Cyber Shujaa

NAME: STEPHEN KYALO -ADC-DP01-25005

PROGRAM: DATA PROTECTION SPECIALIST

CLOUD SLICE TOPIC: MANAGE COMPLIANCE ROLES & MANAGE SENSITIVE INFORMATION TYPES COMPLETION REQUIREMENTS

EXECUTIVE SUMMARY

The **management of Microsoft Purview Message Encryption** and **Sensitivity Labels** plays a pivotal role in securing organisational data. Encryption ensures that sensitive information is transformed into unreadable ciphertext using cryptographic keys, safeguarding data at rest and in transit.

Microsoft Purview utilises either Microsoft-managed or customer-managed keys via Azure Key Vault, offering encrypted email communication, especially to external recipients, through sign-in or OTP verification. Custom encryption templates can be configured via PowerShell to reflect organisational branding.

Meanwhile, **sensitivity labels** allow organisations to classify and protect data based on sensitivity. These labels can be applied manually or automatically using trainable classifiers and predefined rules. The lab demonstrates the enabling of sensitivity labels via PowerShell, the creation of labels and sublabels, and the configuration of auto-labelling policies, ensuring robust data governance and compliance.

1. MANAGE MICROSOFT PURVIEW MESSAGE ENCRYPTION

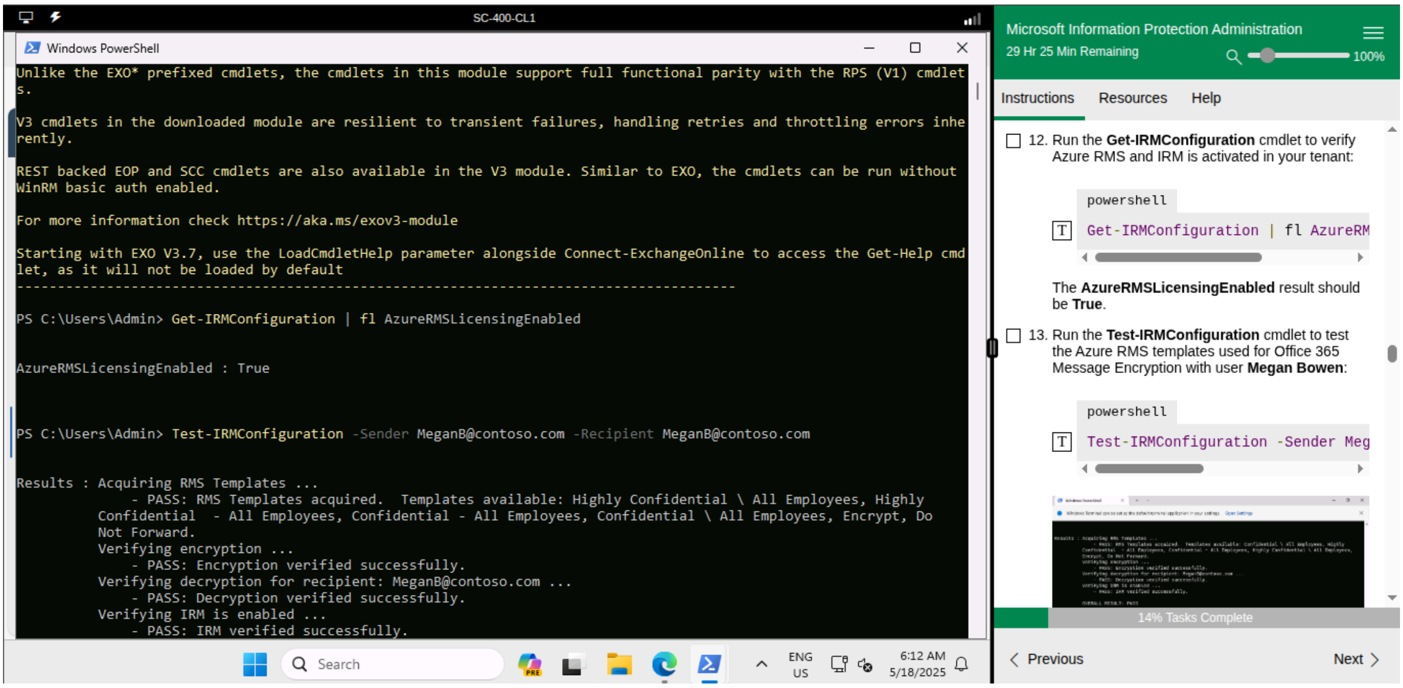
Encryption is a critical process in data security that involves transforming clear-text data or files into an unreadable format known as ciphertext. This transformation is achieved through the use of cryptographic keys—unique strings of characters that serve as the basis for the encryption and decryption processes. Without the correct key, retrieving the original clear-text is virtually impossible, ensuring the confidentiality and integrity of sensitive information against unauthorised access or breaches. This process is widely used in various applications, from securing online communications to protecting stored data.

Microsoft offers this feature through the Microsoft Purview Information Protection portal. It uses multiple layers of encryption to secure data at rest and data in transit. Data at rest includes files stored in SharePoint, OneDrive, email messages and Teams Chat messages. Data in transit includes email messages being delivered or any communication between a client and a Microsoft server.

Purview uses Microsoft Managed keys (provided by Microsoft through the Azure Key Vault) or Customer Managed keys (generated by Tenants and stored in the Azure Key Vault) to encrypt data.

Below is a demonstration of how email messages sent to external users are encrypted by requiring the external users to sign in with their accounts to read the encrypted email or enter an OTP.

