **Publish classifier** window, select **Yes** to publish the classifier.
20. When the right side pane with **Your trainable classifier has been published** is displayed, the trainable classifier was successfully published.
21. Close the right side pane with the **X** in the upper right.
22. Back at the main site, the custom classifier was moved to **Published** and the **Status** has been changed to **Ready to use**.
23. Leave the browser window open.

You have successfully created, trained, and published a custom trainable classifier that matches the files stored on the existing SharePoint sites of Contoso Ltd.

10 Proceed to Exercise 5

11 Exercise 5 - Manage Sensitivity Labels

In this lab you will assume the role of Joni Sherman, a System Administrator for Contoso Ltd. Your organization is based in Rednitzhembach, Germany and is currently implementing a sensitivity plan to ensure that all employee documents in the HR department have been marked with a sensitivity label as part of your organizations information protection policies.

11.0.1 Task 1 Enable support for sensitivity labels

In this task, you will install the MSOnline module and the SharePoint Online PowerShell module and enable support for sensitivity labels on your tenant.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. Open an elevated PowerShell window by selecting the start menu with the right mouse button and then select **Windows PowerShell** and run as administrator.
3. Confirm the **User Account Control** window with **Yes** and press Enter.
4. Enter the following cmdlet to install the latest MS Online PowerShell module version:

   Install-Module -Name MSOnline
5. Confirm the Untrusted repository security dialog with **Y** for Yes and press Enter.

6. Enter the following cmdlet to install the latest SharePoint Online PowerShell module version:

   Install-Module -Name Microsoft.Online.SharePoint.PowerShell

7. Confirm the Untrusted repository security dialog with **Y** for Yes and press Enter.
8. Enter the following cmdlet to connect to the MS Online service:

   Connect-MsolService

9. In the **Sign in to your account** form, sign in as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
10. After signing in, select the PowerShell window.
11. Enter the following cmdlet to get the domain:

    $domain = get-msoldomain

12. Enter the following cmdlet to create the SharePoint admin url:

    $adminurl = "https://" + $domain.Name.split(".")[0] + "-admin.sharepoint.com"

13. Enter the following cmdlet to sign in to the SharePoint Online admin center:

    Connect-SPOService -url $adminurl

14. In the **Sign in to your account** form, sign in as **MOD Administrator**. admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
15. After signing in, select the PowerShell window.
16. Enter the following cmdlet to enable support for sensitivity labels:

    Set-SPOTenant -EnableAIPIntegration $true

17. Confirm the changes with **Y** for Yes and press Enter.
18. Close the PowerShell window.

You have successfully enabled support for sensitivity labels with Teams and SharePoint sites.

11.0.2 Task 2 – Create Sensitivity Labels

In this task, your HR department has requested a sensitivity label to apply to HR employee documents. You will create a sensitivity label for Internal documents and a sublabel for the HR department.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
3. In the **Compliance Center**, in the left navigation pane, select **... Show all** and then select **Information protection**.
4. On the Information protection page, select **+ Create a label**.
5. The **New sensitivity label** wizard will start. On the **Name & description** page for the **Name**, **Description for admins** and **Description for users**, enter the following information:
   - **Name**: Internal
   - **Display name**: Internal
   - **Description for users**: Internal sensitivity label.
   - **Description for admins**: Internal sensitivity label.
6. Select **Next**.
7. On the **Define the scope for this label** page, select the option **Files & emails**.
8. Select **Next**.

9. On the **Choose protection settings for files & emails** page, select **Next**.
10. On the **Auto-Labeling for files and emails** page, select **Next**.
11. On the **Define protection settings for groups & sites** page, select **Next**.
12. On the **Auto-labeling for database columns** page, select **Next**.
13. On the **Finish** page, select **Create label**.
14. The label will be created and when complete a message will display: **Your label was created**
15. Select **Done**.
16. On the Information protection page, highlight (without selecting) the newly created **Internal** label and select the **....**
17. Select the **+ Add sub label** from the drop-down menu.
18. The **New sensitivity label** wizard will start. On the **Name & description** page for the **Name**, **Description for admins** and **Description for users**, enter the following information:

- **Name**: Employee data (HR)
- **Display name**: Employee data (HR)
- **Description for users**: This HR label is the default label for all specified documents in the HR Department.
- **Description for admins**: This label is created in consultation with Ms. Jones (Head of HR department). Contact her, when you want to chance settings of the label.

19. Select **Next**.
20. On the **Scope** page, select the option **Files & emails**.
21. Select **Next**.
22. On the **Files & email** page, select the **Encrypt files and emails** option
23. Select **Next**.
24. Select **Configure encryption settings**.
25. Enter the following information into the encryption settings:

- **Assign permissions now or let users decide?**: Assign permissions now
- **User access to content expires**: Never
- **Allow offline access**: Only for a number of days
- **Users have offline access to the content for this many days**: 15

26. Select the **Assign permissions** link
27. On the Assign permissions side menu, select the **Add any authenticated users**.
28. Select **Save**.
29. On the **Encryption** page, select **Next**.
30. On the **Auto-Labeling** page, select **Next**.
31. On the **Groups & sites** page, select **Next**.
32. On the **Azure Purview assets (preview)** page, select **Next**.
33. On the **Finish** page, select **Create label**.
34. The label will be created and when complete a message will display **Your label was created**.
35. Select **Done**.

You have successfully created a sensitivity label for your organizations internal policies and a sensitivity sublabel for the Human Resources (HR) department.

11.0.3 Task 3 – Publish Sensitivity Labels

You will now publish the Internal and HR sensitivity label so that the published sensitivity labels will be available for the HR users to apply to their HR documents.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**. Sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **... Show all** and then select **Information protection**.
4. On the **Information protection** page, select **Publish labels**.
5. The publish sensitivity labels wizard will start.
6. On the **Choose labels to publish** page, select the **Choose sensitivity labels to publish link**.
7. A side bar called **Sensitivity labels to publish** will appear on the right.
8. Select the **Internal** and **Internal/Employee Data (HR)** checkboxes.
9. Select **Add**.
10. On the **Choose labels to publish** page, select **Next**.
11. On the **publish to users and groups page**, select **Next**.
12. On the **Policy settings** page, select **Next**.
13. On the **Name & Description** page, enter the following information:

- **Name**: Internal HR employee data
- **Enter a description for your sensitivity label policy**: This HR label is to be applied to internal HR employee data.

14. Select **Next**.
15. On the **Review your settings** page, select **Submit**.
16. The policy will be created and when complete a message will display **New policy created**.
17. Select **Done**.

You have successfully published the Internal and HR sensitivity labels. Note that it can take up to 24 hours for changes to replicate to all users and services.

