Microsoft

(SC-400)

Microsoft Information Protection Administrator

Total: **325 Questions**

Link:

Question: 1

You create three sensitivity labels named Sensitivity1, Sensitivity2, and Sensitivity3 and perform the following actions:
➯ Publish Sensitivity1.
➯ Create an auto-labeling policy for Sensitivity2.
You plan to create a file policy named Policy1 in Microsoft Cloud App Security. Which sensitivity labels can you apply to Microsoft SharePoint Online in Policy1?

A. Sensitivity1 only
B. Sensitivity1, Sensitivity2, and Sensitivity3
C. Sensitivity2 only
D. Sensitivity1 and Sensitivity2 only

Answer: A

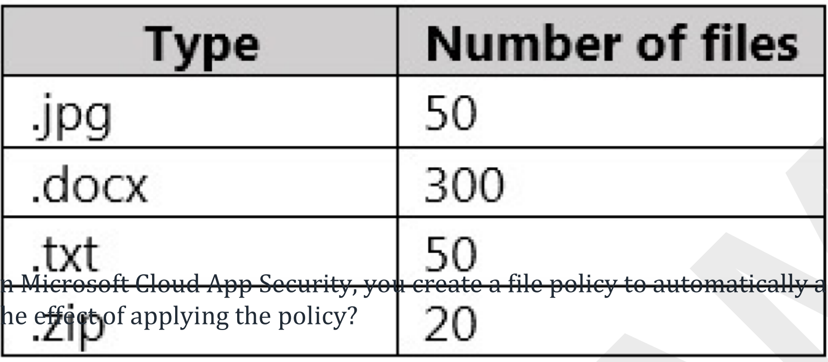
Explanation:

"For Defender for Cloud Apps to apply sensitivity labels, they must be published as part of a sensitivity label policy in the Microsoft 365 compliance center." does not mention auto-labeling policy as an option.

For Defender for Cloud Apps to apply sensitivity labels, they must be published as part of a sensitivity label policy in the Microsoft Purview compliance portal.https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration#prerequisites

Question: 2

You have a Microsoft OneDrive for Business folder that contains the files shown in the following table.



Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

In Microsoft Cloud App Security, you create a file policy to automatically apply a classification. What is the effect of applying the policy?

A. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours. B. The policy will apply to all the files. The policy will classify only 100 files daily.

C. The policy will apply to only the .docx files. The policy will classify only 100 files daily.

D. The policy will apply to only the .docx and .txt files. The policy will classify the files immediately.

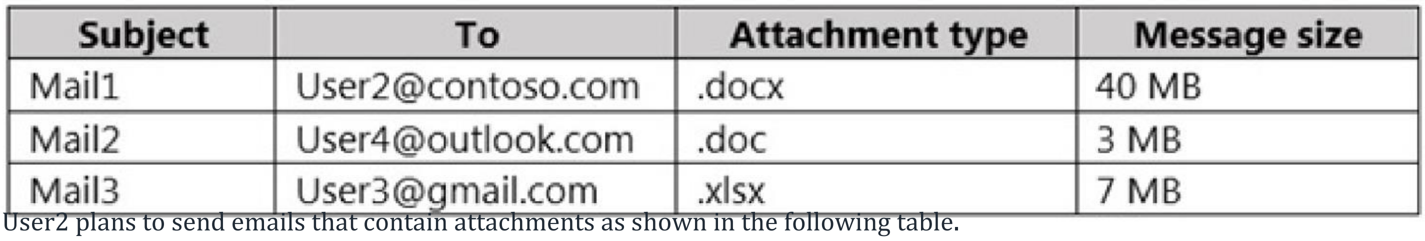
Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

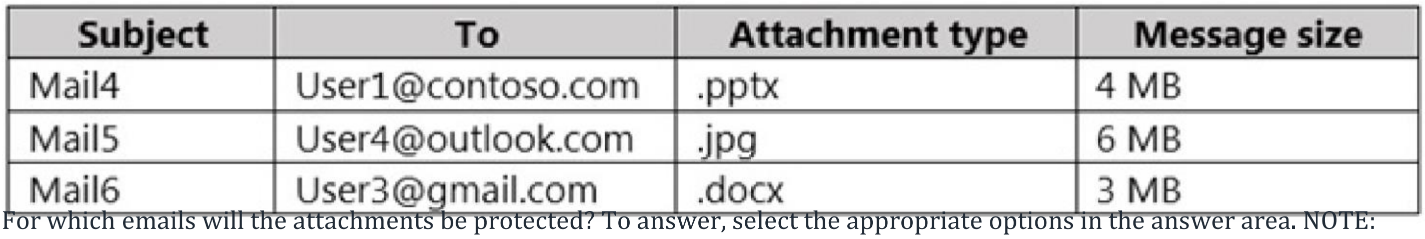
Question: 3

HOTSPOT -
You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Office 365 Message Encryption
(OME).
User1 plans to send emails that contain attachments as shown in the following table.



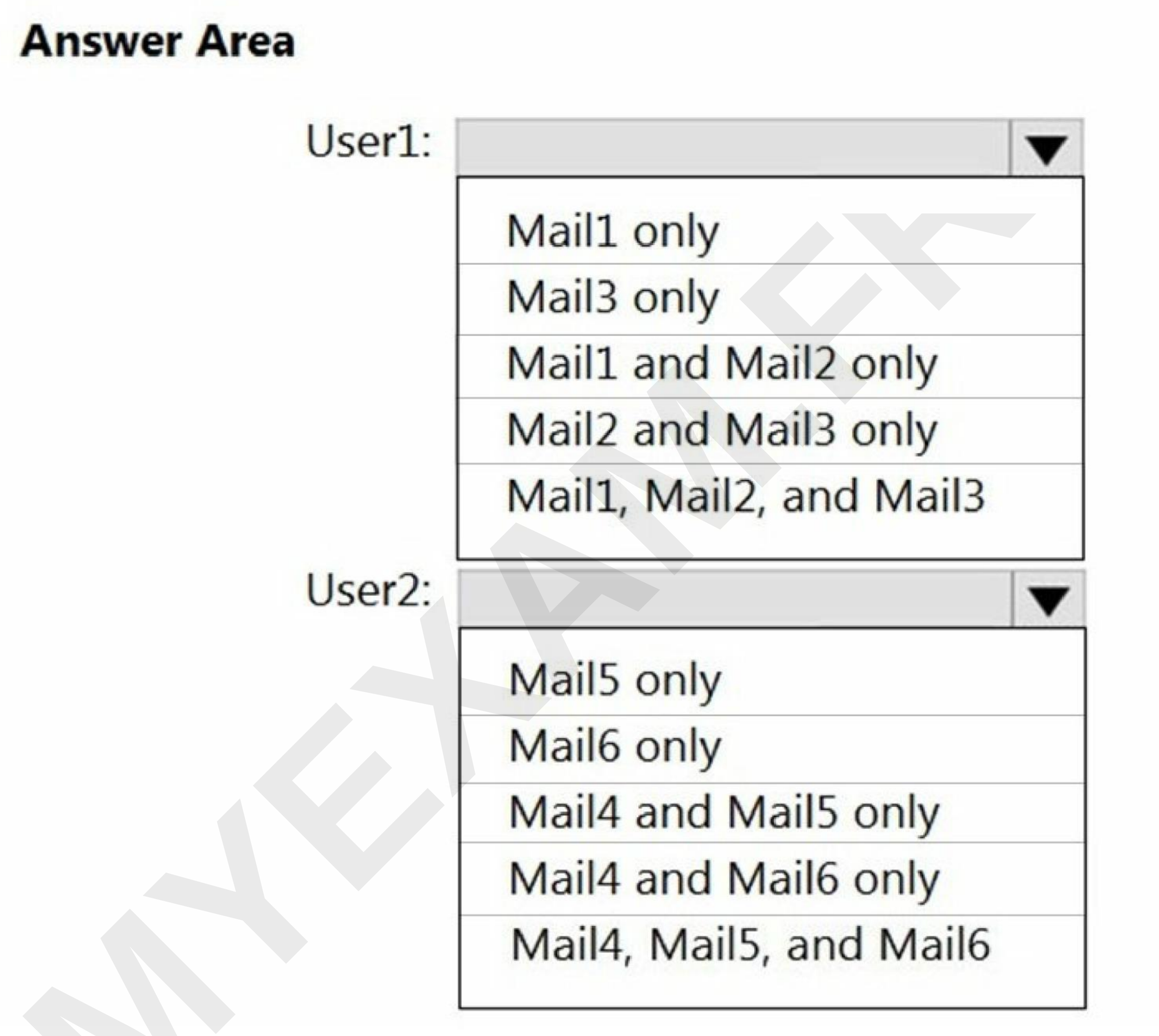
Subject	To	Attachment type	Message size
Mail1	User2@contoso.com	.docx	40 MB
Mail2	User4@outlook.com	.doc	3 MB
Mail3	User3@gmail.com	.xlsx	7 MB

User2 plans to send emails that contain attachments as shown in the following table.



Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

For which emails will the attachments be protected? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Hot Area:

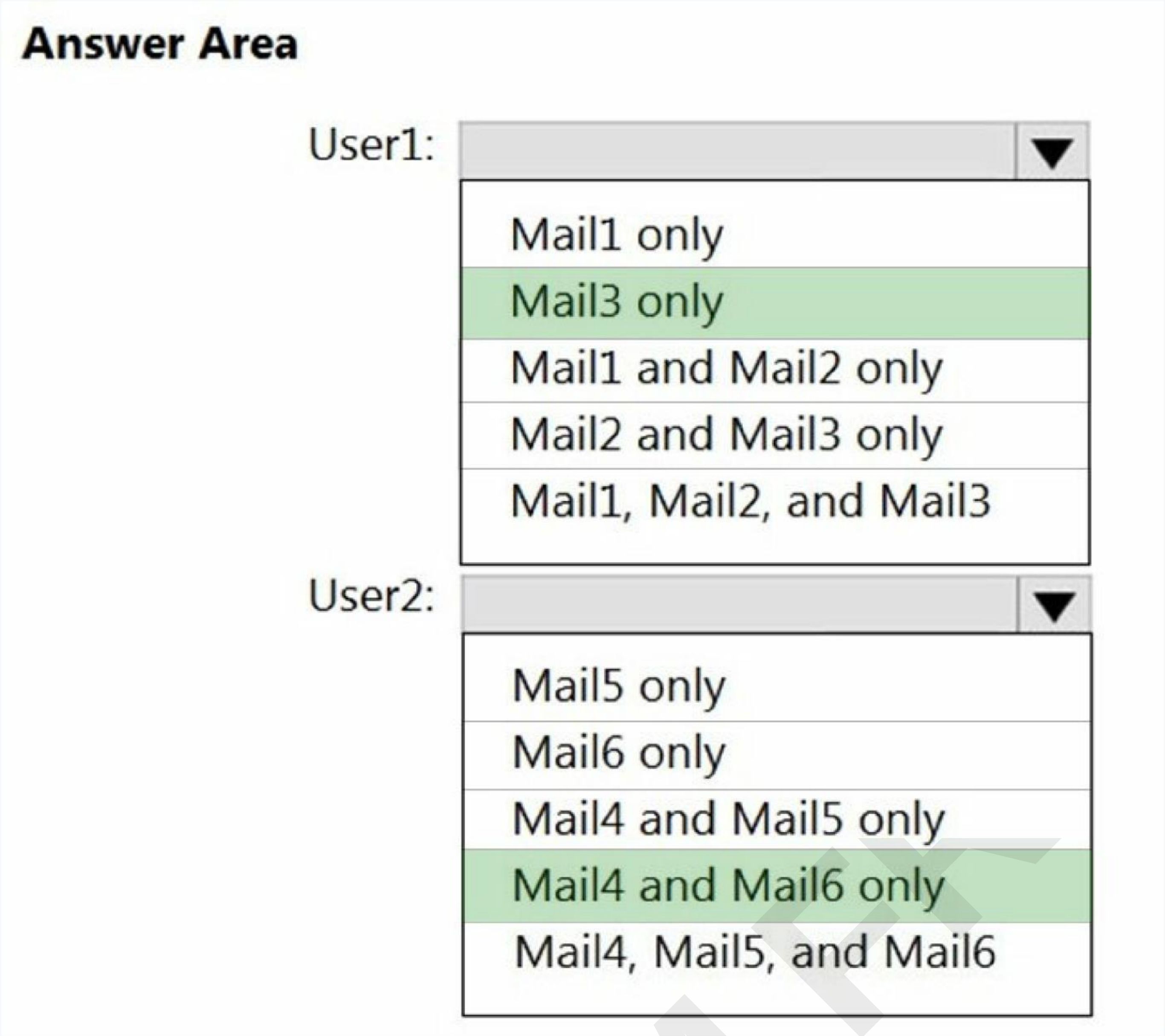


Answer Area

User1:
- Mail1 only
- Mail3 only
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:
- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- Mail4 and Mail6 only
- Mail4, Mail5, and Mail6

Answer:



Answer Area

User1:

- Mail1 only
- [✓ Mail3 only]
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:

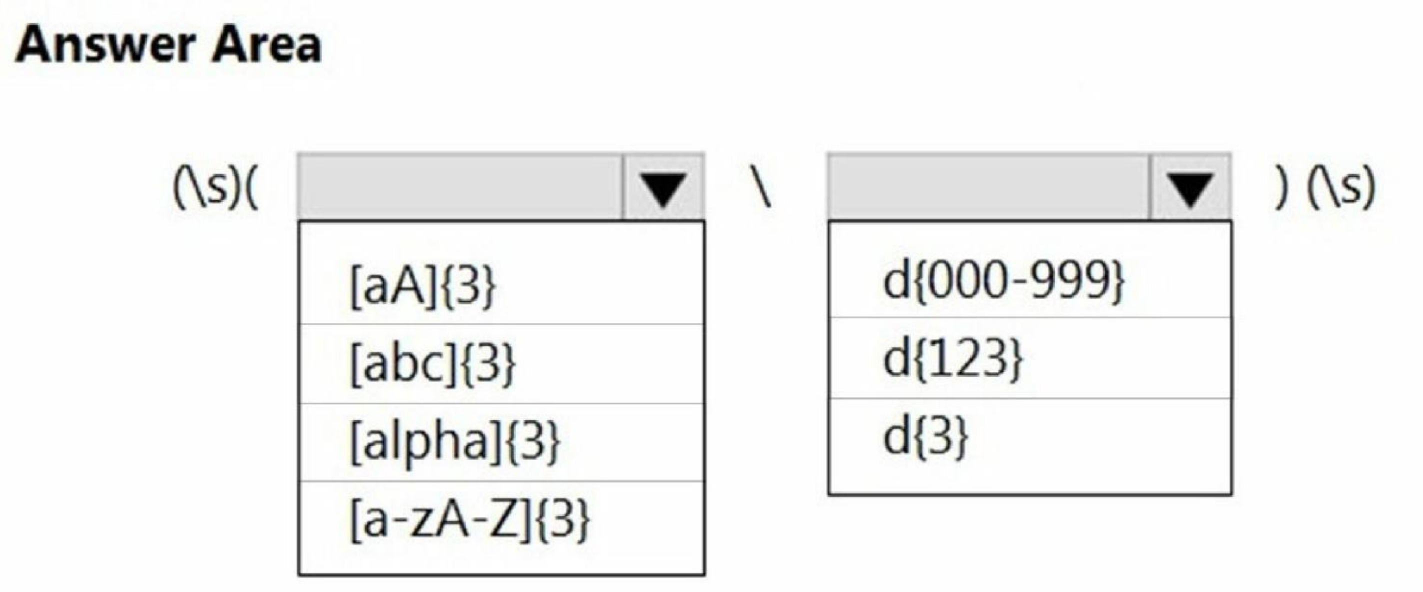
- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- [✓ Mail4 and Mail6 only]
- Mail4, Mail5, and Mail6

Explanation:

Reference:
https://support.microsoft.com/en-gb/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-us&rs=en- gb&ad=gb#FileTypesforIRM https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#message-limits-1

Question: 4

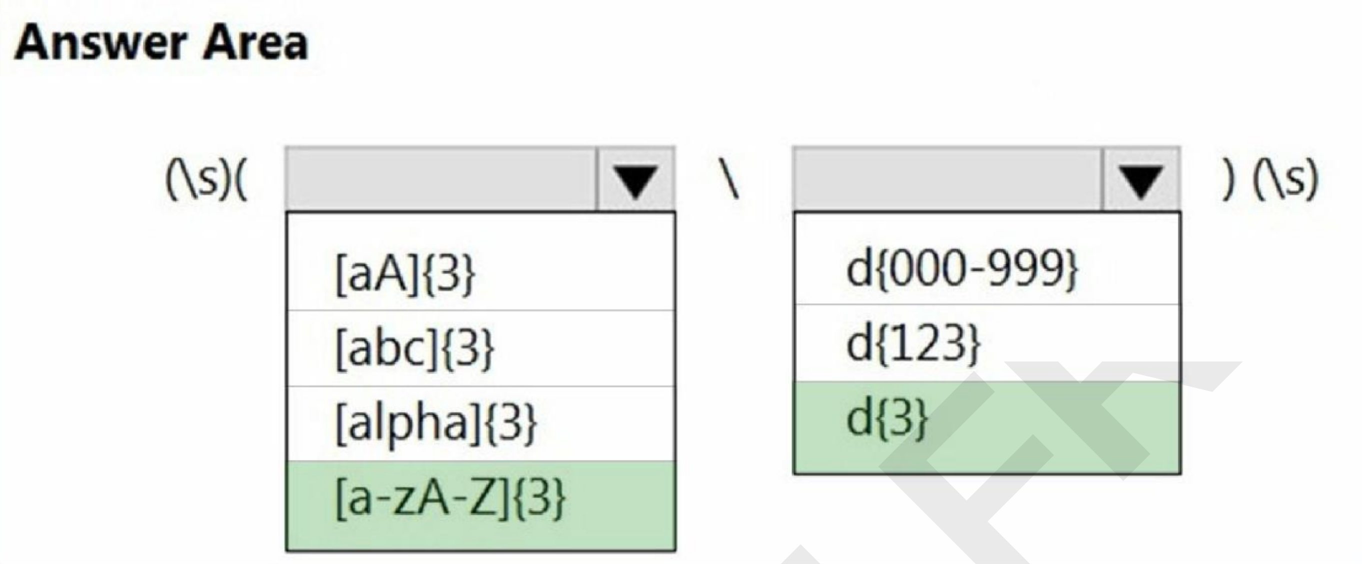
HOTSPOT -
You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.
You need to create a new sensitive info type for the project codes.
How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

(\s)([aA]{3} / [abc]{3} / [alpha]{3} / [a-zA-Z]{3} \ d{000-999} / d{123} / d{3}) (\s)

Answer:



Answer Area

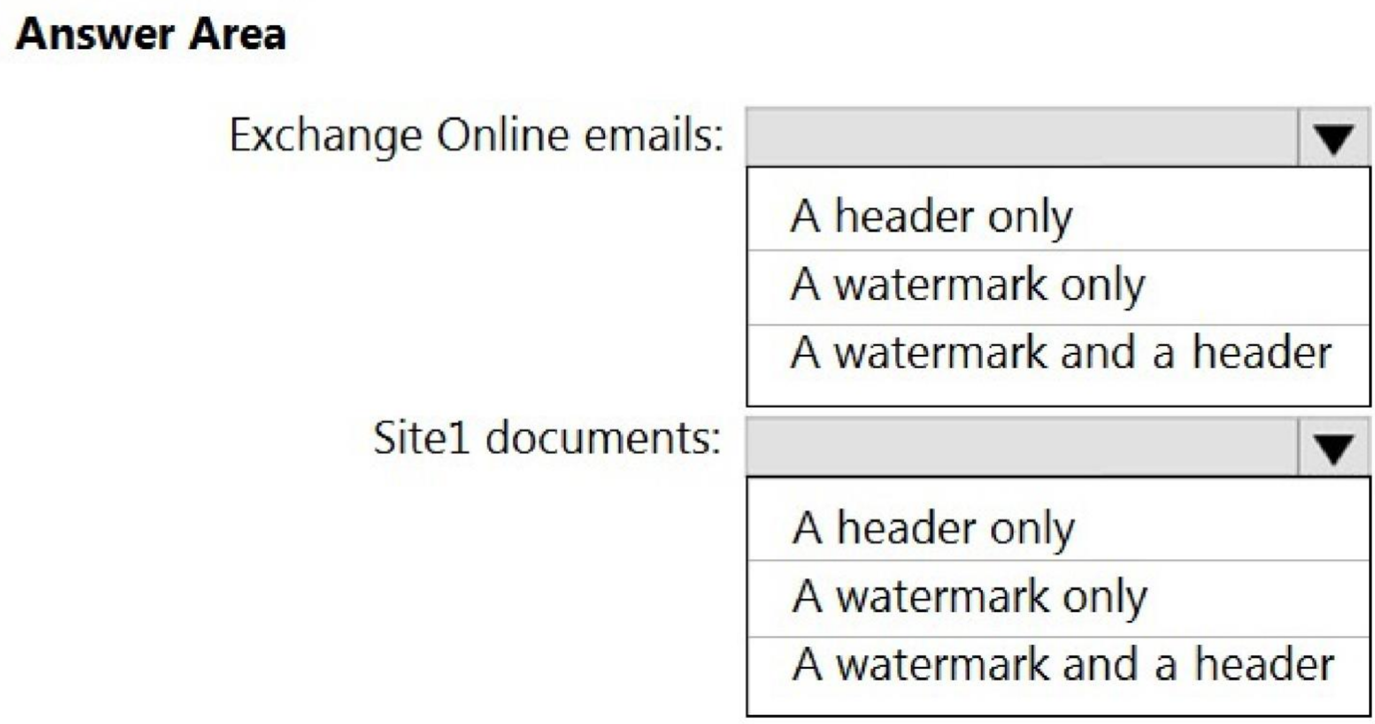
(\s)([aA]{3} / [abc]{3} / [alpha]{3} / [✓ [a-zA-Z]{3}] \ d{000-999} / d{123} / [✓ d{3}]) (\s)

Explanation:

Reference:
https://joannecklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/

Question: 5

HOTSPOT -
You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1. Sensitivity1 adds a watermark and a header to content.
You create a policy to automatically apply Sensitivity1 to emails in Microsoft Exchange Online and Site1. How will Sensitivity1 mark matching emails and Site1 documents? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

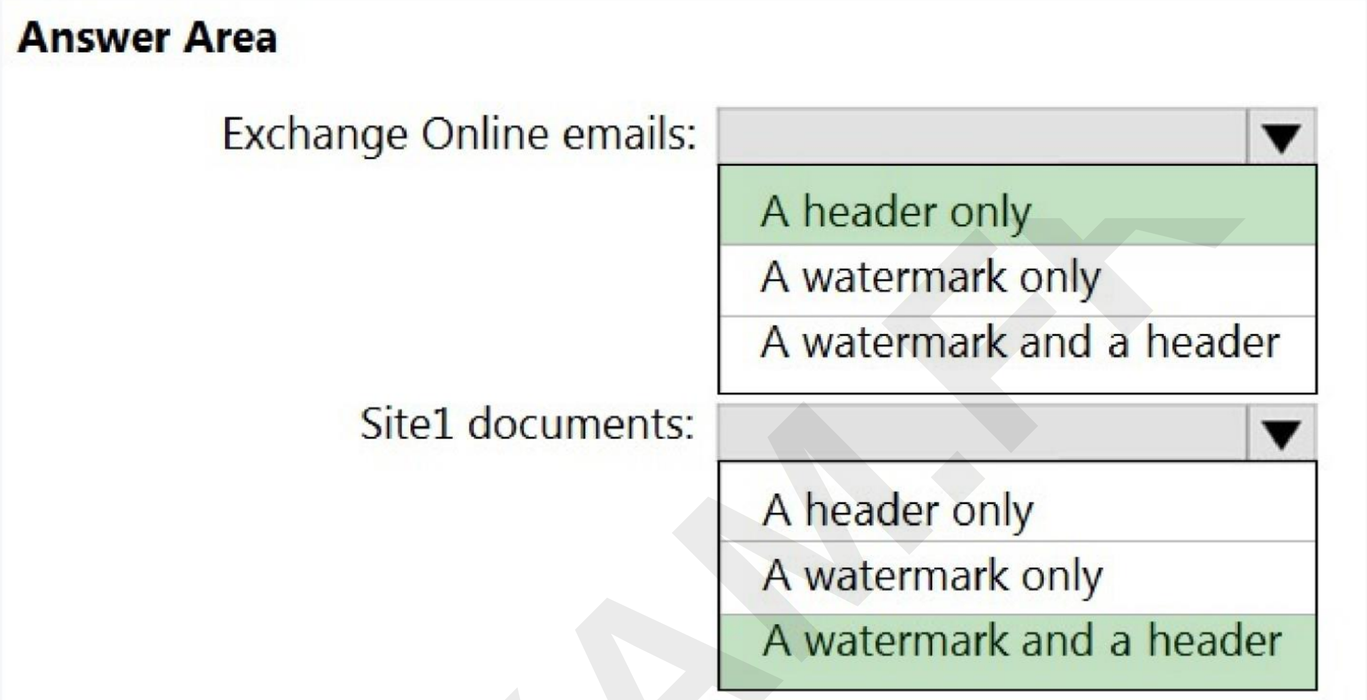
Exchange Online emails:

- A header only
- A watermark only
- A watermark and a header

Site1 documents:

- A header only
- A watermark only
- A watermark and a header

Answer:



Answer Area

Exchange Online emails:

- [✓ A header only]
- A watermark only
- A watermark and a header

Site1 documents:

- A header only
- A watermark only
- [✓ A watermark and a header]

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Question: 6

HOTSPOT -
You need to implement an information compliance policy to meet the following requirements:

➾ Documents that contain passport numbers from the United States, Germany, Australia, and Japan must be identified automatically.

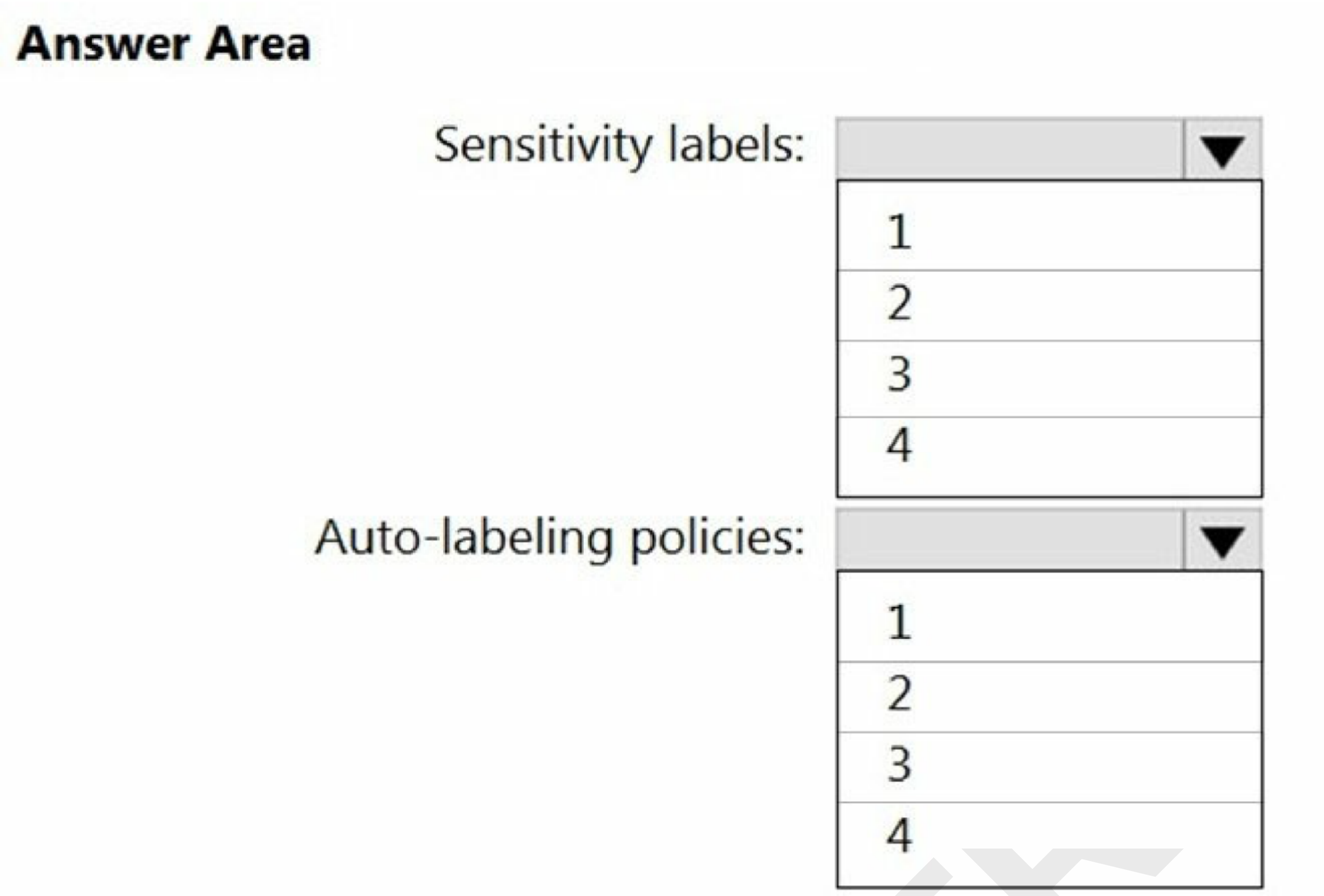
➾ When a user attempts to send an email or an attachment that contains a passport number, the user must receive a tooltip in Microsoft Outlook.

➾ Users must be blocked from using Microsoft SharePoint Online or OneDrive for Business to share a document that contains a passport number.

What is the minimum number of sensitivity labels and auto-labeling policies you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

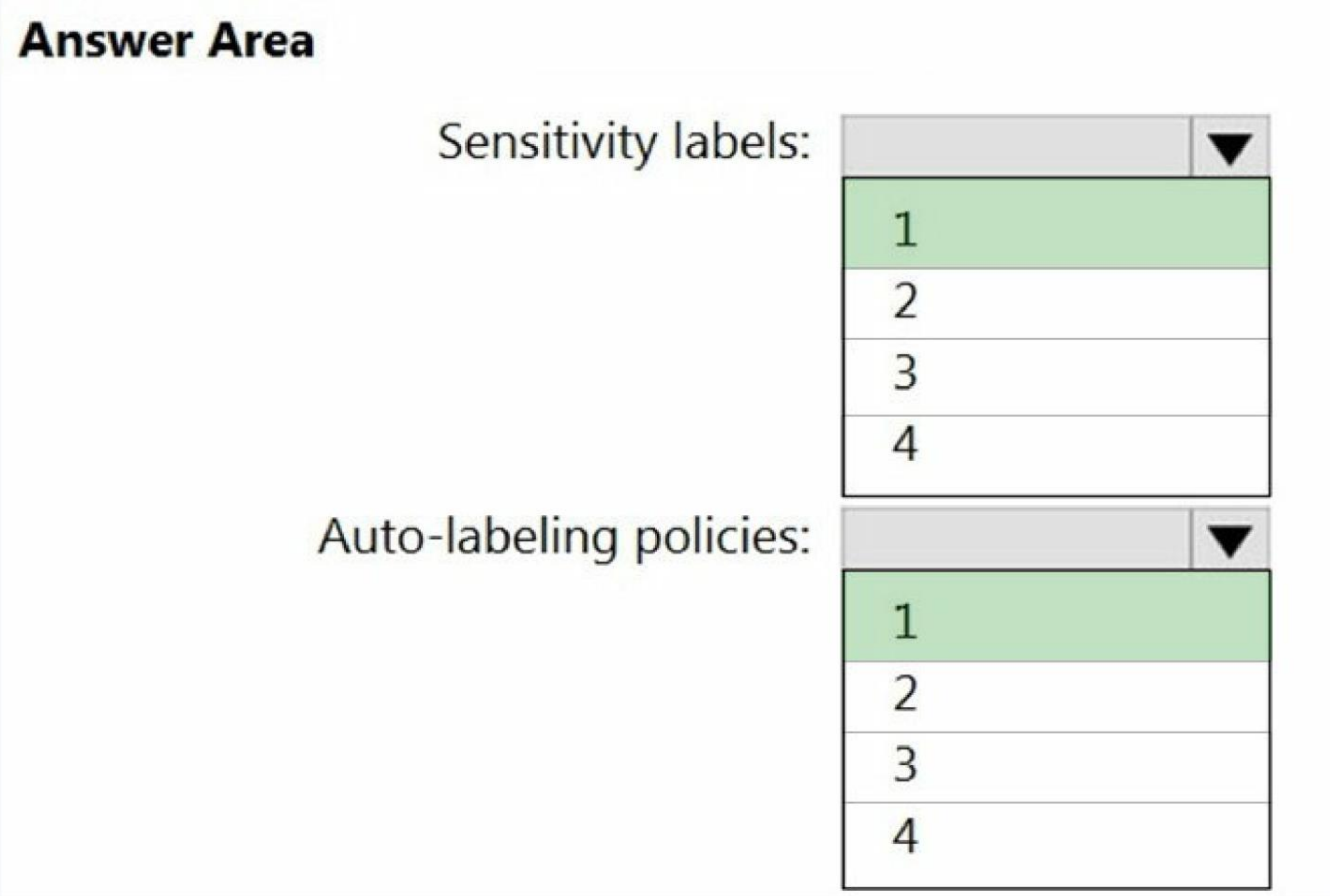


Answer Area

Sensitivity labels:
- 1
- 2
- 3
- 4

Auto-labeling policies:
- 1
- 2
- 3
- 4

Answer:



Answer Area

Sensitivity labels: [✓ 1] 2 3 4

Auto-labeling policies: [✓ 1] 2 3 4

Explanation:

We have four different kind of built-in sensitive information types for United States, Germany, Australia, and Japan in Data classification.

One Autolabeling policy can include all (4) passport sensitive information types in Rule-Conditions. In the same policy you choose one sensitivity label to add to files.

Reference:

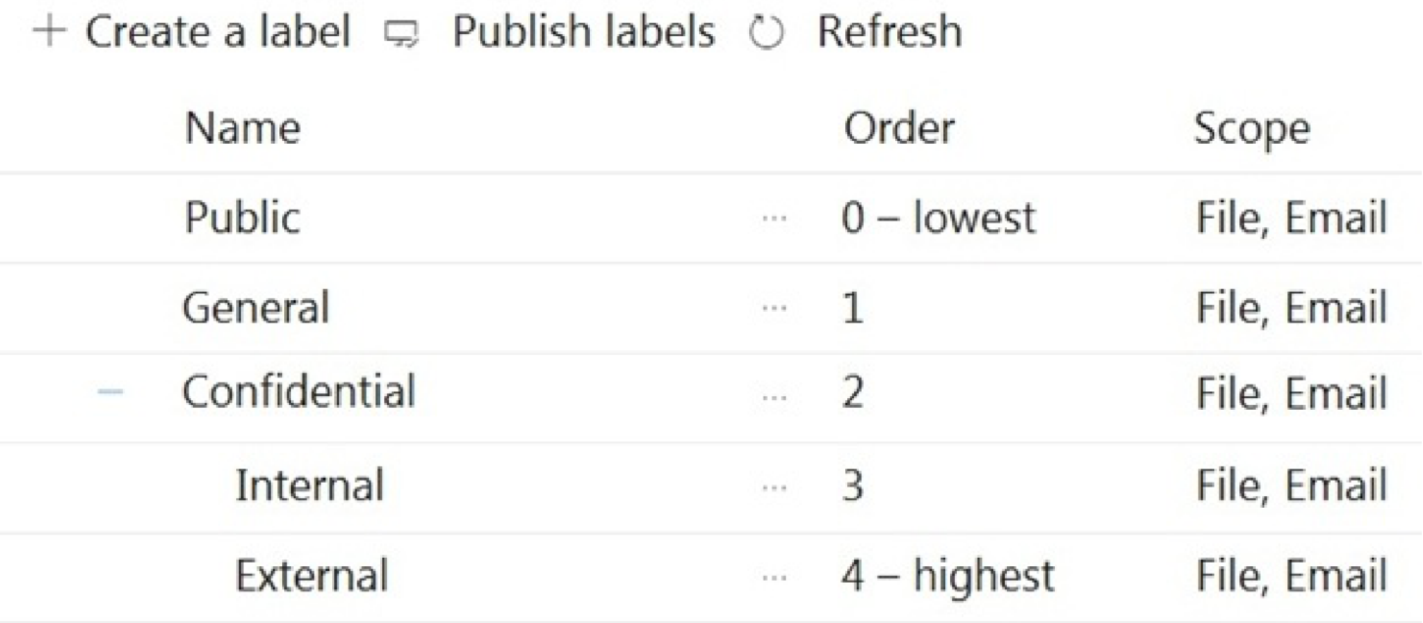
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

Question: 7

HOTSPOT -

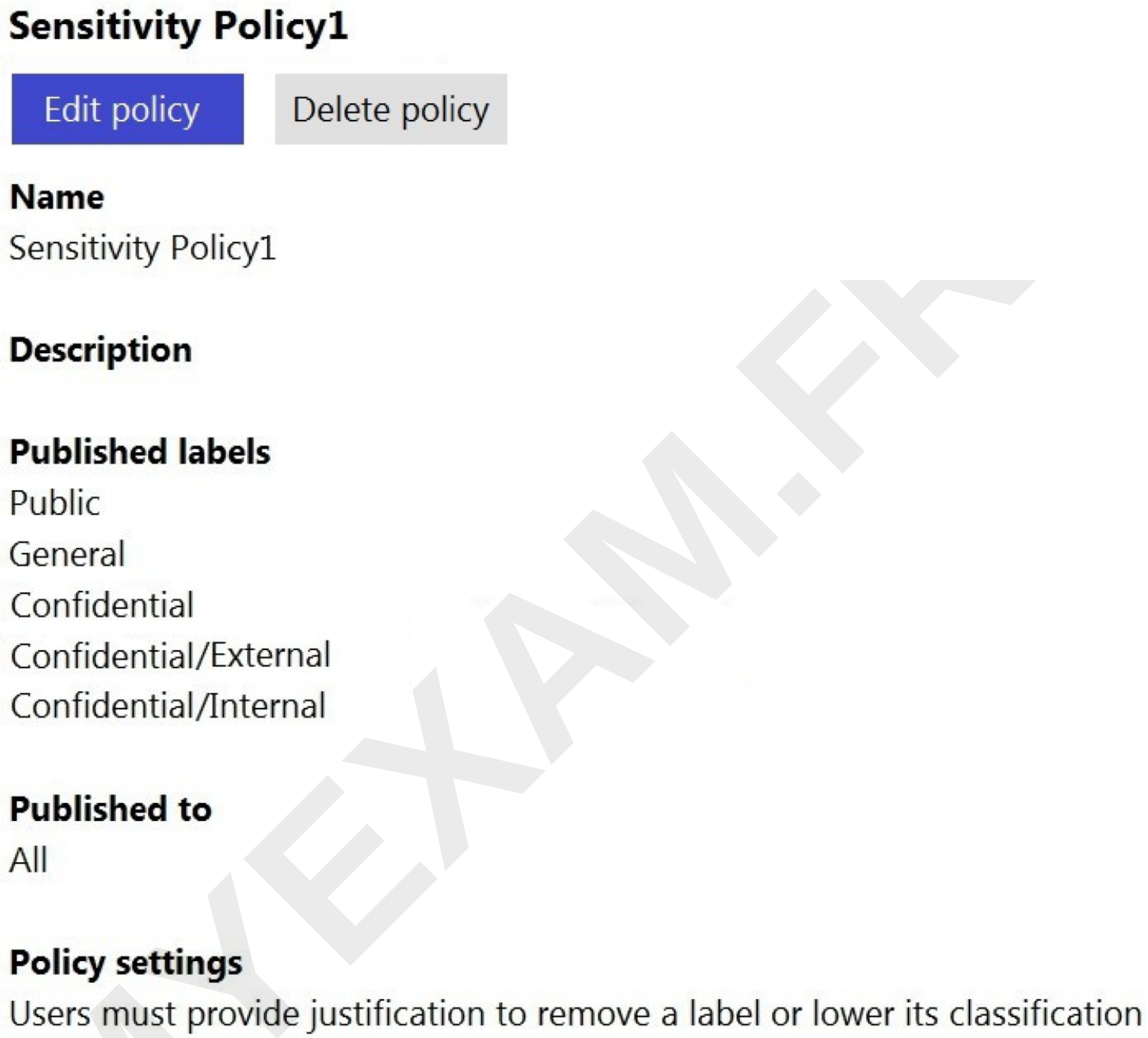
You have a Microsoft 365 E5 tenant.

You create sensitivity labels as shown in the Sensitivity Labels exhibit.



Name		Order	Scope
Public	···	0 – lowest	File, Email
General	···	1	File, Email
– Confidential	···	2	File, Email
Internal	···	3	File, Email
External	···	4 – highest	File, Email

The Confidential/External sensitivity label is configured to encrypt files and emails when applied to content. The sensitivity labels are published as shown in the Published exhibit.