Verification of Azure Rights Management Service (Azure RMS)



```
Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlet
s.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inhe
rently.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without
WinRM basic auth enabled.

For more information check https://aka.ms/exov3-module

Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to access the Get-Help cmd
let, as it will not be loaded by default
----------------------------------------------------------------------------------------

PS C:\Users\Admin> Get-IRMConfiguration | fl AzureRMSLicensingEnabled


AzureRMSLicensingEnabled : True



PS C:\Users\Admin> Test-IRMConfiguration -Sender MeganB@contoso.com -Recipient MeganB@contoso.com


Results : Acquiring RMS Templates ...
              - PASS: RMS Templates acquired.  Templates available: Highly Confidential \ All Employees, Highly
          Confidential  - All Employees, Confidential - All Employees, Confidential \ All Employees, Encrypt, Do
          Not Forward.
          Verifying encryption ...
              - PASS: Encryption verified successfully.
          Verifying decryption for recipient: MeganB@contoso.com ...
              - PASS: Decryption verified successfully.
          Verifying IRM is enabled ...
              - PASS: IRM verified successfully.
```

Microsoft Information Protection Administration

29 Hr 25 Min Remaining

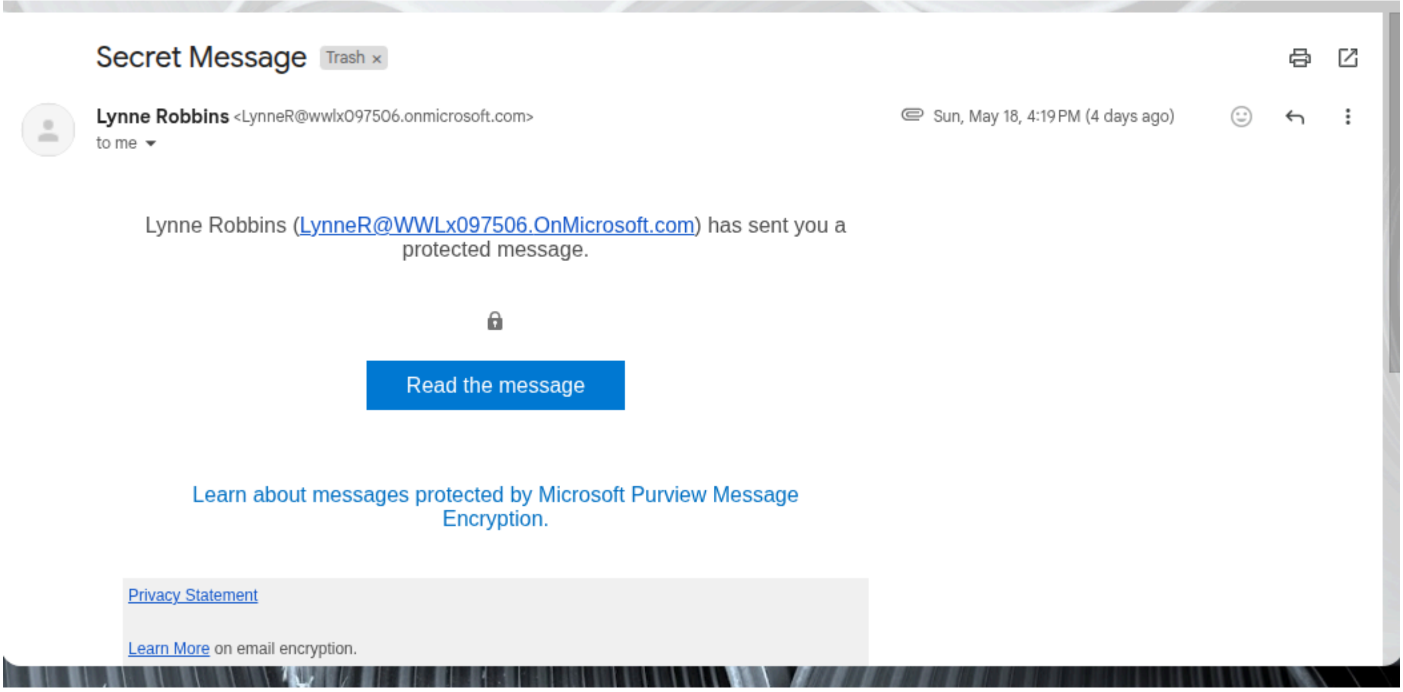
□ 12. Run the **Get-IRMConfiguration** cmdlet to verify Azure RMS and IRM is activated in your tenant:

```
powershell
Get-IRMConfiguration | fl AzureRM
```

The **AzureRMSLicensingEnabled** result should be **True**.

□ 13. Run the **Test-IRMConfiguration** cmdlet to test the Azure RMS templates used for Office 365 Message Encryption with user **Megan Bowen**:

```
powershell
Test-IRMConfiguration -Sender Meg
```



Secret Message

Lynne Robbins <LynneR@wwlx097506.onmicrosoft.com>
to me

Sun, May 18, 4:19 PM (4 days ago)