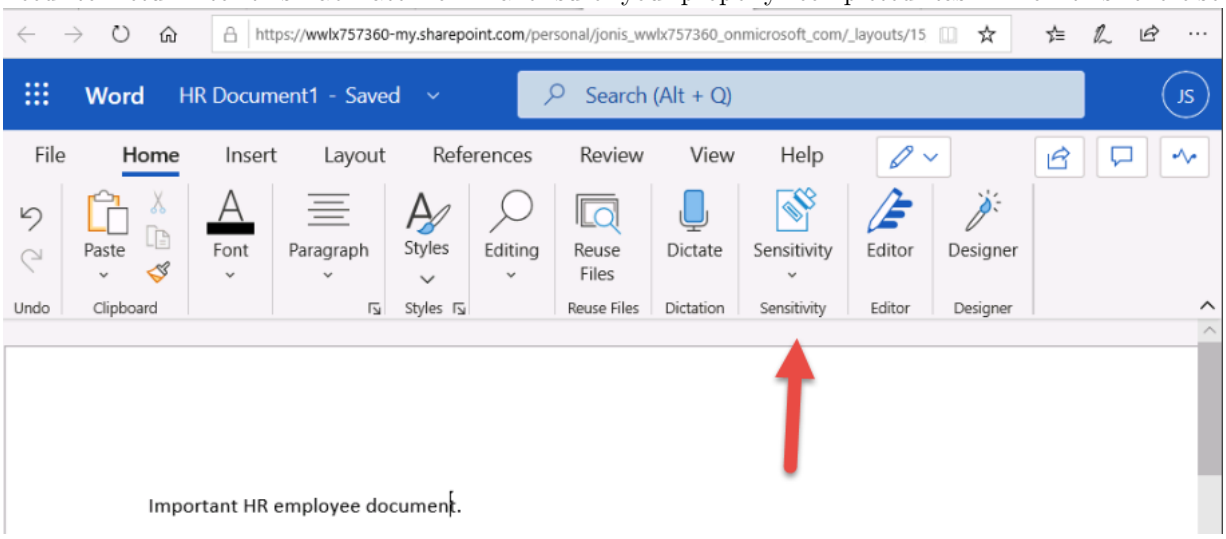
11.0.4 Task 4 – Work with Sensitivity Labels

In this task, you will create sensitivity labels in Word and Outlook emails. The document created will be stored in OneDrive and sent to an HR employee via email.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. Select the address bar and navigate to **https://portal.office.com**.
3. If a **Get your work done with Office 365** message is shown, close it with the **X** in the upper right corner.
4. Select the Microsoft Word symbol from the left side pane to open Word Online.
5. Select **New blank document** to create a new document.
6. If a **Your privacy options** message is shown, close it with selecting **Close**.
7. Enter the following contents into the word document:

- Important HR employee document.

8. Select **Sensitivity** from the top pane top open the dropdown menu. Select **Internal** to apply the label. Be aware, the script you ran in task 1 of this exercise activated sensitivity labels in Word for your tenant. It can sometimes take an hour for that activation to be realized in Microsoft Word online. If you don't see the Sensitivity label menu in Word, you may need to return to this lab later or make sure you properly completed task 1 of this exercise.



9. Select the **Document - Saved** in the upper left of the window, enter **HR Document** as the File Name and press Enter key.
10. Close the tab to return to the Word Online tab. Select the Outlook symbol from the left side pane to open Outlook on the web.
11. If a welcome message is shown, close it with selecting the **X**.
12. In Outlook on the web, select **New message** from the upper left of the window.
13. In the To field enter the name: **Allan** and select **Allan Deyoung** from the drop-down list.
14. In the subject field, enter: **Employee data for HR**
15. Within the email message (the large content panel at the bottom of the page), insert the following message:

    Dear Mr. Deyoung,

    Please find attached the important HR employee document.

    Kind regards,

    Joni Sherman
16. Select the paperclip symbol from the bottom menu and select the **HR Document.docx** below **Suggested attachments** to attach the document.
17. Select **Send** to send out the email message with attached document.
18. Leave the browser window open.

You have successfully created an HR Word document with a sensitivity label, which was saved onto your OneDrive. You then emailed to document to an HR staff member.

You have successfully created an HR Word document with a sensitivity label, which was saved onto your OneDrive. You then emailed to document to an HR staff member where the email was also set with a sensitivity label.

11.0.5 Task 5 – Configure Auto Labeling

In this task, you will create a Sensitivity Label that will auto label documents and emails found to contain information related to the European General Data Protection Regulation (GPDR).

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.

2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman**.
3. In the **Compliance Center**, in the left navigation pane, select **... Show all** and then select **Information protection**.
4. On the Information protection page, highlight (without selecting) the existing **Internal** label, and select the three dots.
5. Select the **+ Add sub label** menu item.
6. The **New sensitivity label** wizard will start. On the **Name & description** page, enter the following information:
   - **Name**: GDPR Germany
   - **Display name**: GDPR Germany
   - **Description for users**: This document or email contains data related to the European General Data Protection Regulation (GPDR) for the region Germany.
   - **Description for admins**: This label is auto applied to German GDPR documents.
7. Select **Next**.
8. On the **Scope** page, select the option **Files & emails**.
9. Select **Next**.
10. On the **Files & email** page, select **Next**.
11. On the **Auto-Labeling** page, set the **Auto-labeling for files and emails** to enabled.
12. In the **Detect content that matches these conditions** section, select **+Add condition** and then select **Content contains**.
13. In **Content contains** section select the **Add** text and then select **Sensitive info types**.
14. A **Sensitive info types** panel will be displayed on the right.
15. In the **Search for sensitive info types** search panel, enter the following information:

    German
16. Press the enter button, the results will display sensitivity info types related to Germany.
17. Press the **Select all** check box.
18. Select **Add**.
19. Select **Next**.
20. On the **Groups & sites** page, select **Next**.
21. On the **Azure Purview assets (preview)** page, select **Next**.
22. On the **Finish** page, select **Create label**.
23. The label will be created and when complete a message will display: **Your label was created**.
24. Select **Done**.
25. On the **Information protection** page, select **Publish labels**.
26. The Publish sensitivity labels wizard will start.
27. On the **Choose labels to publish** page, select the **Choose sensitivity labels to publish link**.
28. A side bar called **Sensitivity labels to publish** will appear on the right.
29. Select the **Internal** and **Internal/GDPR Germany** checkbox.
30. Select **Add**.
31. On the **Choose labels to publish** page, select **Next**.
32. On the **Publish to users and groups page**, select **Next**.
33. On the **Policy settings** page, select **Next**.
34. On the **Name & Description** page, enter the following information:

- **Name**: GDPR Germany policy
- **Enter a description for your sensitivity label policy**: This auto apply sensitivity labels policy is for the GDPR region of Germany.

34. Select **Next**.
35. On the **Review your settings** page, select **Submit**.
36. The policy will be created and when complete a message will display, **New policy created**.
37. Select **Done**.

You have successfully created and published an auto apply sensitivity label for GDPR documents in the region Germany.

Be aware that it can take up to 24 hours for auto applied sensitivity labels to be applied, this duration will be longer when applied to more than 25,000 documents (that is, the daily limit).

11.1 You have completed the lab.

12 Exercise 1 - Manage DLP Policies

You are Joni Sherman, the newly hired Compliance Administrator for Contoso Ltd. tasked to configure the company's Microsoft 365 tenant for data loss prevention. Contoso Ltd. is a company that offers driving instruction in the United States and you need to make sure that sensitive customer information does not leave the organization.

12.0.1 Task 1 – Create a DLP policy in test mode

In this exercise, you will create a Data Loss Prevention policy in the Compliance Center to protect sensitive data from being shared by users. The DLP Policy that you create will inform your users if they want to share content that contains Credit Card information and allow them to provide a justification for sending this information. The policy will be implemented in test mode because you do not want the block action to affect your users yet.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman**. sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Data loss prevention**.
4. In the **Data loss prevention** window select the **Policies** tab, and then select **+Create policy** to start the wizard for creating a new data loss prevention policy.
5. On the **Start with a template or create a custom policy** page, you want to select **Custom** in the left pane and **Custom policy** in the middle pane; however, by default, both these options should already be selected (if not, then select them now), select **Next**.
6. In the **Name your DLP policy** page, type *Credit Card DLP Policy* in the **Name** field and *Protect credit card numbers from being shared.* in the **Description** field. Select **Next**.
7. On the **Choose locations to apply the policy** page, select only the **Teams chat and channel messages** option to be enabled and then select **Next**.
8. On the **Define policy settings** page, the option **Create or customize advanced DLP rules** needs to be selected, which it should be by default. Select **Next**.
9. On the **Customize advanced DLP rules** page, select **+ Create rule**.
10. On the **Create rule** page, type *Credit card information* in the **Name** field.
11. Select **+ Add Condition** and then select **Content contains** from the dropdown menu.
12. On the **Create rule** page, in the new **Content contains** area, select **Add** and select **sensitive info types** from the dropdown menu.
13. On the **Sensitive info types** page, select **Credit Card Number** and select **Add**.