Sensitivity Policy1

Name
Sensitivity Policy1

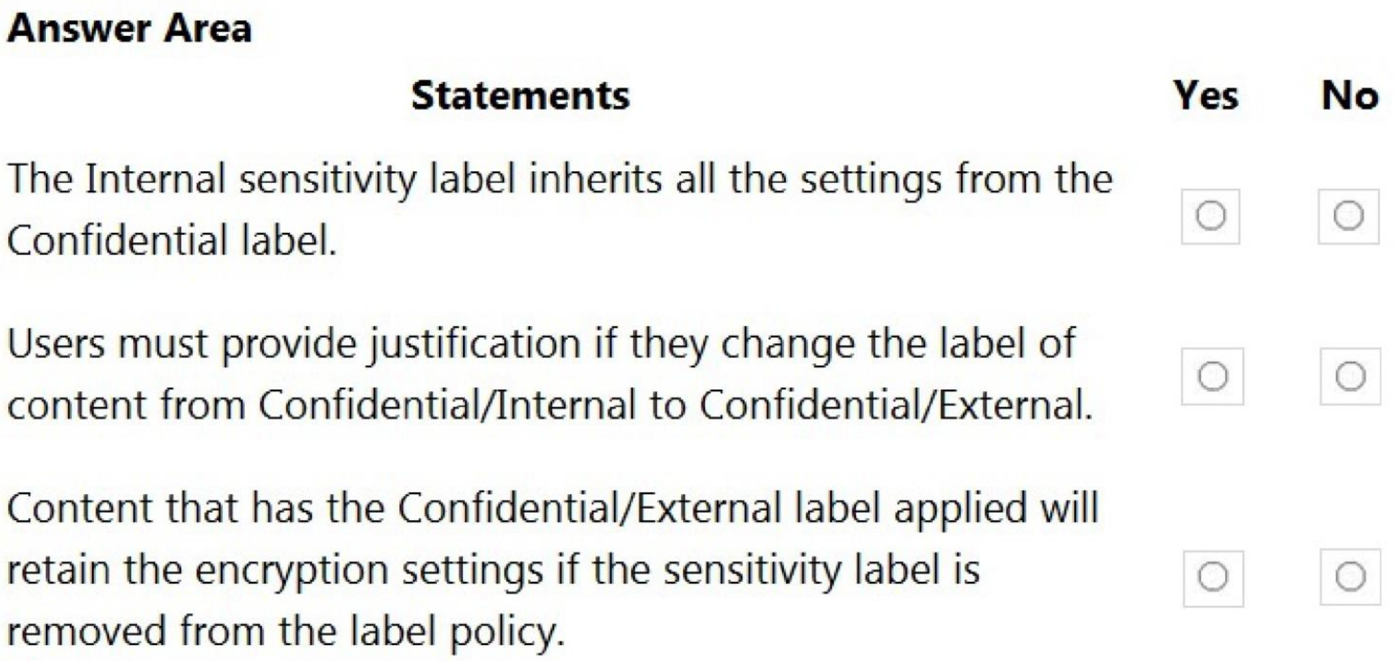
Description

Published labels
Public
General
Confidential
Confidential/External
Confidential/Internal

Published to
All

Policy settings
Users must provide justification to remove a label or lower its classification

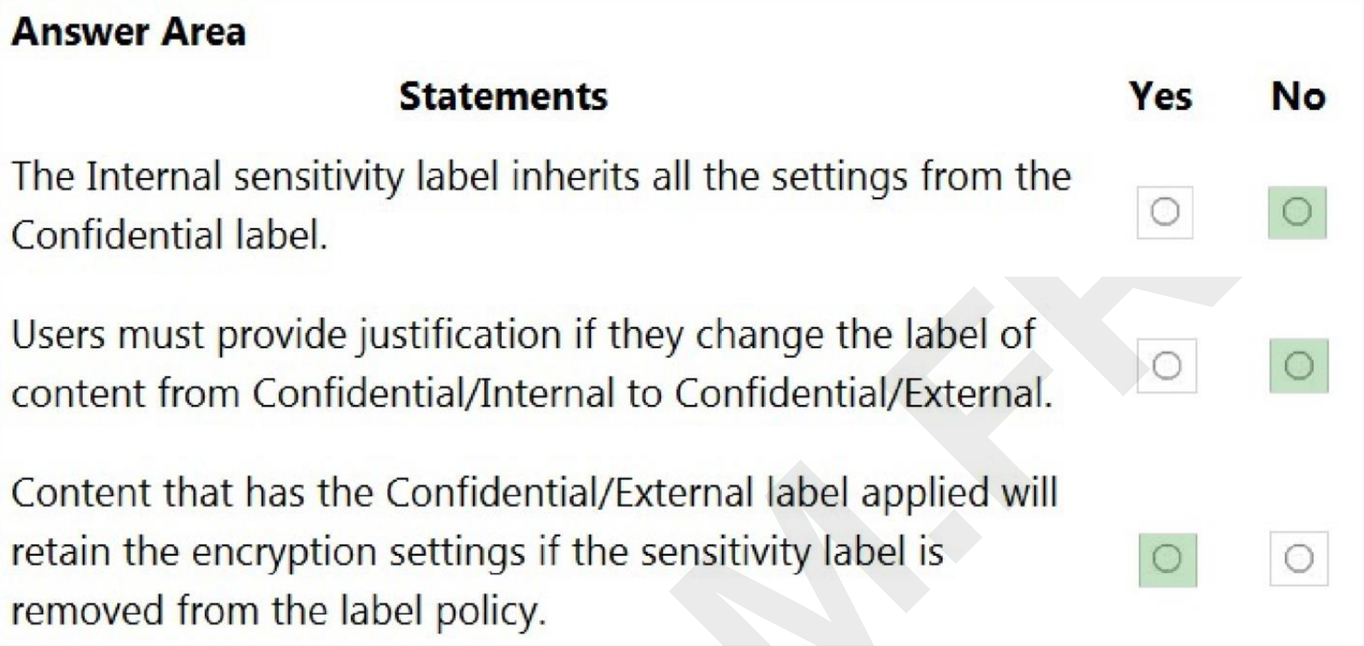
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	○	○
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	○	○
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	○	○

Answer:



Answer Area

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	○	●
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	○	●
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	●	○

Explanation:

Answer is: No/No/Yes.

- Sublabels don't inherit settings from their parent label (https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#sublabels-grouping-labels)
- Moving from Confidential\Internal to Confidential\External isn't lowering the label "level", it's the opposite, just check the labels order (https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#label-priority-order-matters)
- Well, when you remove a label that applied encryption to a document you don't necessarily remove the encryption. You only remove the encryption when you change to a label that removes encryption (you can configure that on the label settings)

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Question: 8

You are implementing a data classification solution.
The research department at your company requires that documents containing programming code be labeled as Confidential. The department provides samples of the code from its document library. The solution must minimize administrative effort.
What should you do?

A. Create a custom classifier.
B. Create a sensitive info type that uses Exact Data Match (EDM).
C. Use the source code classifier.
D. Create a sensitive info type that uses a regular expression.

Answer: C

Explanation:

Resumes, Source code, Harassment, Profanity, Threat are pre-trained classifiers that exist already in Microsoft 365 -> Source code is correct

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide

Question: 9

You have a new Microsoft 365 tenant.
You need to ensure that custom trainable classifiers can be created in the tenant. To which role should you be assigned to perform the configuration?

A. Security administrator
B. Security operator
C. Global administrator
D. Compliance administrator

Answer: C

Explanation:

Correct answer is Global Admin.

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

"the Global admin needs to opt in for the tenant to create custom classifiers.

Compliance Administrator role is required to train a classifier"

Question: 10

You need to automatically apply a sensitivity label to documents that contain information about your company's network including computer names, IP addresses, and configuration information.

Which two objects should you use? Each correct answer presents part of the solution. (Choose two.) NOTE: Each correct selection is worth one point.

A. an Information protection auto-labeling policy
B. a custom trainable classifier
C. a sensitive info type that uses a regular expression
D. a data loss prevention (DLP) policy
E. a sensitive info type that uses keywords
F. a sensitivity label that has auto-labeling

Answer: BF

Explanation:

True, the auto-labeling policy does not support trainable classifiers. So the answer would be B and F.

Question: 11

You are creating a custom trainable classifier to identify organizational product codes referenced in Microsoft 365 content.
You identify 300 files to use as seed content.
Where should you store the seed content?

A. a Microsoft SharePoint Online folder
B. a Microsoft OneDrive for Business folder
C. an Azure file share
D. Microsoft Exchange Online shared mailbox

Answer: A

Explanation:

A Microsoft SharePoint Online folder

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

Question: 12

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft Office 365 logo.
What should you do to create the branding templates?

A. Create a Transport rule.
B. Create an RMS template.
C. Run the Set-IRMConfiguration cmdlet.
D. Run the New-OMEConfiguration cmdlet.

Answer: D

Explanation:

D is correct. You use New-OMEConfiguration to CREATE the branding template (as the question asks). A transport rule is needed to apply it, but not to CREATE it.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide

Question: 13

You create a custom sensitive info type that uses Exact Data Match (EDM).
You plan to periodically update and upload the data used for EDM. What is the maximum frequency with which the data can be uploaded?

A. twice per week
B. twice per day
C. once every six hours
D. once every 48 hours
E. twice per hour

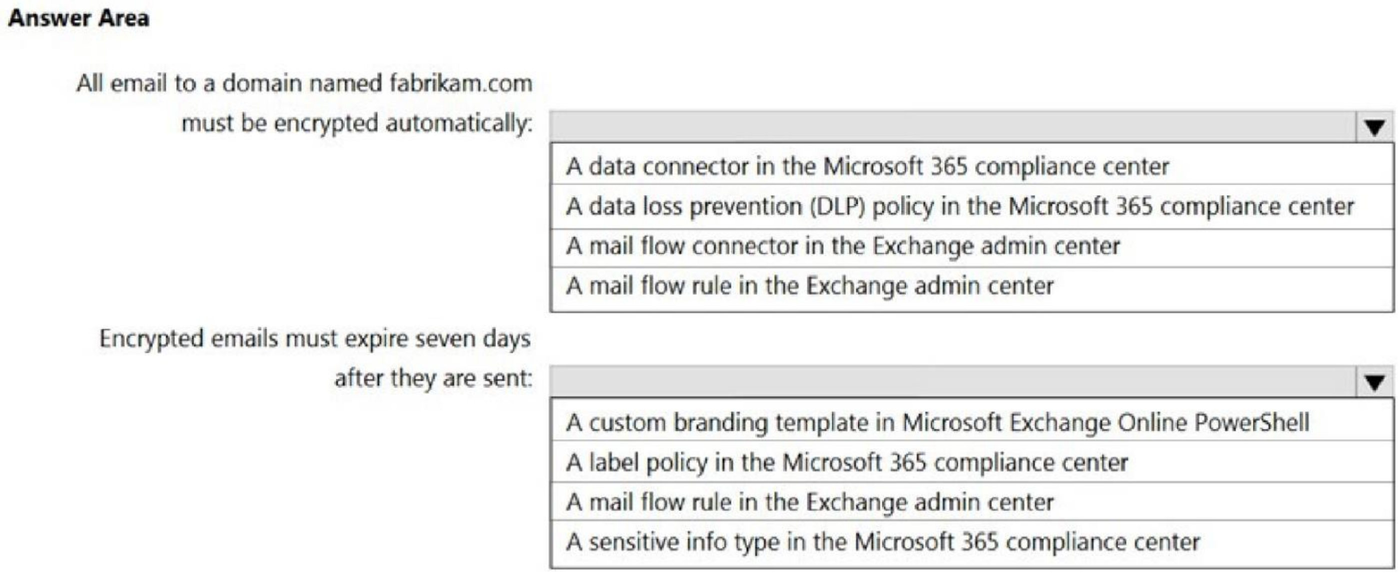
Answer: B

Explanation:
You can upload data with the EDMUploadAgent to any given data store only twice per day.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide

Question: 14

HOTSPOT -
You are implementing Microsoft Office 365 Message Encryption (OME) for a Microsoft 365 tenant named contoso.com.
You need to meet the following requirements:
✑ All email to a domain named fabrikam.com must be encrypted automatically.
✑ Encrypted emails must expire seven days after they are sent.
What should you configure for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

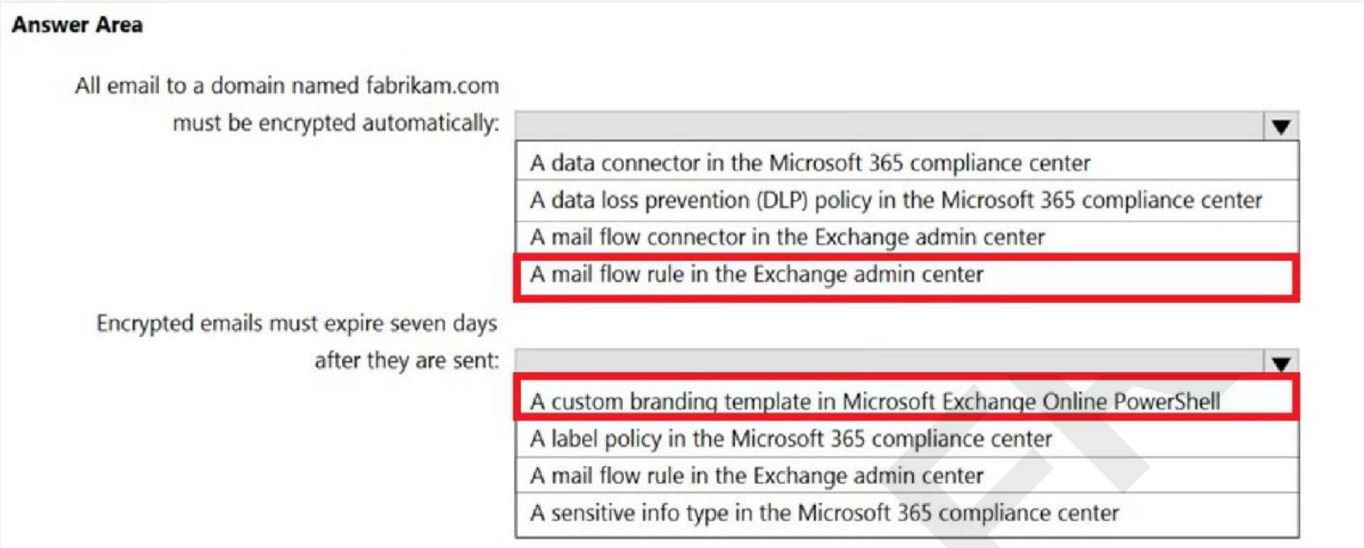
All email to a domain named fabrikam.com must be encrypted automatically: ▼

- A data connector in the Microsoft 365 compliance center
- A data loss prevention (DLP) policy in the Microsoft 365 compliance center
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent: ▼

- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft 365 compliance center
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft 365 compliance center

Answer:



Answer Area

All email to a domain named fabrikam.com must be encrypted automatically: ▼

- A data connector in the Microsoft 365 compliance center
- A data loss prevention (DLP) policy in the Microsoft 365 compliance center
- A mail flow connector in the Exchange admin center
- [✓ A mail flow rule in the Exchange admin center]

Encrypted emails must expire seven days after they are sent: ▼

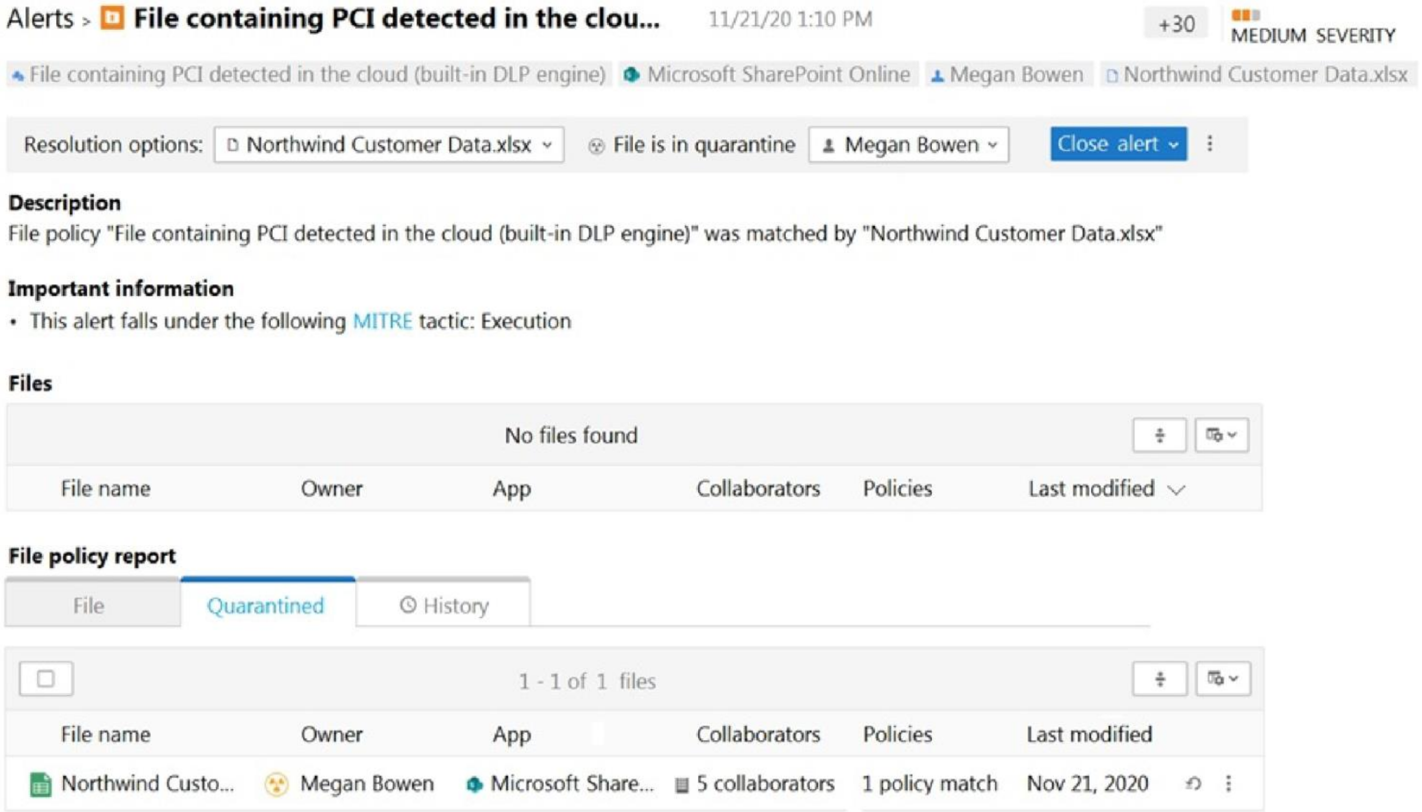
- [✓ A custom branding template in Microsoft Exchange Online PowerShell]
- A label policy in the Microsoft 365 compliance center
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft 365 compliance center

Explanation:

Correct answers are "A Mail Flow Rule" and "Custom Branding Template" .

Question: 15

A user reports that she can no longer access a Microsoft Excel file named Northwind Customer Data.xlsx.
From the Cloud App Security portal, you discover the alert shown in the exhibit.



Alerts > File containing PCI detected in the clou... 11/21/20 1:10 PM +30 MEDIUM SEVERITY

File containing PCI detected in the cloud (built-in DLP engine) · Microsoft SharePoint Online · Megan Bowen · Northwind Customer Data.xlsx

Resolution options: Northwind Customer Data.xlsx · File is in quarantine · Megan Bowen · Close alert

Description

File policy "File containing PCI detected in the cloud (built-in DLP engine)" was matched by "Northwind Customer Data.xlsx"

Important information

- This alert falls under the following MITRE tactic: Execution

Files

No files found

File name	Owner	App	Collaborators	Policies	Last modified

File policy report

File | Quarantined | History

1 - 1 of 1 files

File name	Owner	App	Collaborators	Policies	Last modified
Northwind Custo...	Megan Bowen	Microsoft Share...	5 collaborators	1 policy match	Nov 21, 2020

You restore the file from quarantine.

You need to prevent files that match the policy from being quarantined. Files that match the policy must generate an alert.

What should you do?

A. Modify the policy template.

B. Assign the Global reader role to the file owners.

C. Exclude file matching by using a regular expression.

D. Update the governance action.

Answer: D

Explanation:

Answer is correct IMHO:

A. It's not the answers, since you cannot modify a policy template in MCAS. You can create policies from policies templates

B. Assigning that role is not going to prevent files to be quarantined

C. We don't want to exclude the file, we want to receive an alert instead of the file being sent to quarantine

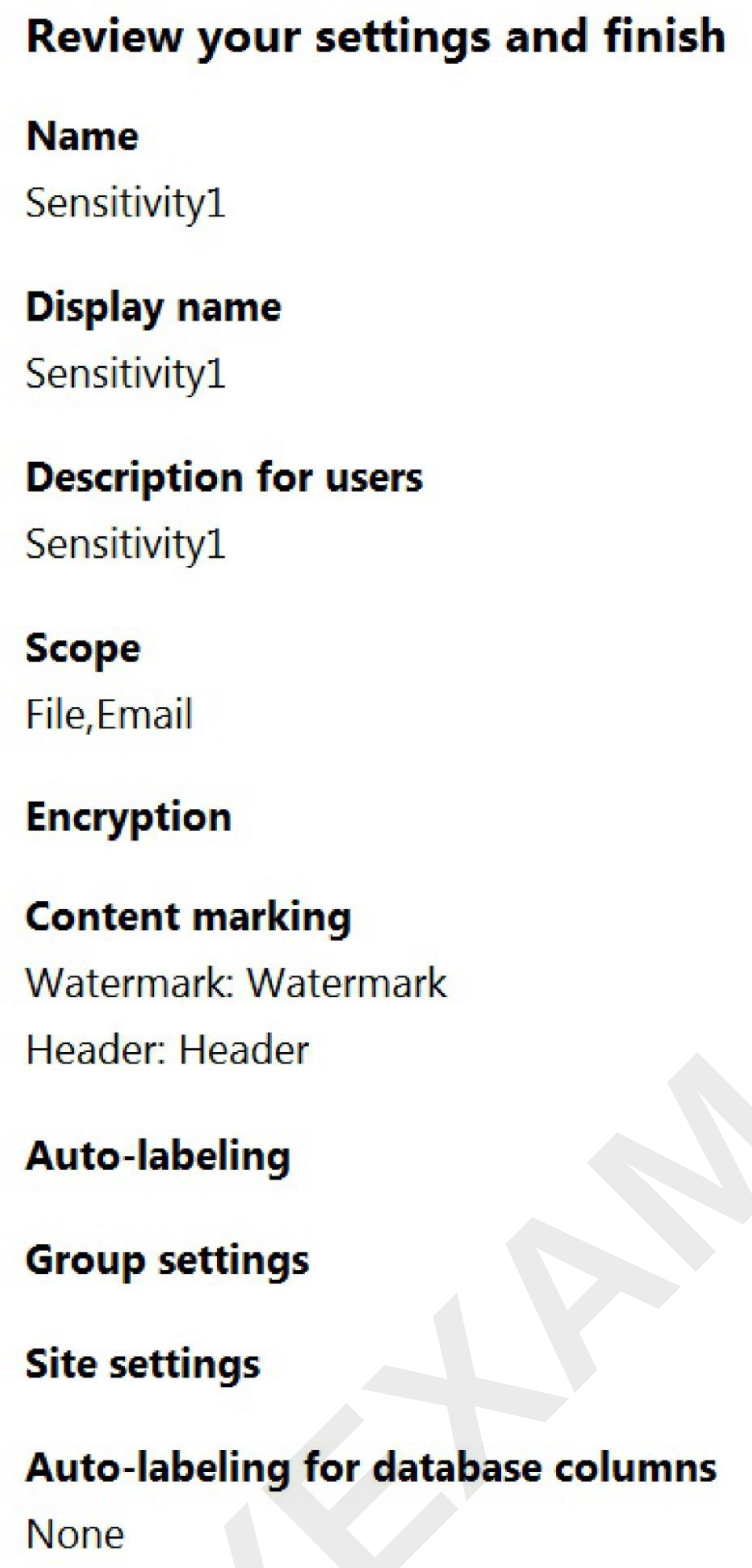
Reference:

https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies#create-a-new-file-policy

Question: 16 HOTSPOT

-

You create a sensitivity label as shown in the Sensitivity Label exhibit.



Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File,Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

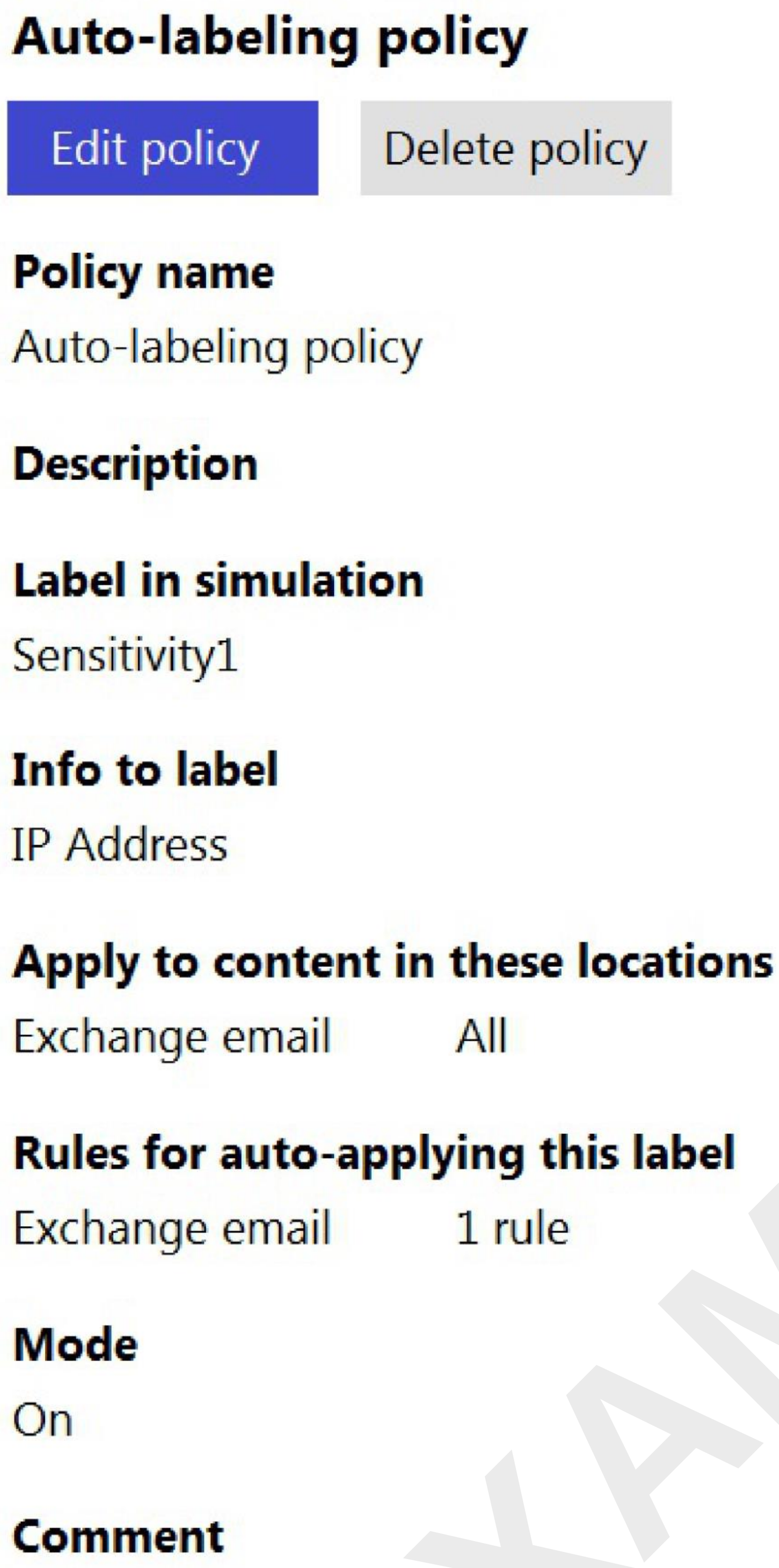
Group settings

Site settings

Auto-labeling for database columns

None

You create an auto-labeling policy as shown in the Auto Labeling Policy exhibit.



Auto-labeling policy

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address

Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

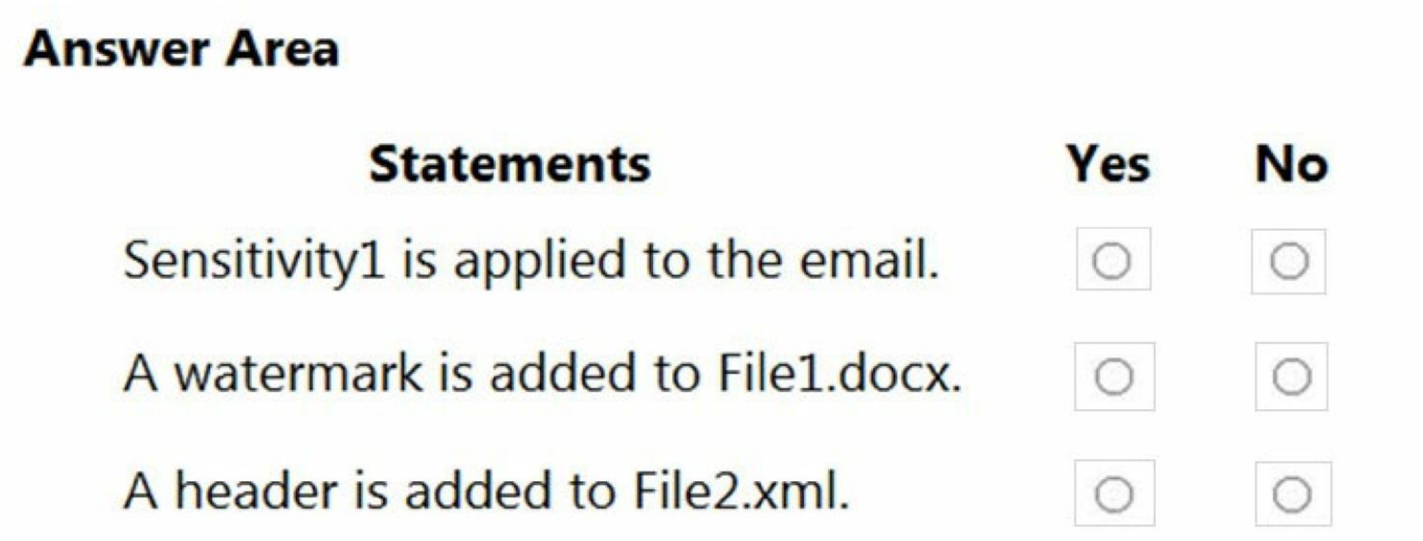
A user sends the following email:

From: [email protected] -

To: [email protected] -

Subject: Address List -
Message Body:
Here are the lists that you requested.
Attachments:
<<File1.docx>>
<<File2.xml>>
Both attachments contain lists of IP addresses.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

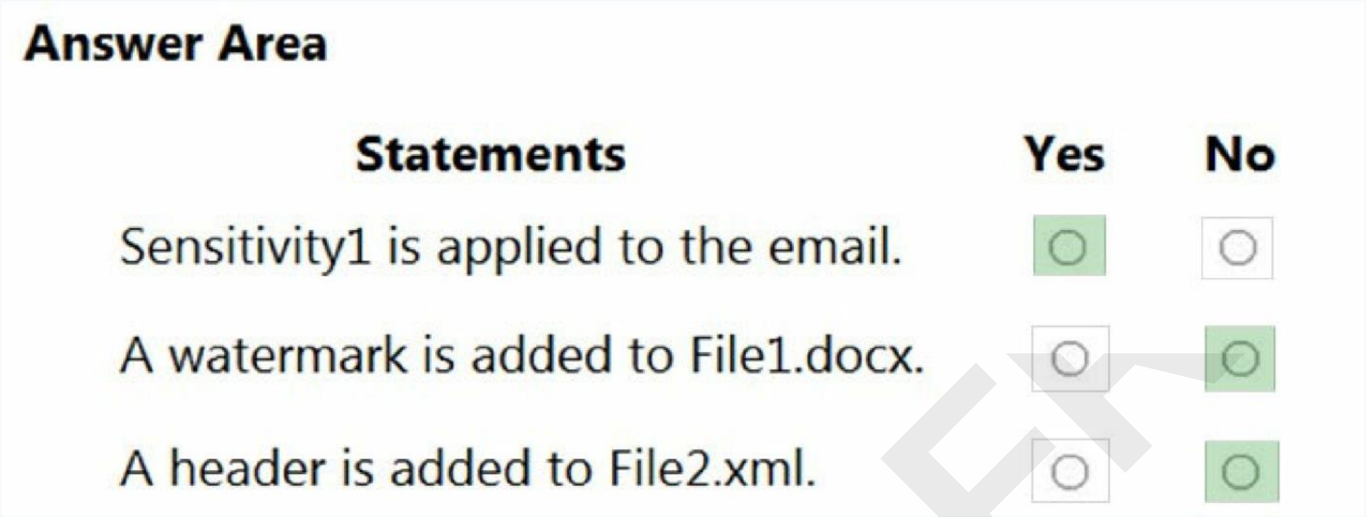
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

Answer:



Answer Area

Statements	Yes	No
Sensitivity1 is applied to the email.	[✓ ○]	○
A watermark is added to File1.docx.	○	[✓ ○]
A header is added to File2.xml.	○	[✓ ○]

Explanation:
Box 1: Yes -

Box 2: No -
The email is labeled but not the attachment.

Box 3: No -

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o36 5-worldwide

Question: 17

You receive an email that contains a list of words that will be used for a sensitive information type. You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list?

A. a JSON file that has an element for each word
B. an ACCDB database file that contains a table named Dictionary
C. an XML file that contains a keyword tag for each word

D. a CSV file that contains words separated by commas

Answer: D

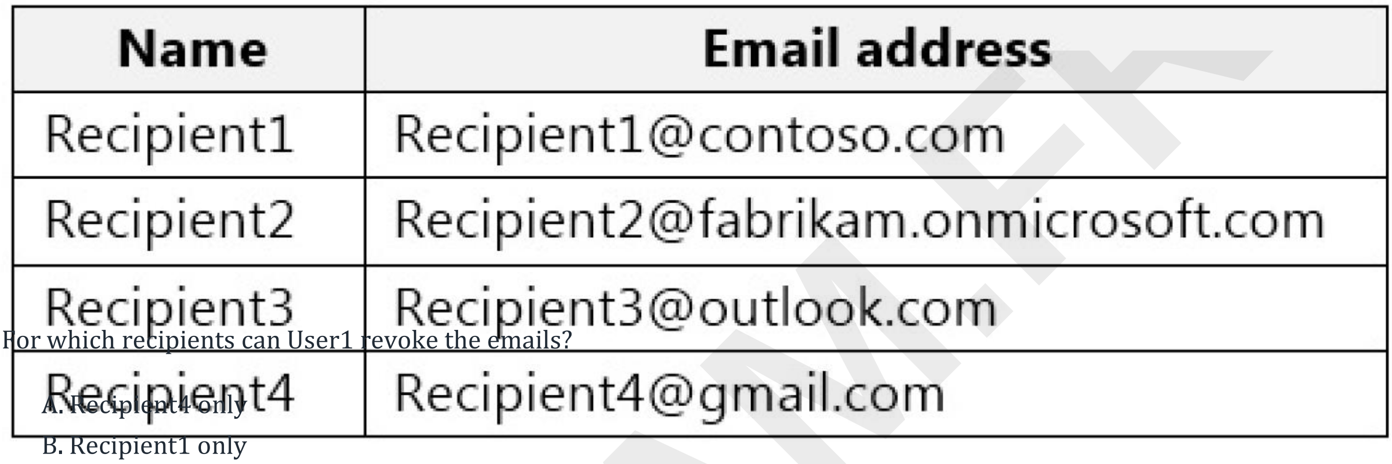
Explanation:
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet.

Note:
There are several versions of this question in the exam. The question has two possible correct answers: 1. a CSV file that contains words separated by commas
2. a text file that has one word on each line
Other incorrect answer options you may see on the exam include the following:
➾ a TSV file that contains words separated by tabs
➾ an XLSX file that contains one word in each cell of the first row
➾ a DOCX file that has one word on each line

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-world wide

Question: 18

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.
A user named User1 sends link-based, branded emails that are encrypted by using Microsoft Office 365 Advanced Message Encryption to the recipients shown in the following table.



Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients can User1 revoke the emails?

A. Recipient4 only
B. Recipient1 only
C. Recipient1, Recipient2, Recipient3, and Recipient4
D. Recipient3 and Recipient4 only
E. Recipient1 and Recipient2 only

Answer: A

Explanation:

Correct answer is "A"

"You cannot revoke a mail that you sent to a recipient that uses a work or school account from Office 365 or Microsoft 365 or a user that uses a Microsoft account, for example, an outlook.com account."

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide

Question: 19

You need to test Microsoft Office 365 Message Encryption (OME) capabilities for your company. The test must verify the following information:

➾ The acquired default template names

➾ The encryption and decryption verification status

Which PowerShell cmdlet should you run?

A. Test-ClientAccessRule
B. Test-Mailflow
C. Test-OAuthConnectivity
D. Test-IRMConfiguration

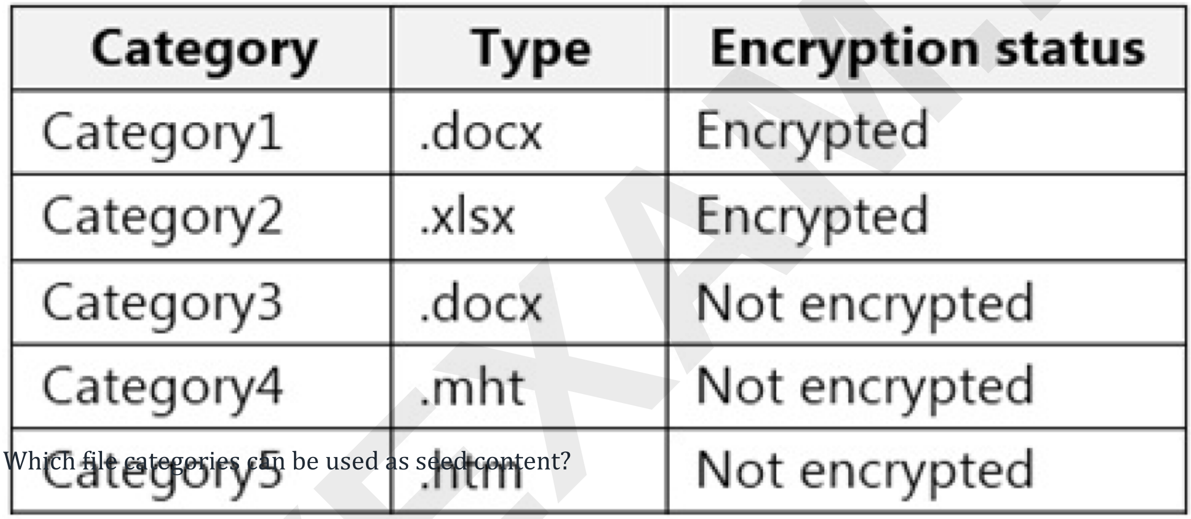
Answer: D

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide

Question: 20

You have a Microsoft 365 tenant that uses trainable classifiers.
You are creating a custom trainable classifier.
You collect 300 sample file types from various geographical locations to use as seed content. Some of the file samples are encrypted.
You organize the files into categories as shown in the following table.



Category	Type	Encryption status
Category1	.docx	Encrypted
Category2	.xlsx	Encrypted
Category3	.docx	Not encrypted
Category4	.mht	Not encrypted
Category5	.htm	Not encrypted

Which file categories can be used as seed content?

A. Category2, Category3, and Category5 only
B. Category3 and Category5 only
C. Category1 and Category3 only
D. Category3 only
E. Category1, Category2, Category3, Category4, and Category5

Answer: B

Explanation:

Classifiers only work with items that are not encrypted and have file name extensions that are supported by SharePoint Online.

Note: SharePoint Online does not support .eml and .mht files.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
https://docs.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

Question: 21

You have a Microsoft 365 tenant that uses Microsoft Office 365 Message Encryption (OME).
You need to ensure that any emails containing attachments and sent to [email protected] are encrypted automatically by using OME.
What should you do?

A. From the Exchange admin center, create a new sharing policy.

B. From the Microsoft 365 security center, create a Safe Attachments policy.

C. From the Exchange admin center, create a mail flow rule.

D. From the Microsoft 365 compliance center, configure an auto-apply retention label policy.

Answer: C

Explanation:
You can create mail flow rules to help protect email messages you send and receive. You can set up rules to encrypt any outgoing email messages and remove encryption from encrypted messages coming from inside your organization or from replies to encrypted messages sent from your organization.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/define-mail-flow-rules-to-encrypt-email?view=o 365-worldwide

Question: 22

You plan to implement sensitivity labels for Microsoft Teams.
You need to ensure that you can view and apply sensitivity labels to new Microsoft Teams sites. What should you do first?

A. Run the Set-SPOSite cmdlet.

B. Create a new sensitivity label scoped to Groups & sites.

C. Run the Execute-AzureAdLabelSync cmdlet.

D. Configure the EnableMIPLabels Azure Active Directory (Azure AD) setting.

Answer: D

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

Step 1 says - ollow the instructions from the Azure AD documentation to enable sensitivity label support The link takes you to

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels Look at step 5 - Enable the feature "EnableMIPLabels"] = "True"

The AzureAdLabelSync cmdlet follows. See troubleshooting #3 and the sentence after #5, You will also need to synchronize your sensitivity labels to Azure AD

Select Groups, and then select New group is #2 in the next section AFTER EnableMIPLabels has been enabled.

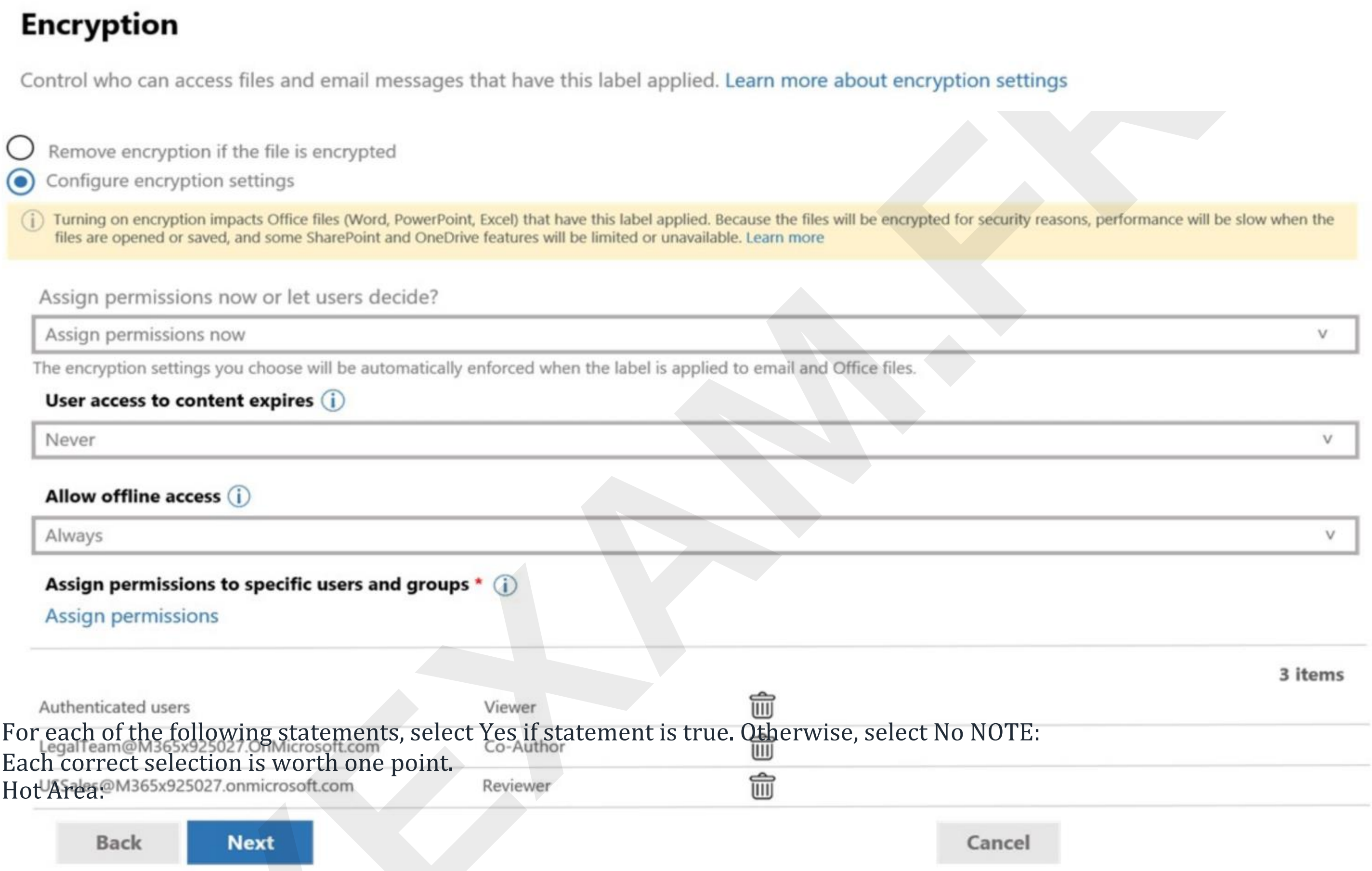
D is the answer.

Question: 23

HOTSPOT

-

You have Microsoft 365 E5 tenant that has a domain name of M365x925027.onmicrosoft.com.
You have a published sensitivity label.
The Encryption settings for the sensitivity label are configured as shown in the exhibit.



Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires: Never

Allow offline access: Always

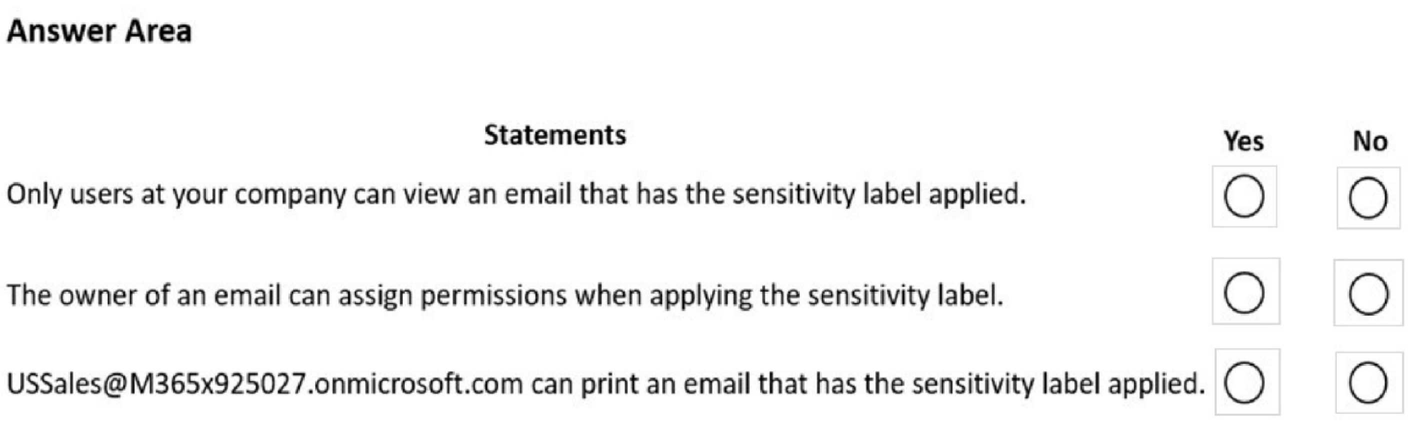
Assign permissions to specific users and groups *

Assign permissions

3 items

Authenticated users	Viewer	🗑
LegalTeam@M365x925027.OnMicrosoft.com	Co-Author	🗑
USSales@M365x925027.onmicrosoft.com	Reviewer	🗑

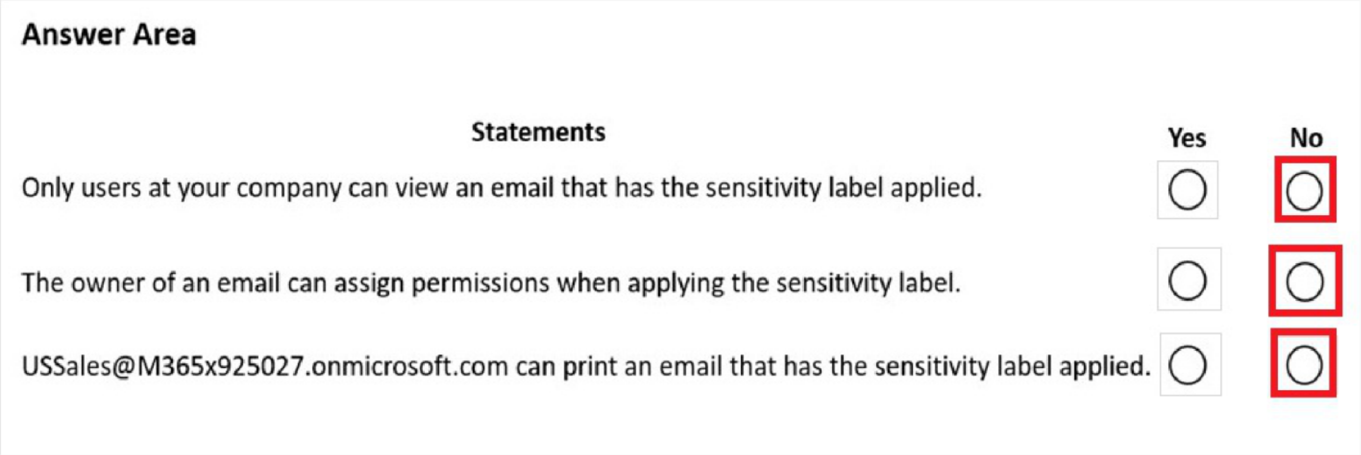
For each of the following statements, select Yes if statement is true. Otherwise, select No NOTE:
Each correct selection is worth one point.
Hot Area:



Answer Area

Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied.	○	○
The owner of an email can assign permissions when applying the sensitivity label.	○	○
USSales@M365x925027.onmicrosoft.com can print an email that has the sensitivity label applied.	○	○

Answer:



Answer Area

Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied.	○	[✓ ○]
The owner of an email can assign permissions when applying the sensitivity label.	○	[✓ ○]
USSales@M365x925027.onmicrosoft.com can print an email that has the sensitivity label applied.	○	[✓ ○]

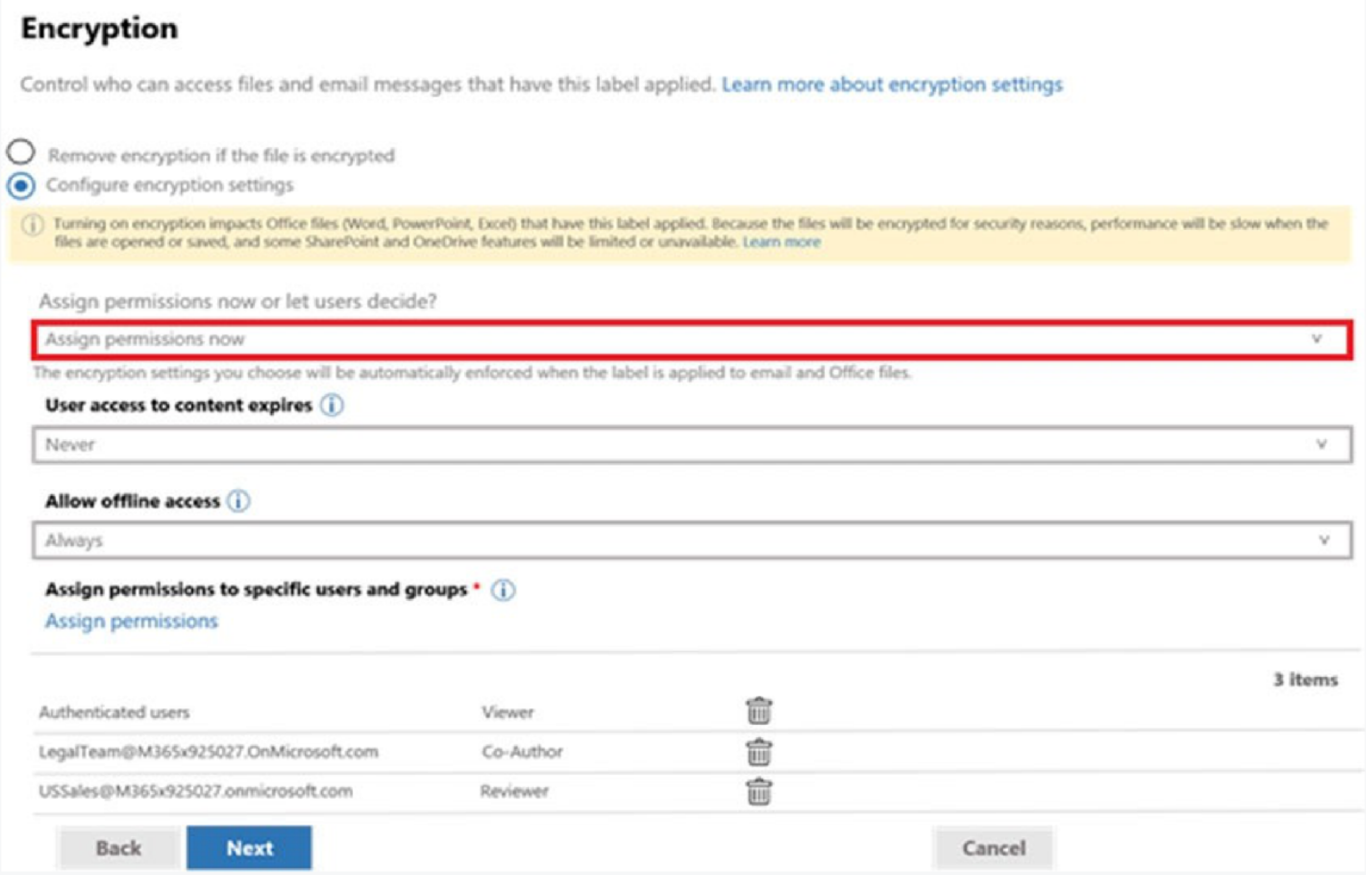
Explanation:

Box 1: No

If you choose to encrypt, you still need to specify who can view/read the documents, that includes your own organization.

Box 2: No -

Assign permissions now has been selected.



Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires: Never

Allow offline access: Always

Assign permissions to specific users and groups *

Assign permissions

3 items

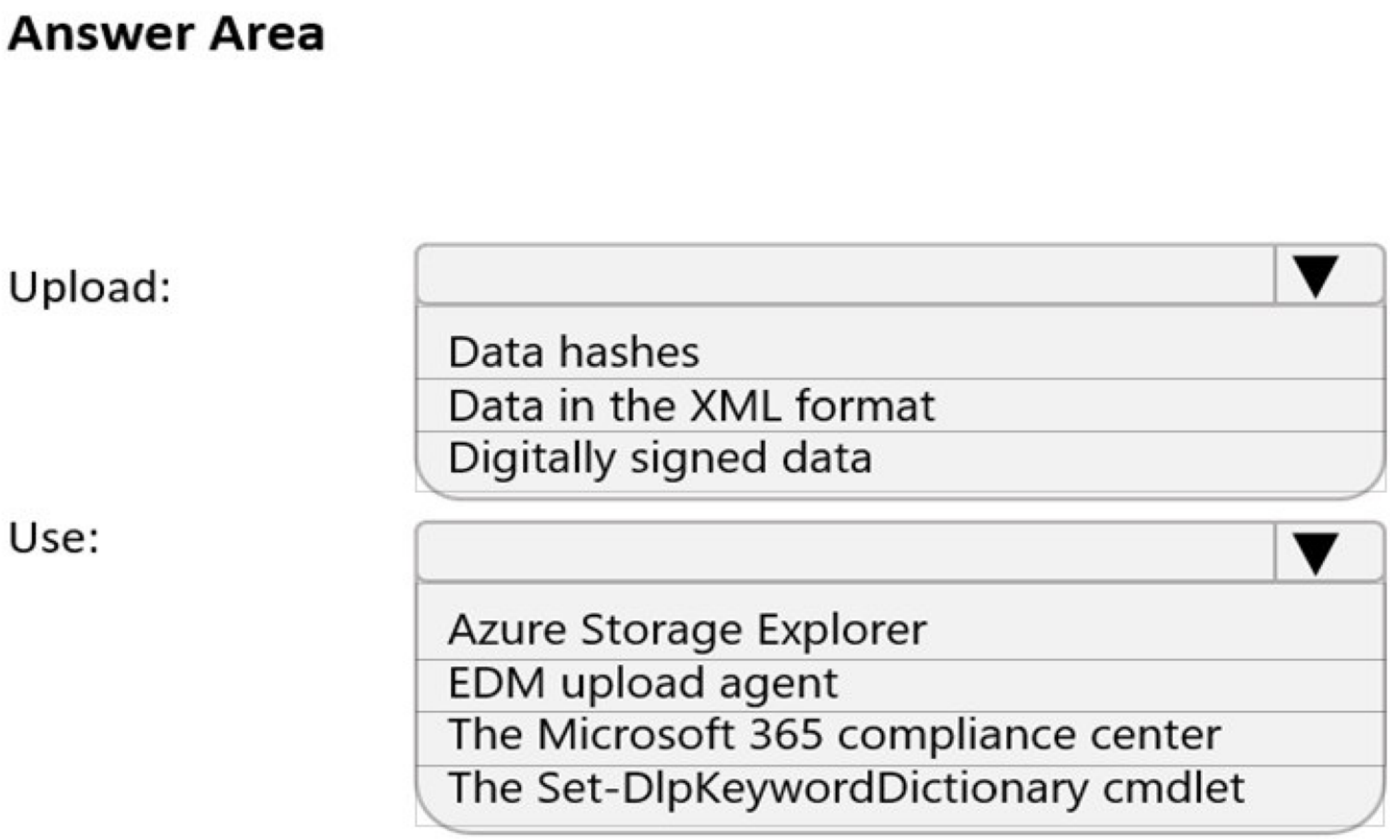
Authenticated users	Viewer
LegalTeam@M365x925027.OnMicrosoft.com	Co-Author
USSales@M365x925027.onmicrosoft.com	Reviewer

Box 3: No -

Only co-author and co-owner can print.

Question: 24

HOTSPOT -
You plan to create a custom sensitive information type that will use Exact Data Match (EDM).
You need to identify what to upload to Microsoft 365, and which tool to use for the upload.
What should you identify? To answer, select the appropriate options in the answer area. NOTE:
Each correct selection is worth one point.
Hot Area:



Answer Area

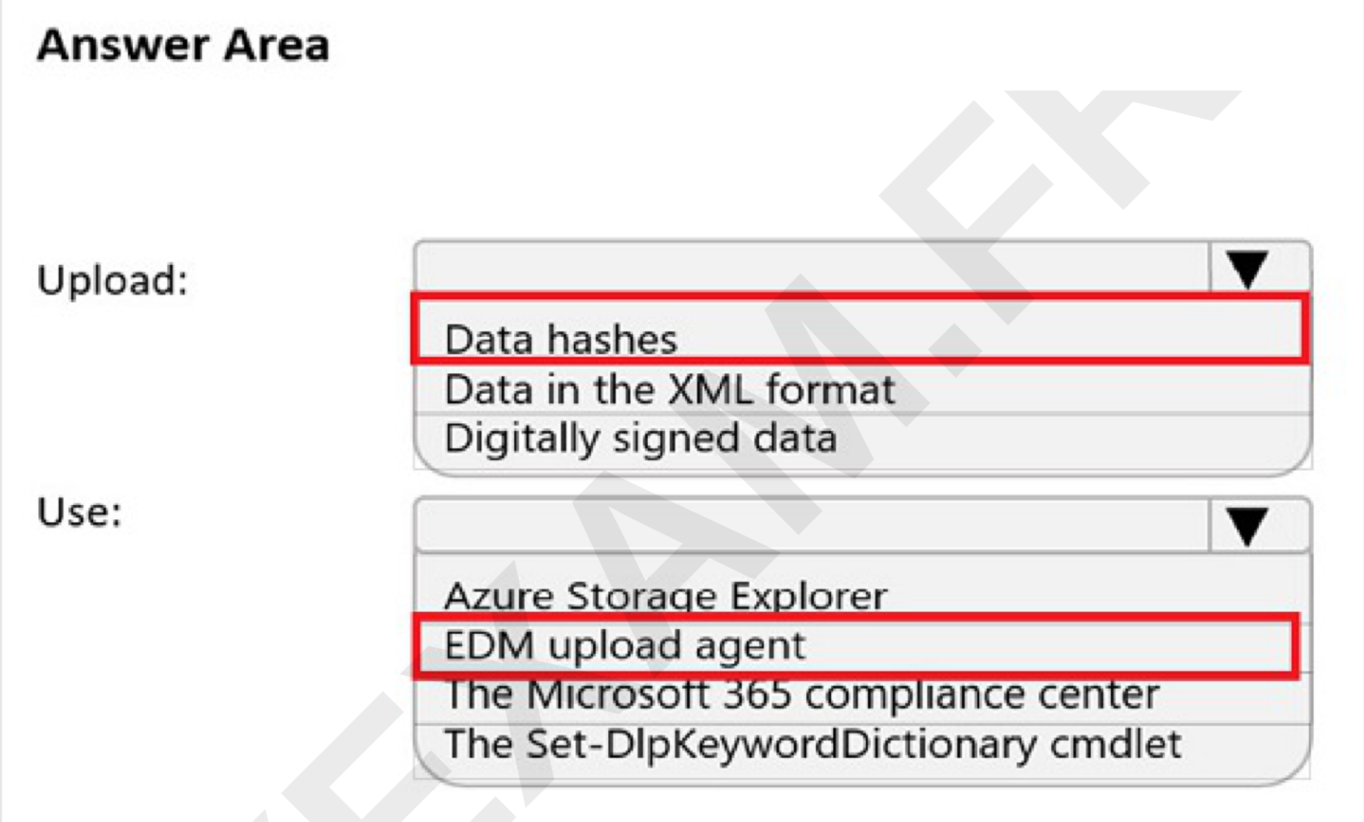
Upload:

Data hashes
Data in the XML format
Digitally signed data

Use:

Azure Storage Explorer
EDM upload agent
The Microsoft 365 compliance center
The Set-DlpKeywordDictionary cmdlet

Answer:



Answer Area

Upload:

Data hashes
Data in the XML format
Digitally signed data

Use:

Azure Storage Explorer
EDM upload agent
The Microsoft 365 compliance center
The Set-DlpKeywordDictionary cmdlet

Explanation:

Correct Data hashes and EDM upload agent

Steps

1. Setup EDM-based classification

2. Hash and upload the sensitive data

3. Use EDM-based classification with your Microsoft cloud services

Hash and upload the sensitive information source table

1. set up a custom security group and user account

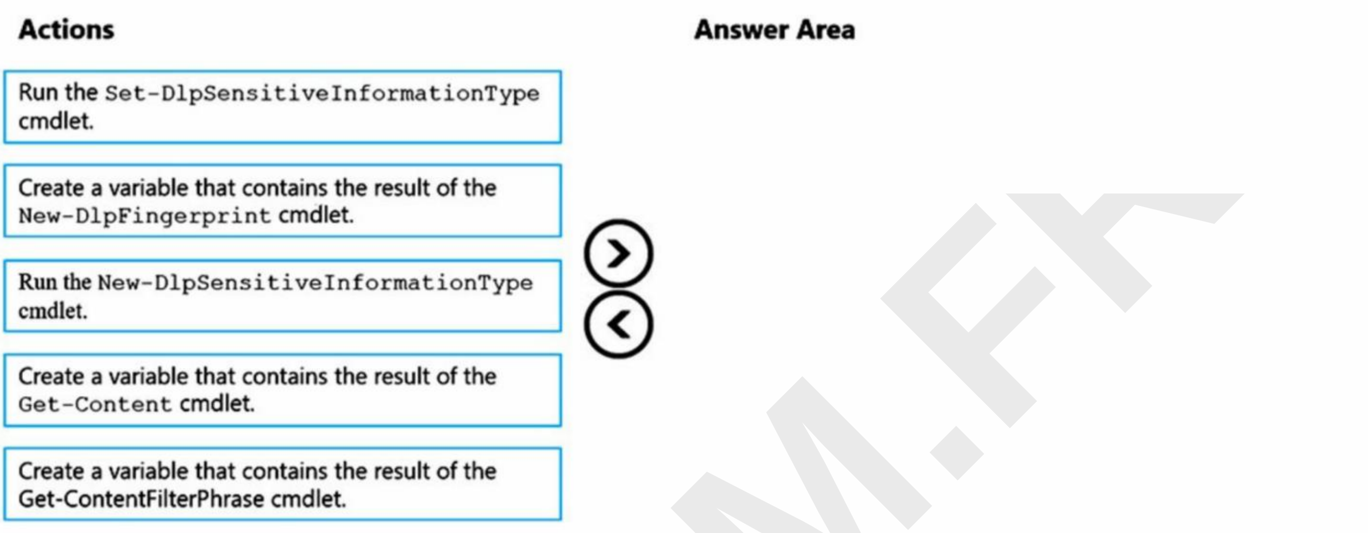
2. set up the EDM Upload Agent tool

3. Use the EDM Upload Agent tool to hash, with a salt value, the sensitive information source table, and upload it.

https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide#hash-and-upload-the-sensitive-information-source-table

Question: 25

DRAG DROP -
You have a Microsoft 365 tenant that uses data loss prevention (DLP).
You have a custom employee information form named Template1.docx.
You need to create a classification rule package based on the document fingerprint of Template1.docx. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:

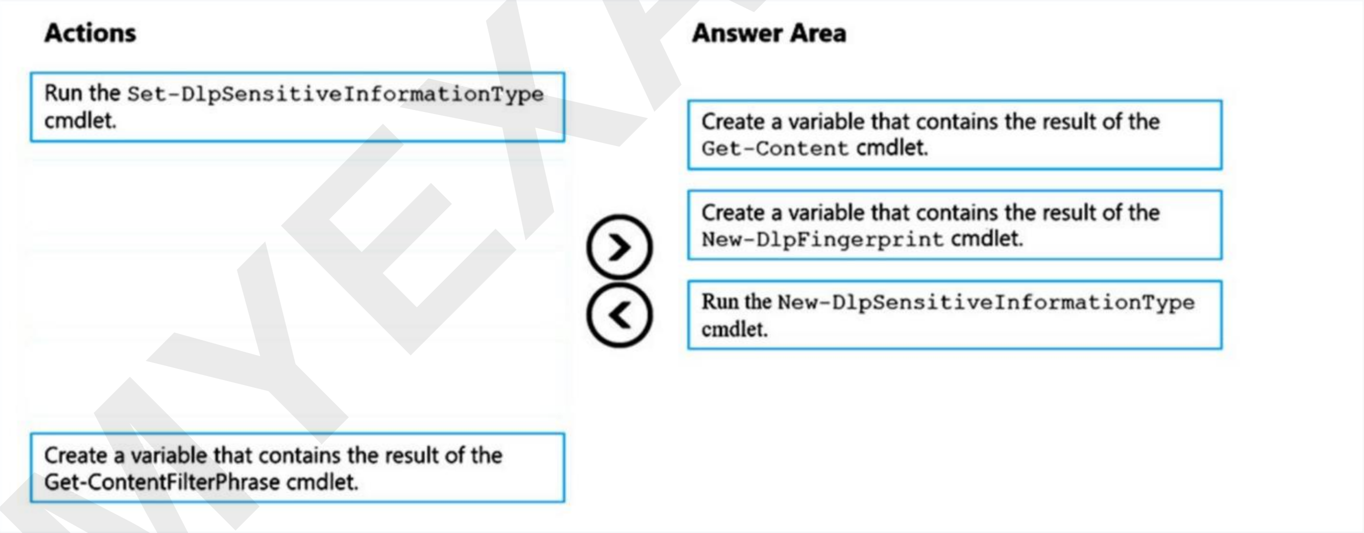


Actions

- Run the `Set-DlpSensitiveInformationType` cmdlet.
- Create a variable that contains the result of the `New-DlpFingerprint` cmdlet.
- Run the `New-DlpSensitiveInformationType` cmdlet.
- Create a variable that contains the result of the `Get-Content` cmdlet.
- Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.

Answer Area

Answer:



Actions

- Run the `Set-DlpSensitiveInformationType` cmdlet.
- Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.

Answer Area

- Create a variable that contains the result of the `Get-Content` cmdlet.
- Create a variable that contains the result of the `New-DlpFingerprint` cmdlet.
- Run the `New-DlpSensitiveInformationType` cmdlet.

Explanation:

$Customer_Form = Get-Content "Cmdlet\My Documents\Contoso Customer Information Form.docx" -Encoding byte -ReadCount 0

$Customer_Fingerprint = New-DlpFingerprint -FileData $Customer_Form -Description "Contoso Customer Information Form"

New-DlpSensitiveInformationType -Name "Contoso Customer Confidential" -Fingerprints

$Customer_Fingerprint -Description "Message contains Contoso customer information."

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/document-fingerprinting?view=o365-worldwide

Question: 26

Your company has a Microsoft 365 tenant that uses a domain named contoso.com.
The company uses Microsoft Office 365 Message Encryption (OME) to encrypt email sent to users in fabrikam.com.
A user named User1 erroneously sends an email to [email protected] You need to prevent [email protected] from accessing the email.
What should you do?

A. Run the Get-MessageTrace cmdlet.
B. Run the Set-OMEMessageRevocation cmdlet.
C. Instruct User1 to delete the email from her Sent Items folder from Microsoft Outlook.
D. Run the New-ComplianceSearchAction cmdlet.
E. Instruct User1 to select Remove external access from Microsoft Outlook on the web.

Answer: B

Explanation:

B would be correct.

https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#how-to-revoke-an-encrypted-message-as-an-administrator
Get the Message ID of the email.

Verify that you can revoke the message.

Revoke the mail.

It's not asking what to do first, but prevent user from accessing the email.

A is the first step, but doesn't prevent user from accessing.

B revokes the message.

C is what the user, not what you would do.

D is about compliance
E is user, not admin.

Question: 27

You have a Microsoft 365 tenant.
You discover that email does NOT use Microsoft Office 365 Message Encryption (OME). You need to ensure that OME can be applied to email.
What should you do first?

A. Enable Microsoft Defender for Office 365.
B. Activate Azure Information Protection.
C. Activate Azure Rights Management (Azure RMS).
D. Create an Azure key vault.

Answer: C

Explanation:

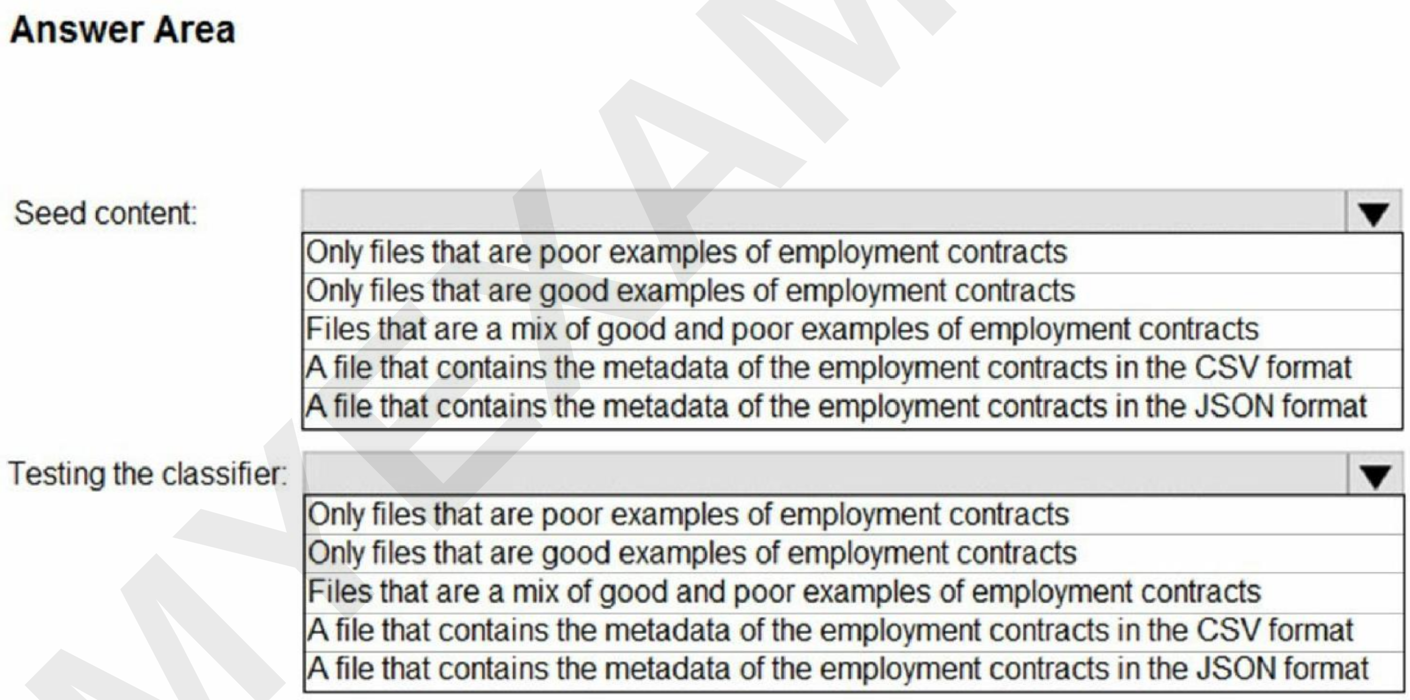
The only prerequisite for using the new OME capabilities is that Azure Rights Management must be activated in your organization's tenant. If it is, Microsoft 365 activates the new OME capabilities automatically and you don't need to do anything.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide

Question: 28

HOTSPOT -
You plan to implement a sensitive information type based on a trainable classifier. The sensitive information type will identify employment contracts.
You need to copy the required files to Microsoft SharePoint Online folders to train the classifier.
What should you use to seed content and test the classifier? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

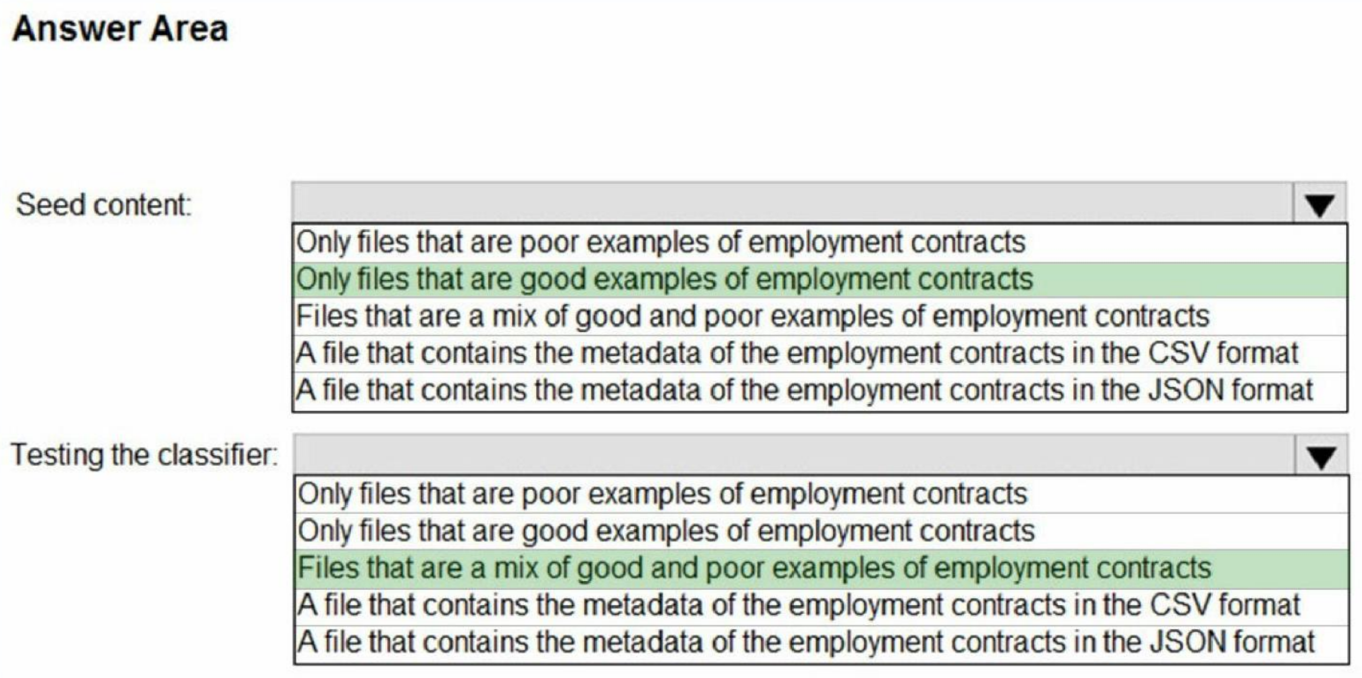


Answer Area

Seed content:
- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Testing the classifier:
- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Answer:



Answer Area

Seed content: ▼

- Only files that are poor examples of employment contracts
- [✓ Only files that are good examples of employment contracts]
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Testing the classifier: ▼

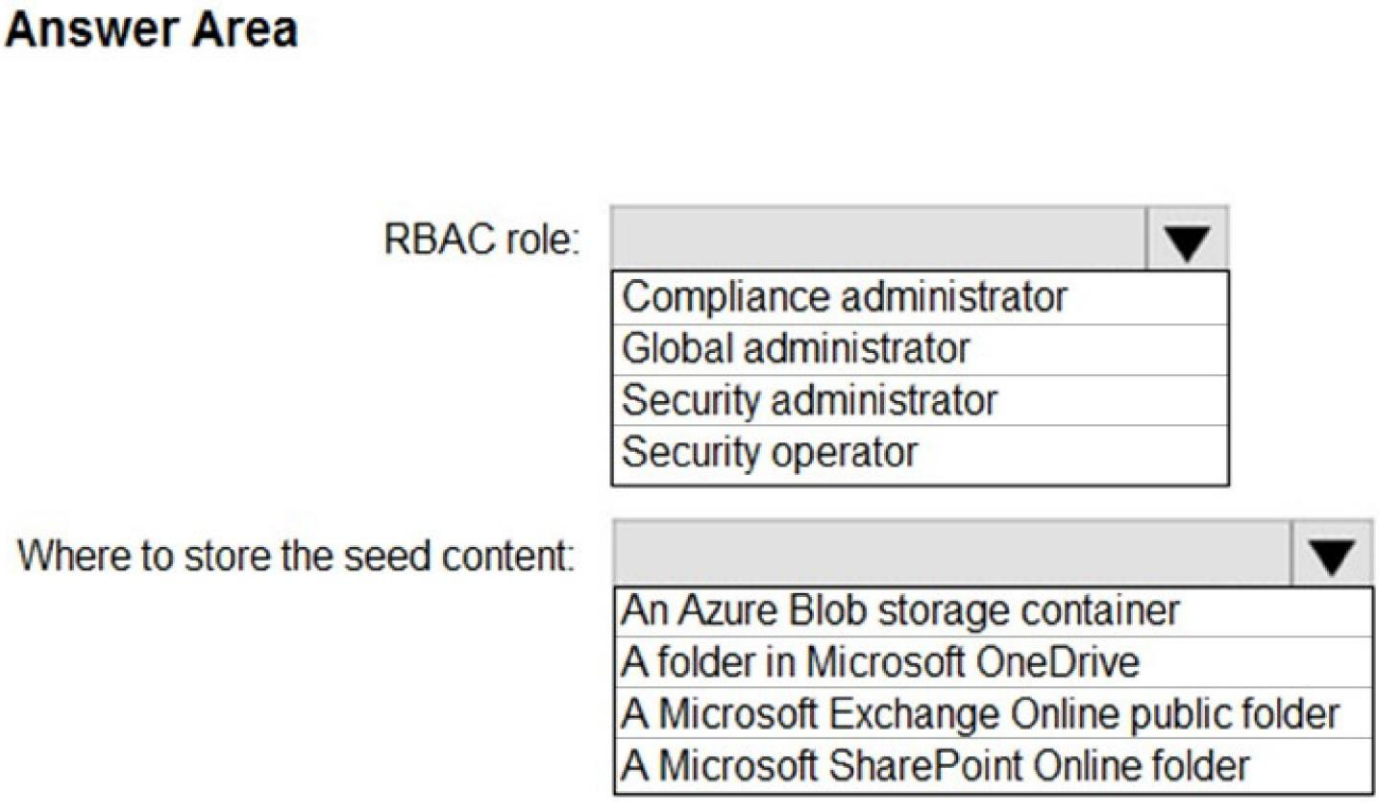
- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- [✓ Files that are a mix of good and poor examples of employment contracts]
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

Question: 29

HOTSPOT -
You plan to create a custom trainable classifier based on an organizational from template.
You need to identify which role-based access control (RBAC) role is required to create the trainable classifier and where to store the seed content for the trainable classifier. The solution must use the principle of least privilege. What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

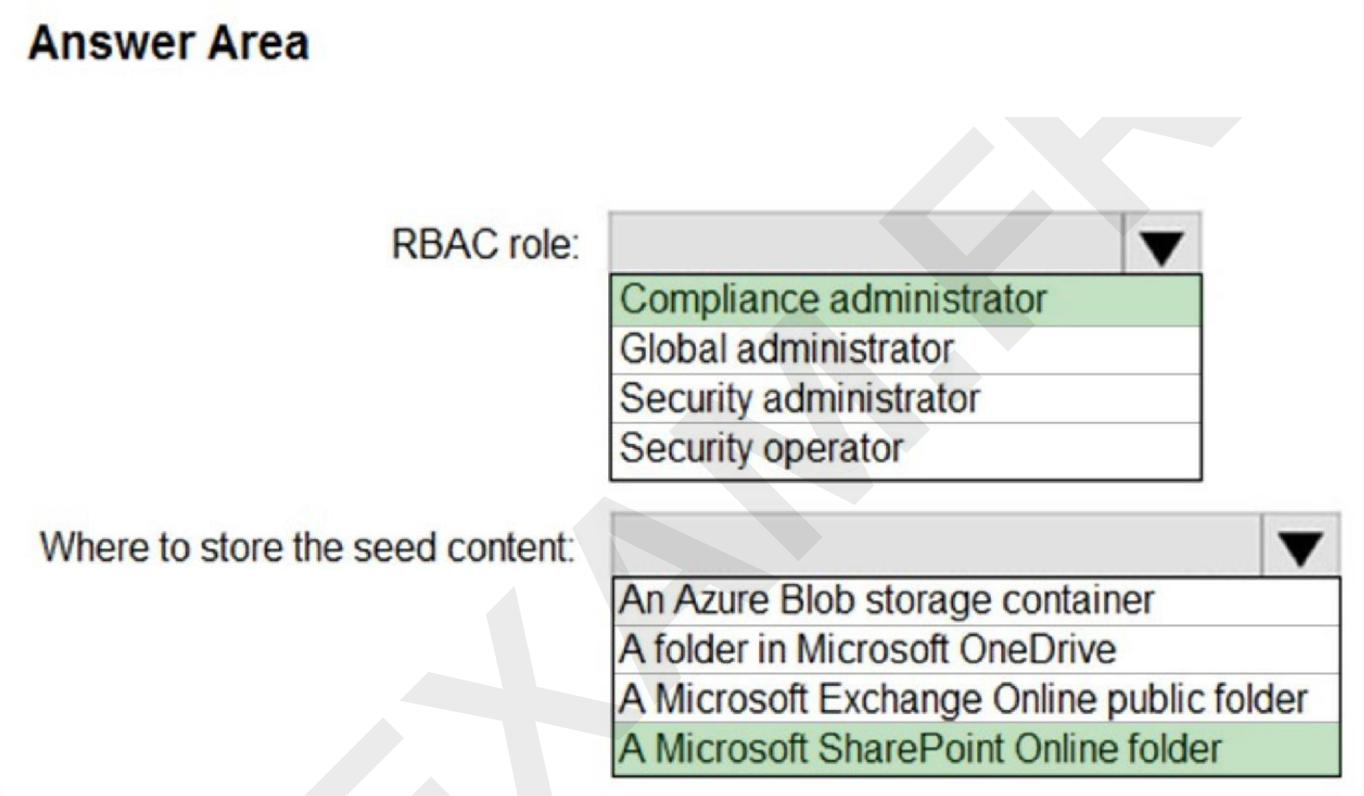
RBAC role: ▼

- Compliance administrator
- Global administrator
- Security administrator
- Security operator

Where to store the seed content: ▼

- An Azure Blob storage container
- A folder in Microsoft OneDrive
- A Microsoft Exchange Online public folder
- A Microsoft SharePoint Online folder

Answer:



Answer Area

RBAC role: ▼

- [✓ Compliance administrator]
- Global administrator
- Security administrator
- Security operator

Where to store the seed content: ▼

- An Azure Blob storage container
- A folder in Microsoft OneDrive
- A Microsoft Exchange Online public folder
- [✓ A Microsoft SharePoint Online folder]

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#prepare-for-a-custom-trainable-classifier

Question: 30

You have a Microsoft 365 tenant.
You create the following:
➮ A sensitivity label
➮ An auto-labeling policy
You need to ensure that the sensitivity label is applied to all the data discovered by the auto-labeling policy. What should you do first?

A. Enable insider risk management.
B. Create a trainable classifier.
C. Run the Enable-TransportRule cmdlet.
D. Run the policy in simulation mode.

Answer: D

Explanation:

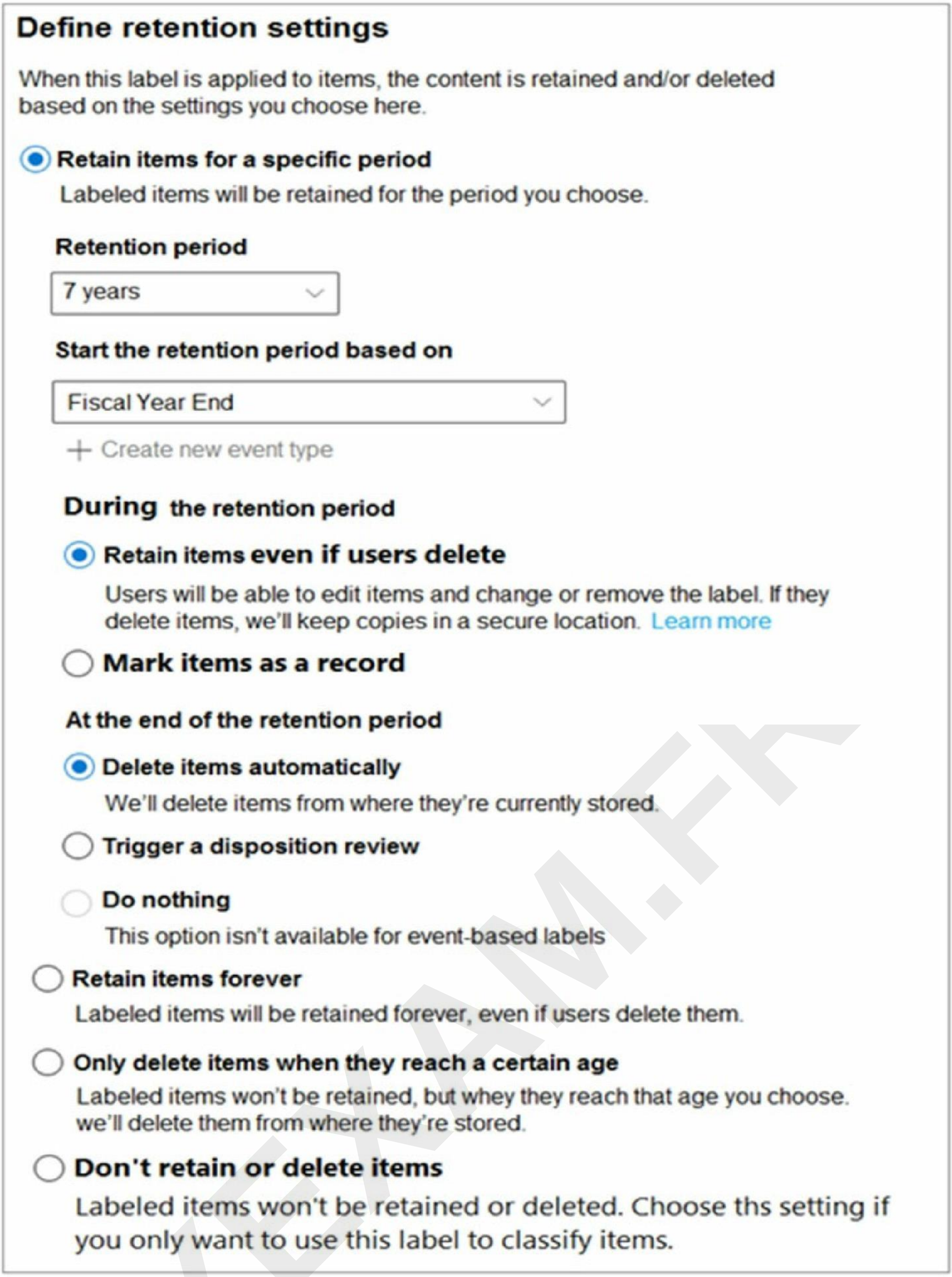
You can't automatically label documents and emails until your policy has run at least one simulation.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

Question: 31

HOTSPOT -
You have the retention label policy shown in the Policy exhibit. (Click the Policy tab.)



Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

● Retain items for a specific period

Labeled items will be retained for the period you choose.

Retention period

7 years

Start the retention period based on

Fiscal Year End

During the retention period

● Retain items even if users delete

Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more

○ Mark items as a record

At the end of the retention period

● Delete items automatically

We'll delete items from where they're currently stored.

○ Trigger a disposition review

○ Do nothing

This option isn't available for event-based labels

○ Retain items forever

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

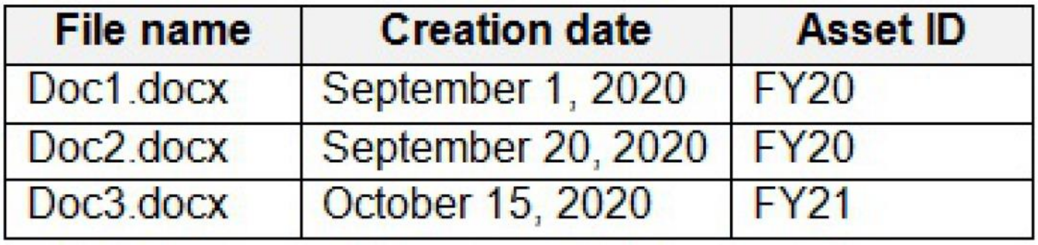
○ Only delete items when they reach a certain age

Labeled items won't be retained, but whey they reach that age you choose. we'll delete them from where they're stored.