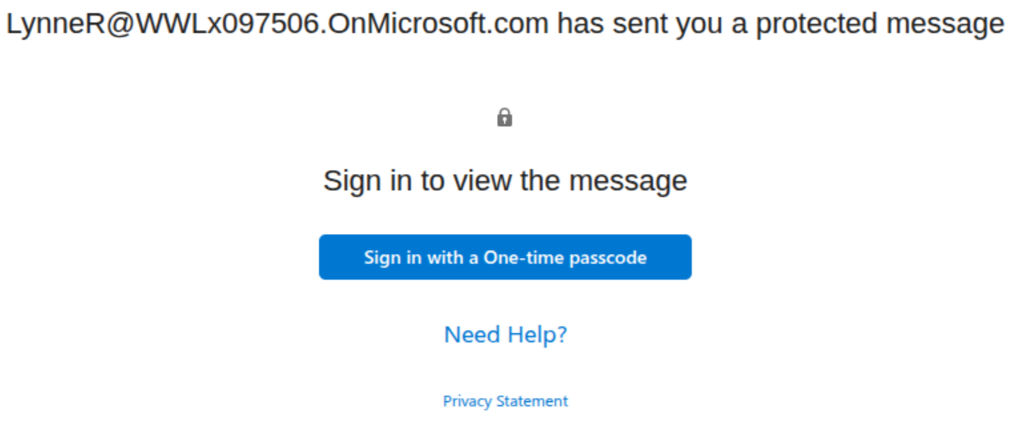
Lynne Robbins (LynneR@WWLx097506.OnMicrosoft.com) has sent you a protected message.

Learn about messages protected by Microsoft Purview Message Encryption.

Privacy Statement

Learn More on email encryption.

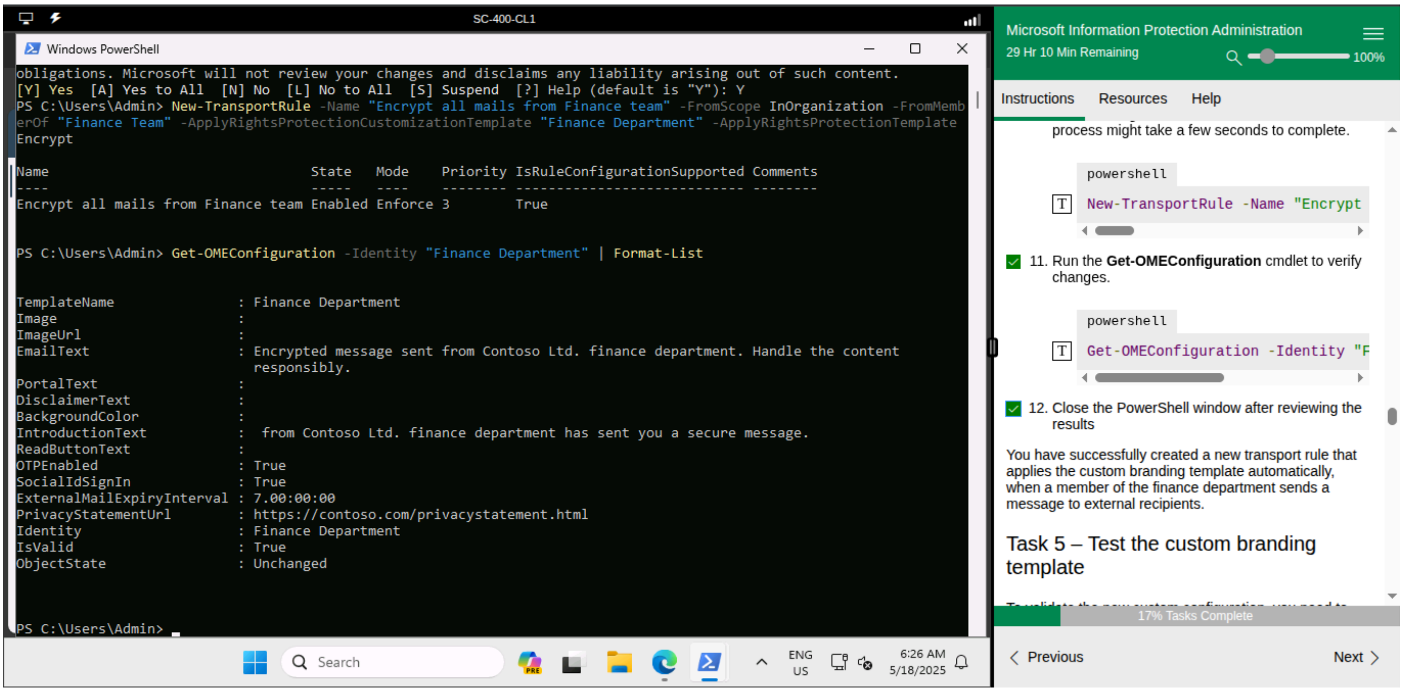
This is how an encrypted email will appear to an external user. This is a default template, how the encrypted message will appear to the external user requiring them to sign in, provided by Azure RMS



LynneR@WWLx097506.OnMicrosoft.com has sent you a protected message

Sign in to view the message

For the user to view the message, they need to sign in with an OTP



```
obligations. Microsoft will not review your changes and disclaims any liability arising out of such content.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\Users\Admin> New-TransportRule -Name "Encrypt all mails from Finance team" -FromScope InOrganization -FromMemb
erOf "Finance Team" -ApplyRightsProtectionCustomizationTemplate "Finance Department" -ApplyRightsProtectionTemplate
Encrypt

Name                                State   Mode    Priority IsRuleConfigurationSupported Comments
----                                -----   ----    -------- ---------------------------- --------
Encrypt all mails from Finance team Enabled Enforce 3        True


PS C:\Users\Admin> Get-OMEConfiguration -Identity "Finance Department" | Format-List


TemplateName                : Finance Department
Image                       :
ImageUrl                    :
EmailText                   : Encrypted message sent from Contoso Ltd. finance department. Handle the content
                              responsibly.
PortalText                  :
DisclaimerText              :
BackgroundColor             :
IntroductionText            :  from Contoso Ltd. finance department has sent you a secure message.
ReadButtonText              :
OTPEnabled                  : True
SocialIdSignIn              : True
ExternalMailExpiryInterval  : 7.00:00:00
PrivacyStatementUrl         : https://contoso.com/privacystatement.html
Identity                    : Finance Department
IsValid                     : True
ObjectState                 : Unchanged


PS C:\Users\Admin> _
```

process might take a few seconds to complete.

```
powershell
New-TransportRule -Name "Encrypt
```

☑ 11. Run the **Get-OMEConfiguration** cmdlet to verify changes.