14. On the **Create rule** page, select **+ Add condition** and select **Content is shared from Microsoft 365** from the dropdown menu.
15. In the **Content is shared from Microsoft 365** section, select the **Only with people inside my organization** option, which should be selected by default.
16. On the **Create rule** page, select **+ Add an action** and select **Restrict access or encrypt the content in Microsoft 365 locations**.
17. Check the box in front of **Restrict access or encrypt the content in Microsoft 365 locations** and then select **Block Everyone. Only the content owner, last modifier, and site admin will continue to have access**.
18. On the **Create rule** page, in the **User Notifications** section, select the switch to put it in the **On** position.
19. On the **Create rule** page, in the **User Overrides** section, select the switch to put it in the **On** position and select the **Require a business justification to override** option.
20. In the **Incident reports** section, in the **Use this severity in admin alerts and reports** dropdown, select **Low**.
21. In the **Incident reports** section, select the **Send an alert to admins when a rule match occurs.** switch to put it in the **On** position and review the options. The default settings will notify the user creating the policy.
22. Select **Save**, then select **Next**.
23. On the **Test or turn on the policy** page select **I'd like to test it out first** and select **Show policy tips while in test mode**.
24. Select **Next** and review the policy configuration.
25. Select **Submit** to create the policy.

You have now created a DLP policy that scans for Credit Card numbers in Microsoft Teams chats and channels and notifies allows users to provide a business justification to override the policy.

12.0.2 Task 2 - Modify a DLP policy

In this task, you will modify the existing DLP policy you created in the previous to also scan e-mails for Credit Card information and inform users if they want to share this content in an e-mail.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Data loss prevention**.
4. In the **Data loss prevention** window select the **Policies** tab, then select the policy named **Credit Card DLP policy** and then select **Edit policy** to open the policy wizard.
5. On the **Name your DLP policy** page, select **Next**.
6. On the **Choose locations to apply the policy** page, enable the **Exchange email** option and then select **Next** until you reach the **Review your policy and create it** page.
7. Select **Submit** to apply the change you made in the policy.

You have now modified an existing DLP policy and changed the locations it scans for content.

12.0.3 Task 3 - Create a DLP policy in PowerShell

In this task, you use PowerShell to create a DLP policy to protect driver's license numbers of your customers and prevent them from being shared in Exchange. Users will be informed that they are attempting to share sensitive data and are blocked from sending the e-mail if it includes driver license numbers.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.

2. In the start menu, select **Windows PowerShell**.
3. In the **PowerShell** window, type **Connect-IPPSSession** and then sign in as **Joni Sherman**. sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
4. Enter the following command into PowerShell to create a DLP policy that scans all Exchange mailboxes:

   New-DlpCompliancePolicy -Name "Driver's License DLP Policy" -Comment "This policy blocks sharing of Driver's License Numbers." -ExchangeLocation All
5. Enter the following command into PowerShell to add a DLP rule to the DLP policy you created in step 4:

   New-DlpComplianceRule -Name "Driver's License Rule" -Policy "Driver's License DLP Policy" -BlockAccess $true -ContentContainsSensitiveInformation @{Name="U.S. Driver's License Number";minCount="1";minconfidence="75"}
6. Use the following command to review the **Driver's License DLP Policy**:

   Get-DLPComplianceRule -Identity "Driver's License Rule"

You have now created a DLP Policy that scans for Driver's license numbers in Exchange by using PowerShell.

12.0.4 Task 4 - Activate a policy in test mode

In this task, you will activate the credit card information DLP policy you created in test mode so it enforces its protective actions.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Data loss prevention**.
4. In the **Data loss prevention** window select the **Policies** tab, and then select the policy named **Credit Card DLP policy** and then select **Edit policy** to open the policy wizard.
5. Select **Next** until you reach the **Test or turn on the policy** page and then select **Yes, turn it on right away**.
6. Select **Next** and then **Submit** to activate the policy.

You have successfully activated the DLP Policy. If the policy detects an attempt to share credit card information, it will now block the attempt and allow the users to provide a business justification to override the block action.

12.0.5 Task 5 - Modify policy priority

After creating two DLP policies, you want to make sure that the more restrictive policy is processed at a higher priority than the less restrictive policy. For this reason, you want to move the Driver's license policy into the higher priority.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Data loss prevention**.
4. In the **Data loss prevention** window select the **Policies** tab, select the three vertical dots next to the **Driver's License DLP Policy** to open the **Actions** selection.
5. Select **Move to top**.
6. In the **Data loss prevention** window, select **Refresh** and then review the priority in the **Order** column of the policy table.

You successfully modified the priority of your DLP policies. If both policies match the same content the action of the higher priority policy will be enforced.

12.0.6 Task 6 - Enable file monitoring in Microsoft Cloud App Security (MCAS)

You want to use file policies in Microsoft Cloud App Security to protect files in your OneDrive for Business and SharePoint Online locations. Before you can create a file policy, you need to enable file monitoring so MCAS can scan files in your organization.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://portal.cloudappsecurity.com** and log into the Cloud App Security Portal as **MOD Administrator**. admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
3. In the top-right corner, next to your profile information, select the **Settings** cogwheel and select **Settings** in the dropdown menu.
4. On the **Settings** page, under **Information Protection** select **Files**.
5. Select the **Enable file monitoring** checkbox and then select **Save**.

You successfully enabled file monitoring in MCAS and can now scan files for sensitive content using file policies.

12.0.7 Task 7 - Create File Policy for MCAS

In this task, you want to create a file policy in Microsoft Cloud App Security to scan files in OneDrive for Business and SharePoint Online and automatically quarantine files containing credit card information if they are shared.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
2. In **Microsoft Edge**, the Cloud app security portal tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://portal.cloudappsecurity.com**.
3. In the **Microsoft Cloud App Security Portal**, in the left navigation pane, expand **Control** and select **Policies**.
4. On the **Policies** page, expand **Create Policy** and then select **File policy**.
5. On the **Create file policy** page, type *Credit Card Information for files* in the **Policy name** field and *Protect credit card numbers from being shared in files.* in the **Description** field.
6. Keep the **Policy Severity** on **Low** and make sure the **Category** is set to **DLP**. For a file policy, this should be the default.
7. In the **Create filters for the files this policy will act on** area, expand the dropdown menu **Public (Internet), External, Public** and add **Internal**.
8. In the **Inspection Method** dropdown menu, select **Data Classification Service**.
9. In the **Choose inspection type...** dropdown menu, select **sensitive information type...**.
10. In the **Select a sensitive information type** dialog, select **Credit Card Number**, then select **Done** in the upper right corner.
11. Under **Alerts**, check the **Create an alert for each matching file** checkbox and review your options. Keep the settings at the default.
12. In the **Governance actions** section, expand **Microsoft OneDrive for Business** and select **Put in user quarantine**.
13. In the **Governance actions** section, expand **Microsoft SharePoint Online** and select **Put in user quarantine**.
14. Select **Create**.

You have now created a file policy that will continuously scan files saved in OneDrive for Business and SharePoint for credit card information and quarantine them if they are shared inside your organization.