○ Don't retain or delete items

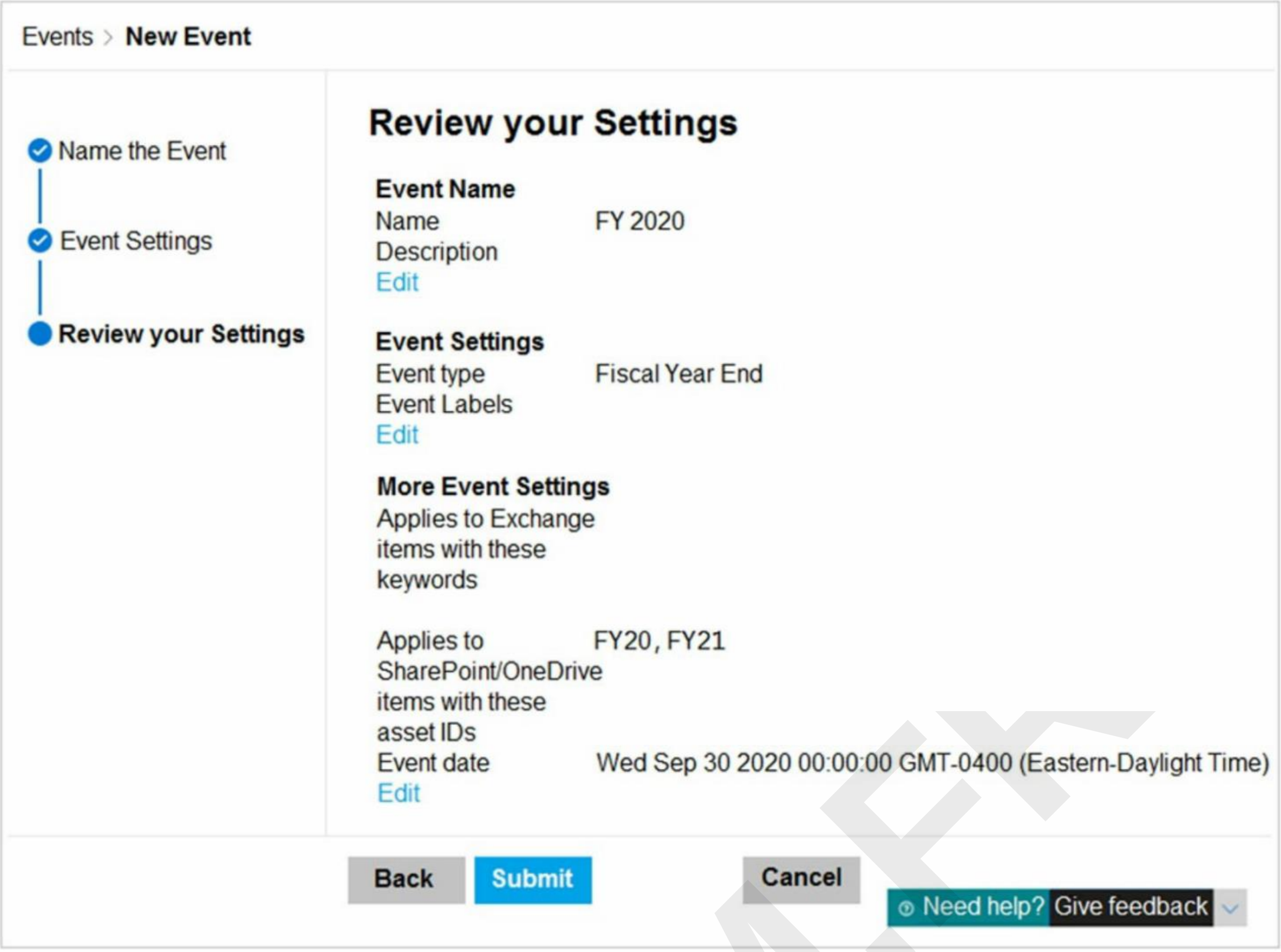
Labeled items won't be retained or deleted. Choose ths setting if you only want to use this label to classify items.

Users apply the retention label policy to files and set the asset ID as shown in the following table.



File name	Creation date	Asset ID
Doc1.docx	September 1, 2020	FY20
Doc2.docx	September 20, 2020	FY20
Doc3.docx	October 15, 2020	FY21

On December 1, 2020, you create the event shown in the Event exhibit. (Click the Event tab.)



Events > New Event

Review your Settings

Event Name

Name FY 2020

Description

Edit

Event Settings

Event type Fiscal Year End

Event Labels

Edit

More Event Settings

Applies to Exchange items with these keywords

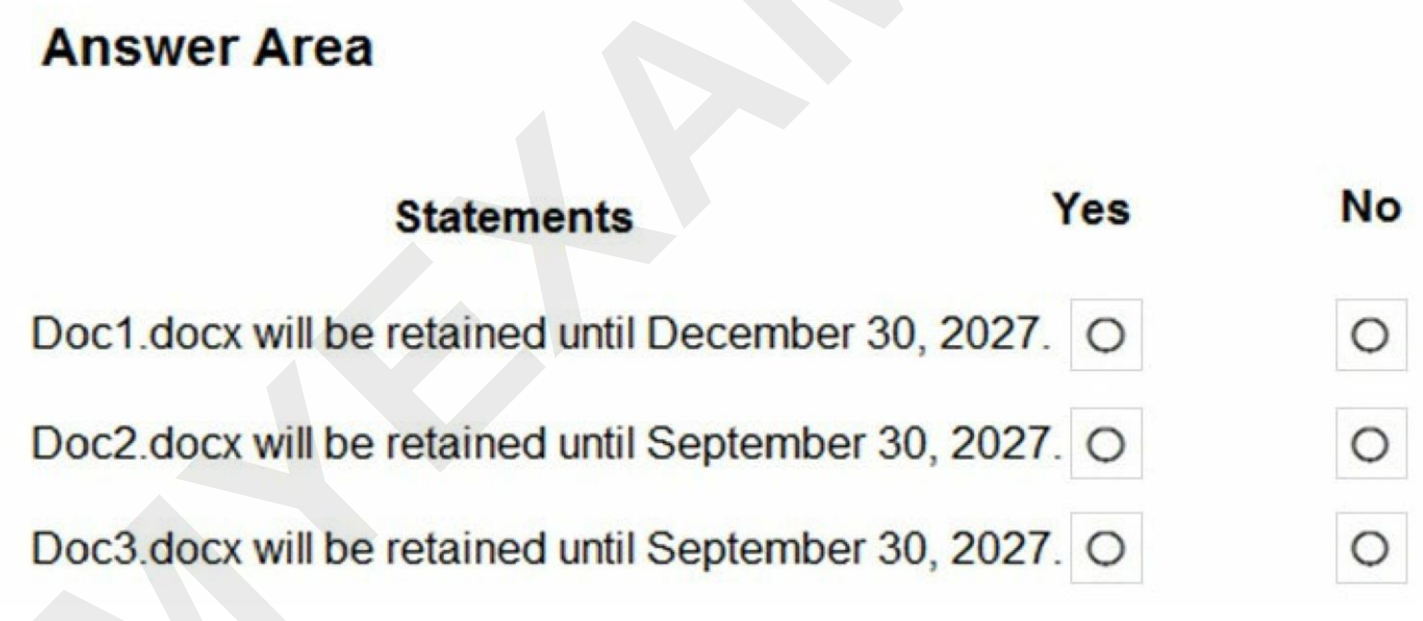
Applies to SharePoint/OneDrive items with these asset IDs FY20, FY21

Event date Wed Sep 30 2020 00:00:00 GMT-0400 (Eastern-Daylight Time)

Edit

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

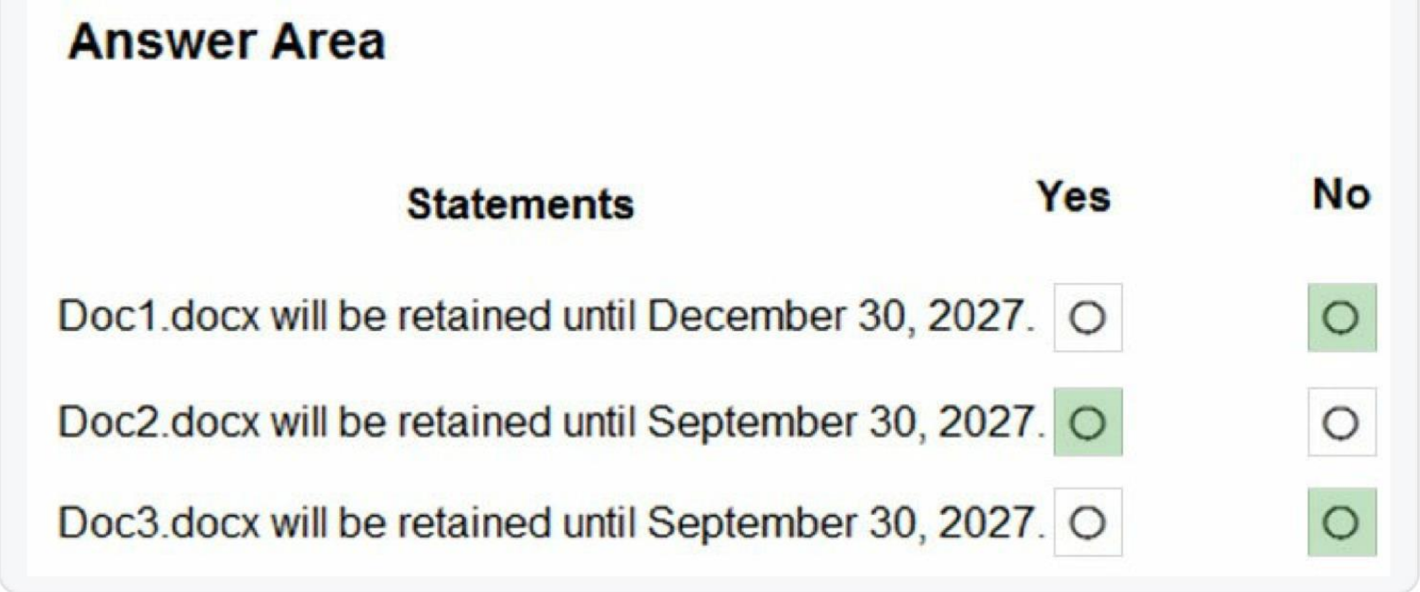
Hot Area:



Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	○
Doc2.docx will be retained until September 30, 2027.	○	○
Doc3.docx will be retained until September 30, 2027.	○	○

Answer:



Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	[✓ ○]
Doc2.docx will be retained until September 30, 2027.	[✓ ○]	○
Doc3.docx will be retained until September 30, 2027.	○	[✓ ○]

Question: 32

You have a sensitive information type based on a trainable classifier. You are unsatisfied with the result of the result of trainable classifier. You need to retrain the classifier.
What should you use in the Microsoft 365 compliance center?

A. Labels from Information protection
B. Labels from Information governance
C. Content explorer from Data classification
D. Content search

Answer: C

Explanation:

How to retrain a classifier in content explorer

Sign in to Microsoft 365 compliance center with compliance admin or security admin role access and open Microsoft 365 compliance center > Data classification > Content explorer.

Under the Filter on labels, info types, or categories list, expand Trainable classifiers.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-how-to-retrain-content-explorer?view=o365-worldwide

Question: 33

You receive an email that contains a list of words that will be used for a sensitive information type. You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list?

A. a JSON file that has an element for each word
B. an ACCDB database file that contains a table named Dictionary C. an XLSX file that contains one word in each cell of the first row D. a text file that has one word on each line

Answer: D

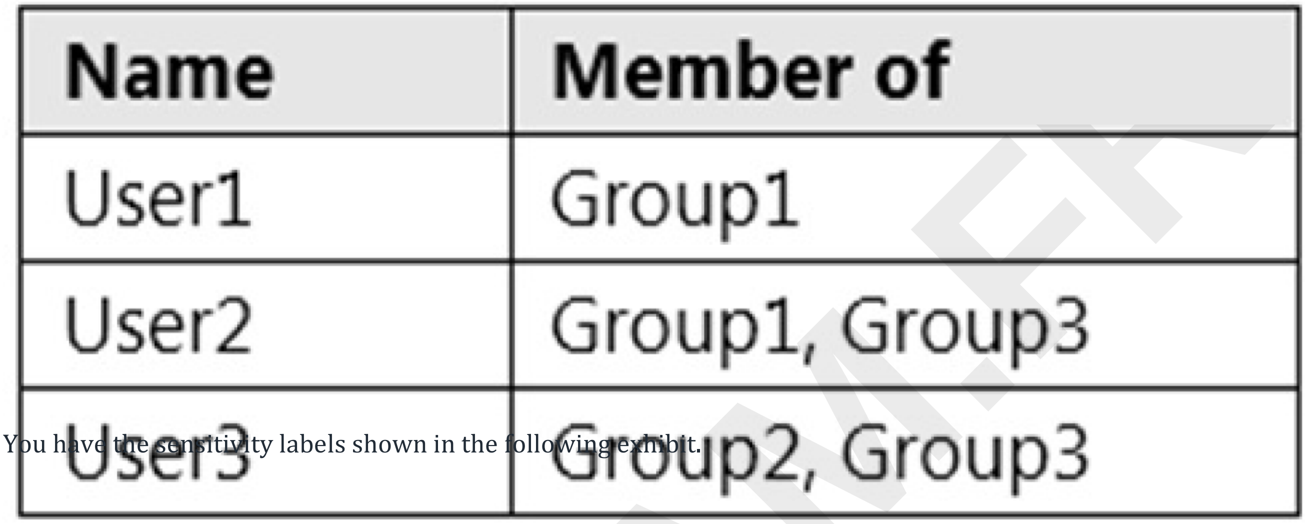
Explanation:
Keyword dictionaries can be created either from a text file or from csv file.

Note:
There are several versions of this question in the exam. The question has two possible correct answers: 1. a CSV file that contains words separated by commas
2. a text file that has one word on each line
Other incorrect answer options you may see on the exam include the following:
✑ a TSV file that contains words separated by tabs
✑ a DOCX file that has one word on each line
✑ an XML file that contains a keyword tag for each word

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-world wide

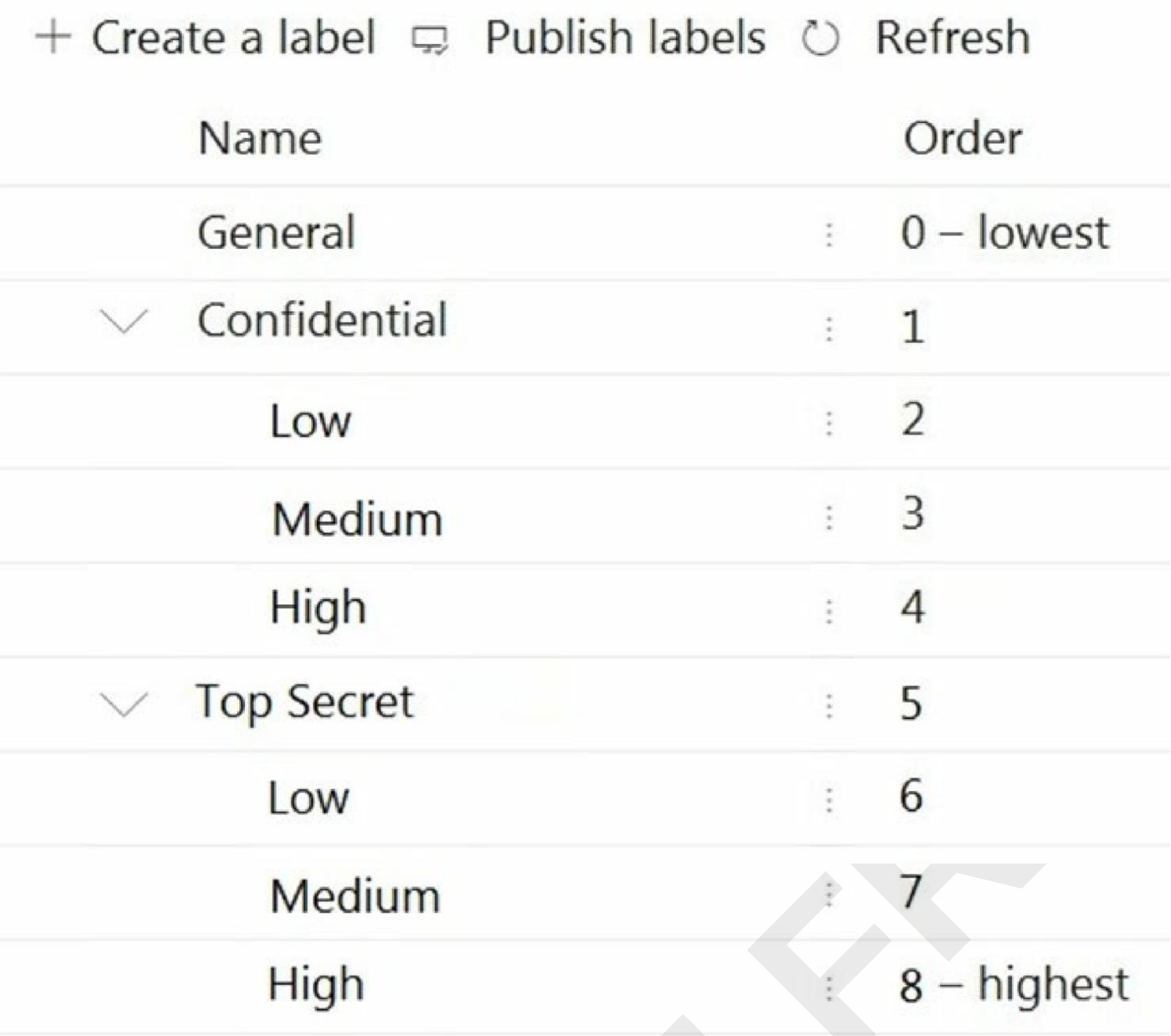
Question: 34

HOTSPOT -
You have a Microsoft 365 E5 tenant that contains three groups named Group1, Group2, and Group3. You have the users shown in the following table.



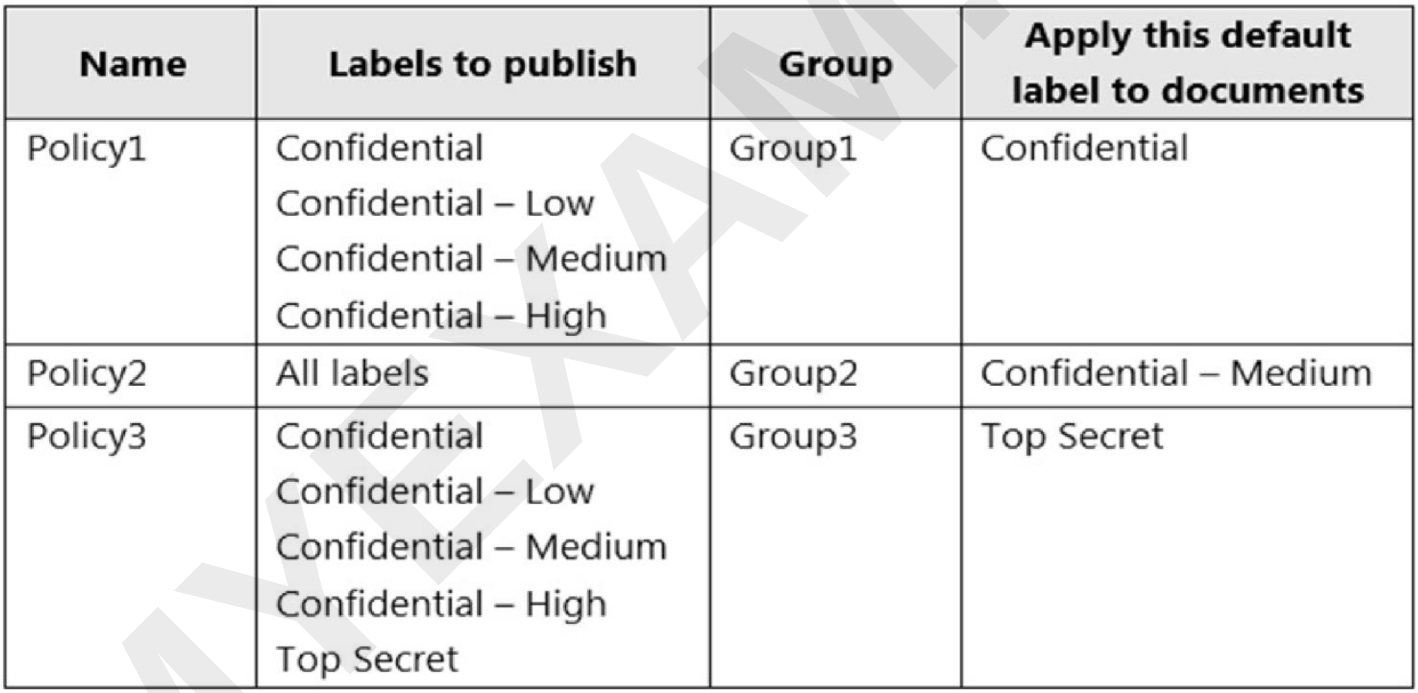
Name	Member of
User1	Group1
User2	Group1, Group3
User3	Group2, Group3

You have the sensitivity labels shown in the following exhibit.



Name	Order
General	0 – lowest
Confidential	1
Low	2
Medium	3
High	4
Top Secret	5
Low	6
Medium	7
High	8 – highest

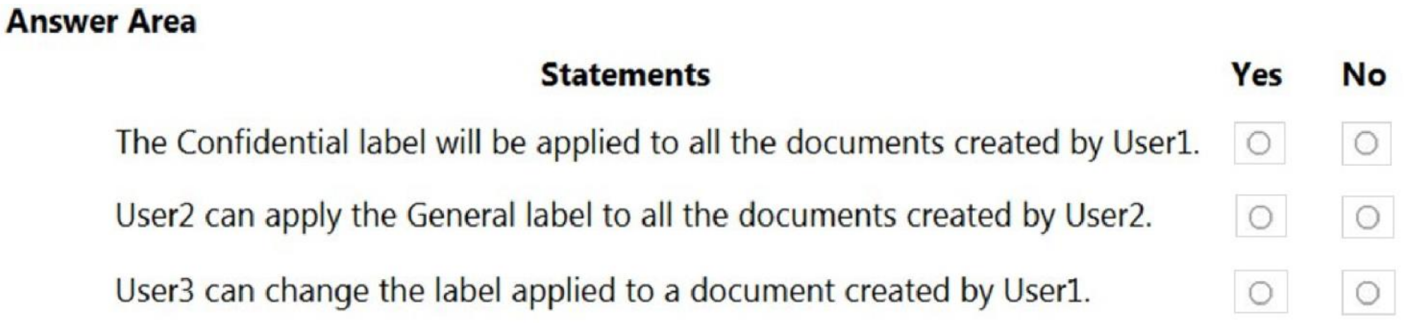
You have the label policies shown in the following table.



Name	Labels to publish	Group	Apply this default label to documents
Policy1	Confidential Confidential – Low Confidential – Medium Confidential – High	Group1	Confidential
Policy2	All labels	Group2	Confidential – Medium
Policy3	Confidential Confidential – Low Confidential – Medium Confidential – High Top Secret	Group3	Top Secret

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

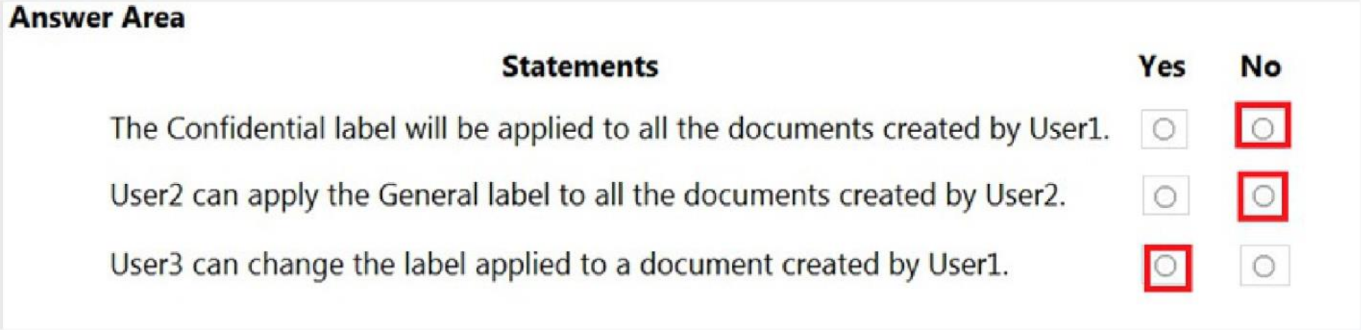
Hot Area:



Answer Area

Statements	Yes	No
The Confidential label will be applied to all the documents created by User1.	○	○
User2 can apply the General label to all the documents created by User2.	○	○
User3 can change the label applied to a document created by User1.	○	○

Answer:



Answer Area

Statements	Yes	No
The Confidential label will be applied to all the documents created by User1.	○	[✓ ○]
User2 can apply the General label to all the documents created by User2.	○	[✓ ○]
User3 can change the label applied to a document created by User1.	[✓ ○]	○

Explanation:

No

The parent label Confidential is simply a text label with no protection settings, and because it has sublabels, it can't be applied to content. Instead, users must choose Confidential to view the sublabels, and then they can choose a sublabel to apply to content. So first will be NO.

NO

(User2 is not member of Group2. He can't use General)

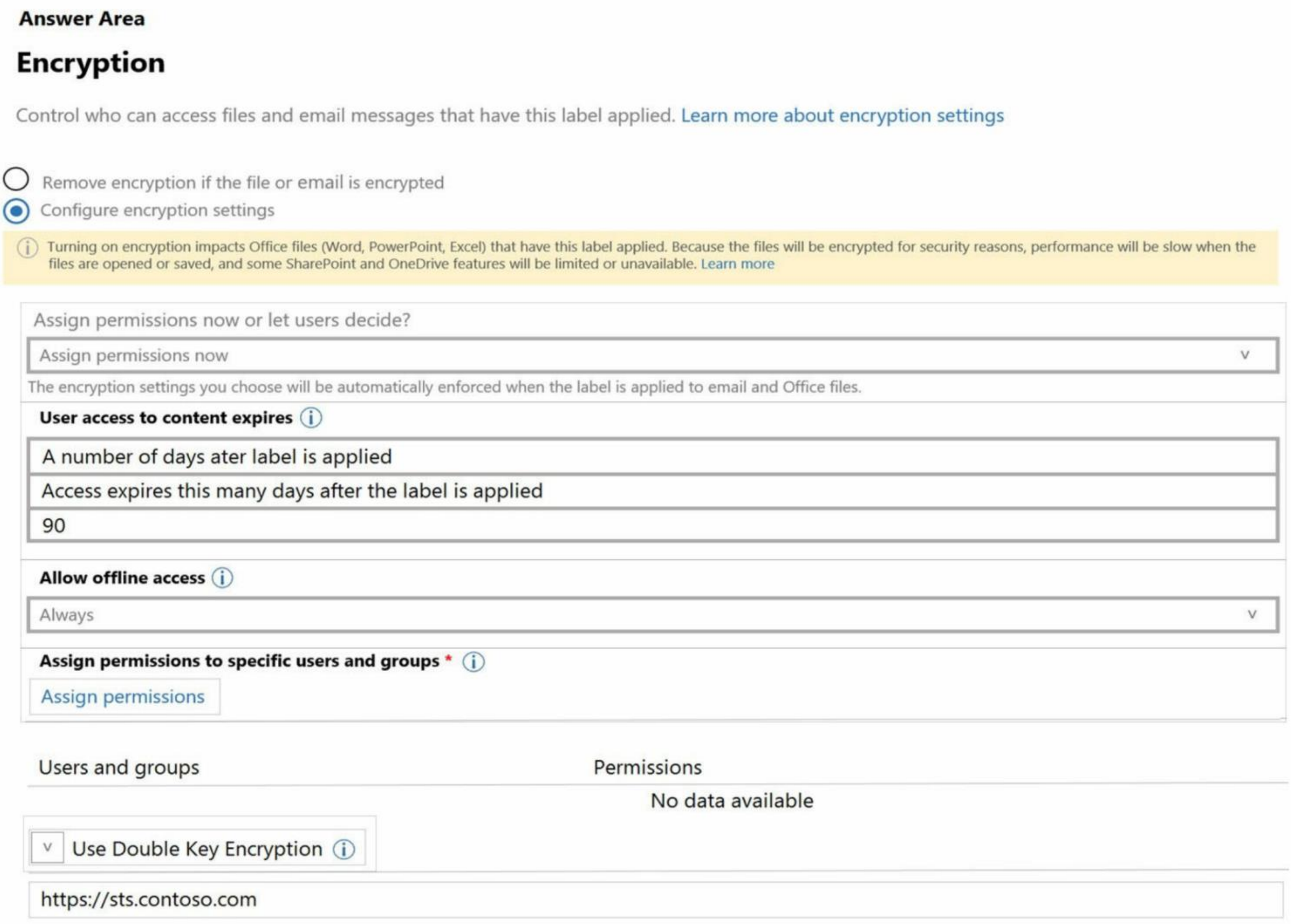
YES

As member of Group 2, User 3 has access to labels with higher priorities (Top Secret - Low, Medium, Hight) than the labels that User 1 has, thus can replace any label set by User1

Question: 35 HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1.
You plan to enable co-authoring for encrypted files.
You need to ensure that files that have label1 applied support co-authoring.
Which two settings should you modify? To answer, select the settings in the answer area. NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file or email is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now ∨

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

A number of days ater label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always ∨

Assign permissions to specific users and groups * ⓘ

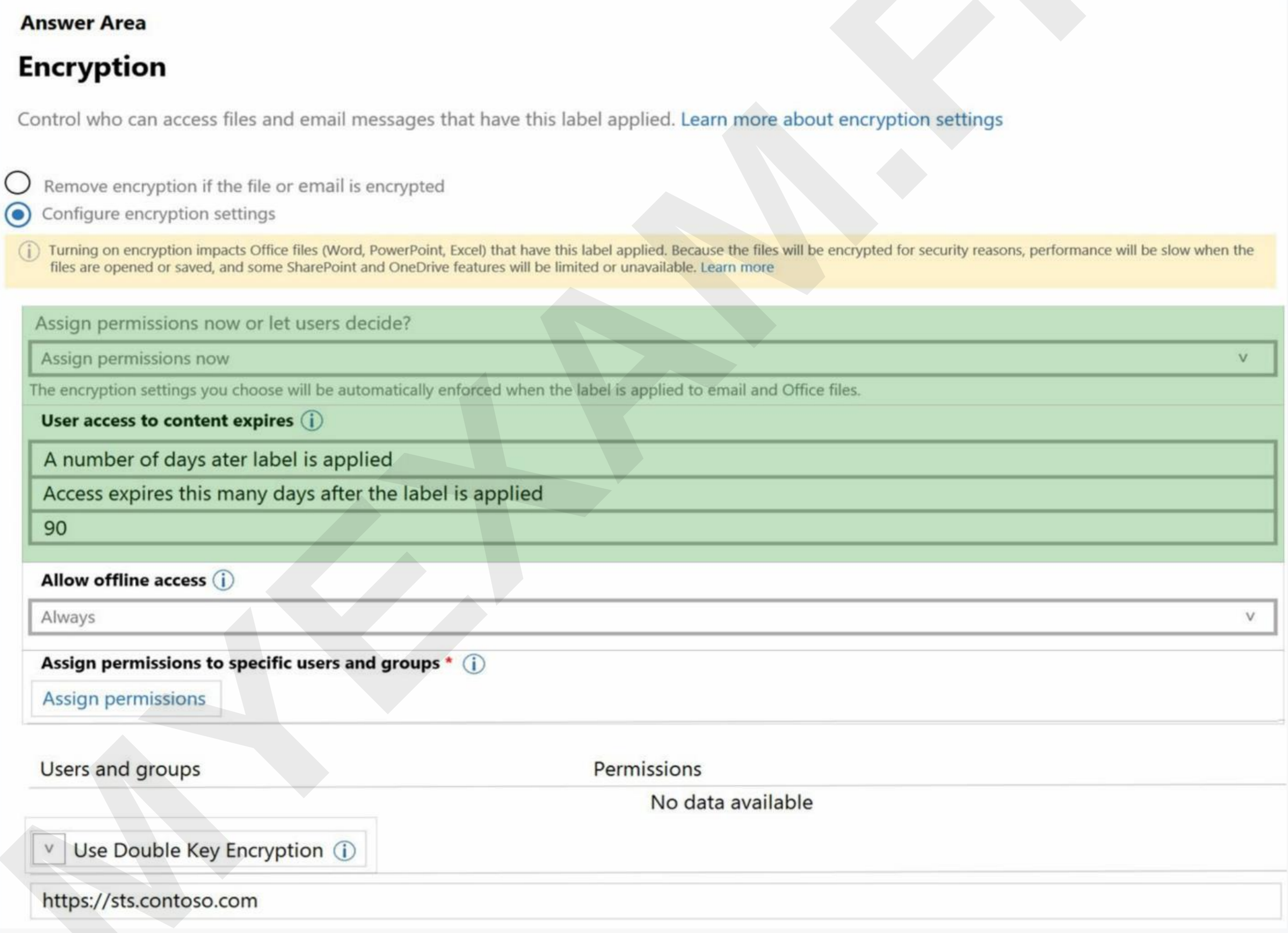
Assign permissions

Users and groups	Permissions
	No data available

∨ Use Double Key Encryption ⓘ

https://sts.contoso.com

Answer:



Answer Area

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file or email is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now ∨

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

A number of days ater label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always ∨

Assign permissions to specific users and groups * ⓘ

Assign permissions

Users and groups	Permissions
	No data available

∨ Use Double Key Encryption ⓘ

https://sts.contoso.com

Explanation:

Co-authoring and AutoSave aren't supported and don't work for labeled and encrypted Office documents that use any of the following configurations for encryption:

✑ Let users assign permissions when they apply the label and the checkbox In Word, PowerPoint, and Excel, prompt users to specify permissions is selected.

This configuration is sometimes referred to as "user-defined permissions".

✑ User access to content expires is set to a value other than Never.

Double Key Encryption is selected.

■

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring?view=o365-world wide
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/co-authoring-files-with-sensi tivity-labels/ba-p/3029768

Question: 36

HOTSPOT

-

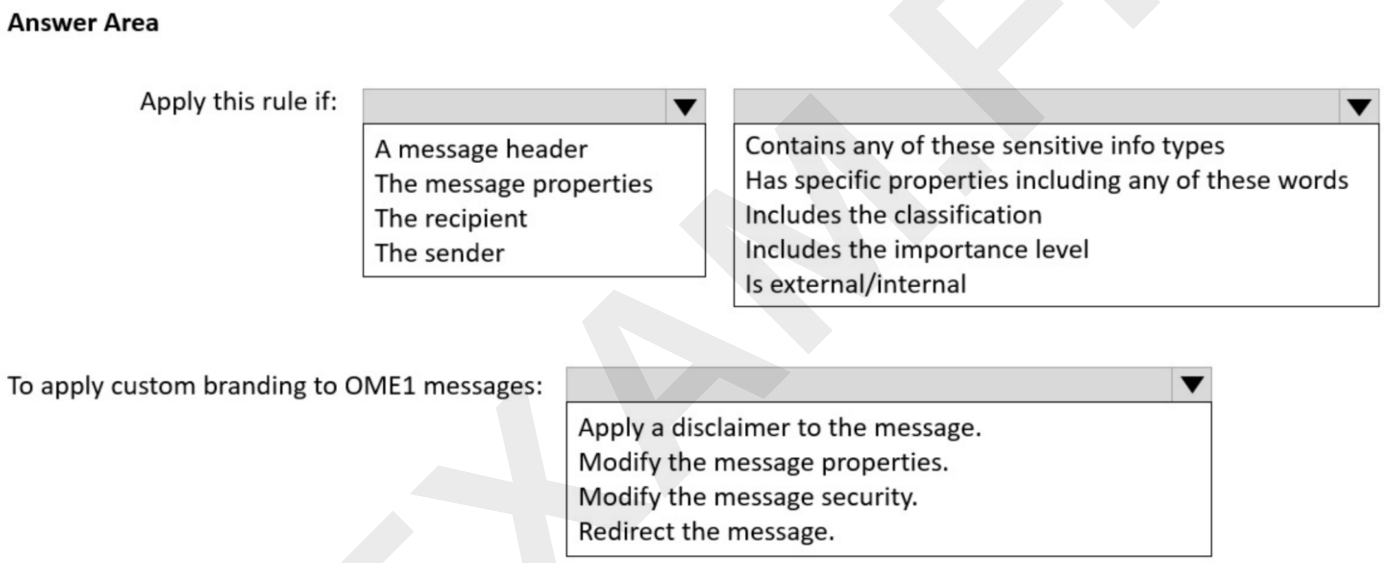
You have a Microsoft 365 E5 subscription.

You have a Microsoft Office 365 Advanced Message Encryption branding template named OME1.

You need to create a Microsoft Exchange Online mail flow rule to apply OME1 to email.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Apply this rule if:

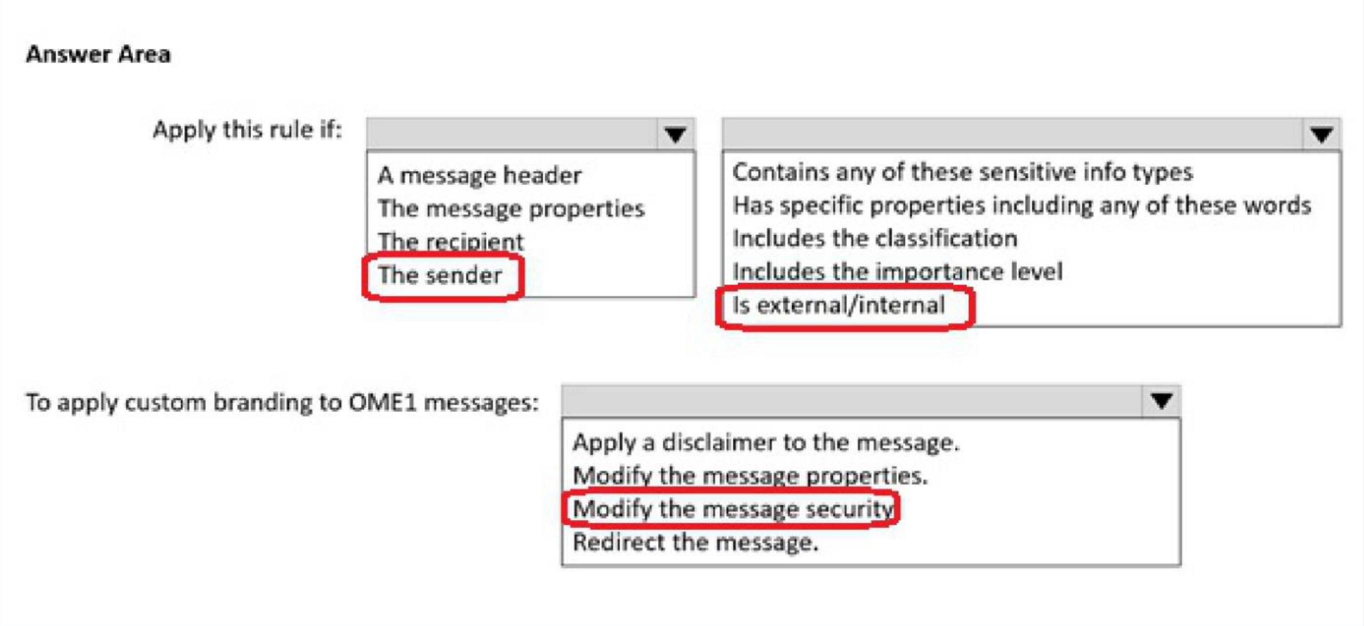
- A message header
- The message properties
- The recipient
- The sender

- Contains any of these sensitive info types
- Has specific properties including any of these words
- Includes the classification
- Includes the importance level
- Is external/internal

To apply custom branding to OME1 messages:

- Apply a disclaimer to the message.
- Modify the message properties.
- Modify the message security.
- Redirect the message.

Answer:



Answer Area

Apply this rule if:

- A message header
- The message properties
- The recipient
- [✓ The sender]

- Contains any of these sensitive info types
- Has specific properties including any of these words
- Includes the classification
- Includes the importance level
- [✓ Is external/internal]

To apply custom branding to OME1 messages:

- Apply a disclaimer to the message.
- Modify the message properties.
- [✓ Modify the message security]
- Redirect the message.

Explanation:

Question: 37

You have a Microsoft 365 tenant that uses the following sensitivity labels:•

Confidential:

o Internal

o External

The labels are published by using a label policy named Policy1.

Users report that Microsoft Office for the web apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.

You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps. What should you do?

A. Modify the scope of the Confidential label.

B. Modify the publishing settings of Policy1.

C. Enable sensitivity label support for Office files in Microsoft SharePoint Online and OneDrive. D. Run the Execute-AzureAdLabelSync cmdlet.

Answer: C

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?

view=o365-worldwide

states:

Enable built-in labeling for supported Office files in SharePoint and OneDrive so that users can apply your sensitivity labels in Office for the web.

Answer C is correct.

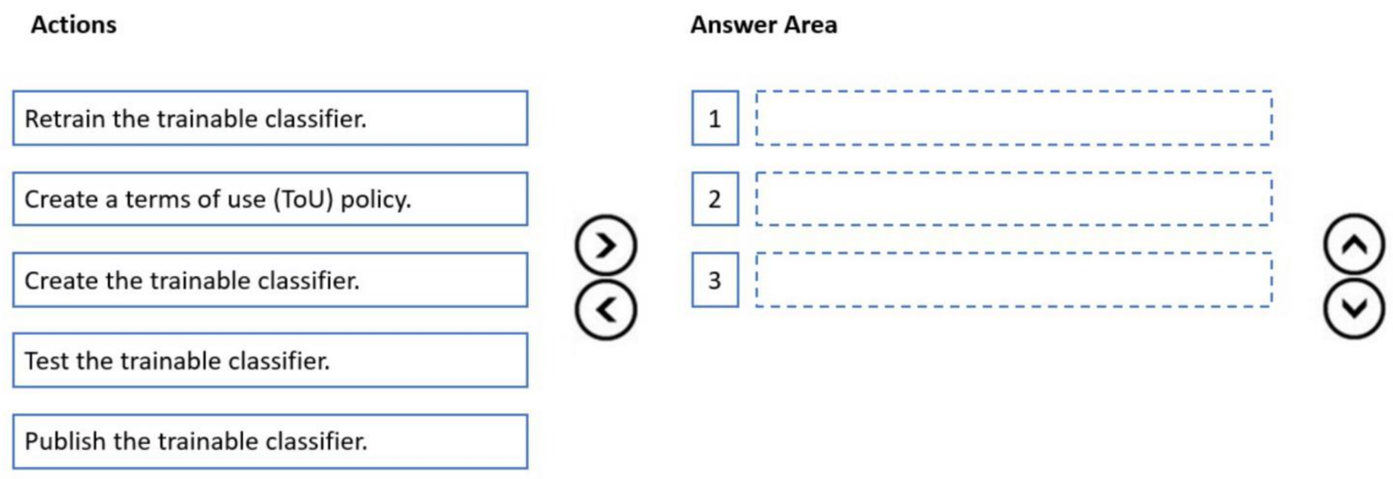
Question: 38

DRAG DROP

-

You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

- Retrain the trainable classifier.
- Create a terms of use (ToU) policy.
- Create the trainable classifier.
- Test the trainable classifier.
- Publish the trainable classifier.