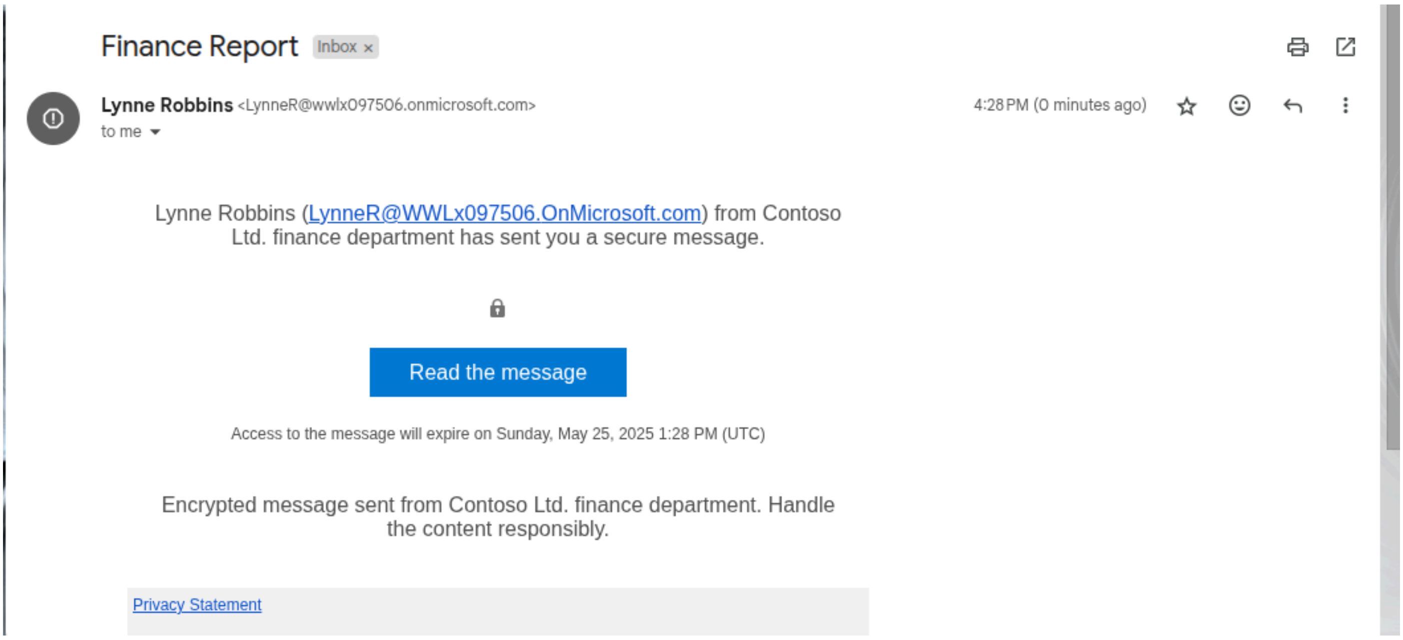
```
powershell
Get-OMEConfiguration -Identity "F
```

☑ 12. Close the PowerShell window after reviewing the results

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

Task 5 – Test the custom branding template

Customising the template in PowerShell.



Finance Report Inbox ×

Lynne Robbins <LynneR@wwlx097506.onmicrosoft.com>
to me

4:28 PM (0 minutes ago)

Lynne Robbins (LynneR@WWLx097506.OnMicrosoft.com) from Contoso Ltd. finance department has sent you a secure message.

Access to the message will expire on Sunday, May 25, 2025 1:28 PM (UTC)

Encrypted message sent from Contoso Ltd. finance department. Handle the content responsibly.