12.0.8 Task 8 - Create a DLP Policy for PowerPlatform

Your company uses PowerAutomate flows to share data between SharePoint Online and SalesForce. In this task, you will create a DLP policy for PowerPlatform that allows your existing flows to keep working, but prevents the creation of flows that will share data between SharePoint Online and Apps defined as non-business.

1. Log into the Client 2 VM (LON-CL1) as the **lon-cl2\admin** account.
2. In **Microsoft Edge**, navigate to **https://admin.powerplatform.microsoft.com** and log into the Power Platform Admin Center as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
3. In the **Power Platform Admin Center**, in the left navigation pane, select **Data policies**.
4. On the **Data policies** page, select **+ New Policy**.
5. On the **Name your policy** page, type *Tenant-wide SharePoint Policy*, then select **Next**.
6. On the **non-business** tab, select **SharePoint** and **Salesforce**, then select **Move to Business** at the top of the page.
7. Select **Next**.
8. On the **Define scope** page, select **Add all environments**, then select **Next**.
9. On the **Review and create policy** page, review your policy settings, then select **Create Policy**.

You have now created a PowerPlatform DLP policy that prevents users from creating flows involving a SharePoint Online Connector and any connector that is not SalesForce.

13 Proceed to Exercise 2

14 Exercise 2 - Manage Endpoint DLP

You are Joni Sherman, the newly hired Compliance Administrator for Contoso Ltd. tasked to configure the company's Microsoft 365 tenant for data loss prevention. Contoso Ltd. is a company offering driving instruction in the United States and you need to make sure that sensitive customer information does not leave the organization. For this reason, you decide to not only implement Microsoft 365 DLP policies but extend this protection to devices in your organization.

14.0.1 Task 1 – Enable device onboarding

In this task, you will turn on device onboarding for your organization.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**. sign in as JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center** in the left navigation pane, select **Settings** and select **device onboarding**.
4. Select **Turn on device onboarding**.
5. Accept the **Turn on device onboarding** dialog by selecting **OK**.
6. Accept the **Device monitoring is being turned on** dialog by selecting **OK**.

You have now enabled device onboarding and can start to onboard Windows 10 devices to be protected with Endpoint DLP policies. The process of enabling the feature may take up to 30 minutes.

14.0.2 Task 2 - Onboard a device to Endpoint DLP

In this task, you will use the local script option to onboard a Windows 10 device to allow it to be protected by Endpoint DLP policies.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **MOD Administrator**.
3. In the **Compliance Center** in the left navigation pane, select **Settings** and select **device onboarding**.
4. On the **Device onboarding** page, in the navigation pane, select **Onboarding**.
5. In the **Deployment Method** dropdown menu, select **Local Script (For up to 10 machines)** and select **Download package**.
6. In the download dialog, select **Save**, then select **Open folder**.
7. Extract the ZIP-file to the **Desktop** of LON-CL1. You should see a script named **DeviceCompliance-LocalOnboardingScript.cmd**.
8. In the start menu, search for **Command Prompt** and right-click the file and select **Run as Administrator**. You might encounter a Windows SmartScreen warning box, if you do choose **Run anyway**. If you encounter the User Account Control window select **Yes** to all this script to make changes to your PC.
9. In the **Command Prompt** screen type **Y** to confirm, and then press Enter.
10. When the script completes **Press any key to continue**. It can take a minute to complete the onboarding.
11. Open the start menu then find and select **Access work or school**.
12. In the **Access work or school** window, select **+ Connect**.
13. In the **Set up a work or school account** dialog, select the **Join this device to Azure Active Directory** link and sign in as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
14. In the **Make sure this is your organization** dialog, review the tenant url and select **Join**. If your device fails to join you may need to troubleshoot your Azure AD configuration join settings. Do the following to ensure devices may be joined: 1. Open a new browser tab and go to the Azure Portal https://portal.azure.com 1. Sign in as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com 1. Select **Manage Azure Active Directory**. 1. Select **Devices** 1. Select **Device settings** 1. Scroll-down until you see **Maximum number of devices per user** change the value to **20 (Recommended)** 1. Once you have updated the setting re-try to connect your device.
15. Once your device has connected select **Done**.
16. Restart the Client 1 VM (LON-CL1).

You have successfully onboarded a device and joined it to Azure AD to be protected by Endpoint DLP policies.

14.0.3 Task 3 - Create Endpoint DLP policy

In this exercise, you will create a Data Loss Prevention policy in the Compliance Center to protect sensitive data residing on Windows 10 devices in your organization. The DLP Policy that you create will block your users if they want to copy content from documents that contain Credit Card information.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Data loss prevention**.
4. In the **Data loss prevention** window select the **Policies** tab, and then select **+Create policy** to start the wizard for creating a new data loss prevention policy.

5. On the **Start with a template or create a custom policy** page, you want to select **Custom** in the left pane and **Custom policy** in the middle pane; however, by default, both these options should already be selected (if not, then select them now), select **Next**.
6. In the **Name your DLP policy** page, type *Credit Card Endpoint DLP Policy* in the **Name** field and *Protect credit card numbers from being shared on Endpoints.* in the **Description** field. Select **Next**.
7. On the **Choose locations to apply the policy** page, select only the **Devices** option and then select **Next**.
8. On the **Define policy settings** page, the option **Create or customize advanced DLP rules** needs to be selected, which it should be by default. Select **Next**.
9. On the **Customize advanced DLP rules** page, select **+ Create rule**.
10. On the **Create rule** page, type **Endpoint Credit Card information**.
11. Select **+ Add Condition** and then select **Content contains** from the dropdown menu.
12. On the **Create rule** page, in the new **Content contains** area, select **Add** and select **sensitive info types** from the dropdown menu.
13. On the **Sensitive info types** page, select **Credit card number** and select **Add**.
14. On the **Create rule** page, select **+ Add an action** and select **Audit or restrict activities on Windows devices**.
15. Uncheck every checkbox except **Copy to Clipboard**.
16. In the dropdown menu behind **Copy to Clipboard** select **Block**.
17. On the **Create rule** page, in the **User Notifications** section, select the switch to put it in the **On** position.
18. In the **Incident reports** section, in the **Use this severity in admin alerts and reports** dropdown, select **Low**.
19. In the **Incident reports** section, select the **Send an alert to admins when a rule match occurs.** switch to put it in the **On** position and review the options. The default settings will notify the user creating the policy.
20. Select **Save**, then select **Next**.
21. On the **Test or turn on the policy** page select **Yes, turn it on right away**.
22. Select **Next** and review the policy configuration.
23. Select **Submit** to create the policy.

You have successfully activated the DLP Policy. If the policy detects an attempt to copy content from a file containing credit card information, it will now block the attempt and inform your user.

14.0.4 Task 4 - Configure Endpoint DLP Settings

In this task, you will configure a file path exclusion to a folder on your Windows 10 devices to make sure that the content of this folder is not monitored by the Endpoint DLP policy you created.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Data loss prevention**.
4. In the **Data loss prevention** window, select the **Endpoint DLP settings** tab.
5. In the **Endpoint DLP settings** tab, expand the **file path exclusions** area and select **+ Add file path exclusion**.
6. In the **Enter a path to exclude** field, type *C:\FilePathExclusionTest*, then select **+**.
7. Select **Add**.

You have now configured a general exception to your Endpoint DLP policies. Every policy you create will ignore content in the folder you configured.

15 Proceed to Exercise 3

16 Exercise 3 - Manage DLP reports

You are Joni Sherman, the Compliance Administrator for Contoso Ltd. tasked to configure the company's Microsoft 365 tenant for data loss prevention. Contoso Ltd. is a company offering driving instruction in the United States and you need to make sure that sensitive customer information does not leave the organization. You are informed that a new compliance officer will help you review DLP reports.