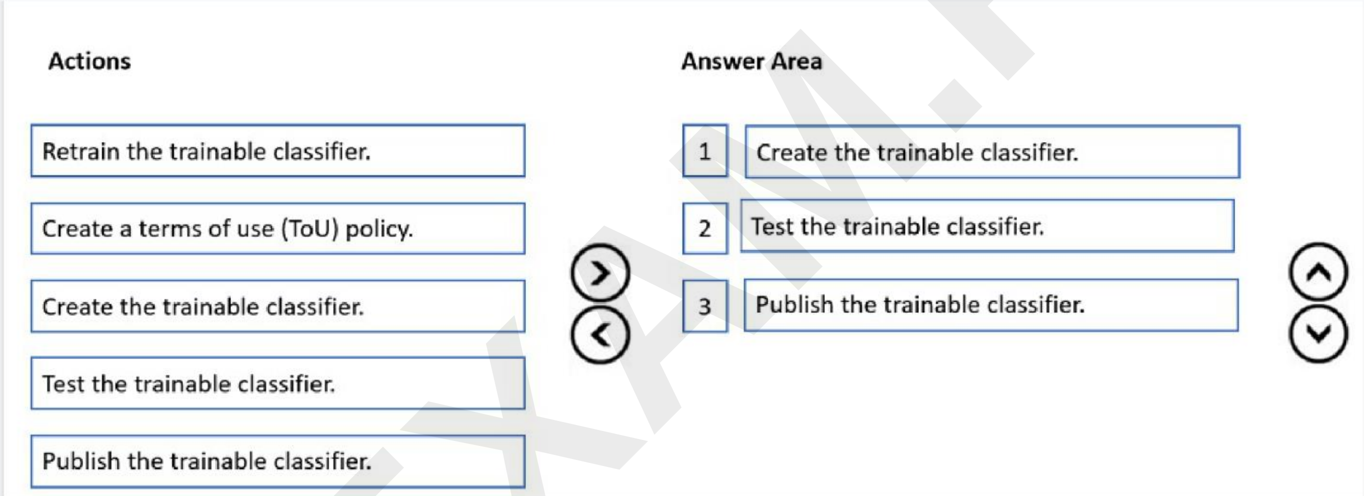
Answer Area

1

2

3

Answer:



Actions

- Retrain the trainable classifier.
- Create a terms of use (ToU) policy.
- Create the trainable classifier.
- Test the trainable classifier.
- Publish the trainable classifier.

Answer Area

1 Create the trainable classifier.

2 Test the trainable classifier.

3 Publish the trainable classifier.

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide#process-flow-for-creating-custom-classifiers

Contains flow chart with 3 major steps: Create Classifier, Test Classifier and Publish Classifier.

Question: 39 You have a Microsoft 365 E5 tenant.

You need to add a new keyword dictionary.
What should you create?

A. a trainable classifier
B. a sensitivity label
C. a sensitive info type
D. a retention policy

Answer: C

Explanation:

https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide

Connect to the Microsoft Purview compliance portal.

Navigate to Classifications > Sensitive info types.

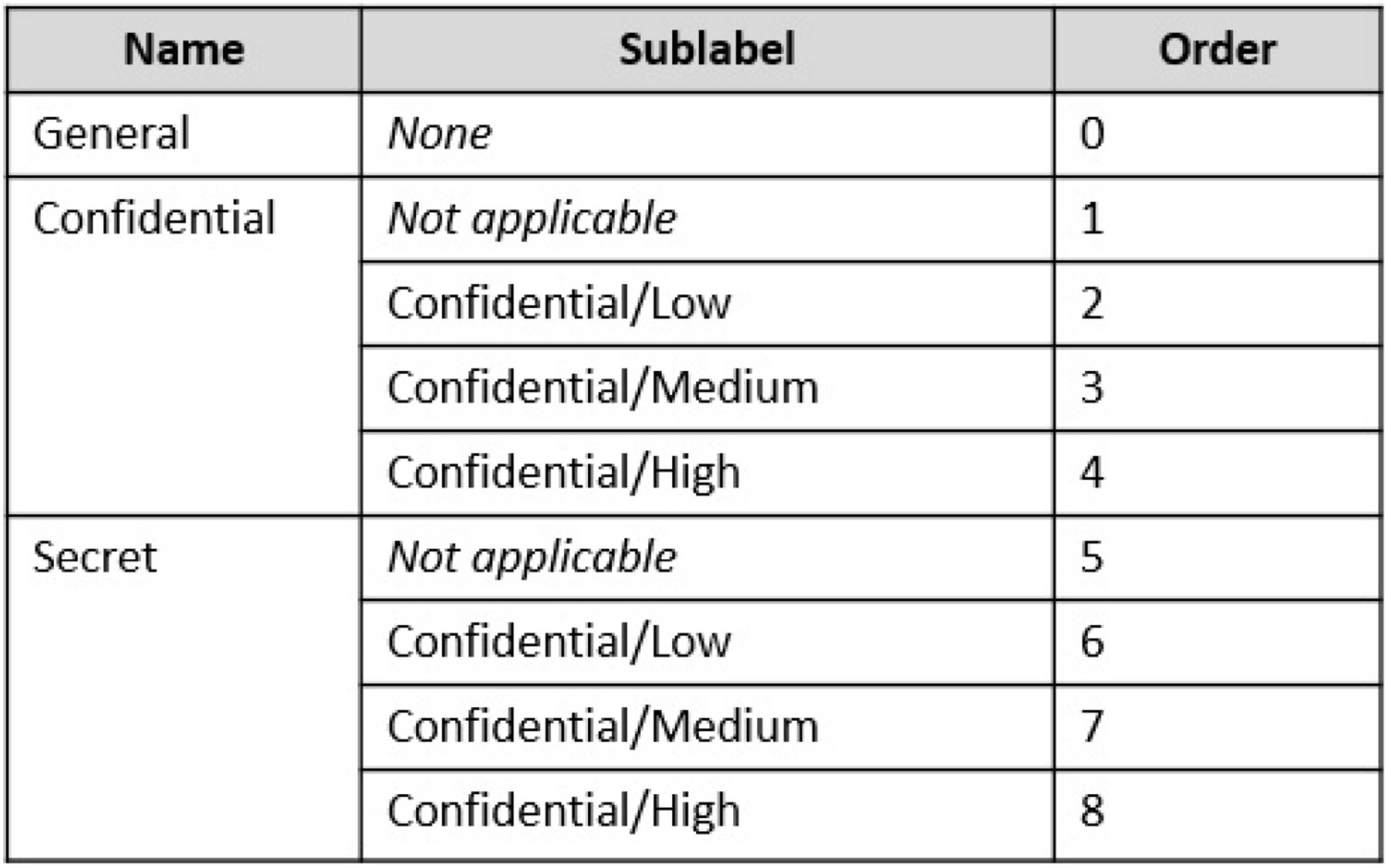
Select Create and enter a Name and Description for your sensitive info type, then select Next

Question: 40 HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2 and a group named Group1. User1 is a member of Group1.

The subscription contains the sensitivity labels shown in the following table.



Name	Sublabel	Order
General	*None*	0
Confidential	*Not applicable*	1
	Confidential/Low	2
	Confidential/Medium	3
	Confidential/High	4
Secret	*Not applicable*	5
	Confidential/Low	6
	Confidential/Medium	7
	Confidential/High	8

You have a sensitivity label policy named Policy1 that is published to User1 and User2. The policy includes the following labels:

- General
- Confidential
- Confidential/Low
- Confidential/High
- Confidential/Medium

For Policy1, the default label for documents is Confidential/Low.

You have a sensitivity label policy named Policy2 that is published to Group1. The policy includes the following labels:

- Secret
- General
- Secret/Low
- Secret/High
- Secret/Medium

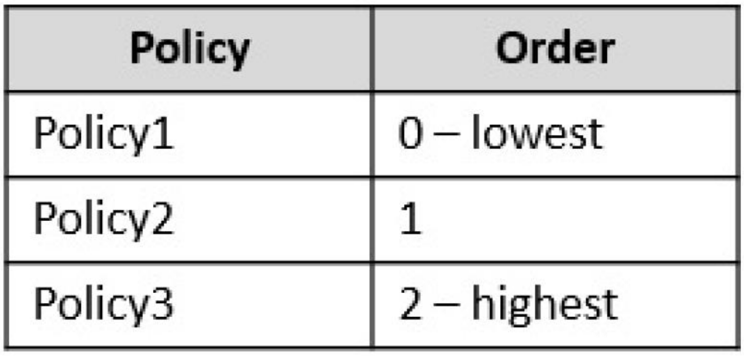
For Policy2, the default label for documents is Secret/Low.

You have a sensitivity label policy named Policy3 that is published to User1 and User2. The policy includes the following labels:

- Secret
- General
- Secret/Low
- Secret/High
- Secret/Medium

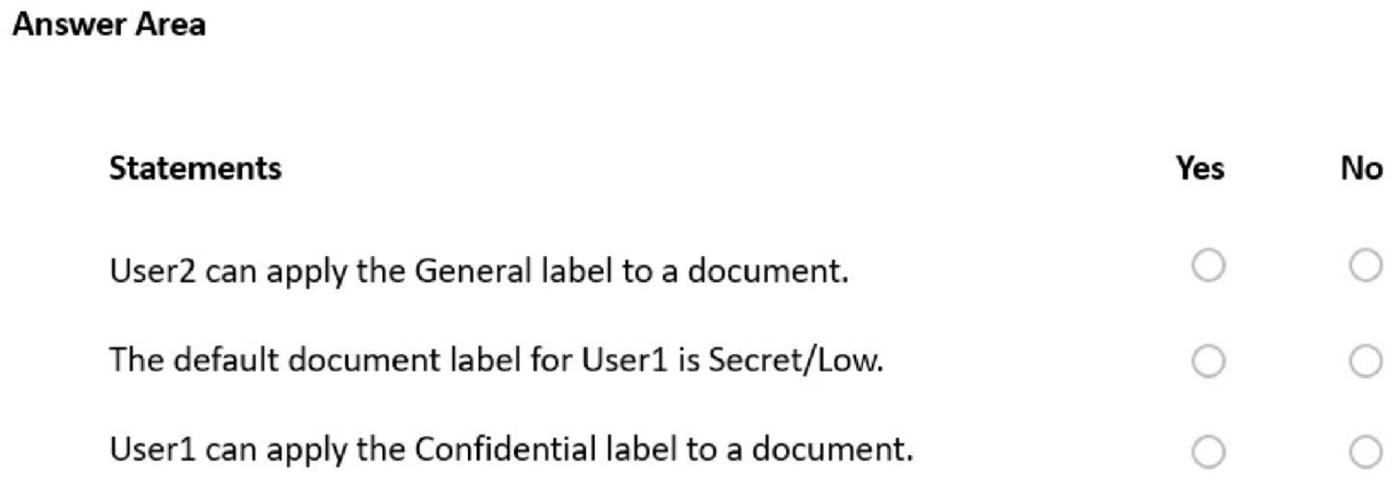
For Policy3, the default label for documents is Secret/Medium.

The order of the policies is shown in the following table.



Policy	Order
Policy1	0 – lowest
Policy2	1
Policy3	2 – highest

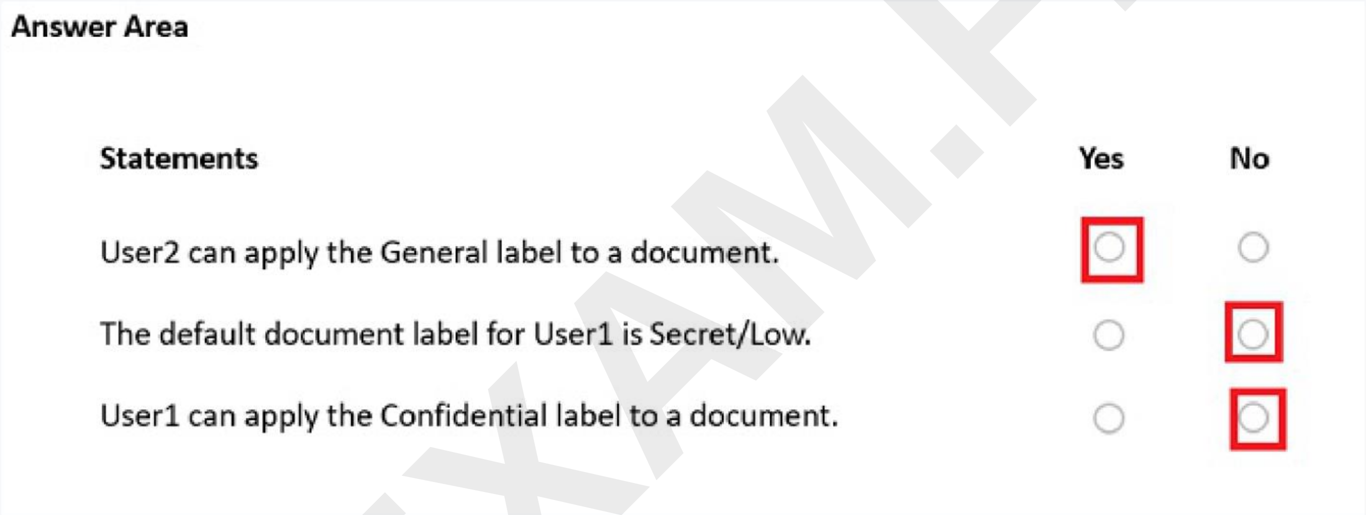
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User2 can apply the General label to a document.	○	○
The default document label for User1 is Secret/Low.	○	○
User1 can apply the Confidential label to a document.	○	○

Answer:



Answer Area

Statements	Yes	No
User2 can apply the General label to a document.	[✓ ○]	○
The default document label for User1 is Secret/Low.	○	[✓ ○]
User1 can apply the Confidential label to a document.	○	[✓ ○]

Explanation:

Yes, since User2 are a member of Policy1 and the General label are not a parent label

No, if you have several labels as default label through different policys which we have here the policy with the higher priority is the one that will get used as default document label, in this is it is Confiddential/Low No, since you cannot use parent labels they are there to give users a logical GUI/interface.

Question: 41

You plan to implement Microsoft Office 365 Advanced Message Encryption.

You need to ensure that encrypted email sent to external recipients expires after seven days.

What should you create first?

A. a custom branding template
B. a remote domain in Microsoft Exchange
C. a mail flow rule
D. an X.509 version 3 certificate
E. a connector in Microsoft Exchange

Answer: A

Explanation:

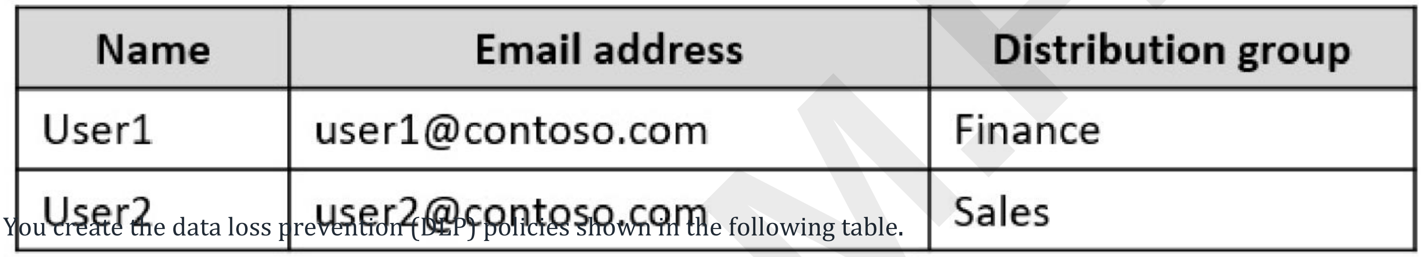
Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide#create-a-custom-branding-template-to-force-mail-expiration-by-using-powershell

Question: 42

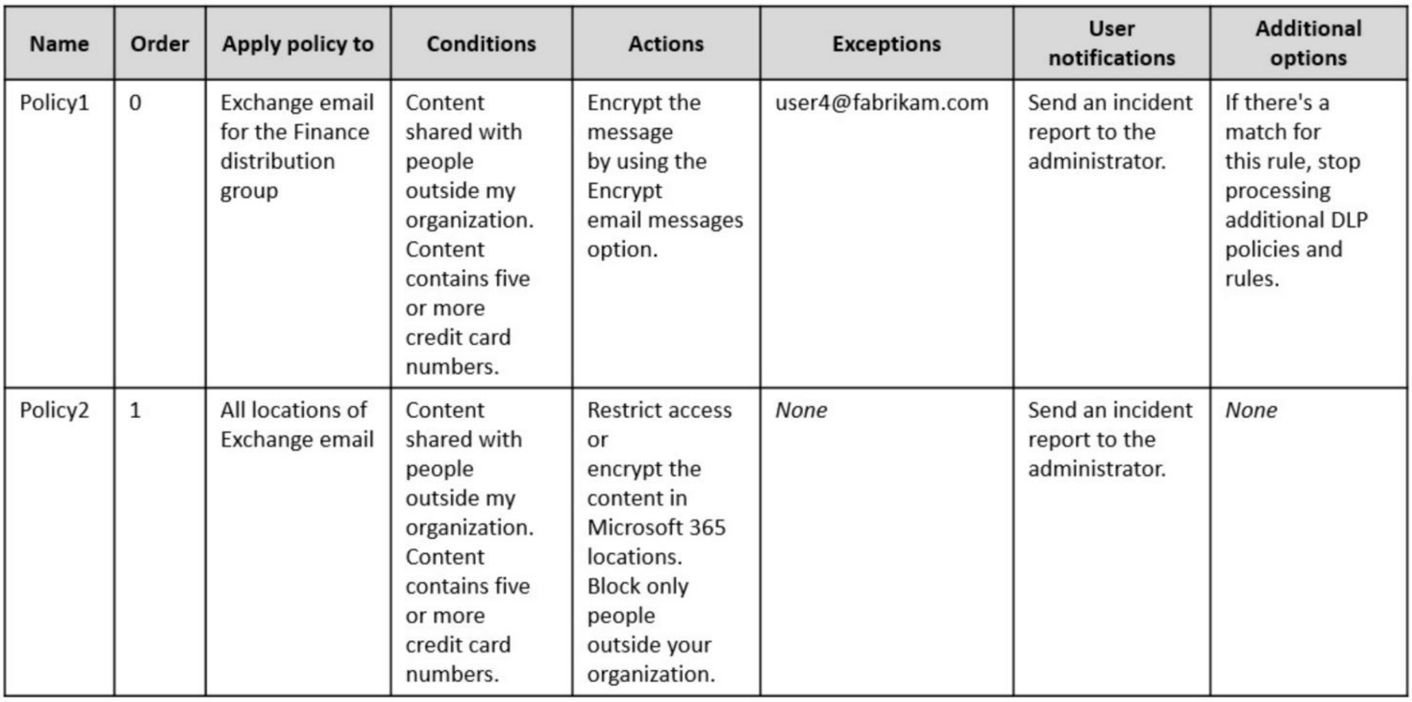
HOTSPOT
-

You have a Microsoft 365 subscription that contains the users shown in the following table.



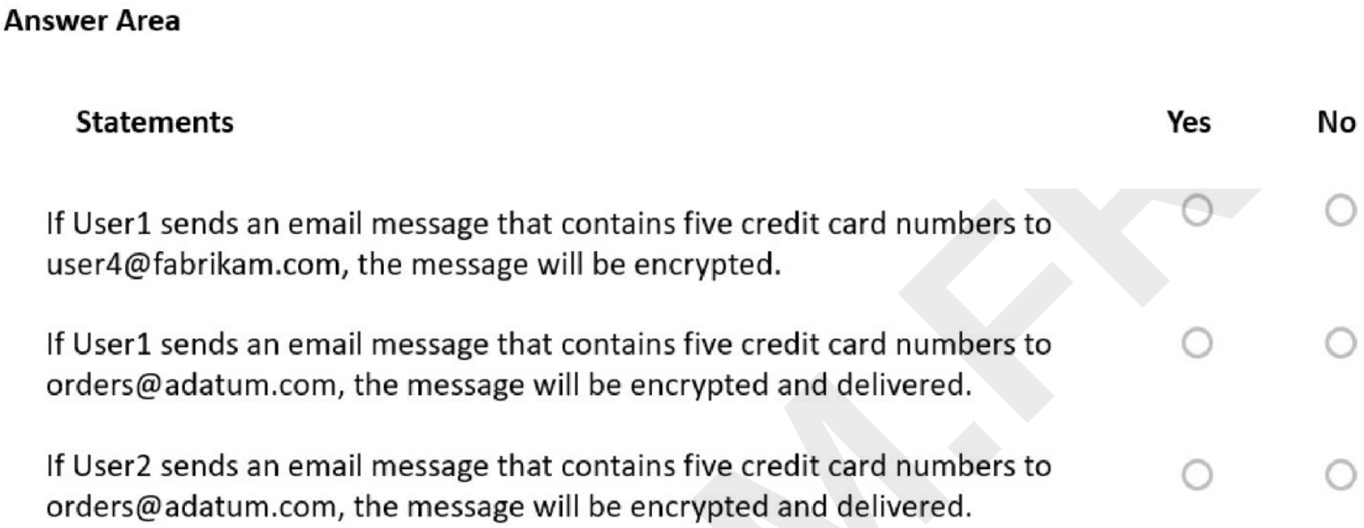
Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

You create the data loss prevention (DLP) policies shown in the following table.



Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	*None*	Send an incident report to the administrator.	*None*

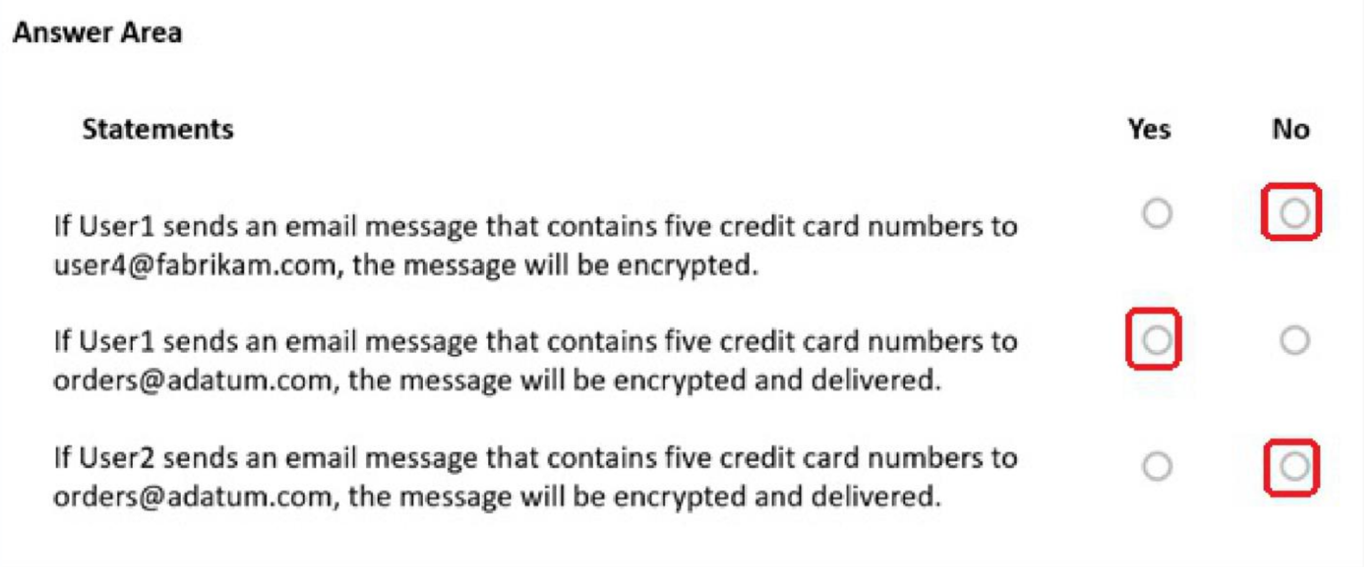
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.	○	○
If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	○
If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	○

Answer:



Answer Area

Statements	Yes	No
If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.	○	[✓ ○]
If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	[✓ ○]	○
If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	[✓ ○]

Explanation:

NYN

First is not encrypted because of the exclusion.

Second is encrypted because this time the recipient is not excluded.

Third is not encrypted because policy 2 is the only policy for user 2 and policy 2 does not do the encryption

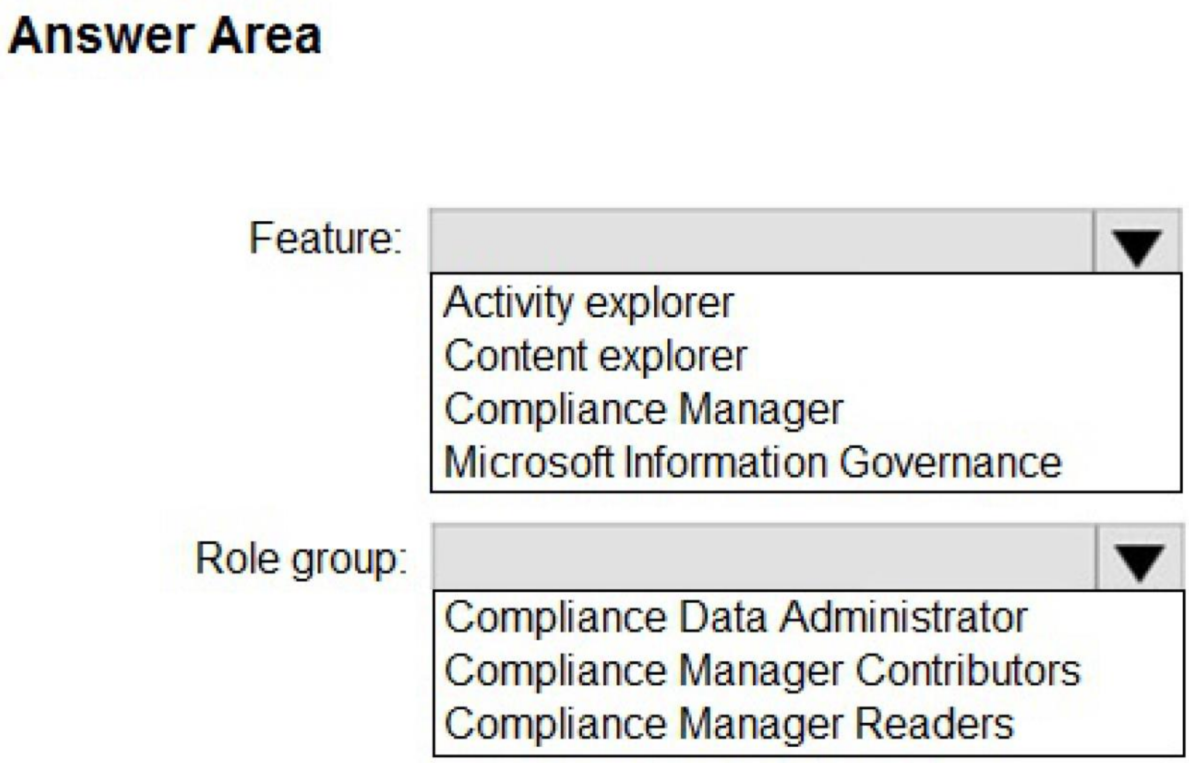
Question: 43 HOTSPOT

-

You have a Microsoft 365 E5 tenant that contains a trainable classifier named Classifier1.

You need to increase the accuracy of Classifier1. The solution must use the principle of least privilege. Which feature should you use and to which role group should you be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

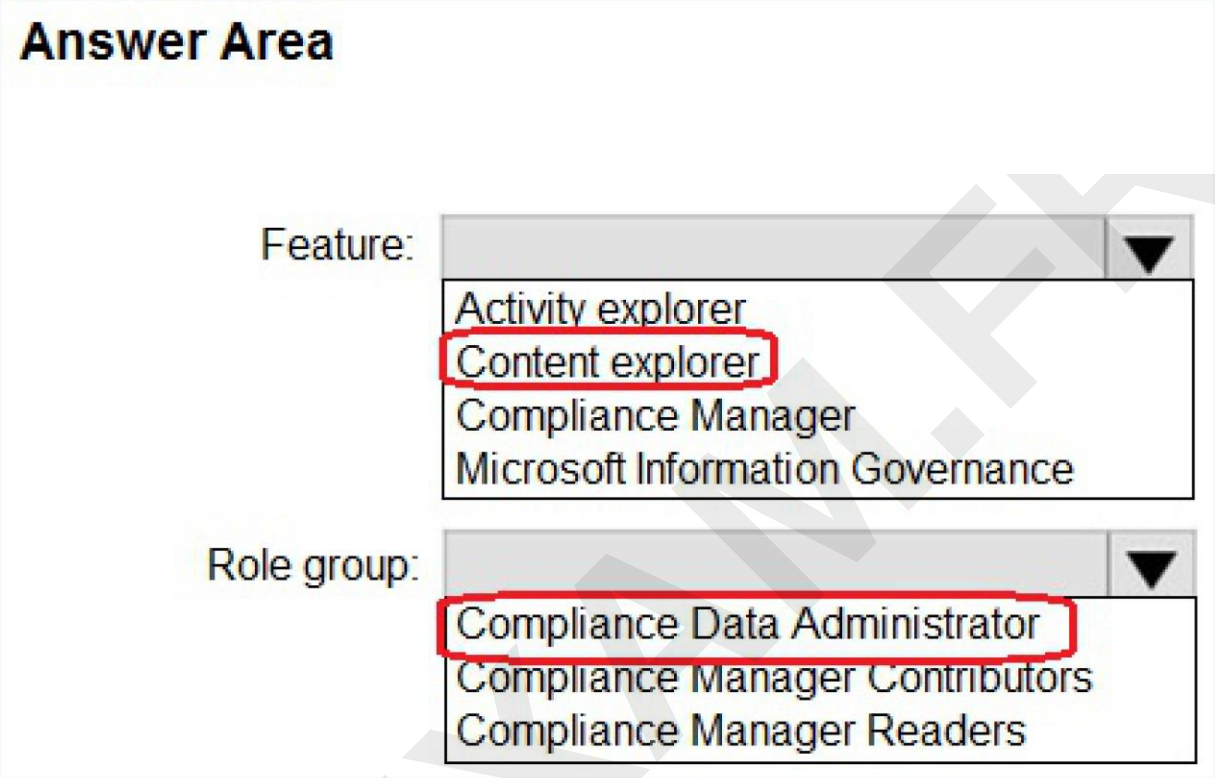
Feature:

Activity explorer
Content explorer
Compliance Manager
Microsoft Information Governance

Role group:

Compliance Data Administrator
Compliance Manager Contributors
Compliance Manager Readers

Answer:



Answer Area

Feature:

Activity explorer
[✓ Content explorer]
Compliance Manager
Microsoft Information Governance

Role group:

[✓ Compliance Data Administrator]
Compliance Manager Contributors
Compliance Manager Readers

Explanation:

To make trainable classifier better you can use Content explorer, found under data classification.To retrain trainable classifiers you need to be Compliance Data Administrator or Compliance Administrator

Question: 44

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.

What should you do?

A.From the Microsoft Purview compliance portal, start a data investigation.
B.From the Microsoft Defender for Cloud Apps portal, create a file policy.
C.From the Azure Active Directory admin center, configure an Identity Protection policy.
D.From the Exchange admin center, create a data loss prevention (DLP) policy.

Answer: B

Explanation:

This question is asking for a function that will detect when users SHARE sensitive information outside your company, which means with need to create a DLP policy.The only logical answer here for creating a DLP policy is Cloud Apps - File Policy since we have a DLP category available here

Question: 45 HOTSPOT

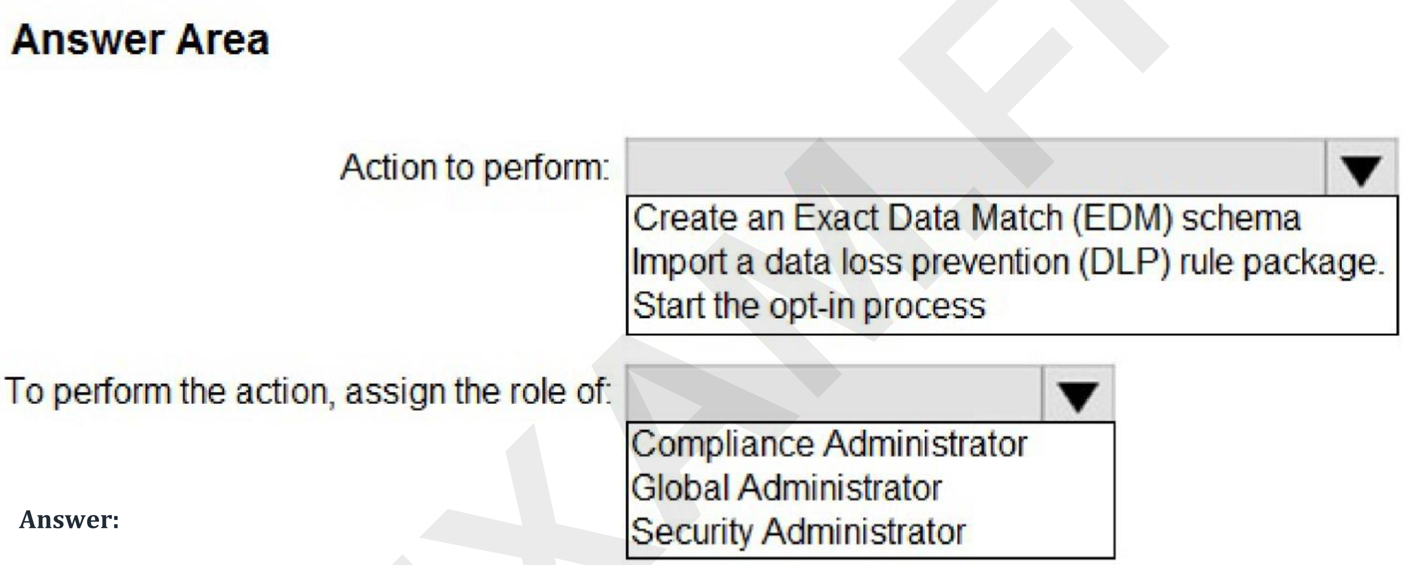
-

You have a Microsoft 365 E5 tenant.

You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.

What should you do first? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

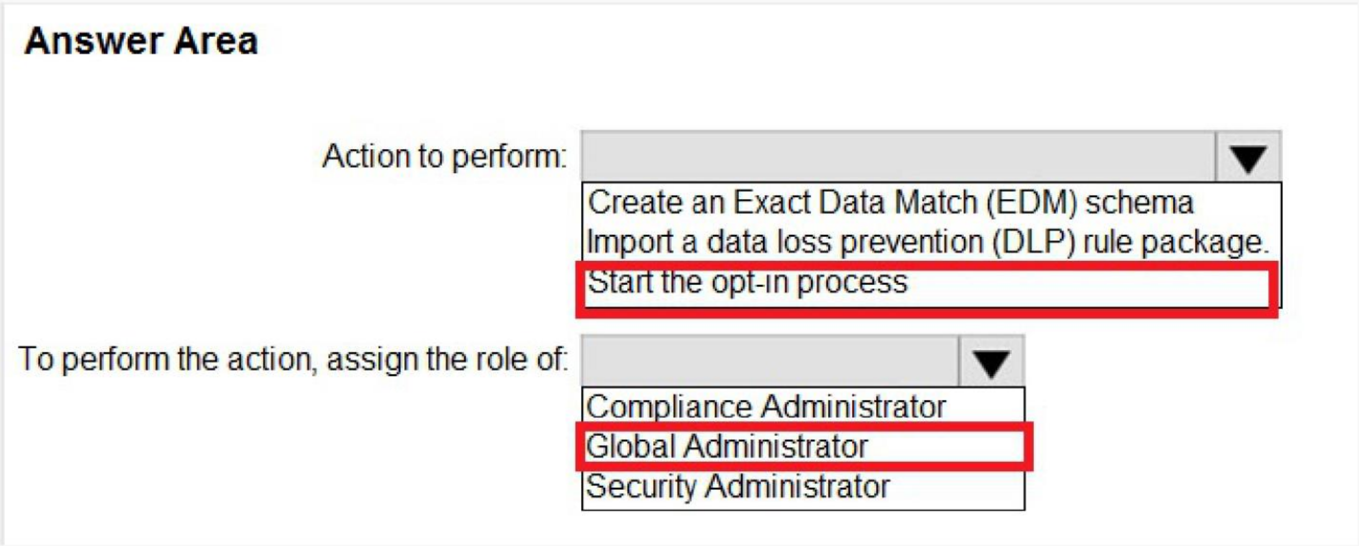
Action to perform:

Create an Exact Data Match (EDM) schema
Import a data loss prevention (DLP) rule package.
Start the opt-in process

To perform the action, assign the role of:

Compliance Administrator
Global Administrator
Security Administrator

Answer:



Answer Area

Action to perform:
- Create an Exact Data Match (EDM) schema
- Import a data loss prevention (DLP) rule package.
- [✓ Start the opt-in process]

To perform the action, assign the role of:
- Compliance Administrator
- [✓ Global Administrator]
- Security Administrator

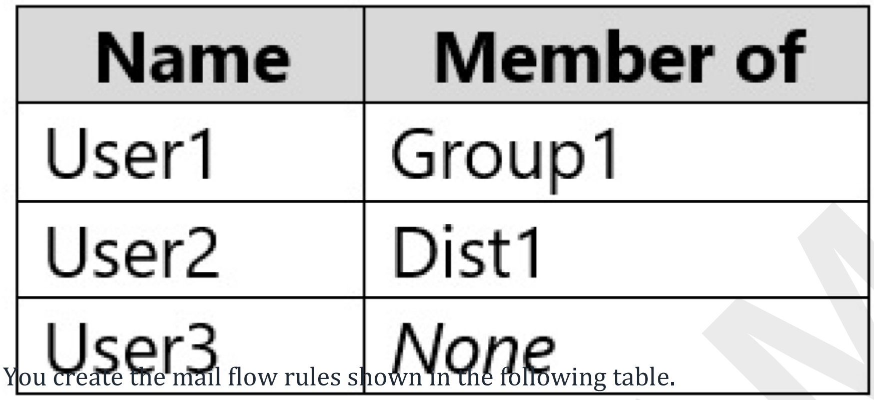
Explanation:

Start the Opt-in process and the role required to perform this action is Global Admin

Question: 46 HOTSPOT

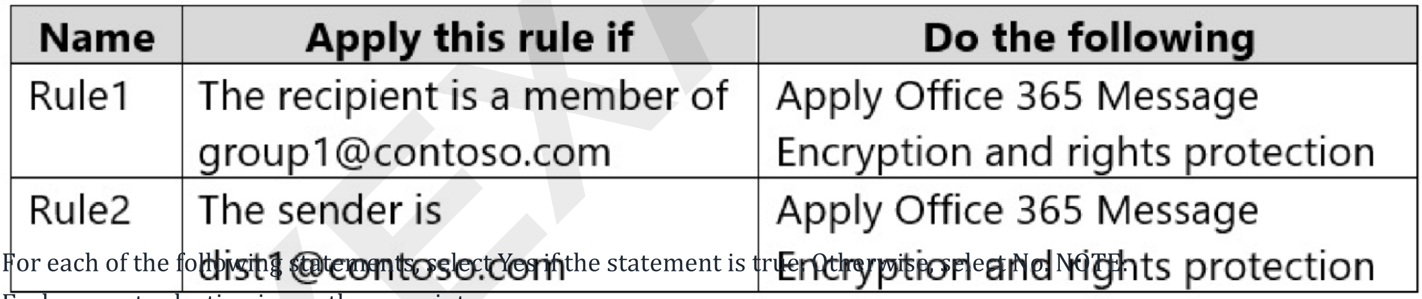
-

The subscription contains the users shown in the following table.



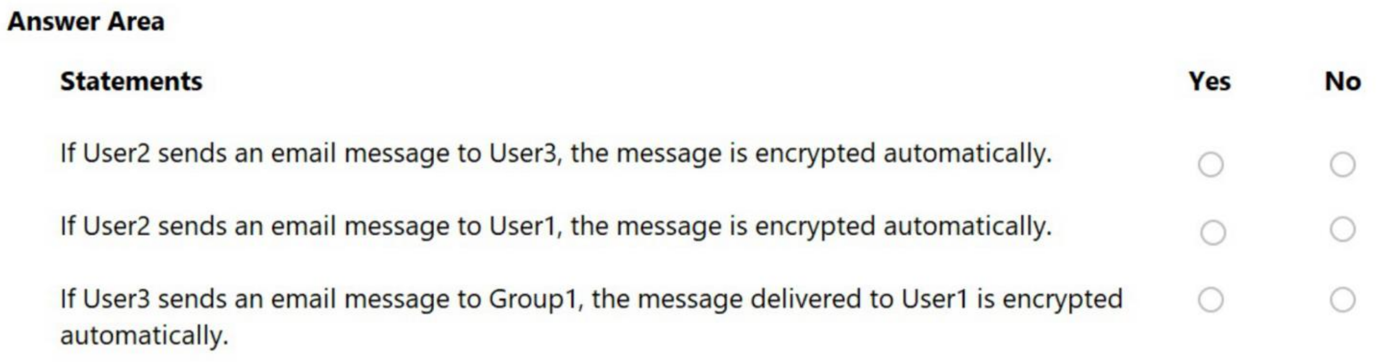
Name	Member of
User1	Group1
User2	Dist1
User3	*None*

You create the mail flow rules shown in the following table.



Name	Apply this rule if	Do the following
Rule1	The recipient is a member of group1@contoso.com	Apply Office 365 Message Encryption and rights protection
Rule2	The sender is dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

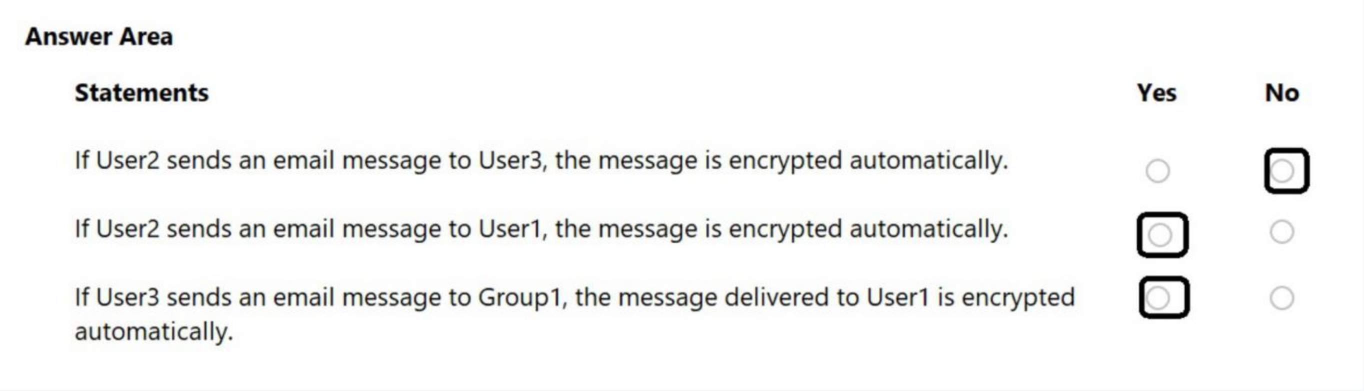
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	○
If User2 sends an email message to User1, the message is encrypted automatically.	○	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	○

Answer:



Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	[✓ ○]
If User2 sends an email message to User1, the message is encrypted automatically.	[✓ ○]	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	[✓ ○]	○

Explanation:

Answer 1-N user 2 IS NOT (rule 2 specifies USER IS)

Answer2- Y since user 1 is MEMBER of (rule 1 applies to the RECIPIENT)

Answer3- Y since user one is MEMBER and the email was sent to the recipient group

Question: 47

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You need to ensure that you receive an alert when a user uploads a document to a third-party cloud storage service.

What should you use?