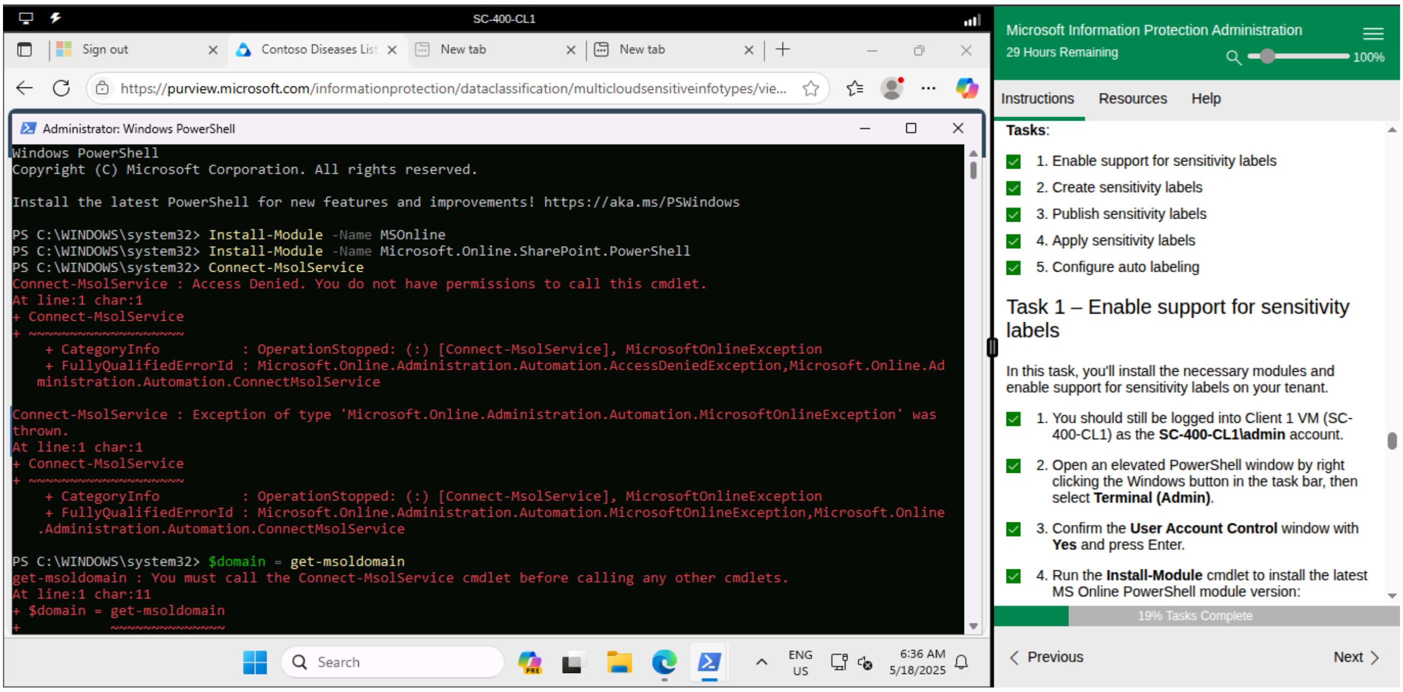
Privacy Statement

Customised brand template.

2. MANAGE SENSITIVITY LABELS

Sensitivity labels are crucial tags that organisations utilise to classify, protect, and facilitate secure sharing of data across various platforms and devices. These labels help in enforcing data governance policies, ensuring compliance with regulations, and reducing the risk of data breaches. Sensitivity labels can be applied manually by users based on their discretion or automatically implemented through predefined rules leveraging Trainable classifiers, which utilise machine learning models to identify and categorise sensitive information effectively.

The accompanying demo images illustrate how sensitivity labels are enabled for Azure Tenants through PowerShell commands, providing step-by-step guidance on the process. Additionally, we detail the creation of sensitivity labels and their associated sublabels, enabling finer control over data classification. Furthermore, we explore the setup of autolabelling policies in Microsoft Purview, showcasing how organisations can streamline the process of protecting their data by automatically applying the appropriate sensitivity labels based on specified criteria, thereby enhancing data security and compliance efforts.


SC-400-CL1
Sign out
Contoso Diseases List
New tab
New tab
https://purview.microsoft.com/informationprotection/dataclassification/multicloudsensitiveinfotypes/vie...
Administrator: Windows PowerShell
Search
ENG
US
6:36 AM
5/18/2025

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Install-Module -Name MSOnline
PS C:\WINDOWS\system32> Install-Module -Name Microsoft.Online.SharePoint.PowerShell
PS C:\WINDOWS\system32> Connect-MsolService
Connect-MsolService : Access Denied. You do not have permissions to call this cmdlet.
At line:1 char:1
+ Connect-MsolService
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [Connect-MsolService], MicrosoftOnlineException
    + FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.AccessDeniedException,Microsoft.Online.Ad
   ministration.Automation.ConnectMsolService

Connect-MsolService : Exception of type 'Microsoft.Online.Administration.Automation.MicrosoftOnlineException' was
thrown.
At line:1 char:1
+ Connect-MsolService
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [Connect-MsolService], MicrosoftOnlineException
    + FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.MicrosoftOnlineException,Microsoft.Online
   .Administration.Automation.ConnectMsolService

PS C:\WINDOWS\system32> $domain = get-msoldomain
get-msoldomain : You must call the Connect-MsolService cmdlet before calling any other cmdlets.
At line:1 char:11
+ $domain = get-msoldomain
+           ~~~~~~~~~~~~~~
```

Microsoft Information Protection Administration

29 Hours Remaining

Tasks:

- ☑ 1. Enable support for sensitivity labels
- ☑ 2. Create sensitivity labels
- ☑ 3. Publish sensitivity labels
- ☑ 4. Apply sensitivity labels
- ☑ 5. Configure auto labeling