16.0.1 Task 1 - Grant access to DLP reports

In this exercise, you will grant the new compliance officer access to the DLP reports. As a non-technical user this compliance officer will only read reports and not change the DLP configuration.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://protection.office.com** and log into the Security & Compliance Center as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
3. In the left navigation pane, select **Permissions** and then select the **Security Reader** role.
4. In the role overview pane, select **Edit** in the **Members** category.
5. Select **Choose Members** and then select **+ Add**.
6. Search for **Megan Bowen** and select the checkbox in front of their name, then select **Add**.
7. Review the changes to the member list and then select **Done**.
8. Select **Save**.

You have now granted the new compliance officer access to the DLP reports in the Compliance Center.

16.0.2 Task 2 - Test access to DLP reports

In this task, you will test that the access to the DLP reports you granted in Task 1 is applied correctly.

1. Log into the Client 2 VM (LON-CL2) as the **lon-cl2\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Megan Bowen** MeganB@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Megan's password should be provided by your lab hosting provider.
3. In the left navigation pane, select **Reports** and observe your access to the Reports Dashboard.

You now verified that the access has been configured and the new compliance officer can view reports in the Compliance Center.

16.1 You have completed the lab.

17 Exercise 1 - Configure Retention Policies

In this exercise, you will assume the role of Joni Sherman, a System Administrator for Contoso Ltd. Your organization is based in Texas and wants to implement retention policies to adhere to state laws, which stipulates that records may be deleted after three years without constituting an offense.

In order to adhere to this law your organization has created a retention plan to retain all items in the organization for three years.

17.0.1 Task 1 – Create company-wide Retention Policy

In this exercise you will create a company-wide retention policy, apply a retention period, and set the locations that the policy will be applied to.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Retention**.
4. On the **Information Governance** page, in the **Retention** tab, select **+ New retention policy**.
5. On the **Name your policy page**, for the **Name** and **Description** enter the following information:
   - Name: Company Wide
   - Description: All locations except for teams
6. Select the **Next** button.
7. In the **Choose locations to apply the policy** area make sure Exchange Email, SharePoint sites, OneDrive accounts, and Microsoft 365 Groups are selected and then select **Next**.
8. On the **Retention settings** page, for the **Retain items for a specific period** section, enter the following information:
   - Retain items for a specific period: Three Years
   - **Start the retention period based on**: When it was last modified
9. Select the **Next** button.
10. On the **Review your settings** page, select the **Submit** button

You have successfully created a retention policy for the Exchange email, Microsoft 365 groups, OneDrive, and SharePoint sites locations. This retention policy will retain items in these locations for three years from when the item was last modified date. This can take up to 24 hours to be apply in your tenant.

17.0.2 Task 2 – Create location-based Retention Policies with Filter

You will now create a retention policy for the Teams locations. As Teams channels can contain documents, they will all be retained. Your organization has decided that a limited number of users are required to have their Team chats require a retention period.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Retention**.
4. On the **Information Governance** page, in the **Retention** tab, select **+ New retention policy**.
5. On the **Name your policy** page, for the **Name** and **Description** enter the following information:
   - **Name**: Teams Retention
   - **Description**: Retention for Teams locations
6. Select the **Next** button.
7. On the **Locations** page, enter the following settings
   - **Exchange email** location - **Status**: Disable
   - **SharePoint sites** location - **Status**: Disable
   - **OneDrive accounts** location - **Status**: Disable
   - **Office 365 groups** location - **Status**: Disable
   - **Skype for Business** location - **Status**: Disable

- **Exchange public folders** location - **Status**: Disable
- **Teams channel messages** location – **Status**: Enable
- **Teams chats location** – **Status**: Enable

8. For the Teams chat location, select the **Edit** text link in the **Included** column
9. On the **Edit locations** page, in the Teams chats window, add the users:
   - Adele Vance
   - Pradeep Gupta
10. Select the **Done** button
11. On the locations page, a notification will display: **2 users** have been added
12. Select the **Next** button.
13. On the **Retention settings** page, for the **Retain items for a specific period** section, enter the following information:
    - Retain items for a specific period: 3 Years
    - **Start the retention period based on**: When it was last modified
14. Select the **Next** button.
15. On the **Review your settings** page, select the **Submit** button.

You have successfully created a retention policy for the Teams locations. You set a retention period of three years for all Teams channel locations. You have set a filter for Teams Chat locations to apply only to specific users.

17.0.3 Task 3 – Create Retention Policy via PowerShell

You will create the same retention policies with PowerShell

1. Log into the Client 2 VM (LON-CL1) as the **lon-cl1\admin** account.
2. Open an elevated PowerShell window by selecting the Windows button with the right mouse button and then select **Windows PowerShell (Admin)** select **Yes** if confronted with a User Account Control window.
3. Connect to the Security & Compliance Center in your tenant with the following cmdlet:

   Connect-IPPSSession
4. If prompted with a sign in dialog box, sign in as **MOD Administrator** admin@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Admin's password should be provided by your lab hosting provider.
5. Run the following cmdlet to create the first retention policy for all locations except teams:

   New-RetentionCompliancePolicy -Name "Company Wide PS" -ExchangeLocation All -ModernGroupLocation All -PublicFolderLocation All -SharePointLocation All -OneDriveLocation All
6. Run the following cmdlet to set the retention period, using days as units based the on the date modified:

   New-RetentionComplianceRule -Name "Company Wide PS Rule" -Policy "Company Wide PS" -RetentionDuration 1095 -ExpirationDateOption ModificationAgeInDays -RetentionComplianceAction Keep
7. Run the following cmdlet to create the second retention policy for Teams locations:

   New-RetentionCompliancePolicy -Name "Teams Retention PS" -TeamsChannelLocation All -TeamsChatLocation "Adele Vance", "Pradeep Gupta"
8. Run the following cmdlet to set the retention period, using days as units:

   New-RetentionComplianceRule -Name "Teams Retention PS Rule" -Policy "Teams Retention PS" -RetentionDuration 1095 -RetentionComplianceAction Keep

You have successfully created retention policies through PowerShell with a retention period of three years.

18 Proceed to Exercise 2

19 Exercise 2 - Implement Retention Labels

In this exercise, you will assume the role of Joni Sherman, a System Administrator for Contoso Ltd. Your organization is based in Sudbury England and has legal obligations to retain finance documents.

Your finance department has created a retention plan to set retention labels on documents for Value Added Tax (VAT) returns with supporting documents and Credit Card receipts.

19.0.1 Task 1 – Create Retention Labels

In this task, you will create a retention label that can be assigned to documents and emails that contain VAT returns and a retention label that can be applied to Credit Card receipts.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Retention**.
4. On the Information Governance Page, select **Labels** tab.
5. Select the **+ Create a label** button
6. On the **Name your retention label page** for the **Name**, **Description for admins** and **Description for users**, enter the following information:
   - **Name**: VAT Returns and supporting documents
   - **Description for admins**: VAT returns with seven-year retention.
   - **Description for users**: Assign this label to VAT Documents to ensure they are retained for the legal period of seven years.
7. Select the **Next** button.
8. On the **Retention settings** page, enable the **Retain items for a specific period** setting.
9. For the **Define retention settings** section set the following information:
   - **Retention period**: 7 Years
   - **At the end of the retention period**: Do nothing
   - **Start the retention period based on**: When items were created
10. Select the **Next** button.
11. On the Review and finish page, select the **Create label** button. Select **Just save the label for now** and select **Done**.
12. Return yourself to the **Information Governance** Page on the **Labels** tab. We will publish labels in a later exercise.
13. Select the **+ Create a label** button
14. On the Name your policy page for the **Name**, **Description for admins** and **Description for users**, enter the following information:
    - **Name**: Credit Card Receipts
    - **Description for admins**: Auto applied retention label Credit for card receipts with three-year retention.
    - **Description for users**: This label is auto applied to Credit card receipts with a retention period of three years
15. Select the **Next** button.
16. For the **Define retention settings** section set the following information:
    - **Retention period**: 3 Years
    - **At the end of the retention period**: Do nothing
    - **Start the retention period based on**: When items were created

17. Select the **Next** button.
18. On the **Review your settings** page, select the **Create label** button. Select **Just save the label for now** and select **Done**.