A.an insider risk policy
B.a file policy
C.a sensitivity label
D.an activity policy

Answer: B

Explanation:

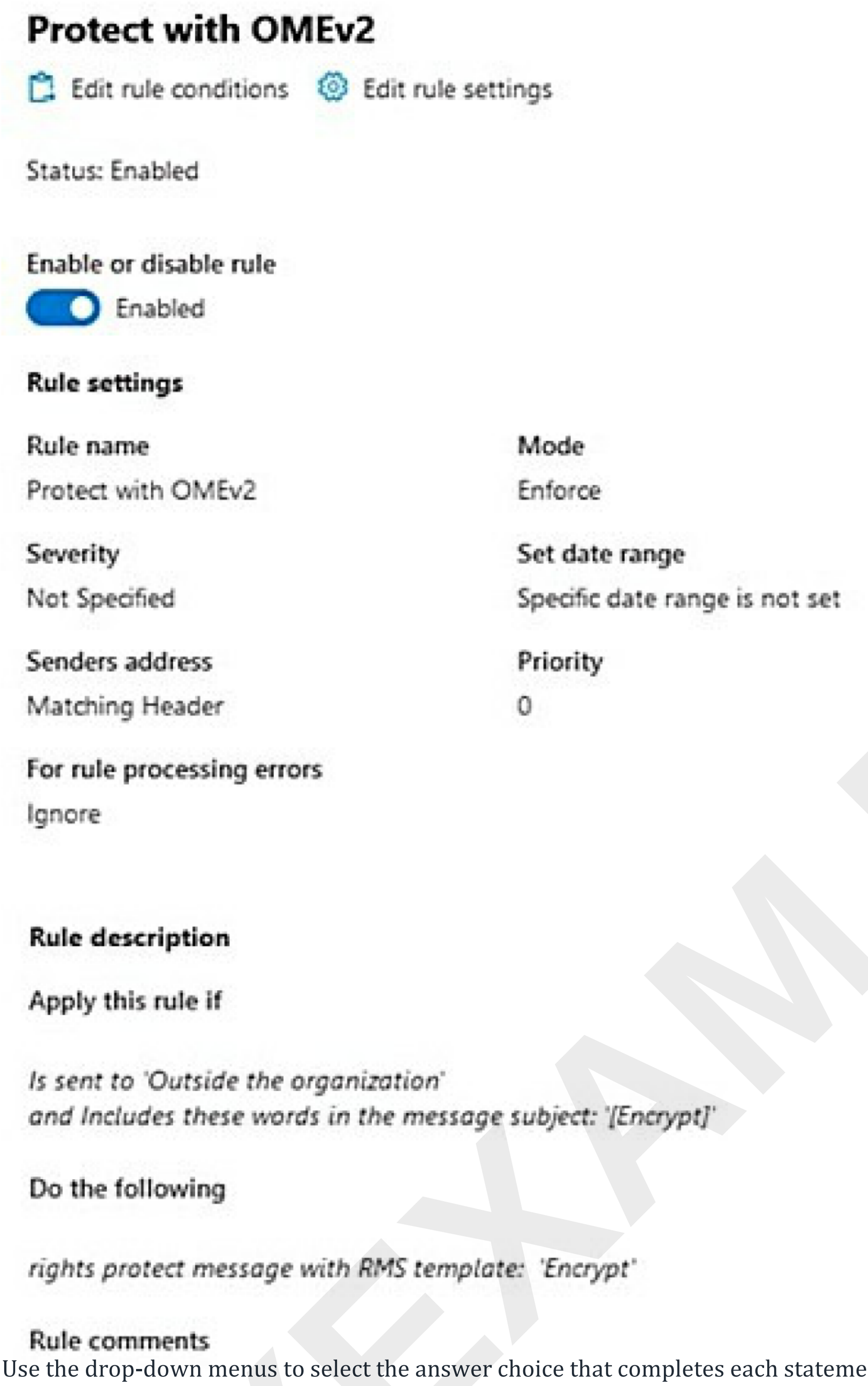
Correct answer is B:a file policy.

Question: 48 HOTSPOT

-

You have a Microsoft 365 subscription.

In Microsoft Exchange Online, you configure the mail flow rule shown in the following exhibit.



Protect with OMEv2

Status: Enabled

Enable or disable rule

Enabled

Rule settings

Rule name
Protect with OMEv2

Mode
Enforce

Severity
Not Specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
0

For rule processing errors
Ignore

Rule description

Apply this rule if

Is sent to 'Outside the organization'
and Includes these words in the message subject: '[Encrypt]'

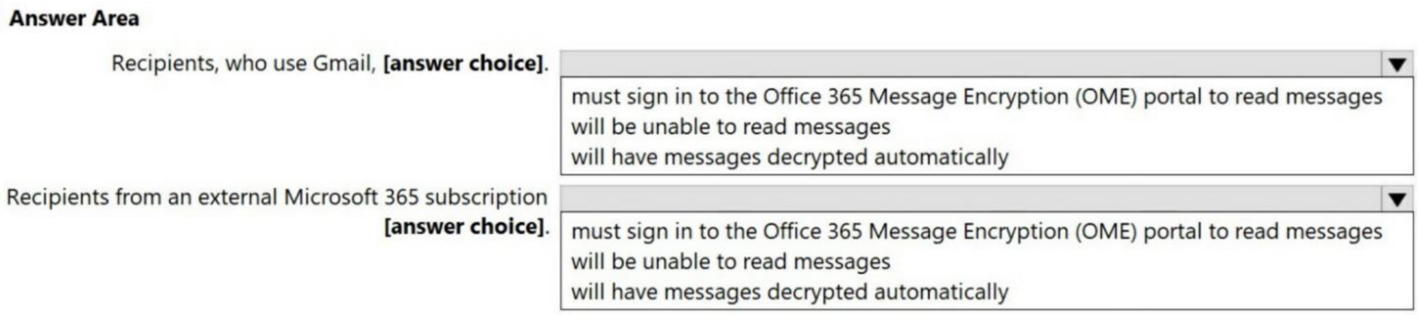
Do the following

rights protect message with RMS template: 'Encrypt'

Rule comments

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer Area

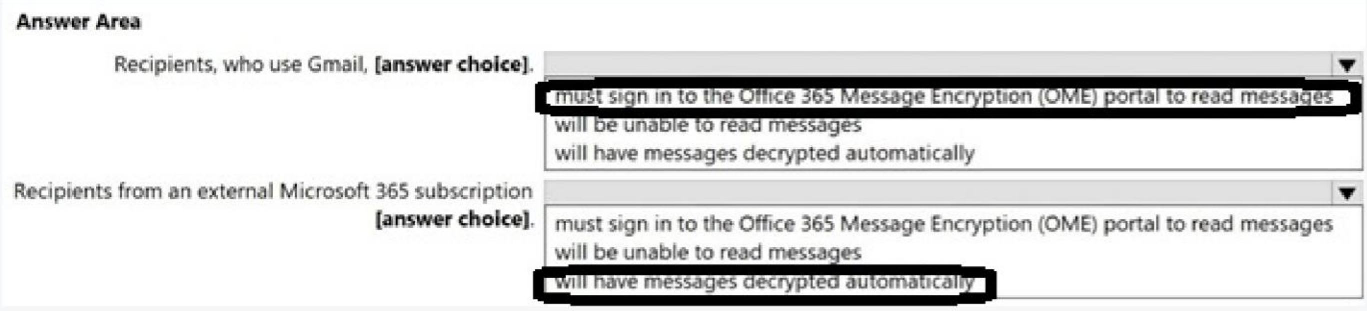
Recipients, who use Gmail, **[answer choice]**. ▼

- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription **[answer choice]**. ▼

- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Answer:



Answer Area

Recipients, who use Gmail, **[answer choice]**. ▼

- [✓ must sign in to the Office 365 Message Encryption (OME) portal to read messages]
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription **[answer choice]**. ▼

- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- [✓ will have messages decrypted automatically]

Question: 49

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a retention label.

Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

Correct answer is B:NO.

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

Question: 50

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.
Solution: You create an auto-labeling policy for a sensitivity label.

Does this meet the goal?

A.Yes
B.No

Answer: A

Explanation:

Correct answer is A:yes.

Question: 51 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create a data loss prevention (DLP) policy.

Does this meet the goal?

A.Yes
B.No

Answer: B

Explanation:

You can't use trainable classifiers in a (custom) DLP policy.

Question: 52 You have a Microsoft 365 E5 subscription.

You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.

What should you configure first?

A.a custom branding template
B.a mail flow rule

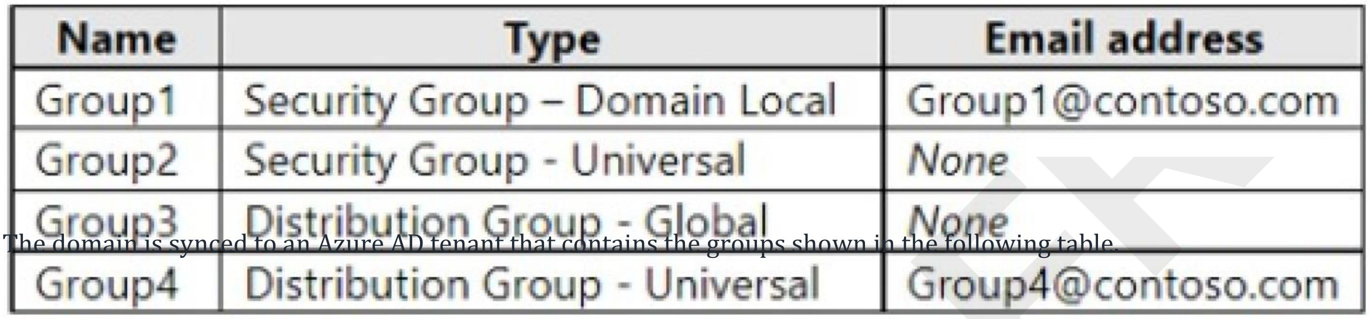
C.a Conditional Access policy
D.a sensitivity label

Answer: A
Explanation:
Answer is a custom branding template. "With Microsoft Purview Advanced Message Encryption, anytime you apply custom branding, the Office 365 applies the wrapper to email that fits the mail flow rule to which you apply the template. In addition, you can only use expiration if you use custom branding.

Reference:
"https://learn.microsoft.com/en-us/purview/ome-advanced-expiration

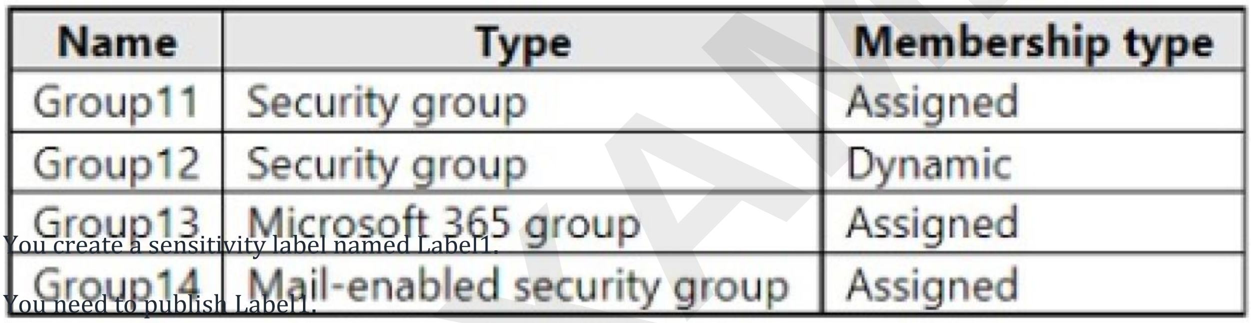
Question: 53 HOTSPOT

-
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.



Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group - Universal	*None*
Group3	Distribution Group - Global	*None*
Group4	Distribution Group - Universal	Group4@contoso.com

The domain is synced to an Azure AD tenant that contains the groups shown in the following table.

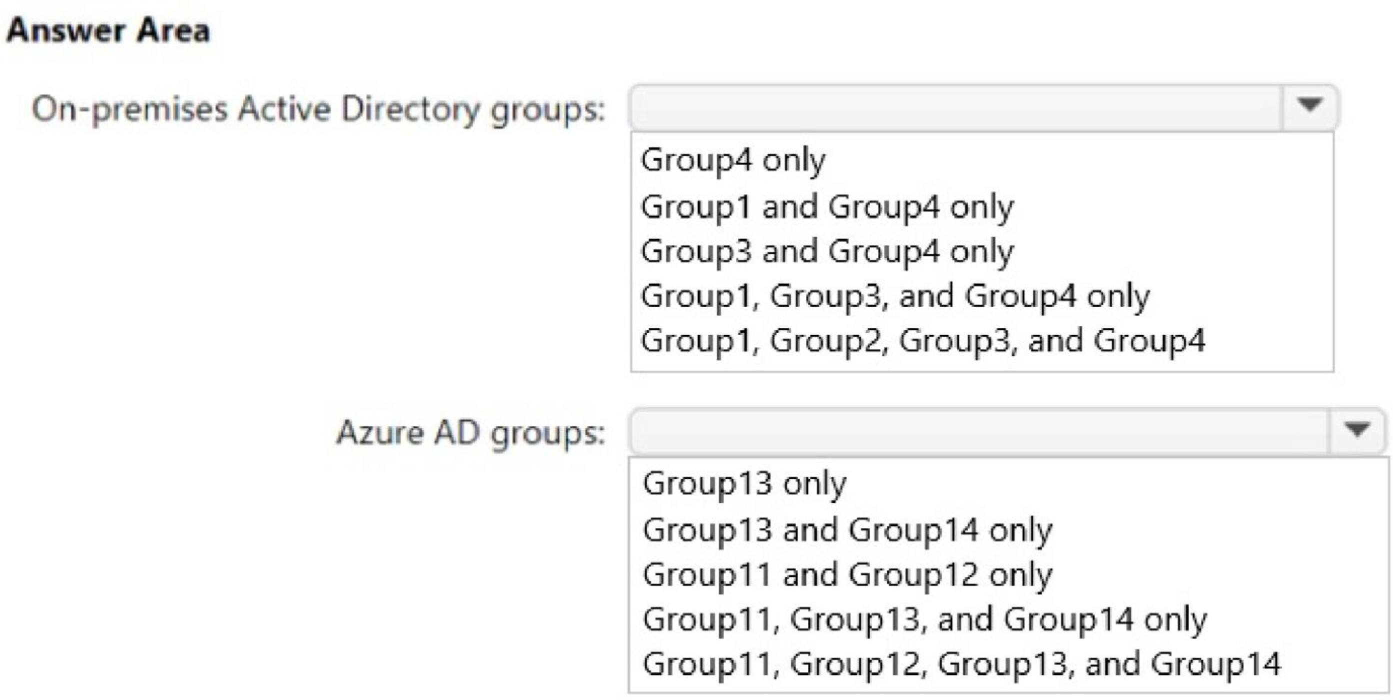


Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Microsoft 365 group	Assigned
Group14	Mail-enabled security group	Assigned

You create a sensitivity label named Label1.

You need to publish Label1.

To which groups can you publish Label1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

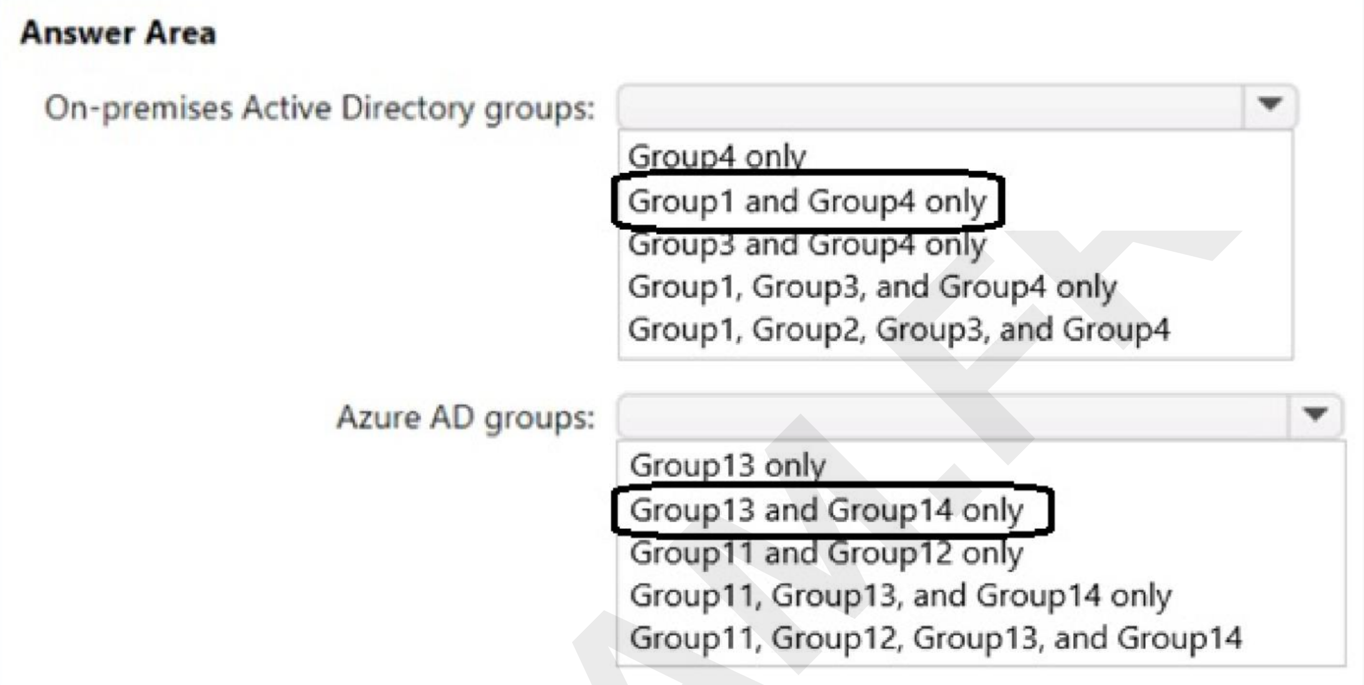
On-premises Active Directory groups:

- Group4 only
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12, Group13, and Group14

Answer:



Answer Area

On-premises Active Directory groups:

- Group4 only
- [✓ Group1 and Group4 only]
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 only
- [✓ Group13 and Group14 only]
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12, Group13, and Group14

Explanation:

Group 1 and Group 4 only.

Group 13 and Group 14 only.

Question: 54 HOTSPOT

-

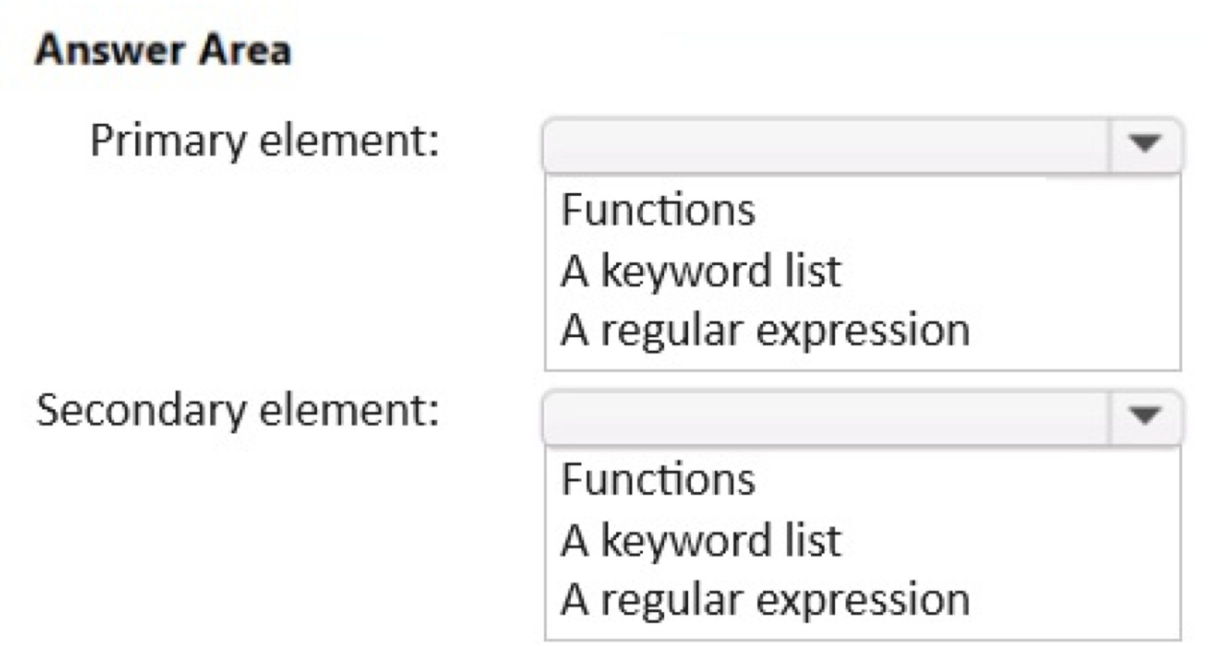
You have a Microsoft 365 tenant.

You need to create a new sensitive info type for items that contain the following:

•An employee ID number that consists of the hire date of the employee followed by a three digit number•The words “Employee”, “ID”, or “Identification” within 300 characters of the employee ID number

What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

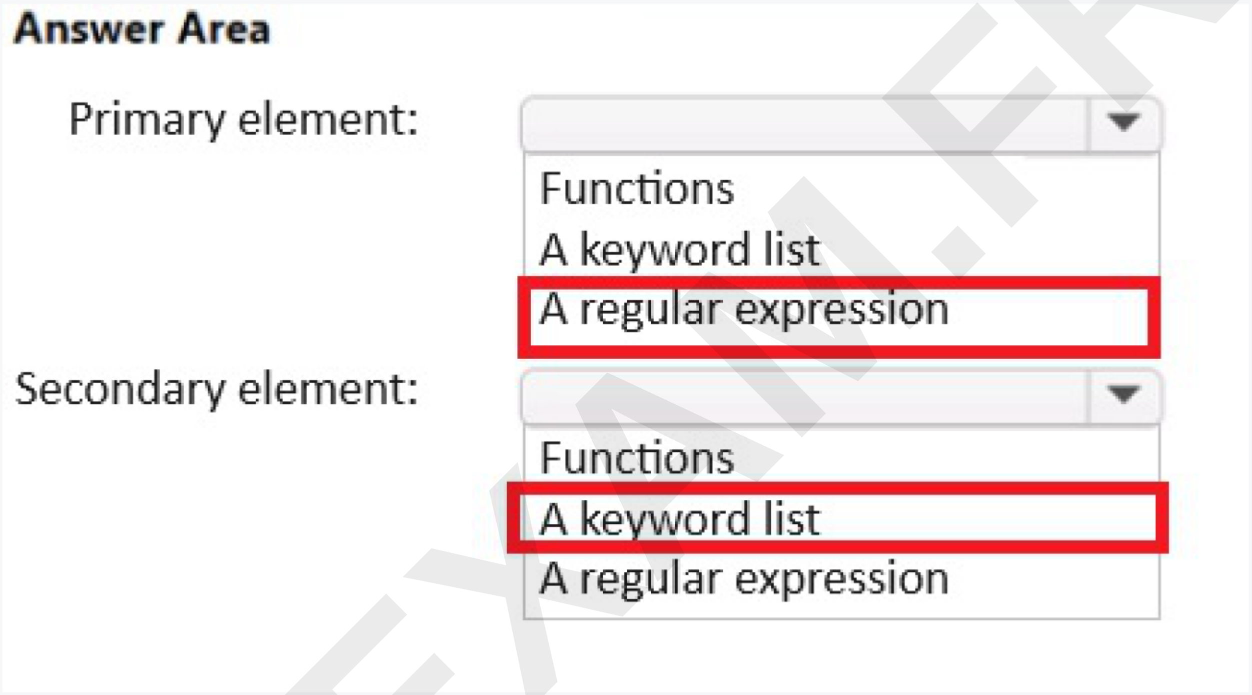
Primary element:

Functions
A keyword list
A regular expression

Secondary element:

Functions
A keyword list
A regular expression

Answer:



Answer Area

Primary element:

Functions
A keyword list
[✓ A regular expression]

Secondary element:

Functions
[✓ A keyword list]
A regular expression

Explanation:

A regular expression.

A keyword list.

Question: 55 You have

a Microsoft 365 tenant that has data loss prevention (DLP) policies.
You need to review DLP policy matches for the tenant.

What should you use?

A.Content explorer
B.Activity explorer
C.Compliance Manager
D.records management events

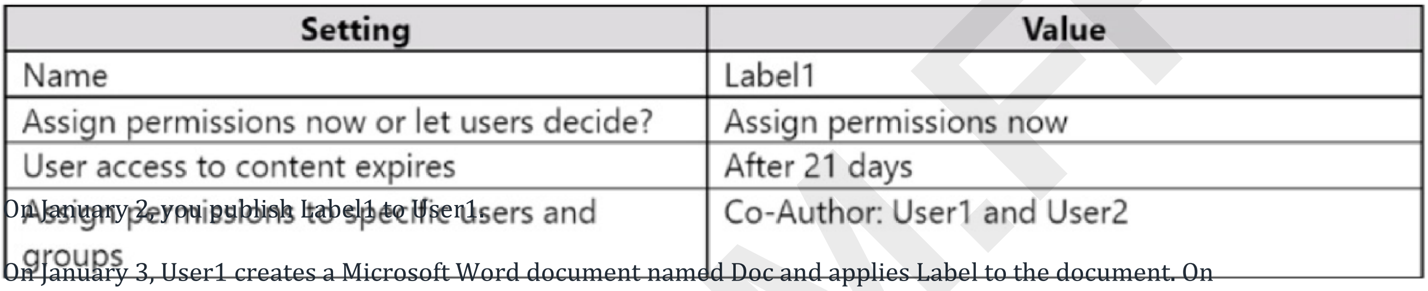
Answer: A

Explanation:

The Content Explorer in the Microsoft 365 compliance center allows you to view and manage sensitive information that matches your Data Loss Prevention (DLP) policies. It provides insights into where sensitive information resides in your organization and helps you manage risks associated with this data. Please note that appropriate permissions are required to access the Content Explorer.

Question: 56 You have

a Microsoft 365 E5 subscription that contains two users named User1 and User2.
On January 1, you create the sensitivity label shown in the following table.



Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish Label1 to User1.

On January 3, User1 creates a Microsoft Word document named Doc and applies Label to the document. On January 4, User2 edits Doc1.

On January 15, you increase the content expiry period for Label1 to 28 days.

When will access to Doc1 expire for User2?

A.January 23
B.January 24
C.January 25
D.January 31

Answer: D

Explanation:

Correct answer is D:January 31.

Question: 57 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create a retention policy.

Does this meet the goal?

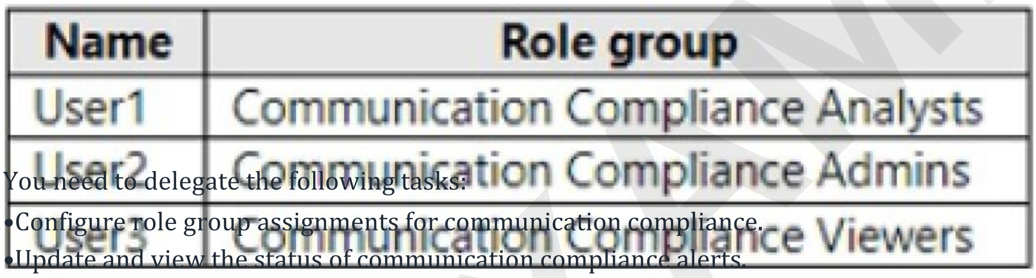
A.Yes
B.No

Answer: B

Explanation:
Solution to create retention policy isn't used to identify such files stored in organization. That kind of policies are used for retain (keep item) based on settings defined in it.

Question: 58 HOTSPOT

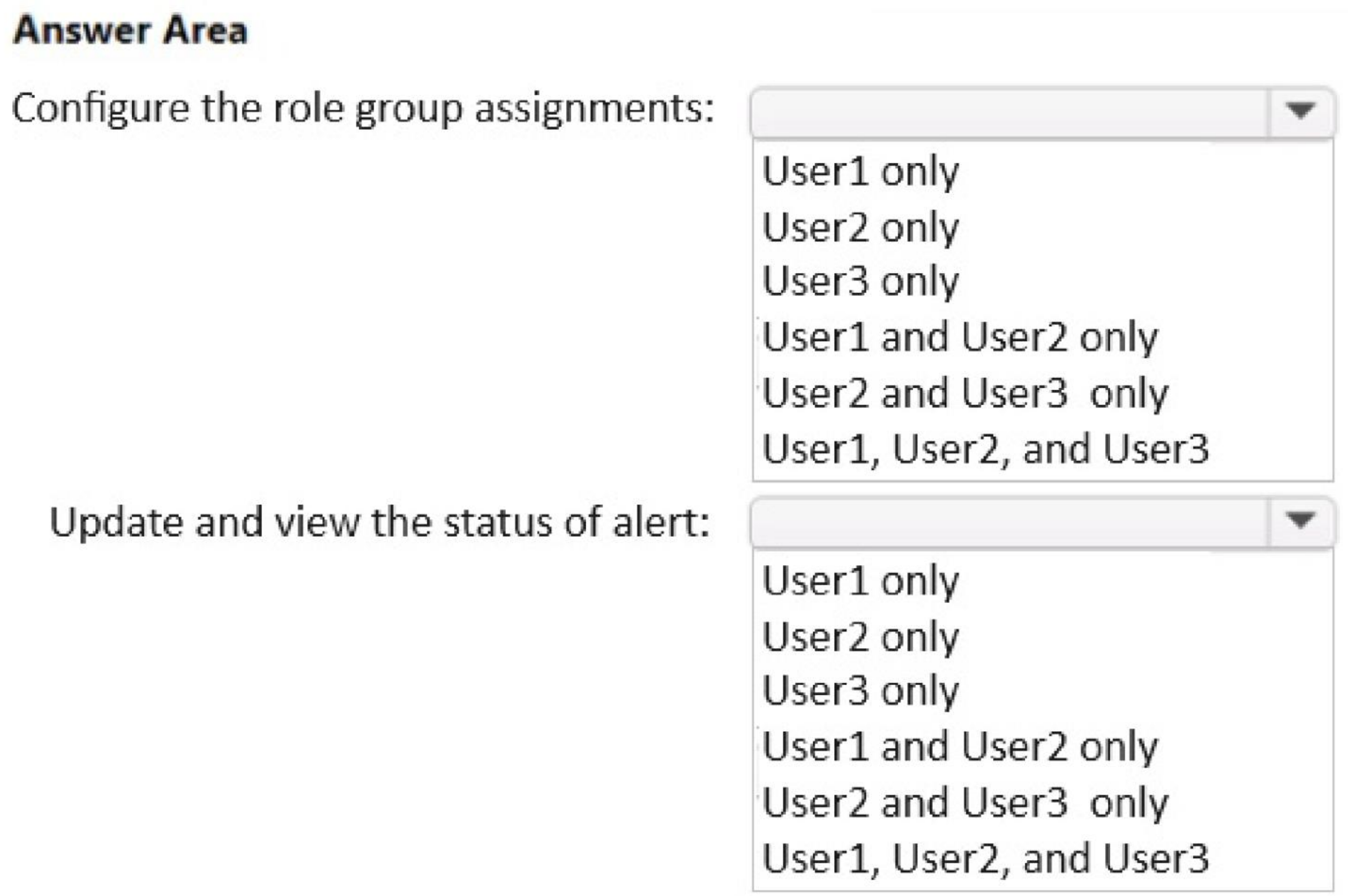
-
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Role group
User1	Communication Compliance Analysts
User2	Communication Compliance Admins
User3	Communication Compliance Viewers

You need to delegate the following tasks:
•Configure role group assignments for communication compliance.
•Update and view the status of communication compliance alerts.

Which users can perform each task? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

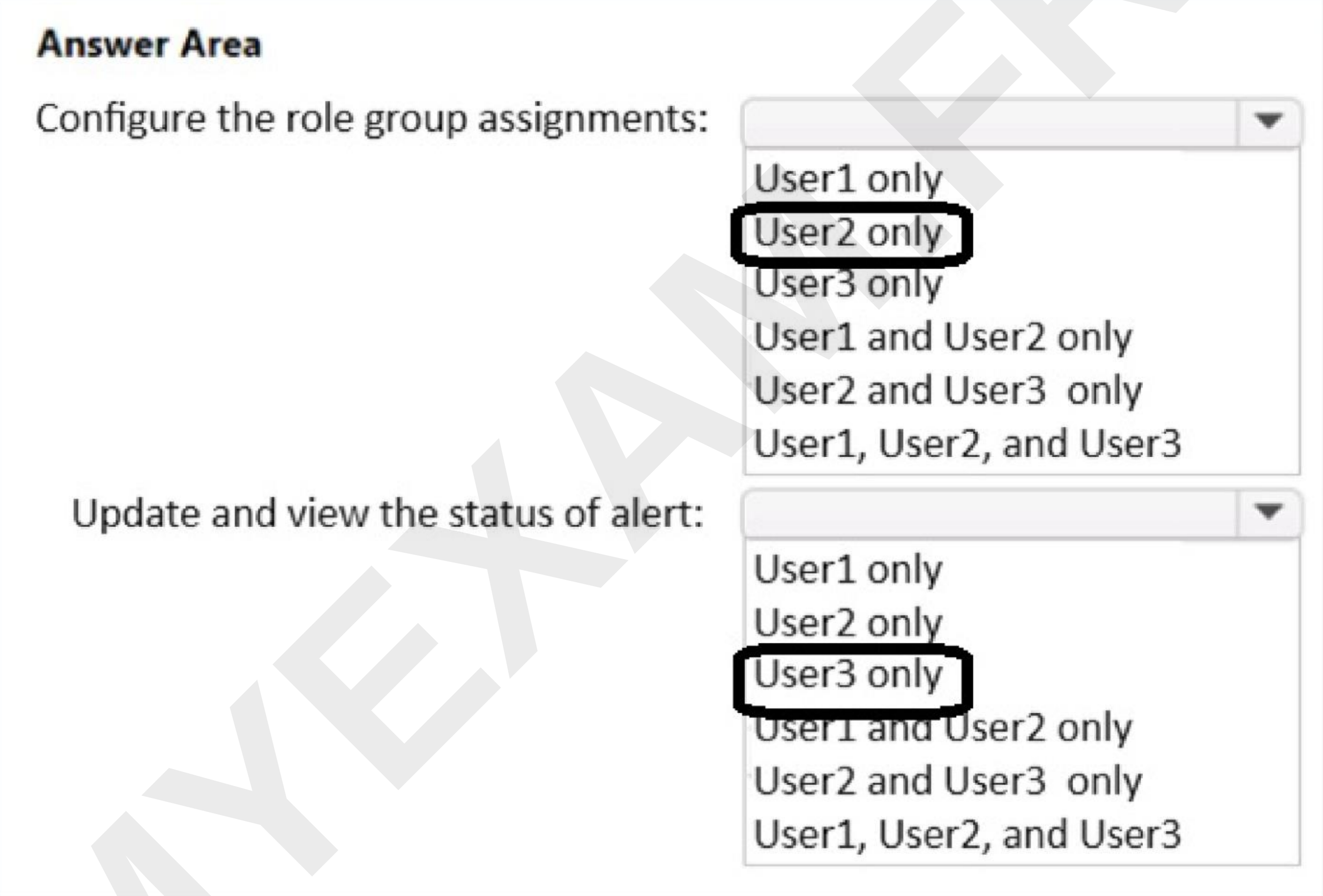
Configure the role group assignments:

User1 only
User2 only
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Update and view the status of alert:

User1 only
User2 only
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Answer:



Answer Area

Configure the role group assignments:

User1 only
[✓ User2 only]
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Update and view the status of alert:

User1 only
User2 only
[✓ User3 only]
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Explanation:

User 2 only.

User 3 only.

Question: 59

You have a Microsoft 365 E5 tenant that contains a user named User1. User1 is assigned the Compliance Administrator role.

User1 cannot view the regular expression in the IP Address sensitive info type.

You need to ensure that User1 can view the regular expression.

What should you do?

A.Assign User1 the Global Reader role.
B.Assign User1 to the Reviewer role group.
C.Instruct User to use the Test function on the sensitive info type.
D.Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.

Answer: D

Explanation:

Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.

Question: 60

You have a Microsoft 365 E5 subscription.

You need to ensure that any message or document containing a credit card number is deleted automatically 12 months after it was created. The solution must minimize administrative effort.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A.a sensitivity label
B.an auto-labeling policy for a sensitivity label
C.a retention label
D.an auto-labeling policy for a retention label
E.a sensitive information type (SIT)

Answer: CD

Explanation:

C.a retention label.

D.an auto-labeling policy for a retention label.

Question: 61 You have a Microsoft 365 subscription.

You create a new trainable classifier.

You need to train the classifier.

Which source can you use to train the classifier?

A.a Microsoft SharePoint Online site
B.an on-premises Microsoft SharePoint Server site
C.an NFS file share
D.an Azure Files share

Answer: A

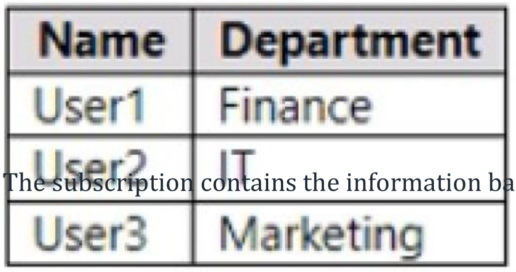
Explanation:

a Microsoft SharePoint Online site.

Question: 62 HOTSPOT

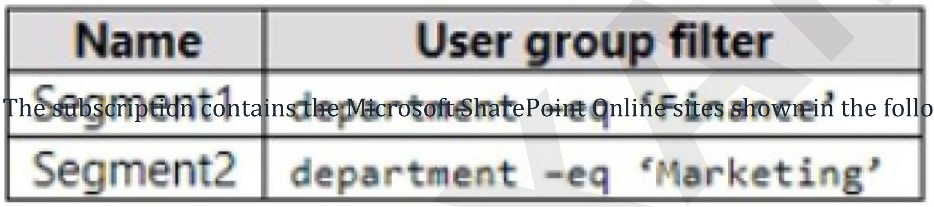
-

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



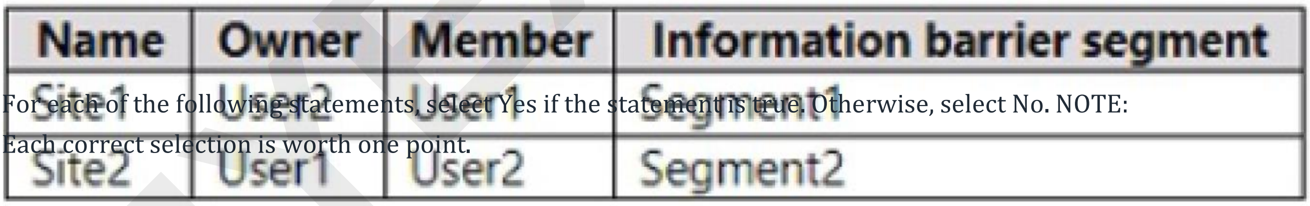
Name	Department
User1	Finance
User2	IT
User3	Marketing

The subscription contains the information barrier segments shown in the following table.



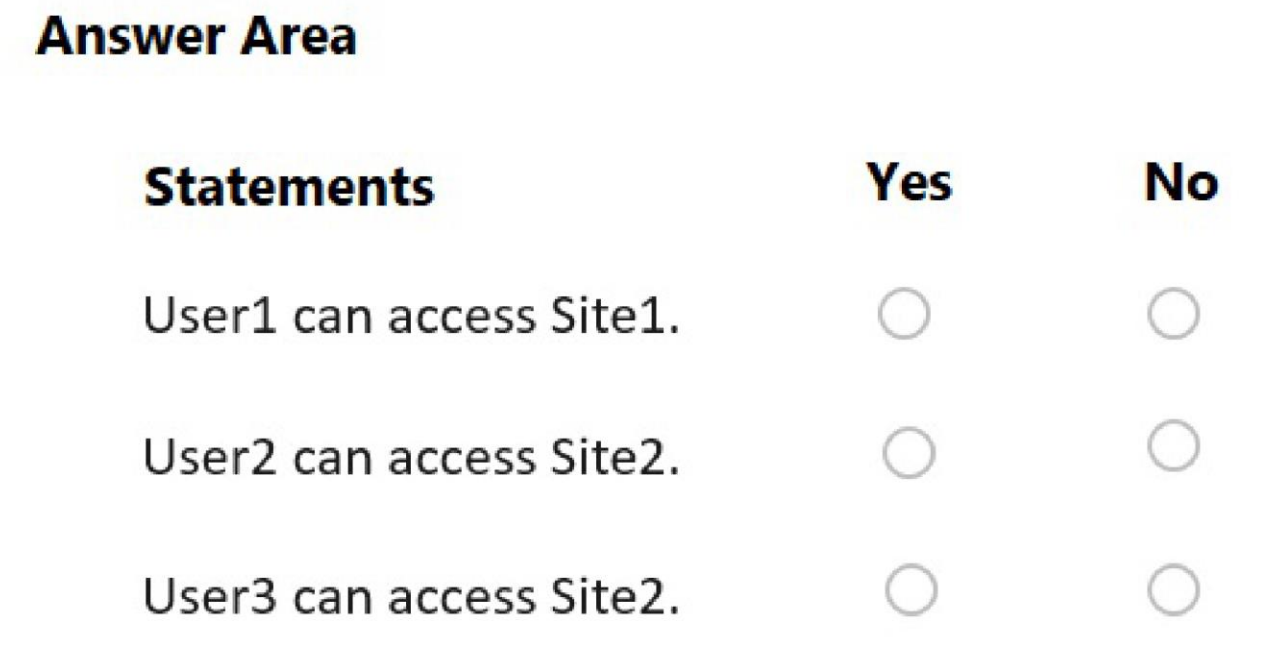
Name	User group filter
Segment1	department -eq 'Finance'
Segment2	department -eq 'Marketing'

The subscription contains the Microsoft SharePoint Online sites shown in the following table.



Name	Owner	Member	Information barrier segment
Site1	User2	User1	Segment1
Site2	User1	User2	Segment2

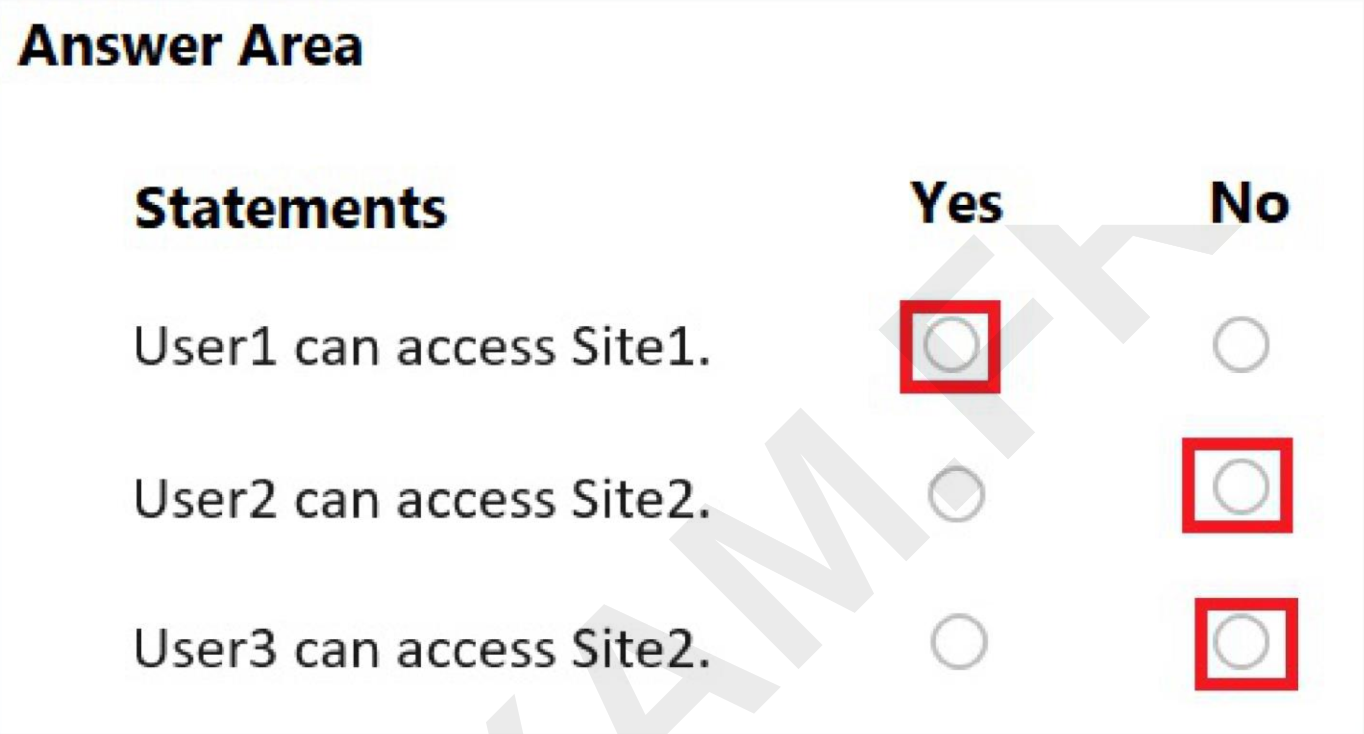
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can access Site1.	○	○
User2 can access Site2.	○	○
User3 can access Site2.	○	○

Answer:



Answer Area

Statements	Yes	No
User1 can access Site1.	[✓ ○]	○
User2 can access Site2.	○	[✓ ○]
User3 can access Site2.	○	[✓ ○]

Explanation:

Y: User1 is a member of the site also in Finance department (Segment1)

N: User2 is a member of the site but not in Marketing department (Segment2)

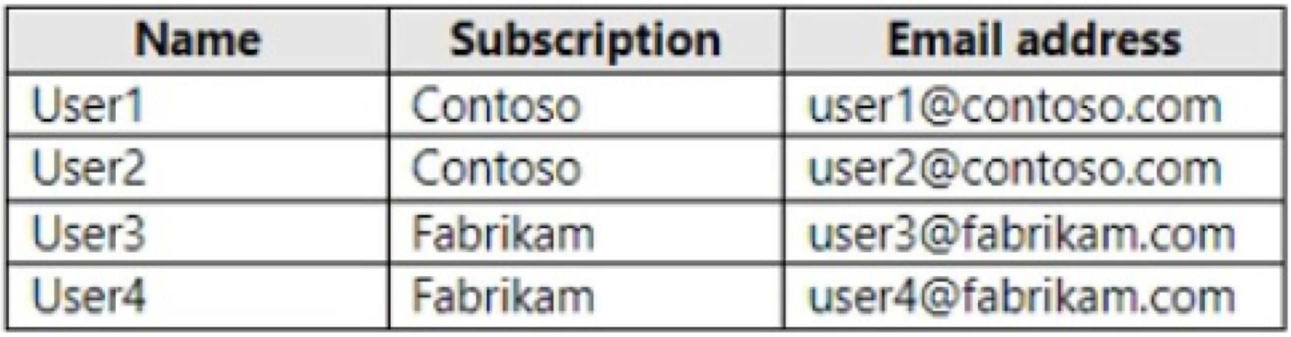
N: User3 is not a member of the site and it is in Marketing department (Segment2). If a user is not a member of a SharePoint site, they will not be able to access the site, even if they match the information barrier segment associated with the site12.