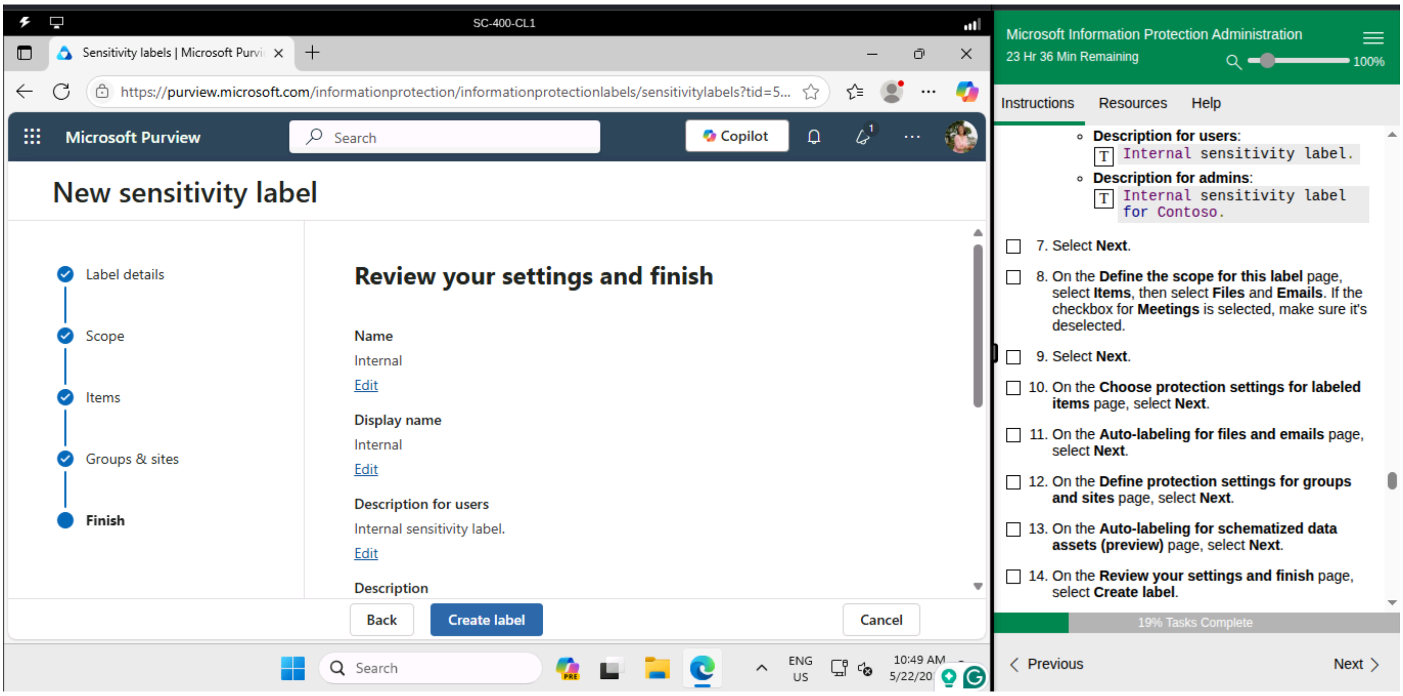
Task 1 – Enable support for sensitivity labels

In this task, you'll install the necessary modules and enable support for sensitivity labels on your tenant.

- ☑ 1. You should still be logged into Client 1 VM (SC-400-CL1) as the **SC-400-CL1\admin** account.
- ☑ 2. Open an elevated PowerShell window by right clicking the Windows button in the task bar, then select **Terminal (Admin)**.
- ☑ 3. Confirm the **User Account Control** window with **Yes** and press Enter.
- ☑ 4. Run the **Install-Module** cmdlet to install the latest MS Online PowerShell module version:

19% Tasks Complete

Enabling support for sensitivity labels.



New sensitivity label

Review your settings and finish

Name
Internal
Edit

Display name
Internal
Edit

Description for users
Internal sensitivity label.
Edit

Description

- **Description for users**:
  `Internal sensitivity label.`
- **Description for admins**:
  `Internal sensitivity label for Contoso.`

☐ 7. Select **Next**.

☐ 8. On the **Define the scope for this label** page, select **Items**, then select **Files** and **Emails**. If the checkbox for **Meetings** is selected, make sure it's deselected.

☐ 9. Select **Next**.

☐ 10. On the **Choose protection settings for labeled items** page, select **Next**.

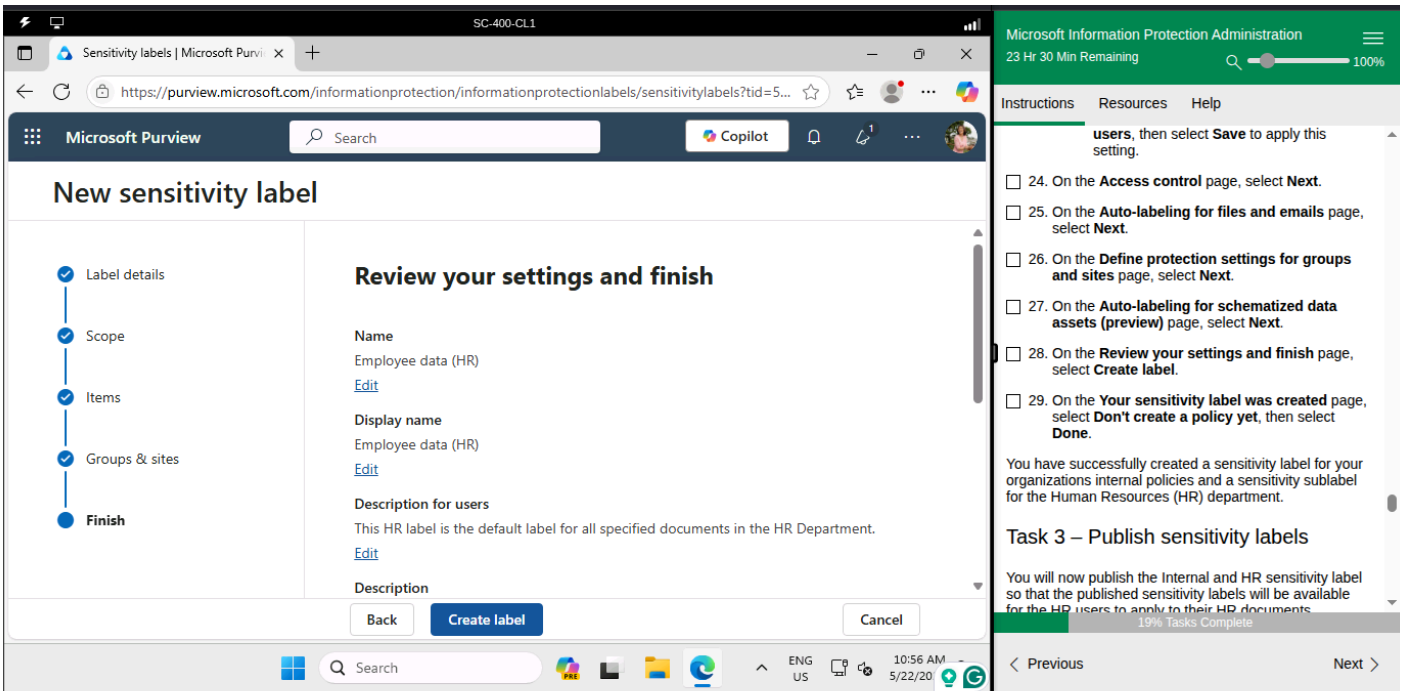
☐ 11. On the **Auto-labeling for files and emails** page, select **Next**.