You have successfully created a retention label for VAT returns with a seven-year retention period and a retention label for Credit Card receipts.

19.0.2 Task 2 – Publish Retention Labels

Following from Task 1 you will now publish the VAT returns retention label so that the published label will be available for the finance users to apply to the documents in locations Exchange emails and Sharepoint documents.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Retention**.
4. On the **Information Governance** Page, select the tab **Labels**.
5. Select the label **VAT Returns and supporting documents**, that you created in Task 1.
6. Select the **Publish labels** button.
7. On the Choose labels to publish page select the **Next** button.
8. On the Choose locations page enable the option **Let me choose specific locations**.
9. Enter the following information:
   - **Exchange email** location - **Status**: Enable
   - **SharePoint sites** location - **Status**: Enable
   - **OneDrive accounts** location - **Status**: Enable
   - **Office 365 groups** location - **Status**: Disable
10. Select the **Next** button.
11. On the **Name your policy** page for **Name** and **Description** enter the following information:
    - **Name**: VAT Returns and supporting documents Retention Label
    - **Description**: VAT Returns and supporting documents Retention label, retention period 3 years, Exchange email and SharePoint site locations.
12. Select the **Next** button.
13. On the **Review your settings** page, select the **Submit** button. When your policy is published select **Done**.

You have successfully published the retention label for VAT Returns and supporting documents.

19.0.3 Task 3 – Publish auto-apply Retention Labels

Following from Task 1 you will now auto-apply the Credit Card receipts retention label so that the

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Office 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com**.
3. In the **Compliance Center**, in the left navigation pane, select **Policies** and under **Data** select **Retention**.
4. On the **Information Governance** page, select the tab **Labels**.
5. Select the label **Credit Card Receipts**, that you created in Task 1.

6. Select the **Auto-apply a label** button. The Automatically apply a label to content wizard will be displayed.
7. On the **Name your auto-labeling policy** page, for **Name** and **Description** enter the following information:
    - **Name**: Credit Card Receipts auto-applied
    - **Description**: Credit Card Receipts auto-applied retention label, with a retention period of three years for all location
8. Select the **Next** button.
9. On the **Info to label** page select the following option for Choose the type of content you want to apply this label to:
    - **Apply label to content that contains sensitive info**
10. Select the **Next** button.
11. On the Content that contains sensitive info page, select the following category **Financial**.
12. Financial templates will then be displayed as results to the right of the template categories panel.
13. On the Financial templates panel, scroll down through the results and select the **U.K. Financial Data**.
14. Select the **Next** button.
15. On the Define content that contains sensitive info page, select the **Next** button.
16. On the **Locations** page enable the options for: **Exchange email, OneDrive, SharePoint sites, and Microsoft 365 Groups** and select **Next**.
17. On the **Label** page, select **Next**.
18. On the **Finish** page select the **Submit** button.

You have successfully published a retention label with auto-apply. Over the next seven days all documents containing credit card details will be automatically labeled with the published label Credit Card Receipts, a retention period of three years will be applied to these items.

19.0.4 Task 4 – Work with retention labels in Outlook emails

In this task, you will assign retention labels to Outlook emails.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. On the taskbar at the bottom of the page, select the Start button, scroll down and then select **Outlook**. If necessary, sign in as **Megan Bowen** MeganB@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Megan's password should be provided by your lab hosting provider.
3. In the Outlook application, select the **Inbox**
4. With the right mouse button select the first email item in the center pane, and in the menu, select **Assign Policy**.
5. A list of retention policies will be displayed.
6. As there is some delay when creating retention policies, the policy created in the previous exercise may not be available for selection. If available select the **VAT Returns and supporting documents** otherwise select **one Month delete** from the existing policies. This is just for applying a setting within this exercise, remember it can take a day or more for retention policies to become available in a tenant.
7. Keep **Outlook** open.

You have successfully applied a retention label to an Outlook email.

19.0.5 Task 5 – Work with retention labels for Outlook folders

In this task, you will assign retention labels to an Outlook folder.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and **Outlook** should be opened. If not open **Outlook** again and sign-in as **Megan Bowen**.

2. Select right click on the **Inbox** in the left panel
3. Select **New folder** and enter: VAT Returns
4. Right-click on the newly created **VAT Returns** folder in the left panel
5. From the menu, select **Properties**
6. Select the **Policy** tab
7. If available set the **Folder Policy** drop down list to **VAT Returns and supporting documents** otherwise select **5 Year delete** from the existing policies (just for applying a setting within this exercise).
8. Select the **OK** button
9. Close the Outlook application by selecting the close **X** button in the top-right corner

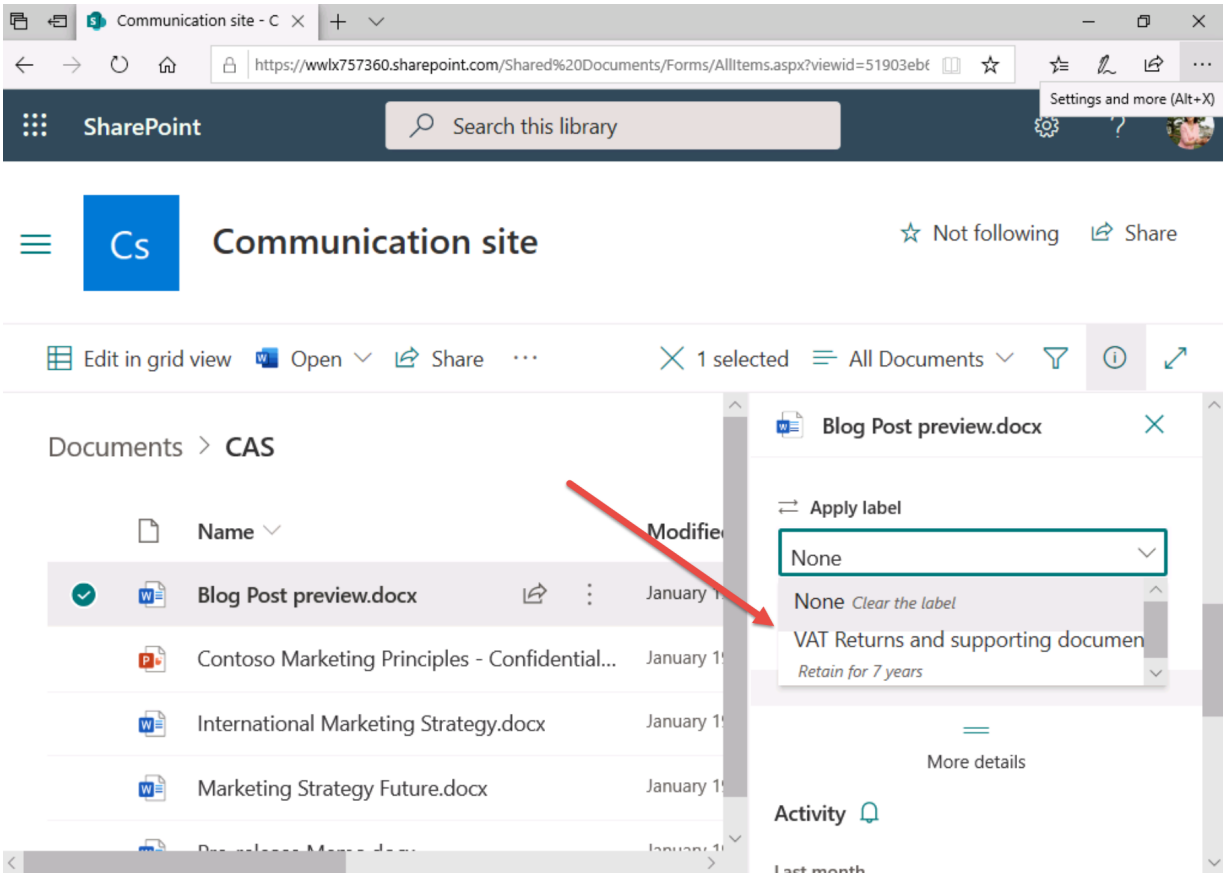
You have successfully applied a retention label to an Outlook folder, the default retention label for all emails within this folder will be assigned this based on your selection from this subtask.