Question: 63

HOTSPOT

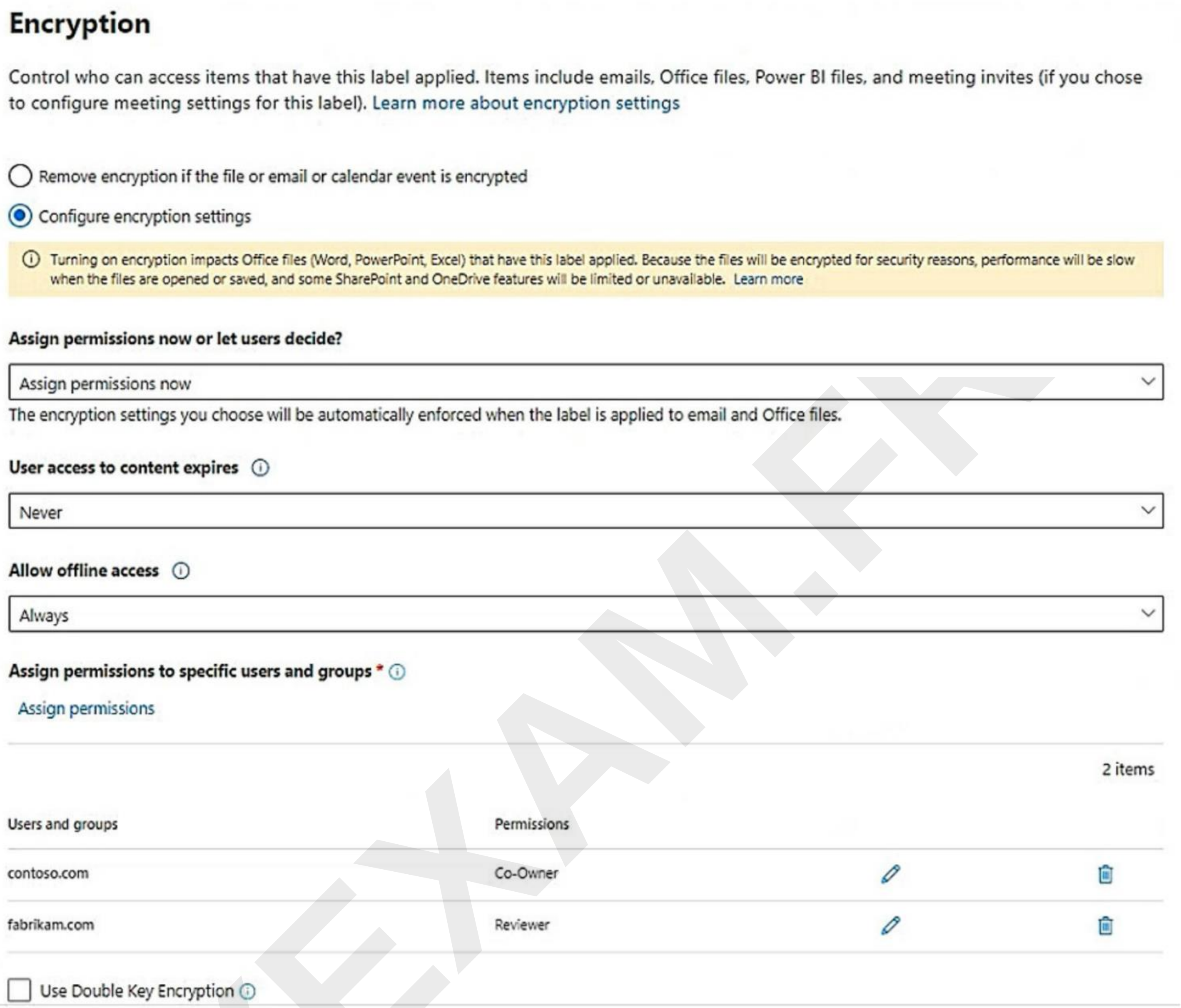
-

You have two Microsoft 365 subscriptions named Contoso and Fabrikam. The subscriptions contain the users shown in the following table.



Name	Subscription	Email address
User1	Contoso	user1@contoso.com
User2	Contoso	user2@contoso.com
User3	Fabrikam	user3@fabrikam.com
User4	Fabrikam	user4@fabrikam.com

You have a sensitivity label named Sensitiviy1 as shown in the exhibit. (Click the Exhibit tab.)



Encryption

Control who can access items that have this label applied. Items include emails, Office files, Power BI files, and meeting invites (if you chose to configure meeting settings for this label). Learn more about encryption settings

○ Remove encryption if the file or email or calendar event is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

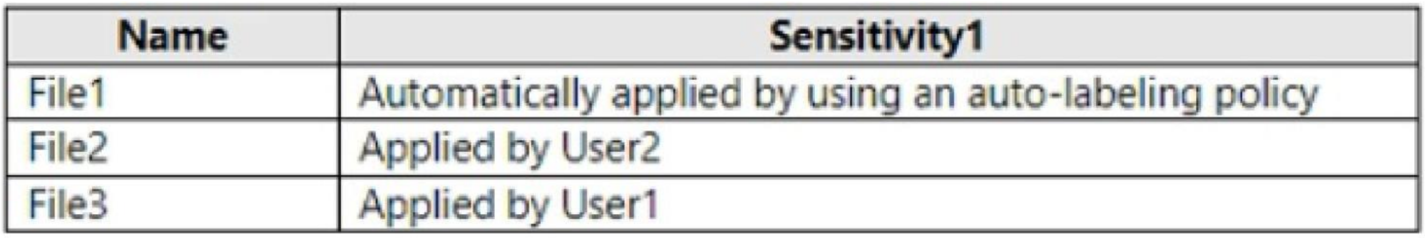
Assign permissions

2 items

Users and groups	Permissions
contoso.com	Co-Owner
fabrikam.com	Reviewer

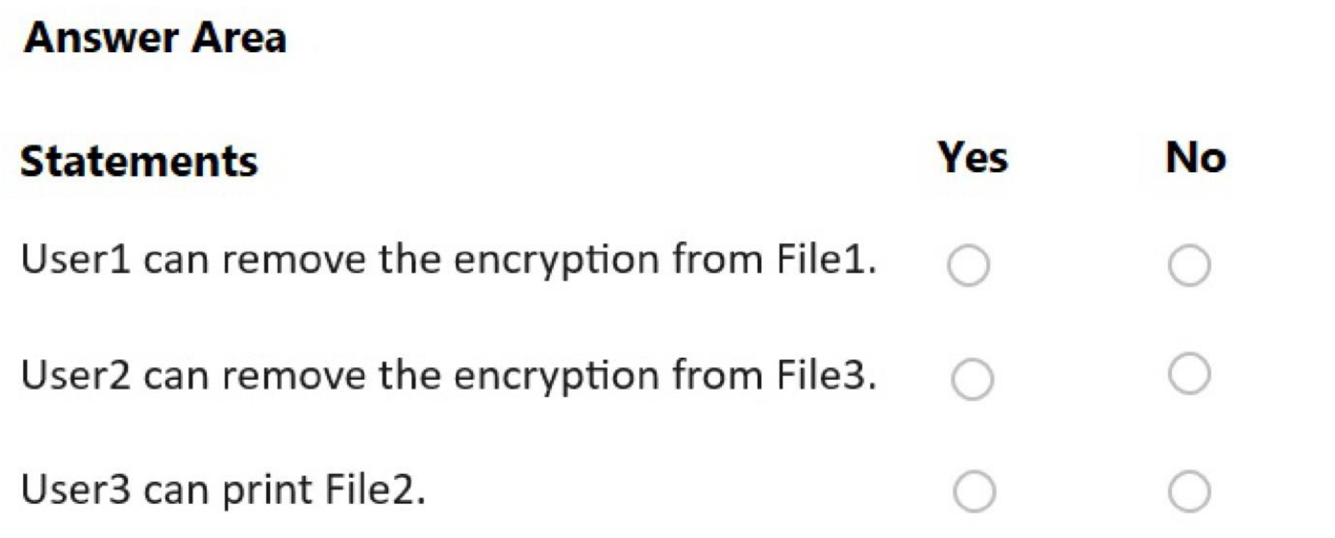
□ Use Double Key Encryption ⓘ

You have the files shown in the following table.



Name	Sensitivity1
File1	Automatically applied by using an auto-labeling policy
File2	Applied by User2
File3	Applied by User1

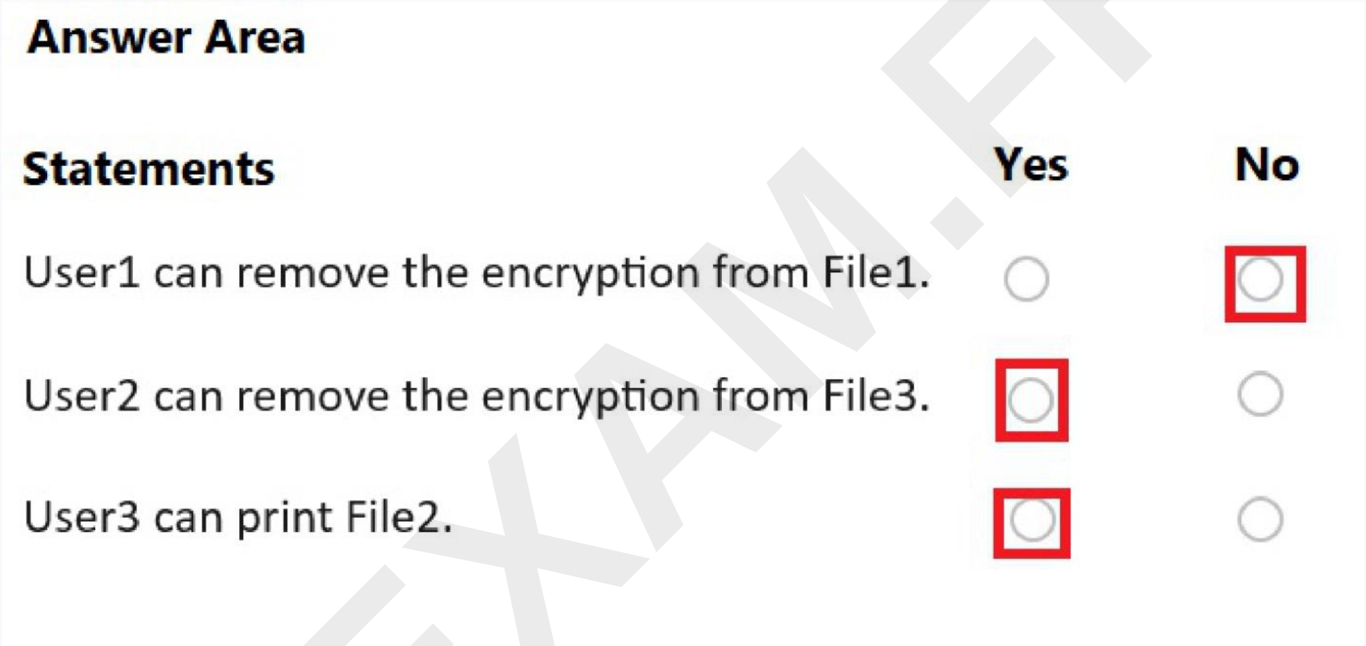
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can remove the encryption from File1.	○	○
User2 can remove the encryption from File3.	○	○
User3 can print File2.	○	○

Answer:



Answer Area

Statements	Yes	No
User1 can remove the encryption from File1.	○	[✓ ○]
User2 can remove the encryption from File3.	[✓ ○]	○
User3 can print File2.	[✓ ○]	○

Explanation:

No

yes

yes

Question: 64 DRAG

DROP

-

You have a Microsoft 365 E5 subscription.

You need to label Microsoft Exchange Online emails that match the following conditions:•Contain employment offers

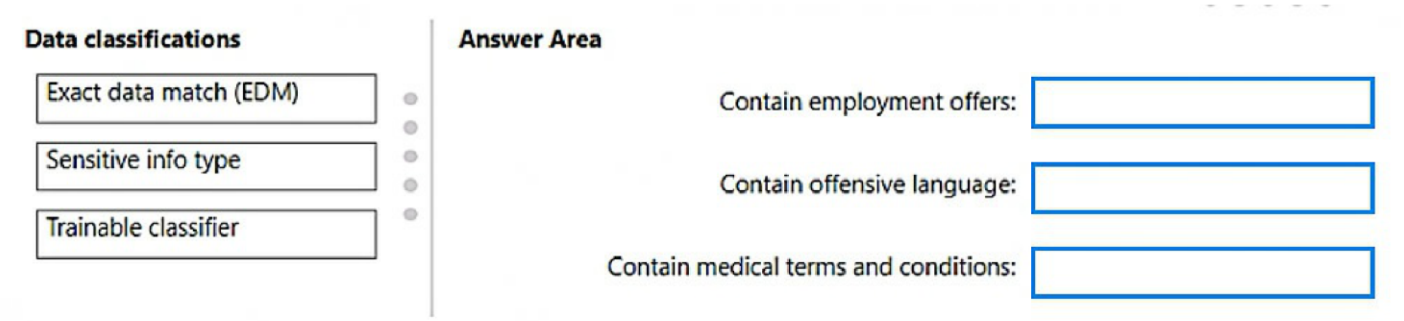
•Contain offensive language

•Contain medical terms and conditions

The solution must minimize administrative effort.

Which type of data classification should you use for each condition? To answer, drag the appropriate data classification types to the correct conditions. Each data classification type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Data classifications

- Exact data match (EDM)
- Sensitive info type
- Trainable classifier

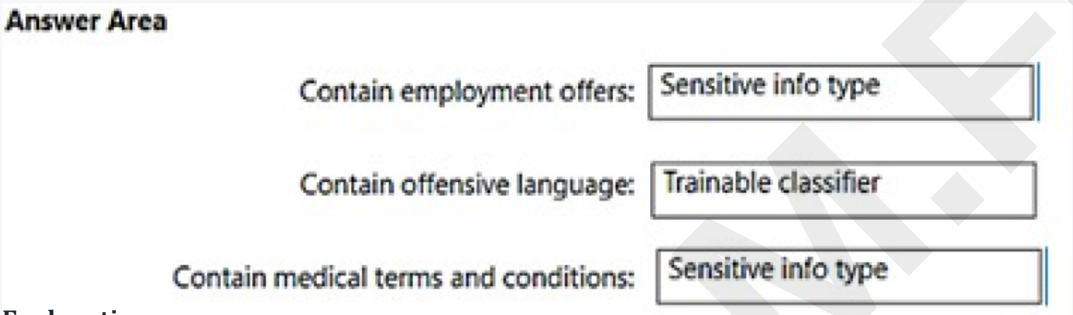
Answer Area

Contain employment offers:

Contain offensive language:

Contain medical terms and conditions:

Answer:



Answer Area

Contain employment offers: Sensitive info type

Contain offensive language: Trainable classifier

Contain medical terms and conditions: Sensitive info type

Explanation:

Sensitive info type.

Trainable classifier.

Sensitive info type.

Question: 65 HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You create a sensitivity label that has the following settings:

•Name: Sensitivity1
•Define the scope for this label: Items
•Choose protection settings for files and emails: Mark the content of files
•Add custom headers, footers, and watermarks to files and emails that have this label applied

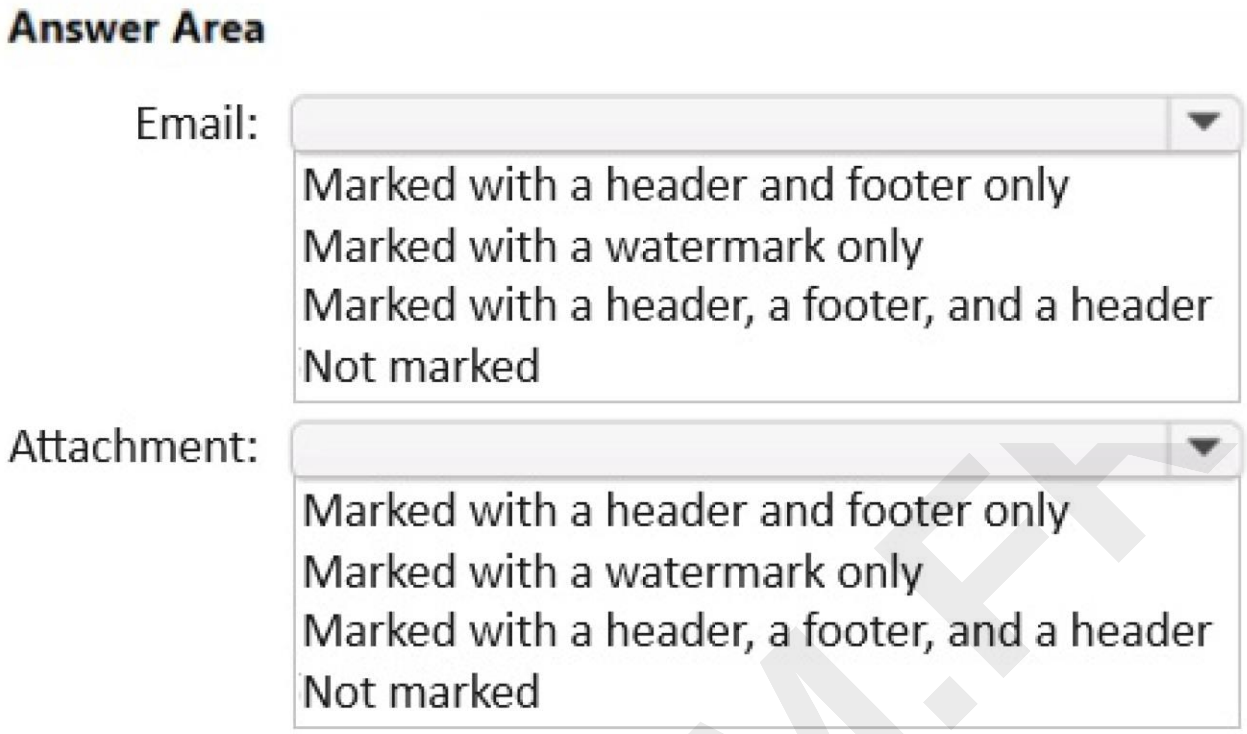
You make Sensitivity available to User1.

User1 performs the following actions:

•Creates a new email
•Adds a file named File1.docx as an attachment to the email
•Applies Sensitivity1 to the email
•Sends the email to User2

How will the email and the attachment be marked? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

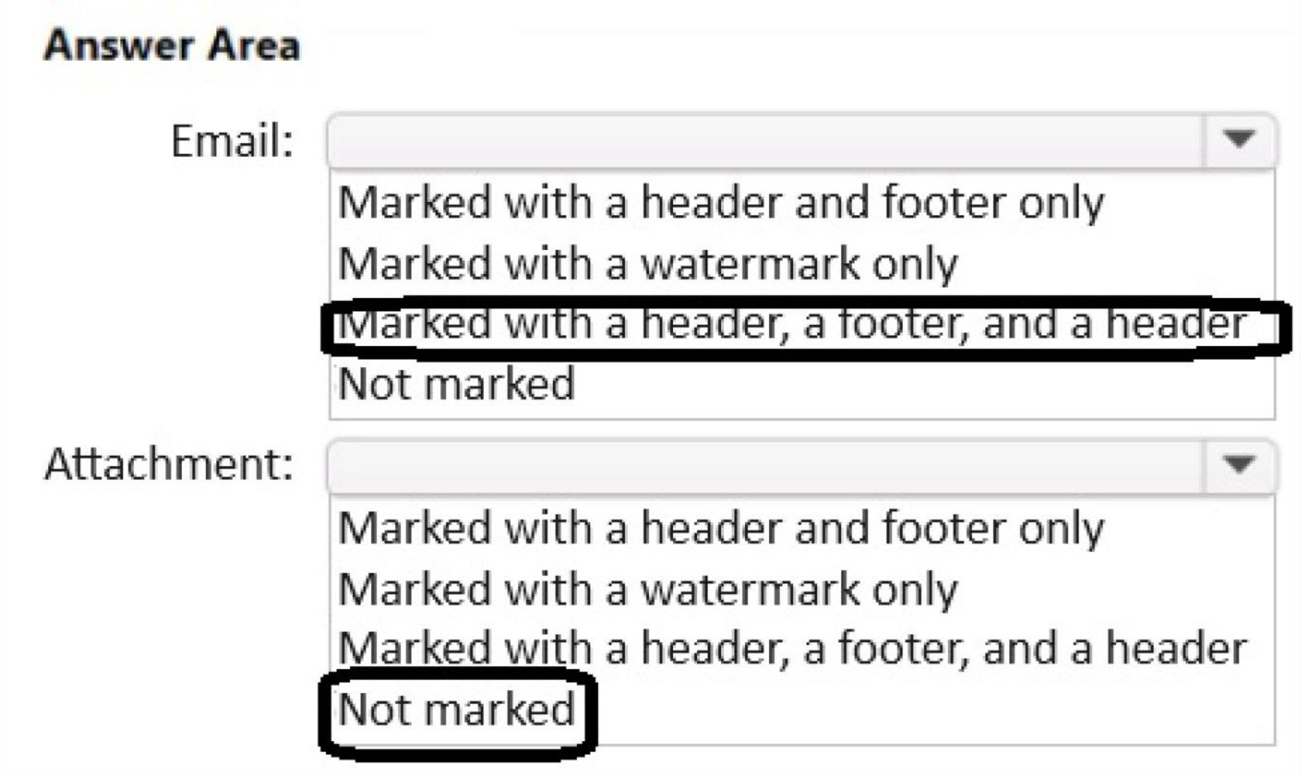


Answer Area

Email:
Marked with a header and footer only
Marked with a watermark only
Marked with a header, a footer, and a header
Not marked

Attachment:
Marked with a header and footer only
Marked with a watermark only
Marked with a header, a footer, and a header
Not marked

Answer:



Answer Area

Email:

- Marked with a header and footer only
- Marked with a watermark only
- [✓ Marked with a header, a footer, and a header]
- Not marked

Attachment:

- Marked with a header and footer only
- Marked with a watermark only
- Marked with a header, a footer, and a header
- [✓ Not marked]

Explanation:

Marked with a header, a footer, and a header.

Not marked.

Question: 66 You have a Microsoft 365 subscription that contains 100 users and a Microsoft 365 group named Group1. All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.

A sensitivity label named Label1 is published as the default label for Group1.

You add two sublabels named Sublabel1 and Sublabel2 to Label1.

You need to ensure that the settings in Sublabel1 are applied by default to Group1.

What should you do?

A.Change the order of Sublabel1.
B.Modify the policy of Label1.
C.Delete the policy of Label1 and publish Sublabel1.
D.Duplicate all the settings from Sublabel1 to Label1.

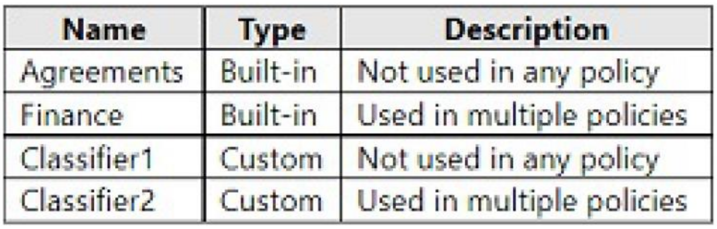
Answer: B

Explanation:

Modify the policy of Label1.

Question: 67

You have a Microsoft 365 E5 subscription that has the trainable classifiers shown in the following table.



Name	Type	Description
Agreements	Built-in	Not used in any policy
Finance	Built-in	Used in multiple policies
Classifier1	Custom	Not used in any policy
Classifier2	Custom	Used in multiple policies

Which trainable classifiers can you retrain?

A.Classifier1 only
B.Agreements and Classifier1 only
C.Classifier1 and Classifier2 only
D.Agreements, Finance, Classifier1, and Classifier2

Answer: C

Explanation:

Classifier1 and Classifier2 only.

Question: 68 HOTSPOT

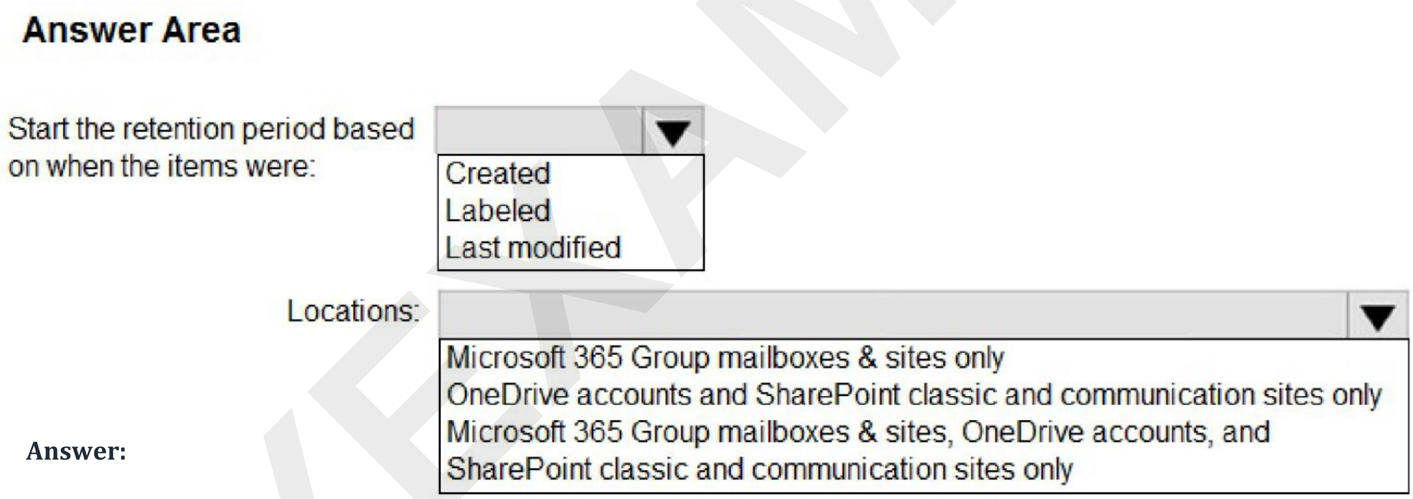
-

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online and Teams.

You need to ensure that when a user sends a message containing a cloud attachment, a retention label is applied to the cloud attachment by using auto-labeling policy.

How should you configure the retention label to start the retention period, and to which locations should you apply the auto-labeling policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

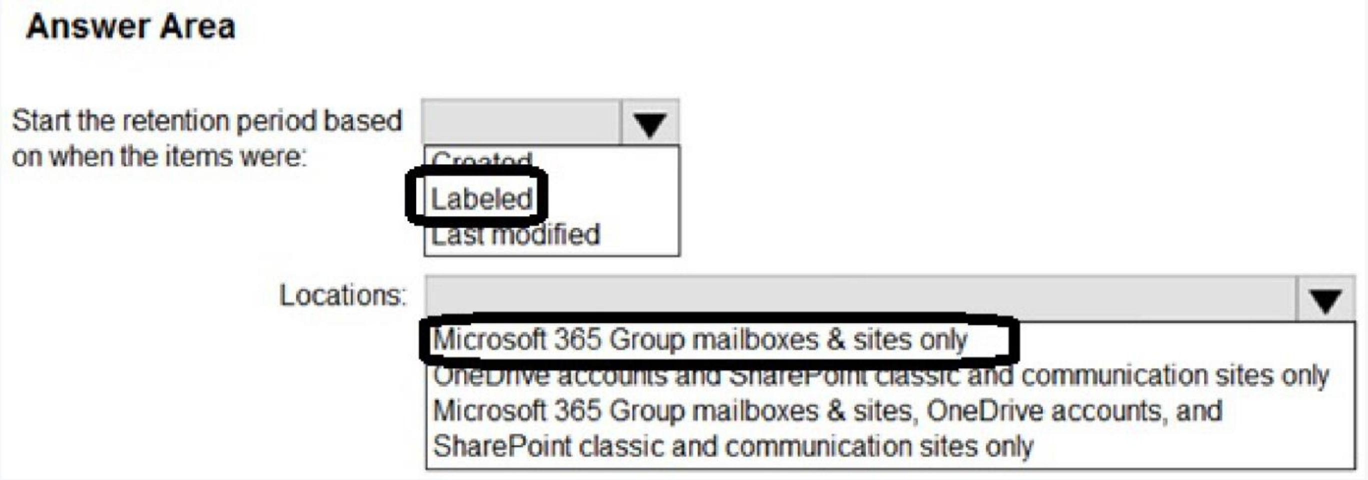
Start the retention period based on when the items were:

▼
Created
Labeled
Last modified

Locations:

▼
Microsoft 365 Group mailboxes & sites only
OneDrive accounts and SharePoint classic and communication sites only
Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

Answer:



Answer Area

Start the retention period based on when the items were:

Created
[✓ Labeled]
Last modified

Locations:

[✓ Microsoft 365 Group mailboxes & sites only]
OneDrive accounts and SharePoint classic and communication sites only
Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

Explanation:

Labeled.

Microsoft 365 Group Mailboxes & sites only.

Question: 69

HOTSPOT

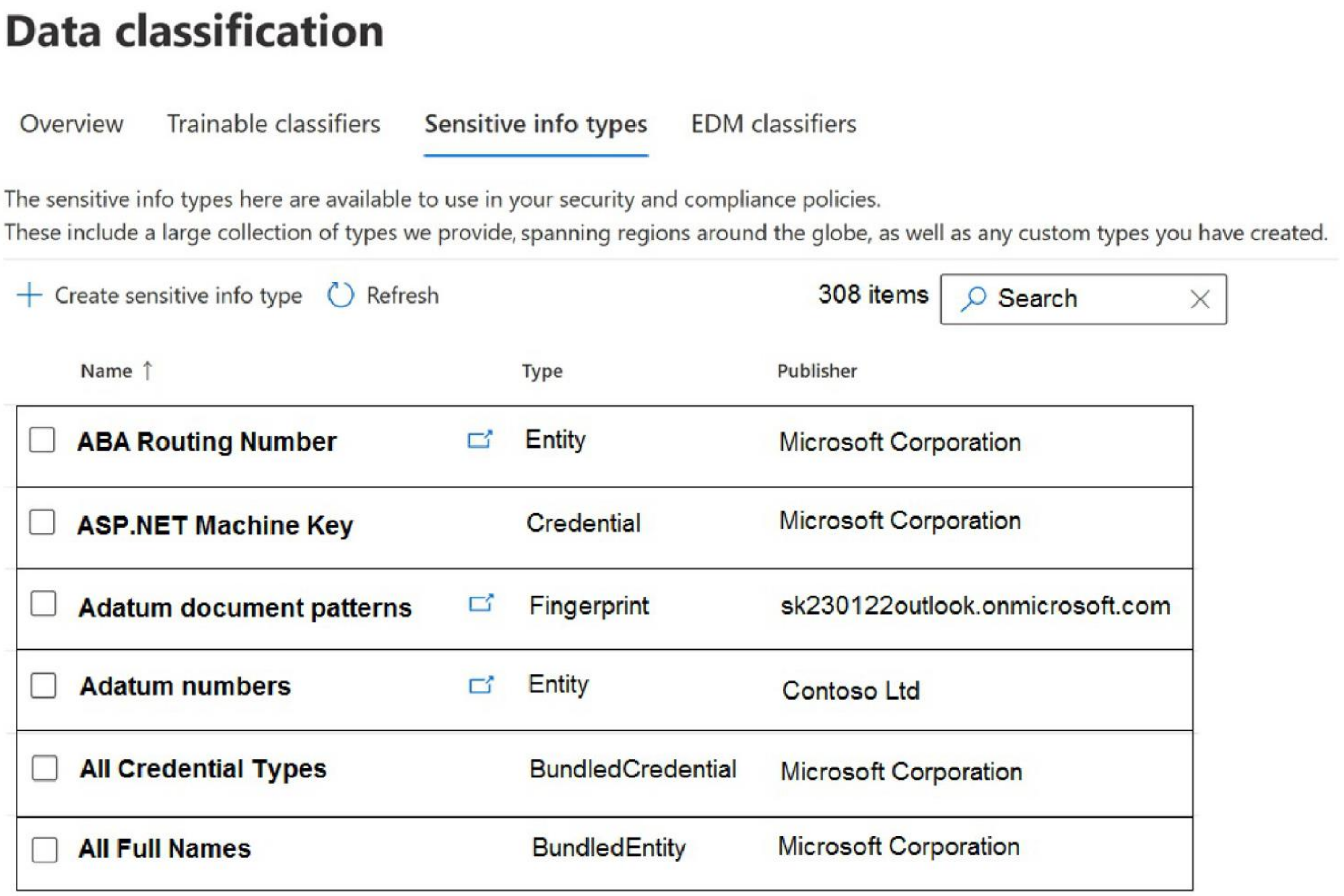
-

You have a Microsoft 365 E5 subscription.

You plan to create a new sensitive information type (SIT) by using the Microsoft Purview compliance portal. You need to copy and modify an existing SIT from which to create the new SIT.

What are two SITs that you can copy and modify? To answer, select the appropriate SITs in the answer area. NOTE: Each selection is worth one point.

Answer Area



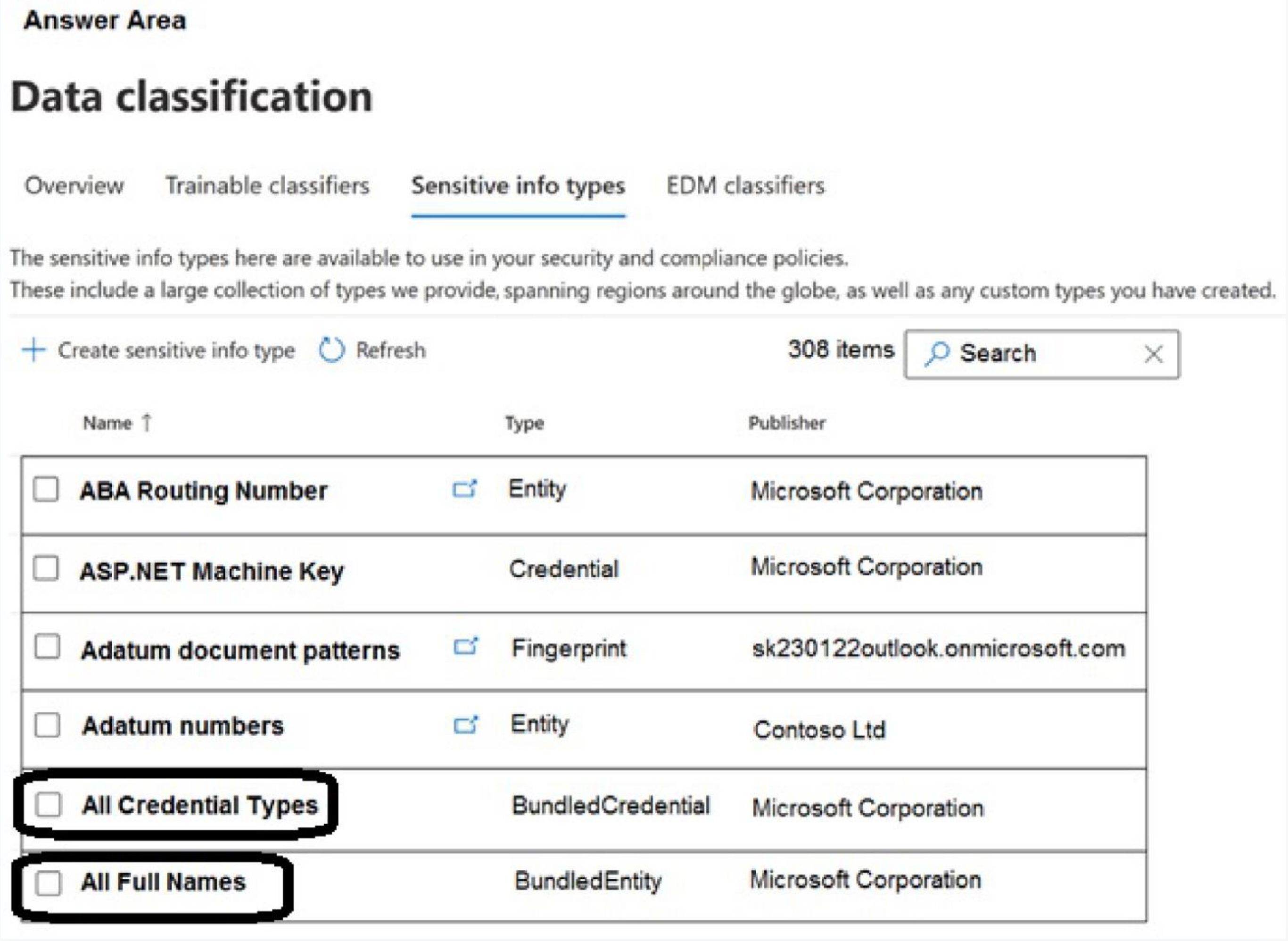
Data classification

The sensitive info types here are available to use in your security and compliance policies.
These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

308 items

	Name ↑	Type	Publisher
☐	ABA Routing Number	Entity	Microsoft Corporation
☐	ASP.NET Machine Key	Credential	Microsoft Corporation
☐	Adatum document patterns	Fingerprint	sk230122outlook.onmicrosoft.com
☐	Adatum numbers	Entity	Contoso Ltd
☐	All Credential Types	BundledCredential	Microsoft Corporation
☐	All Full Names	BundledEntity	Microsoft Corporation

Answer:



Answer Area

Data classification

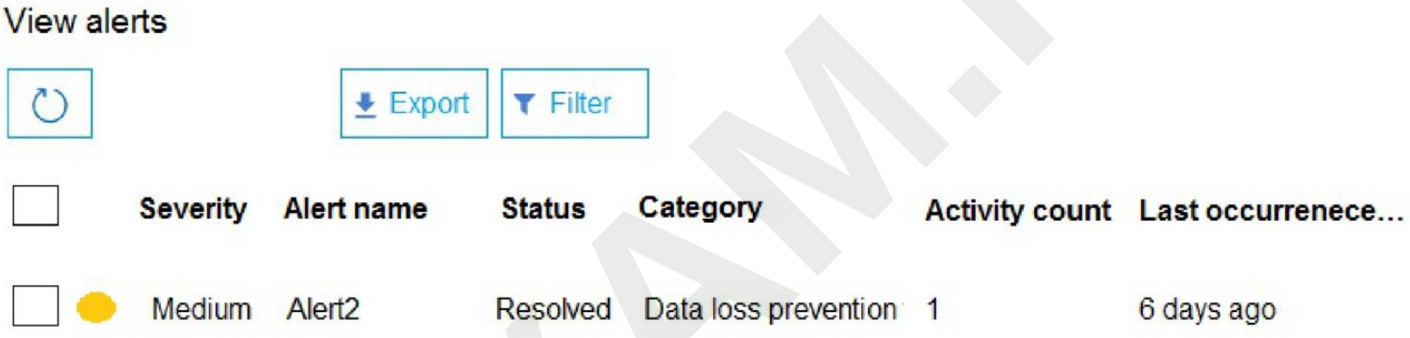
Overview | Trainable classifiers | Sensitive info types | EDM classifiers

The sensitive info types here are available to use in your security and compliance policies.
These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

	Name ↑	Type	Publisher
□	ABA Routing Number	Entity	Microsoft Corporation
□	ASP.NET Machine Key	Credential	Microsoft Corporation
□	Adatum document patterns	Fingerprint	sk230122outlook.onmicrosoft.com
□	Adatum numbers	Entity	Contoso Ltd
□	All Credential Types	BundledCredential	Microsoft Corporation
□	All Full Names	BundledEntity	Microsoft Corporation

Question: 70

You have a Microsoft 365 alert named Alert2 as shown in the following exhibit.



View alerts

□		Severity	Alert name	Status	Category	Activity count	Last occurrenece...
□	●	Medium	Alert2	Resolved	Data loss prevention	1	6 days ago

You need to manage the status of Alert2.

To which status can you change Alert2?

A.The status cannot be changed.
B.Dismissed only
C.Investigating only
D.Active or Investigating only
E.Investigating, Active, or Dismissed.

Answer: A

Explanation:

The status cannot be changed.

Question: 71

You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.

You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.

You need to identify and categorize the resumes. The solution must minimize administrative effort.

What should you include in the solution?