☐ 12. On the **Define protection settings for groups and sites** page, select **Next**.

☐ 13. On the **Auto-labeling for schematized data assets (preview)** page, select **Next**.

☐ 14. On the **Review your settings and finish** page, select **Create label**.

Creation of labels in Purview



New sensitivity label

Review your settings and finish

Name
Employee data (HR)
Edit

Display name
Employee data (HR)
Edit

Description for users
This HR label is the default label for all specified documents in the HR Department.
Edit

Description

users, then select **Save** to apply this setting.

☐ 24. On the **Access control** page, select **Next**.

☐ 25. On the **Auto-labeling for files and emails** page, select **Next**.

☐ 26. On the **Define protection settings for groups and sites** page, select **Next**.

☐ 27. On the **Auto-labeling for schematized data assets (preview)** page, select **Next**.

☐ 28. On the **Review your settings and finish** page, select **Create label**.

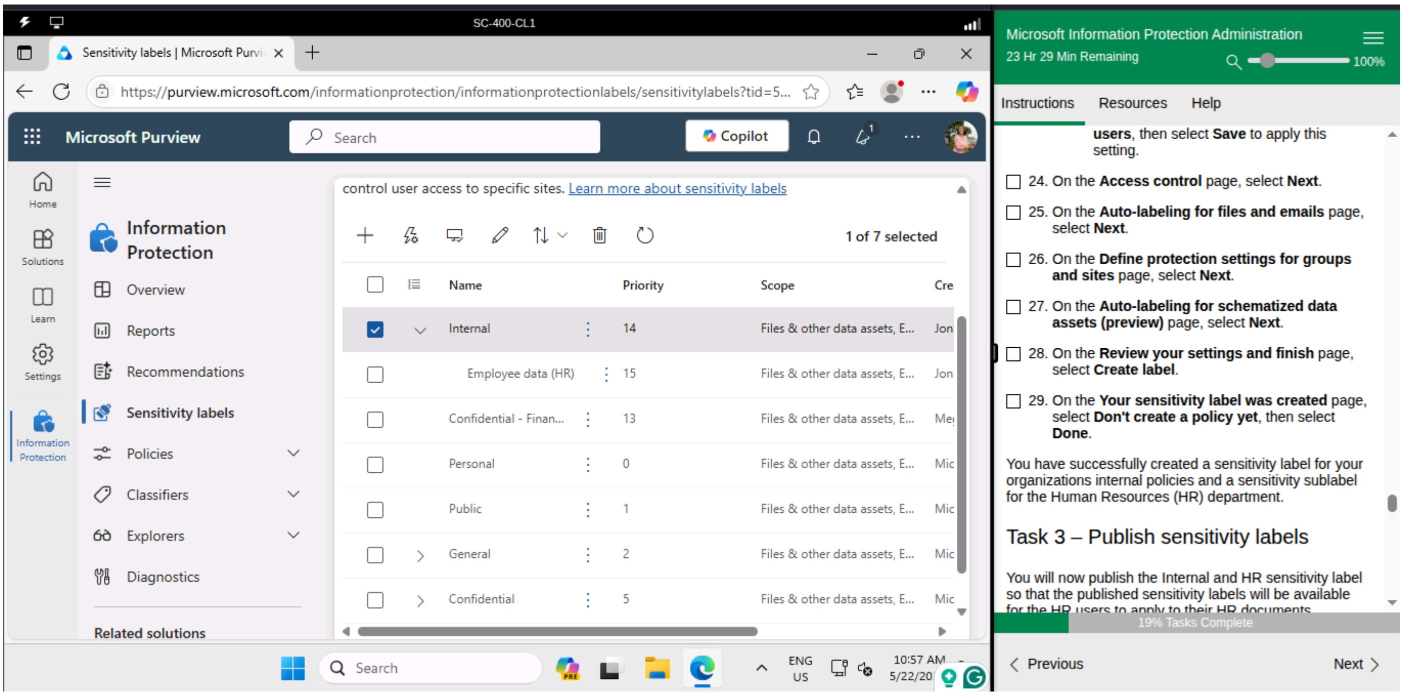
☐ 29. On the **Your sensitivity label was created** page, select **Don't create a policy yet**, then select **Done**.