You have successfully applied a retention label to an Outlook folder.

19.0.6 Task 6 – Work with retention labels in SharePoint

In this task, you will apply a retention label to a document in a SharePoint document library.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://www.office.com** and log into the Microsoft 365 as **Joni Sherman**.
3. In the Microsoft O365 landing page, select the App launcher icon in the top-left corner with nine dots, then select **SharePoint** from the submenu.
4. On the SharePoint landing page, scroll down and select the **Communication site** SharePoint site.
5. In the top navigation bar, select the **Documents** link
6. Select the **CAS** folder
7. Within the CAS folder, highlight (but do not select) the **Blog Post preview.docx** document
8. For the highlighted document, select the **...** button
9. From the menu select, select the **Details** button
10. A side menu will appear on the right.
11. If the option is available, set the **Apply Retention Label** to **VAT Returns and supporting documents**. As it can take some time for retention labels to be published you may not have the option available immediately, if it is not available, do not worry, continue to the next task.



You have successfully applied a retention label to a document in SharePoint.

19.0.7 Task 7 – Work with retention labels in OneDrive

In this task, you will apply a retention label to a document in OneDrive.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, navigate to **https://www.office.com** and log into Microsoft 365 as **Joni Sherman**.
3. In the Microsoft O365 landing page, select the App Launcher icon in the top-left corner with nine dots, then select **OneDrive** from the submenu.
4. Within the OneDrive application, highlight (but do not select) the **Contractor Legal Info.docx**
5. For the highlighted document, select the **...** button
6. From the menu select, select the **Details** button
7. A side menu will appear on the right.
8. If the option is available, set the **Apply Retention Label** to **VAT Returns and supporting documents**. As it can take some time for retention labels to be published you may not have the option available immediately, if it is not available, do not worry, continue to the next exercise.

You have successfully applied a retention label to a document in OneDrive.

20 Proceed to Exercise 3

21 Exercise 3 - Configure Service-based Retention

You assume the role of Joni Sherman, a Compliance Admin for Contoso Ltd. The legal department requires you to assist them in stopping a disgruntled employee from deleting company data.

21.0.1 Task 1 – Configure Mailbox Holds

In this task, you will activate a Mailbox Hold to prevent any content in the employee's mailbox from being deleted.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://outlook.office.com/ecp** and log into the Exchange Admin Center as **Joni Sherman**.
3. In the **Exchange Admin Center**, in the left navigation pane, select **Recipients**, then select **mailboxes**.
4. Select the mailbox of **Alex Wilber**, then select the Pencil icon to edit the mailbox.
5. In the **Edit User Mailbox** window, select **mailbox features**.
6. Under **Litigation Hold: Disabled**, select **Enable**.
7. On the **litigation hold** page, fill in the following information:
   - **Litigation hold duration (days)**: 90
   - **Note**: Your mailbox has been put on hold for the next 90 days. You will not be able to delete any messages.
8. Select **Save** twice.

You have successfully activated the Mailbox Hold on a mailbox in your environment and stopped everyone with access from permanently deleting any content in the mailbox. Applying the hold can take up to 4 hours.

21.0.2 Task 2 – Recover SharePoint Documents

In this task, you will delete and restore the deleted document to make sure you can restore documents the employee might delete after he is informed about the litigation hold against his mailbox.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://www.office.com** and log Microsoft 365 as **Joni Sherman**.
3. In the Microsoft O365 landing page, select the App launcher icon in the top-left corner with nine dots, then select **SharePoint** from the submenu.
4. On the SharePoint landing page, select the **Benefits @ Contoso** SharePoint site.
5. In the left navigation pane, select **Documents**.
6. Highlight **Vacation Policies.pptx** by selecting the checkbox in front of it.
7. in the top action bar, select **Delete**.
8. In the **Delete?** dialog, select **Delete**.
9. In the left navigation pane, select **Recycle bin**, then highlight **Vacation Policies.pptx** by selecting the checkbox in front of it.
10. In the top action bar, select **Restore**.
11. In the left navigation pane, select **Documents** and review if the file has been restored.

You have successfully recovered a document from a SharePoint Site.

22 Proceed to Exercise 4

23 Exercise 4 - Use eDiscovery for Recovery

In this exercise you will assume the role of Joni Sherman, a Compliance Administrator for Contoso Ltd. Your organization is based in Texas and wants to implement retention policies to adhere to local laws. The Uniform Preservation of Private Business Records Act specifies that records may be destroyed after three years without constituting an offense under the law (with some exceptions), to adhere to this law your organization has created a retention plan to retain all items in the organization for three years.

23.0.1 Task 1 – Create eDiscovery Case

In this exercise, you will create an eDiscovery Case and start a search for mails containing Information about the Mark 8 Project sent by Megan Bowen. The legal department requested this information for a compliance review.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman** JoniS@WWLxZZZZZZ.onmicrosoft.com (where ZZZZZZ is your unique tenant ID provided by your lab hosting provider). Joni's password should be provided by your lab hosting provider.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman**.
3. In the Compliance Center, in the left navigation pane, select ***... Show all**, then expand **eDiscovery** and select **Core**.
4. On the **Core eDiscovery** page, select **+ Create a case**.
5. In the **Case name** field, type *Mark 8 Project Case* and in the **Case description** type *This case will be used to evaluate Megan Bowen's mails regarding the Mark 8 Project.*, then select **Save**
6. On the **Core eDiscovery** page, select **Mark 8 Project Case** and select **Open case**.
7. In the Case view, select the **Searches** tab.
8. Select **+ New search**.
9. In the **Keywords** section, type *Mark 8 Project*.
10. In the **Locations** section, select **Specific locations**, then select **Modify...**.
11. In the **Modify locations** dialog, behind **Exchange email**, select **Choose users, groups, or teams**.
12. In the **Edit locations** dialog, select **Choose users, groups, or teams**.
13. In the search bar, type **Megan Bowen** and select the checkbox in front of **Megan Bowen** in the **Users, groups, or teams** list after the search completed, then select **Choose**.
14. Select **Done** and select **Save**.
15. Uncheck the **Add app content for On-Premises Users** checkbox.
16. Select **Save & run**.
17. In the **Save search** dialog, type **Mark 8 Project search** into the **Name** field, then select **Save**.