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

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

Creating a sublabel under a label



control user access to specific sites. Learn more about sensitivity labels

1 of 7 selected

	Name		Priority	Scope	Cre
☑	Internal	⋮	14	Files & other data assets, E...	Jon
□	Employee data (HR)	⋮	15	Files & other data assets, E...	Jon
□	Confidential - Finan...	⋮	13	Files & other data assets, E...	Me
□	Personal	⋮	0	Files & other data assets, E...	Mic
□	Public	⋮	1	Files & other data assets, E...	Mic
□	General	⋮	2	Files & other data assets, E...	Mic
□	Confidential	⋮	5	Files & other data assets, E...	Mic

users, then select **Save** to apply this setting.

□ 24. On the **Access control** page, select **Next**.

□ 25. On the **Auto-labeling for files and emails** page, select **Next**.

□ 26. On the **Define protection settings for groups and sites** page, select **Next**.

□ 27. On the **Auto-labeling for schematized data assets (preview)** page, select **Next**.

□ 28. On the **Review your settings and finish** page, select **Create label**.

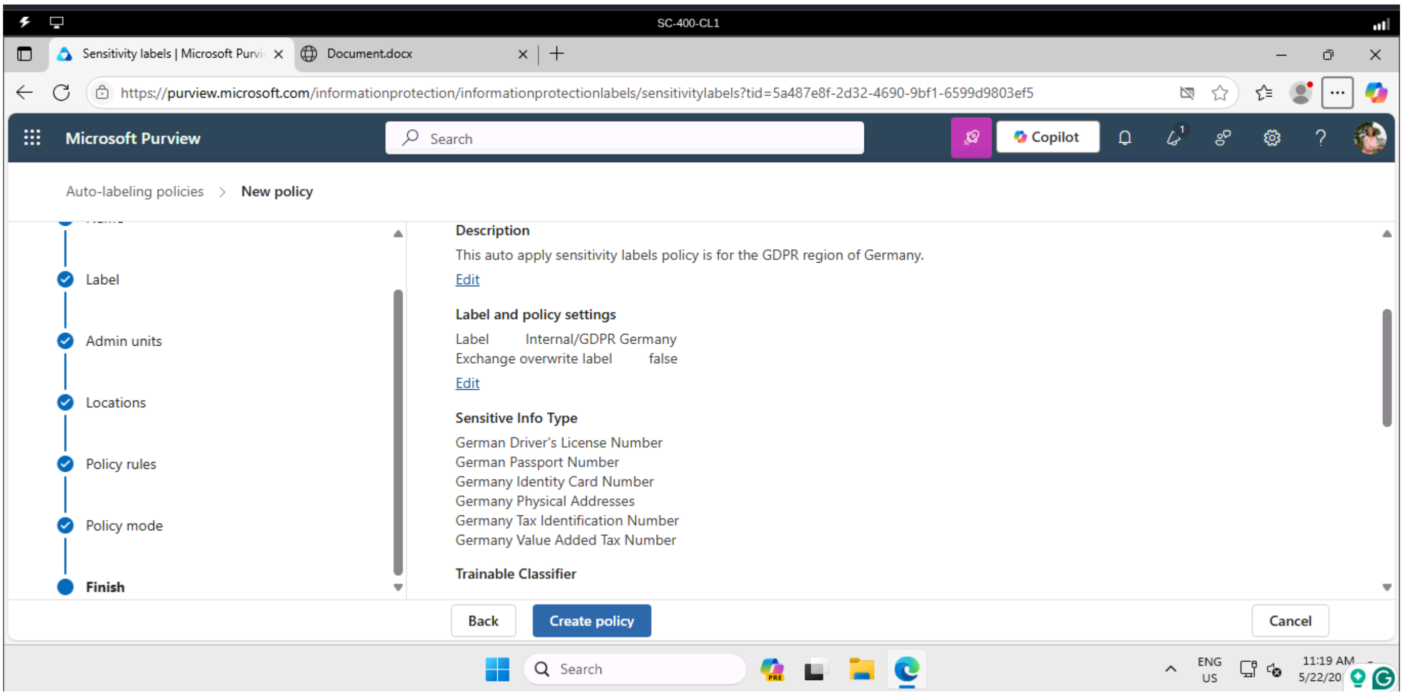
□ 29. On the **Your sensitivity label was created** page, select **Don't create a policy yet**, then select **Done**.

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

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.

Sensitivity labels created and their sublabels.


SC-400-CL1
Sensitivity labels | Microsoft Purvi
Document.docx
https://purview.microsoft.com/informationprotection/informationprotectionlabels/sensitivitylabels?tid=5a487e8f-2d32-4690-9bf1-6599d9803ef5
Microsoft Purview
Search
Copilot
Auto-labeling policies > New policy
Label
Admin units
Locations
Policy rules
Policy mode
Finish

Description

This auto apply sensitivity labels policy is for the GDPR region of Germany.

Edit

Label and policy settings

Label Internal/GDPR Germany

Exchange overwrite label false

Edit

Sensitive Info Type

German Driver's License Number
German Passport Number
Germany Identity Card Number
Germany Physical Addresses
Germany Tax Identification Number
Germany Value Added Tax Number

Trainable Classifier

Configuration of autolabelling policies.