You have successfully created an eDiscovery case and searched for all mails Megan Bowen sent or received containing information about the Mark 8 Project.

23.0.2 Task 2 – Assign Records Management permissions

In this task, you will prepare to export the data you discovered in Task 1 to a PST-file that you can provide to the legal department. First you need to assign the Records Management role to your compliance administrator. Otherwise they will not be able to export search results.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://protection.office.com** and log into the Security & Compliance Center as **MOD Administrator**.
3. In the left navigation pane, select **Permissions** and then select the **Records Management** role.
4. In the role overview pane, select **Edit** next to the **Members** category.
5. Select **Choose Members** and then select **+ Add**.
6. Search for **Joni Sherman** and select the checkbox in front of their name, then select **Add**.
7. Review the changes to the member list and then select **Done**.
8. Select **Save**.

You have successfully granted your compliance administrator the permission to export search results. It can take up to 60 minutes until the permissions are applied.

23.0.3 Task 3 – Export Data from eDiscovery Case

In this task, you will prepare to export the data you discovered in Task 1 so that you can provide to the legal department. Remember it may take 60 minutes for permissions to become available in your tenant.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman**.
3. In the Compliance Center, in the left navigation pane, select ***... Show all**, then expand **eDiscovery** and select **Core**.
4. Check the checkbox in front of **Mark 8 Project Case** and select **Open case**.
5. Navigate to the **Searches** tab and select **Mark 8 Project search**.
6. In the **Mark 8 Project search** dialog, select **Export report**.
7. In **Output options**, select **All items, including ones that have unrecognized format, are encrypted, or weren't indexed for other reasons**. Select **Generate report**.

You have successfully exported the discovered data.

23.0.4 Task 4 – Perform Search & Purge on Mailboxes

An investigation showed that users received a few phishing mails and you are tasked with deleting these across all mailboxes in your environment.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. In **Microsoft Edge**, navigate to **https://compliance.microsoft.com** and log into the Compliance Center as **Joni Sherman**.
3. In the Compliance Center, in the left navigation pane, select ***... Show all**, then select **Content search**.
4. Select **+ New search**.
5. In the **Keywords** field, type *From:phishingmail@outlook.com AND subject:"Password changed"*
6. In the **Locations** section, select **Specific locations**, then select **Modify...**.
7. In the **Modify locations** dialog, next to **Exchange email**, switch **Select all** to **On**, then select **Save**.
8. Select **Save & run** and in the **Name** field, type *Phishing mail removal*, then select **Save**.
9. Once you created the search, you need to use the **Security & Compliance PowerShell** to start a purge. In the start menu, select **Windows PowerShell** run as Administrator.
10. In the **PowerShell** window, use the following cmdlet and then sign in as **MOD Administrator**:

    Connect-IPPSSession
11. In the **PowerShell** window, use the following command and confirm with **Y**:

    New-ComplianceSearchAction -SearchName "Phishing mail removal" -Purge -PurgeType HardDelete
12. In PowerShell type **Y** for Yes to confirm the action.

You have successfully created a new content search to look for specific emails and then used the purge action to delete the phishing mails from your user's mailboxes. You can only run the purge action as a member of the Organization Management role, which a Compliance Admin is not part of.

24 Proceed to Exercise 5

25 Exercise 5 - Configure Records Management

In this exercise, you will assume the role of Joni Sherman, a Compliance Administrator for Contoso Ltd. Regulatory requirements for your organization include having a definitive copy of the employee provided health insurance information available when your company discusses the insurance costs. You are tasked with making sure the records are kept.

25.0.1 Task 1 – Create File Plan Labels

In this task, you will create a file plan label that allows your HR department to label content containing health insurance information that your employees are required to be provided when they are hired.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Microsoft 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com/**.
3. In the **Compliance Center**, in the left navigation pane, select **... Show all**, then select **Records management**.
4. On the **Records management** page, select **file plan**.
5. Select **+ Create a label**
6. Enter the following information, then select **next**:
   - **Name**: Employee Data
   - **Description for users**: Content marked with this label contains sensitive employee data.
   - **Description for admins**: The label was created on request of the HR department and will be automatically applied to Employee Data.
7. Enter the following information on the **Define file plan descriptors for this label** page, then select **Next**:
   - **Reference ID**: HR_EmployeeData
   - **Business function**: Human resources
   - **Category**: Recruiting and hiring
   - **Provision/citation**: Health Insurance Portability and Accountability Act of 1996
8. On the **Define retention settings** page, select the following options, then select **Next**:
   - **Retain items for a specific period**
   - **Retention period**: 7 years
   - **Start the retention period based on**: When items were created
   - **During the retention period**: Mark items as a record
   - **At the end of a retention period**: Trigger a disposition review
9. In the **Disposition reviewers** field, search for **Lynne Robbins** and add her to the list of reviewers by selecting her name, then select **Next**
10. Review the configuration of the label, then select **Create label**.
11. On the **retention label is created** page, select **Just save the label for now**, then select **Done**.

You successfully created a retention label using file plan that keeps all labeled documents from being deleted for seven years and at the end of the retention period Lynne Robbins has to decide if the data can be disposed of or has to be retained further.

25.0.2 Task 2 – Publish Labels

In this task, you will publish the label so users of the HR department can apply it to content containing health insurance information.

1. You should still be logged into your Client 1 VM (LON-CL1) as the **lon-cl1\admin** account, and you should be logged into Microsoft 365 as **Joni Sherman**.
2. In **Microsoft Edge**, the Microsoft 365 Compliance Center tab should still be open. If so, select it and proceed to the next step. If you closed it, then in a new tab, navigate to **https://compliance.microsoft.com/**.
3. In the **Compliance Center**, in the left navigation pane, select **... Show all**, then select **Records management**.
4. On the **Records management** page, select **file plan**.
5. Select **Publish labels**.
6. On the **Choose labels to publish** page, select **Choose labels to publish**.

7. Select the **Employee Data** label and select **Add**, then select **Next**.
8. On the **Choose locations** page, select **All locations. Includes content in Exchange email, Office 365 groups, OneDrive, and SharePoint documents.**, then select **Next**.
9. On the **Name your policy** page, enter the following information, then select **Next**:
    - **Name**: Employee Health Insurance label policy
    - **Description**: This policy contains the record label for health insurance information.
10. Review the configuration of your policy and select **Submit**.

You successfully started the process of publishing a retention label including a record. The publishing of labels may take up to 24 hours. After the label is published the HR department can use it to label files containing the health insurance information, they are required to keep a record of.

25.0.3 Task 3 – Work with Records

In this task, you will assign the published record label to an email in Outlook and observe the results of applying the record. You might need to wait for the 24-hour publishing delay.

1. Log into the Client 1 VM (LON-CL1) as the **lon-cl1\admin** account.
2. On the taskbar at the bottom of the page, select the Start button, scroll down and then select **Outlook**. If necessary, sign in as **Megan Bowen**.
3. In the Outlook application, select **Inbox**
4. With the right mouse button select the first email item in the center pane, and in the menu, select **Assign Policy**.
5. A list of retention policies will be displayed.
6. Select the **Employee Data** label to apply the record label.
7. With the right mouse button, select the email item you labeled with **Employee Data**, and select **Delete**.
8. Review the message you receive.
9. With the right mouse button, select the email item you labeled with **Employee Data**, and select **Assign Policy**.
10. Select the **Use folder policy** to remove labels that exist directly on the mail.
11. With the right mouse button, select the email item you labeled with **Employee Data**, and select **Assign Policy**. You should still see the **Employee Data** label applied.

You have successfully applied a retention label with a record to an email and observed that it now cannot be deleted.

25.1 You have completed the lab.