A.a trainable classifier
B.an exact data match (EDM) classifier
C.a function
D.a keyword dictionary

Answer: A

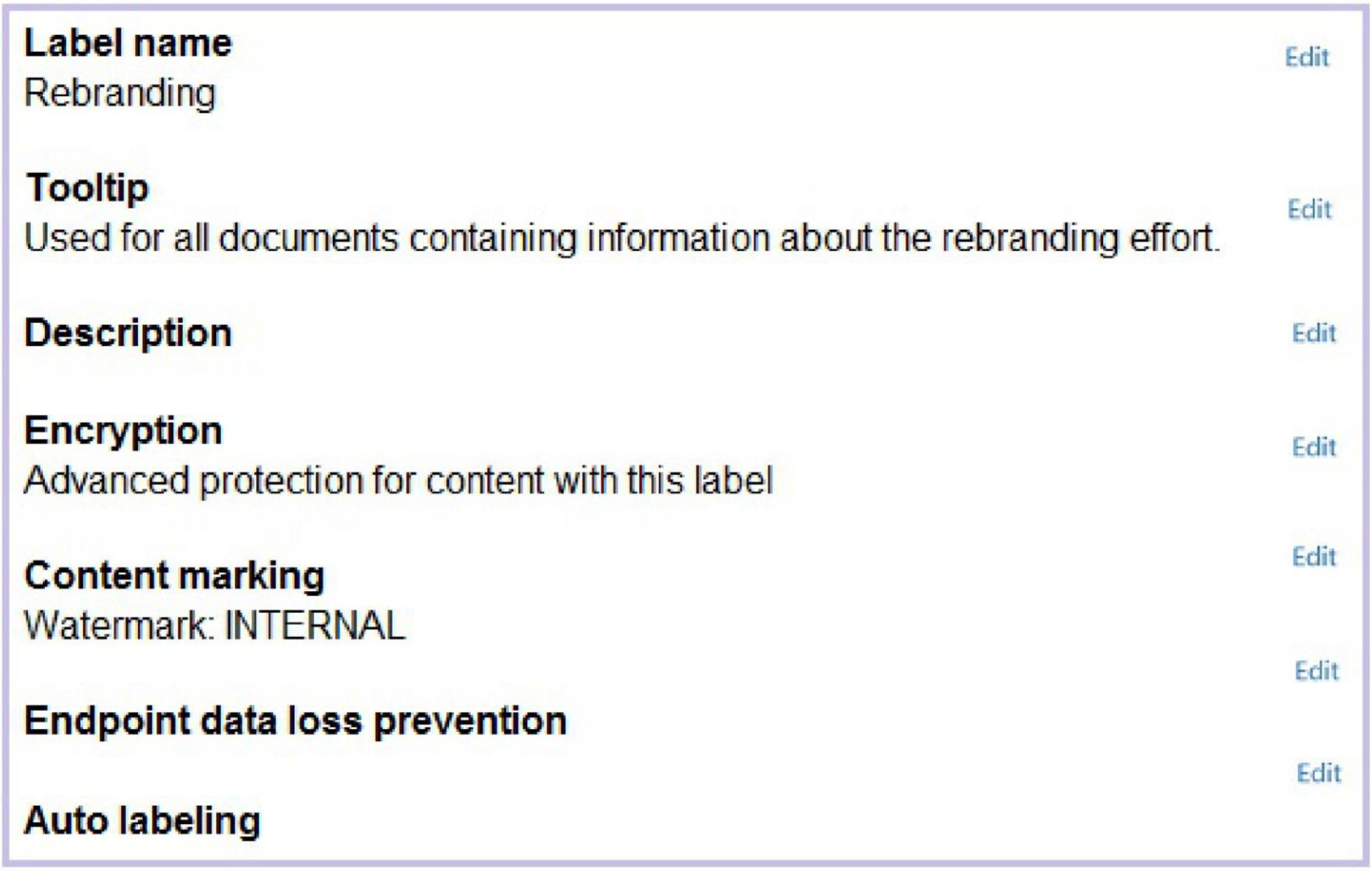
Explanation:

Correct answer is A:a trainable classifier.

Question: 72

HOTSPOT
-

You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.



Label name Edit
Rebranding

Tooltip Edit
Used for all documents containing information about the rebranding effort.

Description Edit

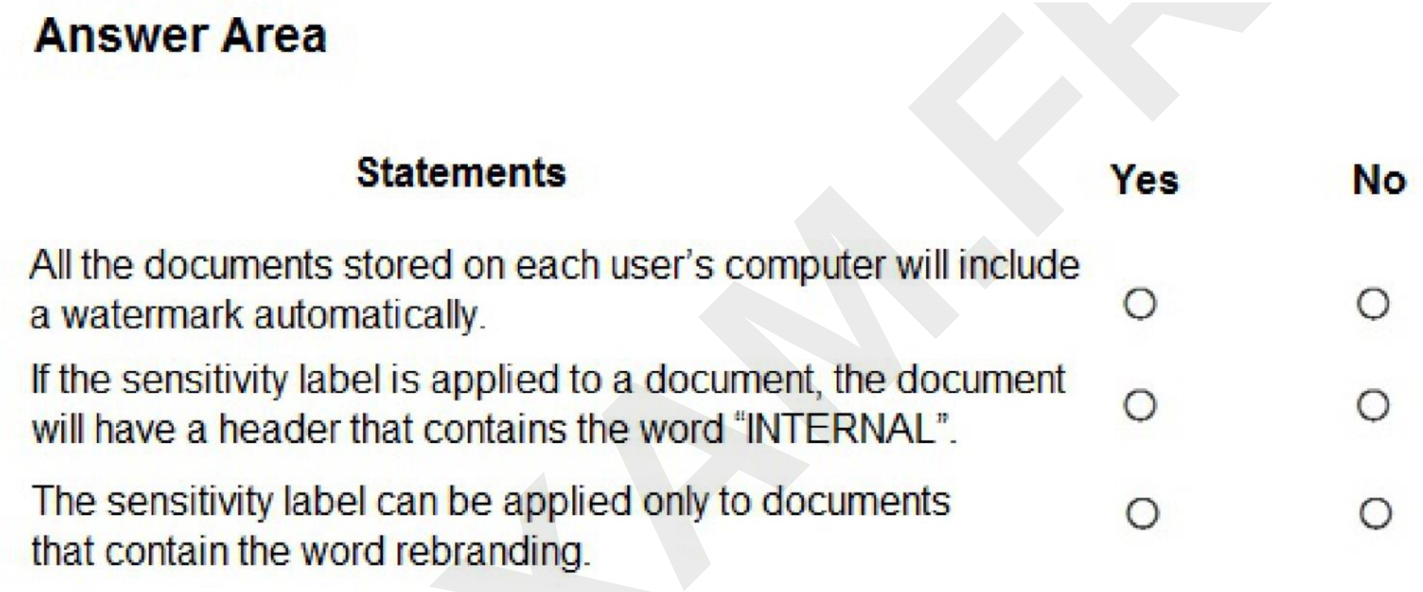
Encryption Edit
Advanced protection for content with this label

Content marking Edit
Watermark: INTERNAL

Endpoint data loss prevention Edit

Auto labeling Edit

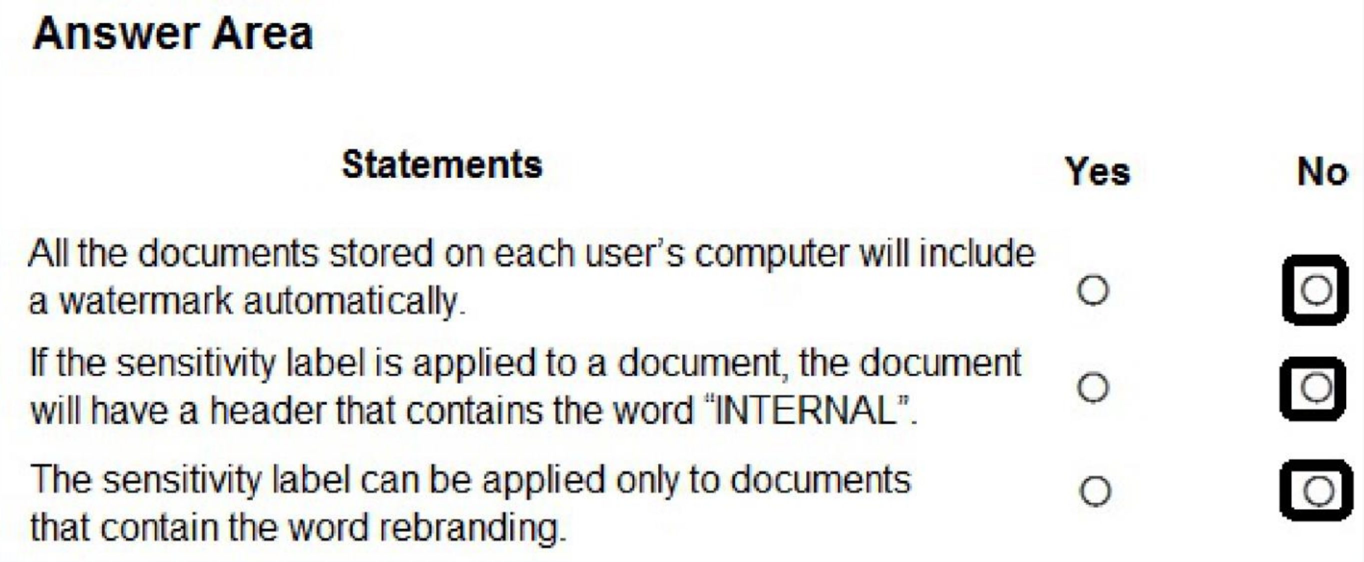
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Answer:



Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	[✓ ○]
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	[✓ ○]
The sensitivity label can be applied only to documents that contain the word rebranding.	○	[✓ ○]

Explanation:

No

No

No

Question: 73

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 contains 100 users and has dynamic user membership.

All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.

You create a sensitivity label named Label1 and publish Label1 as the default label for Group1.

You need to ensure that the users in Group must apply Label1 to their email and documents.

Which two actions should you perform? Each correct answer presents part of the solution NOTE:
Each correct selection is worth one point.

A.From the Microsoft Purview compliance portal, create an auto-labeling policy.

B.Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices, C.From the Microsoft Purview compliance portal, modify the settings of the Label1 policy.

D.Install the Azure Information Protection unified labeling client on the Windows 10 devices.

E.From the Microsoft Entra admin center, set Membership type for Group1 to Assigned.

Answer: CD

Explanation:

C.From the Microsoft Purview compliance portal, modify the settings of the Label1 policy. D.Install the Azure Information Protection unified labeling client on the Windows 10 devices.

Question: 74

SIMULATION

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: [email protected]
Microsoft 365 Password: **********
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

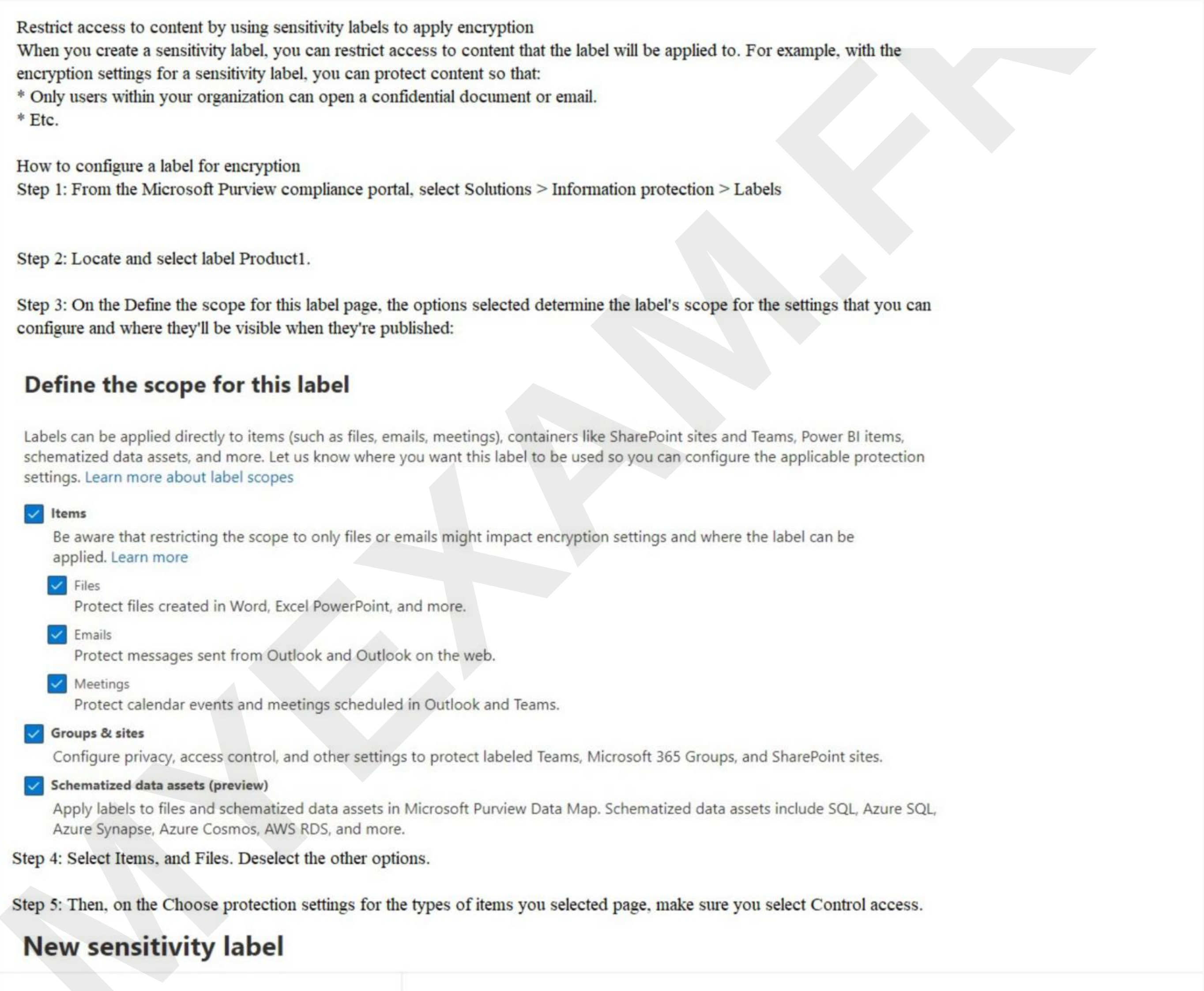
You need to provide users with the ability to manually classify files that contain product information that are stored in SharePoint Online sites. The solution must meet the following requirements:

•The users must be able to apply a classification of Product1 to the files.

•Any authenticated user must be able to open files classified as Product1.
•Files classified as Product1 must be encrypted.

To complete this task, sign in to the appropriate admin center.

Answer:



Restrict access to content by using sensitivity labels to apply encryption
When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:
* Only users within your organization can open a confidential document or email.
* Etc.

How to configure a label for encryption
Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels

Step 2: Locate and select label Product1.

Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published:

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

☑ Items
Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. Learn more

☑ Files
Protect files created in Word, Excel PowerPoint, and more.

☑ Emails
Protect messages sent from Outlook and Outlook on the web.

☑ Meetings
Protect calendar events and meetings scheduled in Outlook and Teams.

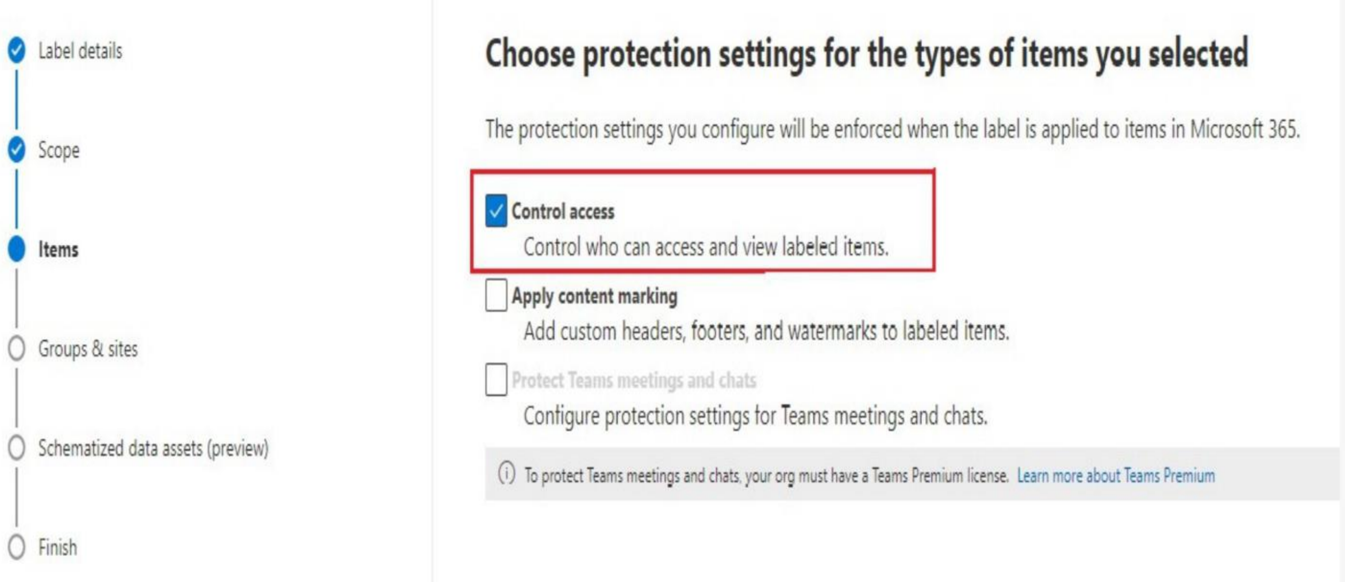
☑ Groups & sites
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

☑ Schematized data assets (preview)
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Step 4: Select Items, and Files. Deselect the other options.

Step 5: Then, on the Choose protection settings for the types of items you selected page, make sure you select Control access.

New sensitivity label



- ✓ Label details
- ✓ Scope
- ● **Items**
- ○ Groups & sites
- ○ Schematized data assets (preview)
- ○ Finish

Choose protection settings for the types of items you selected

The protection settings you configure will be enforced when the label is applied to items in Microsoft 365.

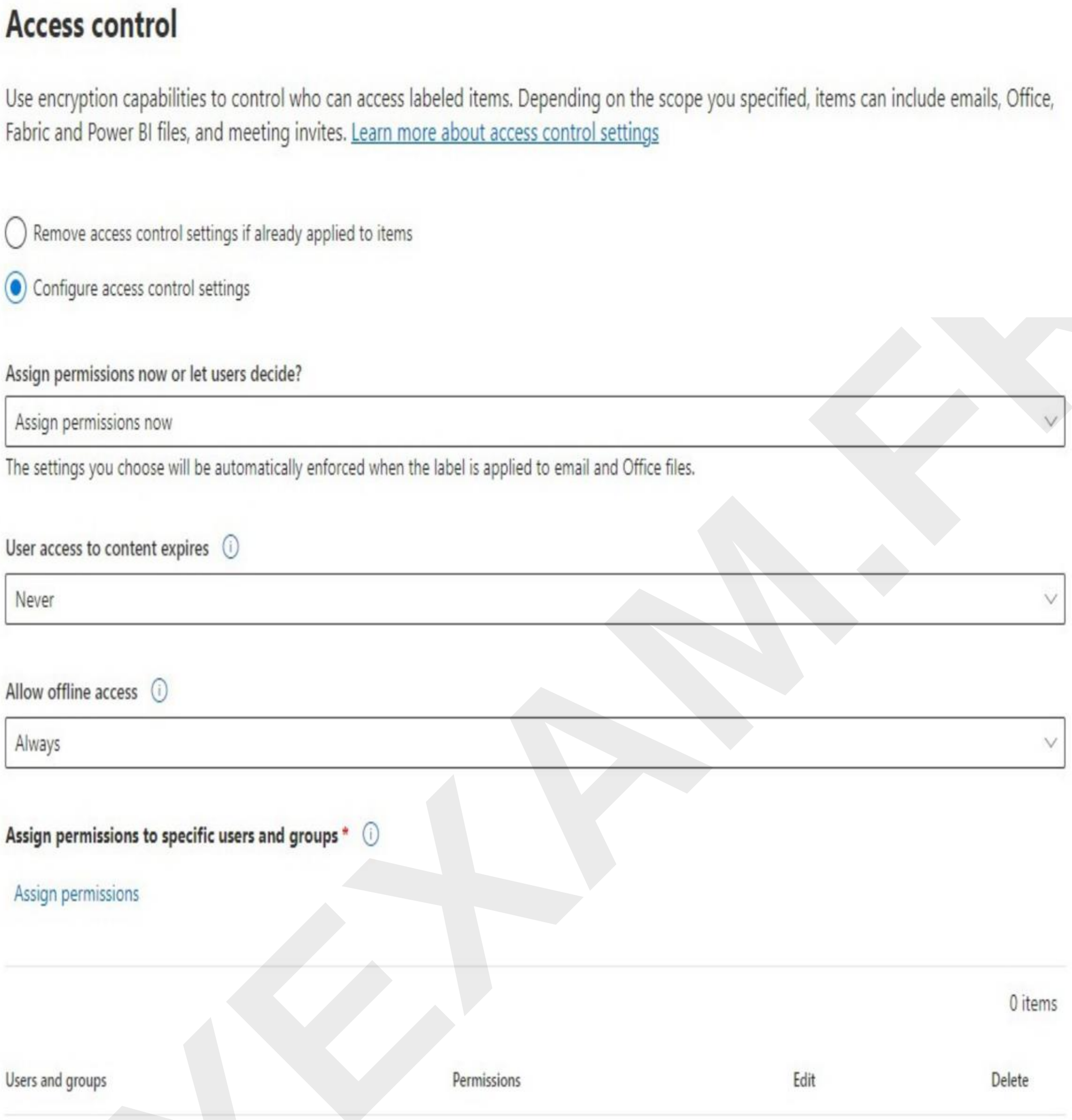
☑ **Control access**
Control who can access and view labeled items.

□ **Apply content marking**
Add custom headers, footers, and watermarks to labeled items.

□ Protect Teams meetings and chats
Configure protection settings for Teams meetings and chats.

ⓘ To protect Teams meetings and chats, your org must have a Teams Premium license. Learn more about Teams Premium

Step 6: On the Access control page, select Configure access control settings: Turns on encryption with rights management and makes the following settings visible:



Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings

○ Remove access control settings if already applied to items

● Configure access control settings

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

0 items

Users and groups	Permissions	Edit	Delete

Step 7: Assign permissions to specific users or groups. Add users or groups

Step 7a: For users: Any authenticated users.

Step 7b: Permissions: Select View

Note: You can grant permissions to specific people so that only they can interact with the labeled content:

Step 8: Click Save

Reference:

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

[illegible]

Question: 75

SIMULATI

ON

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: [email protected]
Microsoft 365 Password: **********
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only: Lab

Instance: 12345678

-

You discover that all users can apply the Confidential - Finance label.

You need to ensure that the Confidential - Finance label is available only to the members of the Finance Team group.

To complete this task, sign in to the appropriate admin center.

Answer:

Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID
Microsoft Entra ID supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups. Sensitivity labels apply to groups across services like Outlook, Microsoft Teams, and SharePoint. F

Assign a label to an existing group in the Microsoft Entra admin center

Step 1: Sign in to the Microsoft Entra admin center as at least a Global Administrator.

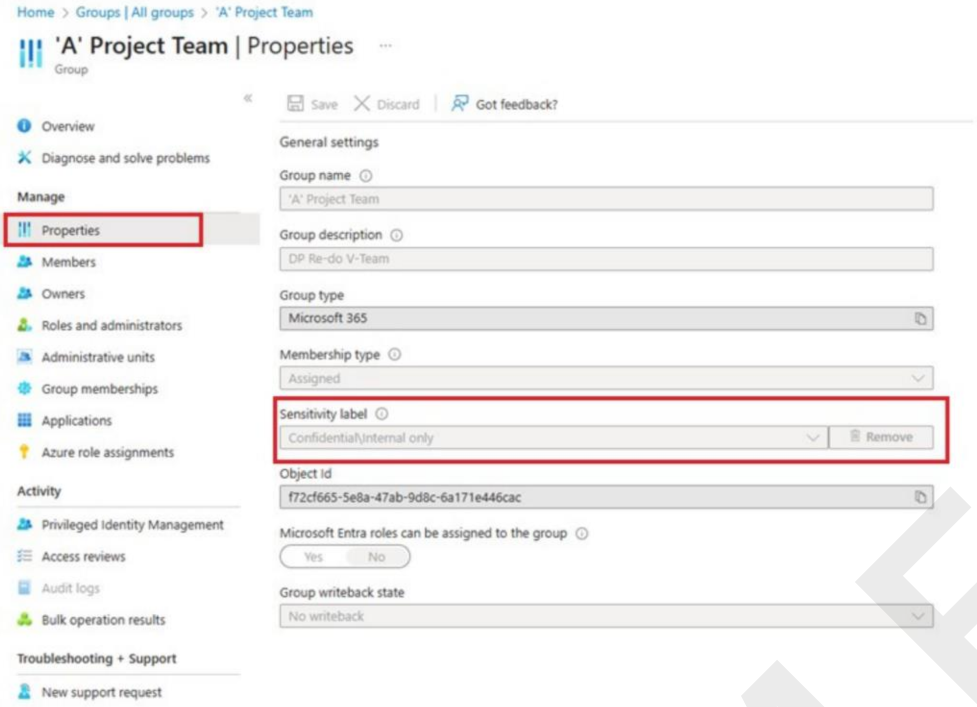
Step 2: Select Microsoft Entra ID.

Step 3: Select Groups

Step 4: From the All groups page, select the group that you want to label.

Step 5: On the selected group's page, select Properties and select a sensitivity label from the list.

Select the Confidential - Finance label



General settings

Group name: 'A' Project Team

Group description: DP Re-do V-Team

Group type: Microsoft 365

Membership type: Assigned

Sensitivity label: Confidential\Internal only

Object Id: f72cf665-5e8a-47ab-9d8c-6a171e446cac

Microsoft Entra roles can be assigned to the group: Yes / No

Group writeback state: No writeback

Step 6: Select Save to save your changes.

Reference:
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels

Question: 76

SIMULATI
ON
-
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: [email protected]
Microsoft 365 Password: **********
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to automatically apply a watermark to the documents of a project named Falcon.

You need to create a label that will add a watermark of “Project Falcon” in red, size-12 font diagonally across the documents.

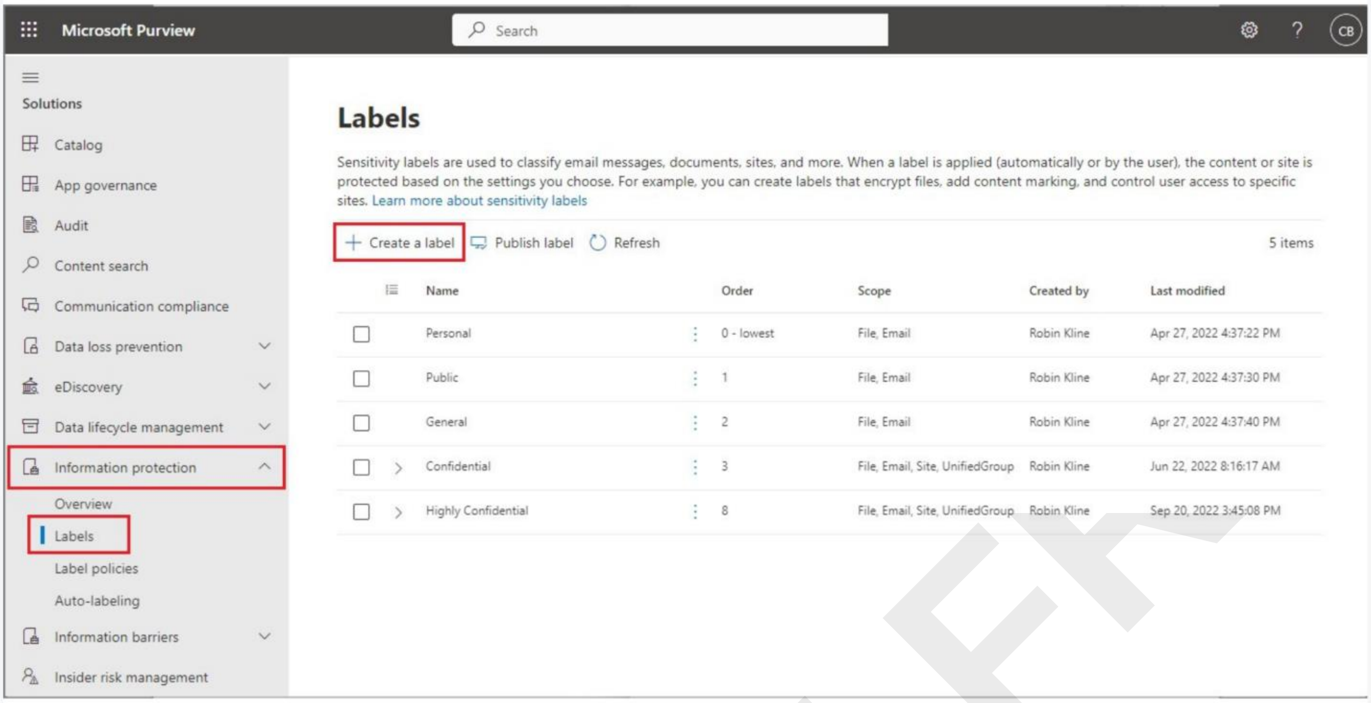
To complete this task, sign in to the appropriate admin center.

Answer:

Create and configure sensitivity labels

Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels

Step 2: On the Labels page, select + Create a label to start the new sensitivity label configuration:

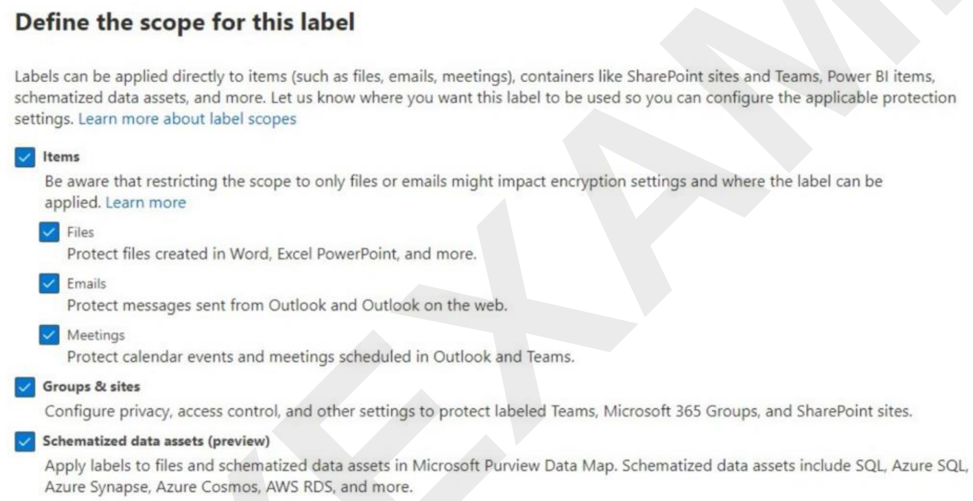


Labels

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name	Order	Scope	Created by	Last modified
Personal	0 - lowest	File, Email	Robin Kline	Apr 27, 2022 4:37:22 PM
Public	1	File, Email	Robin Kline	Apr 27, 2022 4:37:30 PM
General	2	File, Email	Robin Kline	Apr 27, 2022 4:37:40 PM
Confidential	3	File, Email, Site, UnifiedGroup	Robin Kline	Jun 22, 2022 8:16:17 AM
Highly Confidential	8	File, Email, Site, UnifiedGroup	Robin Kline	Sep 20, 2022 3:45:08 PM

Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published. In our case select: Items, Files, and select Word documents.



Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

☑ **Items**
Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. Learn more

- ☑ Files
  Protect files created in Word, Excel PowerPoint, and more.
- ☑ Emails
  Protect messages sent from Outlook and Outlook on the web.
- ☑ Meetings
  Protect calendar events and meetings scheduled in Outlook and Teams.

☑ **Groups & sites**
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

☑ **Schematized data assets (preview)**
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Note: If Items is selected, you can configure settings that apply to apps that support sensitivity labels, such as Office Word and Outlook. Optionally, you can extend these labels to include meetings from Teams and Outlook, and to protecting Teams meetings themselves by enforcing settings for Teams meetings and related chat.

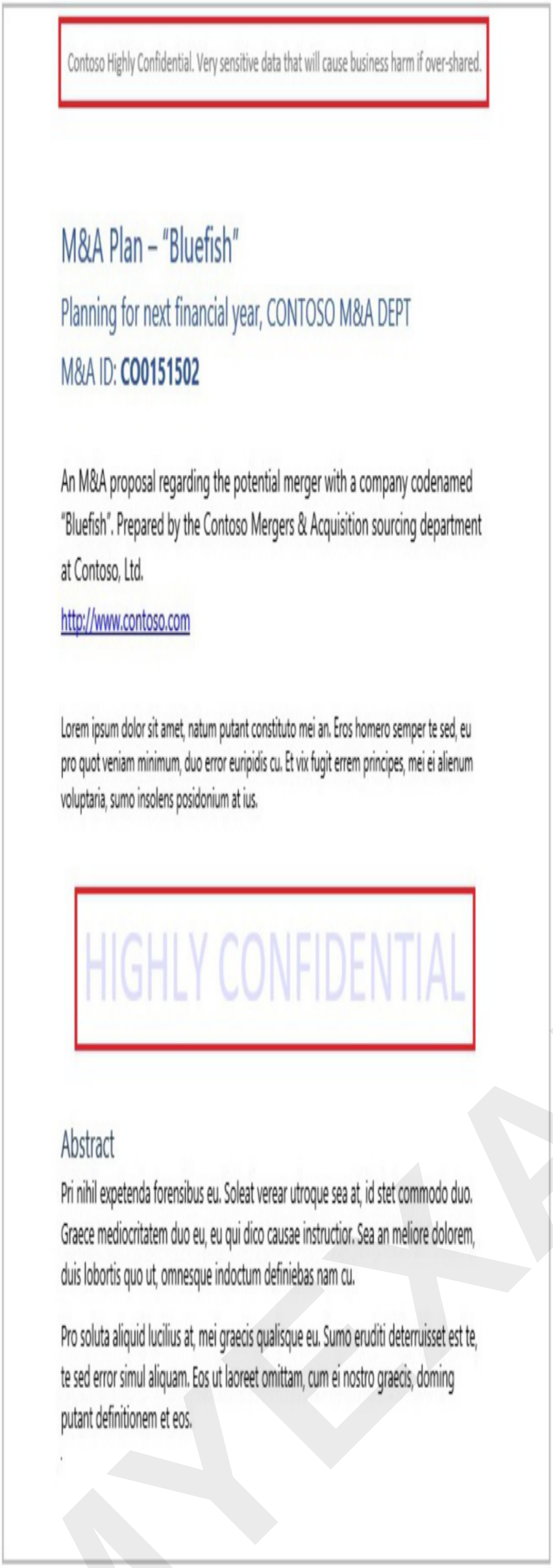
Step 4: Follow the configuration prompts for the label settings. Use the help in the UI for individual settings.

Step 5: In the UI add a watermark of “Project Falcon” in red, size-12 font diagonally across the document.

Note: What sensitivity labels can do
After a sensitivity label is applied to an email, meeting invite, or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:

* Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can

be applied to documents but not email or meeting invites. Example header and watermark:



Contoso Highly Confidential. Very sensitive data that will cause business harm if over-shared.

M&A Plan – "Bluefish"

Planning for next financial year, CONTOSO M&A DEPT

M&A ID: **CO0151502**

An M&A proposal regarding the potential merger with a company codenamed "Bluefish". Prepared by the Contoso Mergers & Acquisition sourcing department at Contoso, Ltd.

http://www.contoso.com

Lorem ipsum dolor sit amet, natum putant constituto mei an. Eros homero semper te sed, eu pro quot veniam minimum, duo error euripidis cu. Et vix fugit errem principes, mei ei alienum voluptaria, sumo insolens posidonium at ius.

HIGHLY CONFIDENTIAL

Abstract

Pri nihil expetenda forensibus eu. Soleat verear utroque sea at, id stet commodo duo. Graece mediocritatem duo eu, eu qui dico causae instructior. Sea an meliore dolorem, duis lobortis quo ut, omnesque indoctum definiebas nam cu.

Pro soluta aliquid lucilius at, mei graecis qualisque eu. Sumo eruditi deterruisset est te, te sed error simul aliquam. Eos ut laoreet omittam, cum ei nostro graecis, doming putant definitionem et eos.

.

Step 6: Finish the Wizard

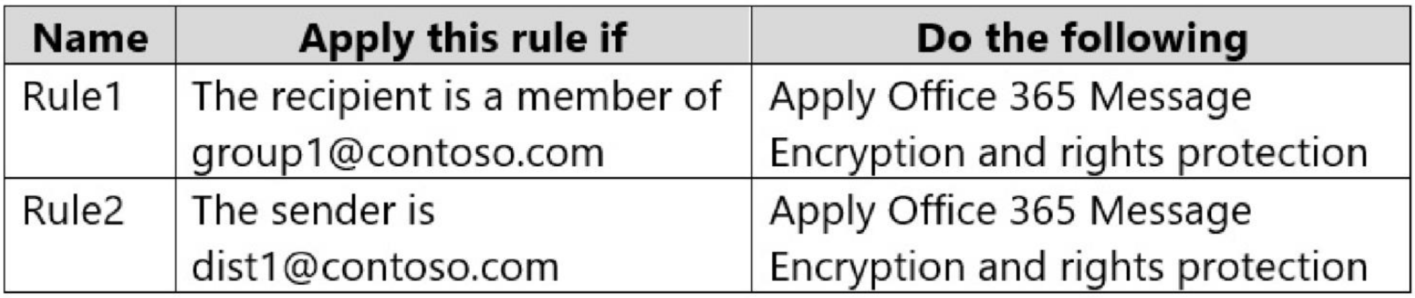
Question: 77

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

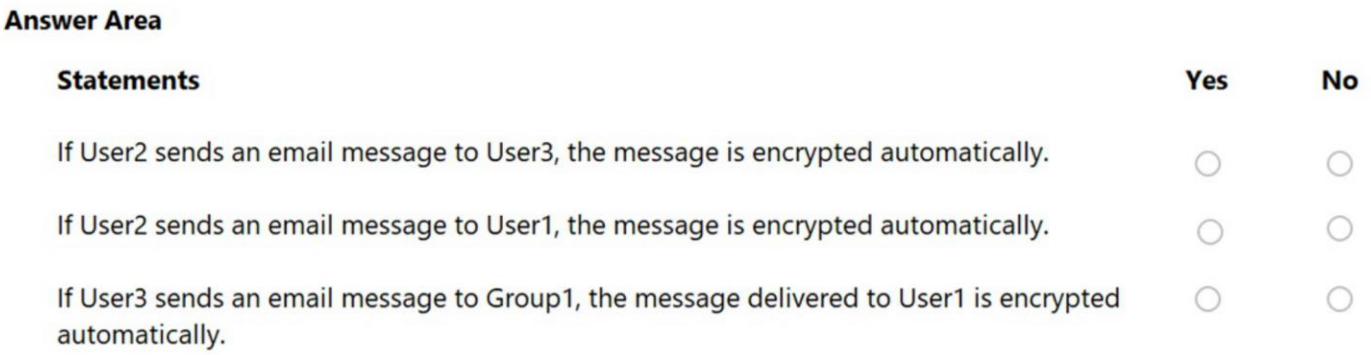
The subscription contains the users shown in the following table.

You create the mail flow rules shown in the following table.



Name	Apply this rule if	Do the following
Rule1	The recipient is a member of group1@contoso.com	Apply Office 365 Message Encryption and rights protection
Rule2	The sender is dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

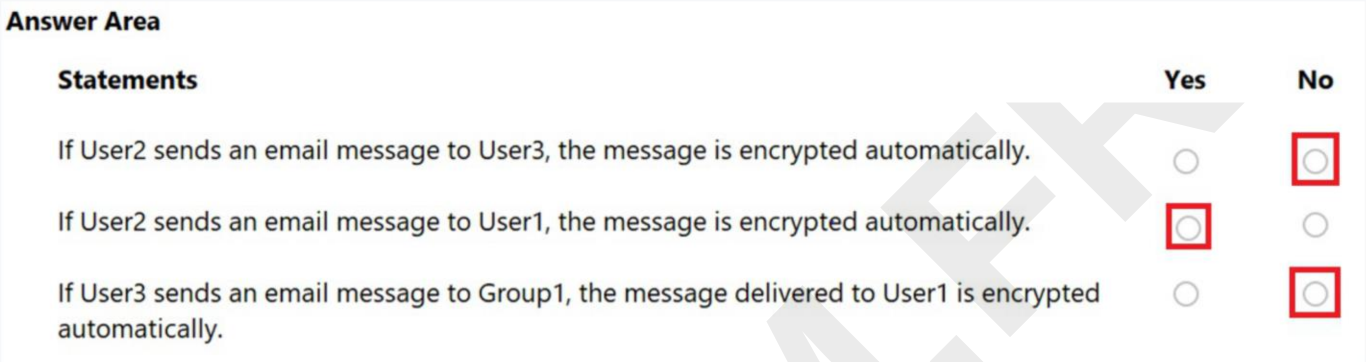
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	○
If User2 sends an email message to User1, the message is encrypted automatically.	○	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	○

Answer:



Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	[✓ ○]
If User2 sends an email message to User1, the message is encrypted automatically.	[✓ ○]	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	[✓ ○]

Explanation:

No

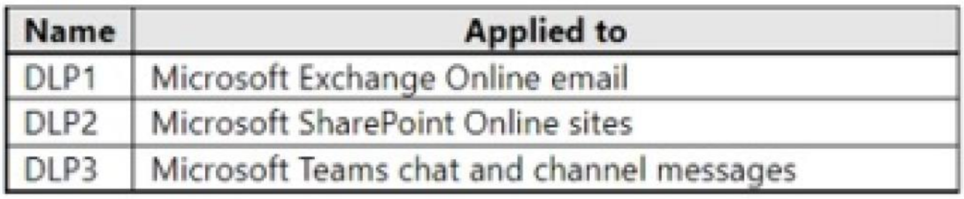
Yes

No

Question: 78 HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.



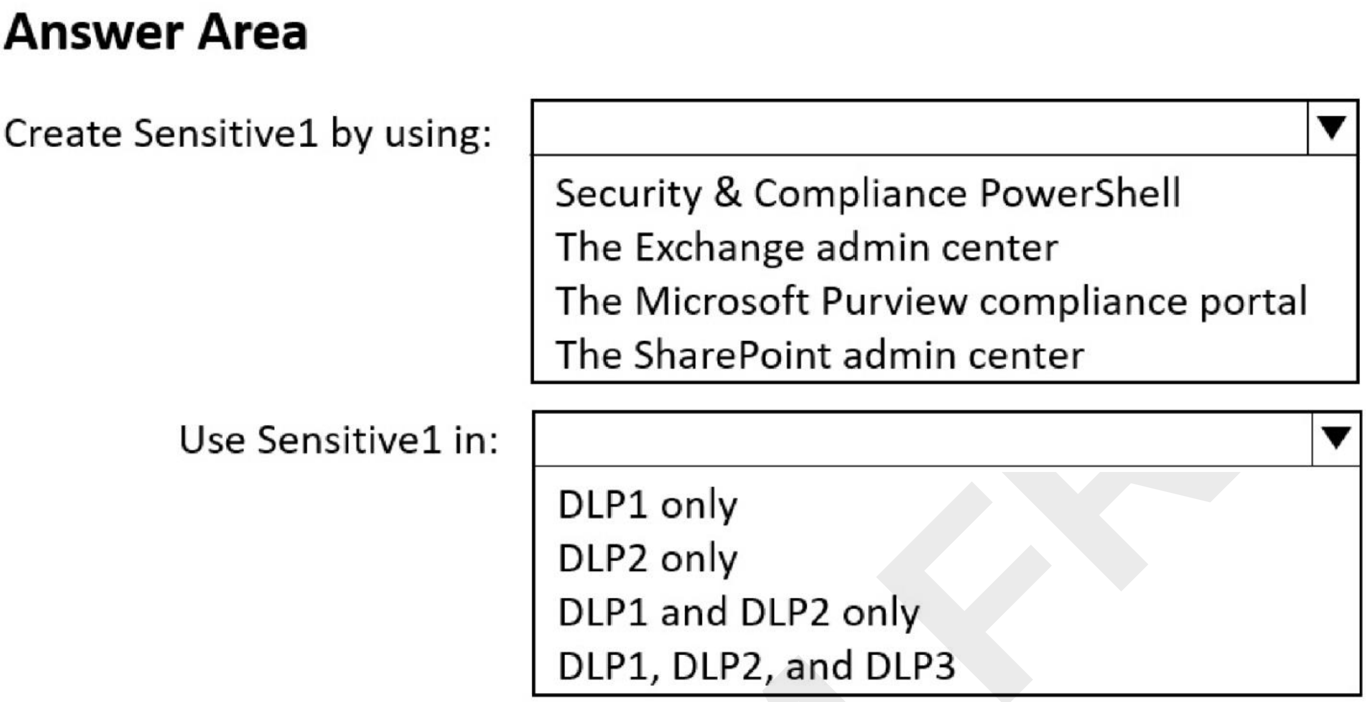
Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

You have a custom employee information form named Templatel.docx.

You plan to create a sensitive info type named Sensitive1 that will use the document fingerprint from Template1.docx.

What should you use to create Sensitive1, and in which DLP policies can you use Sensitive1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

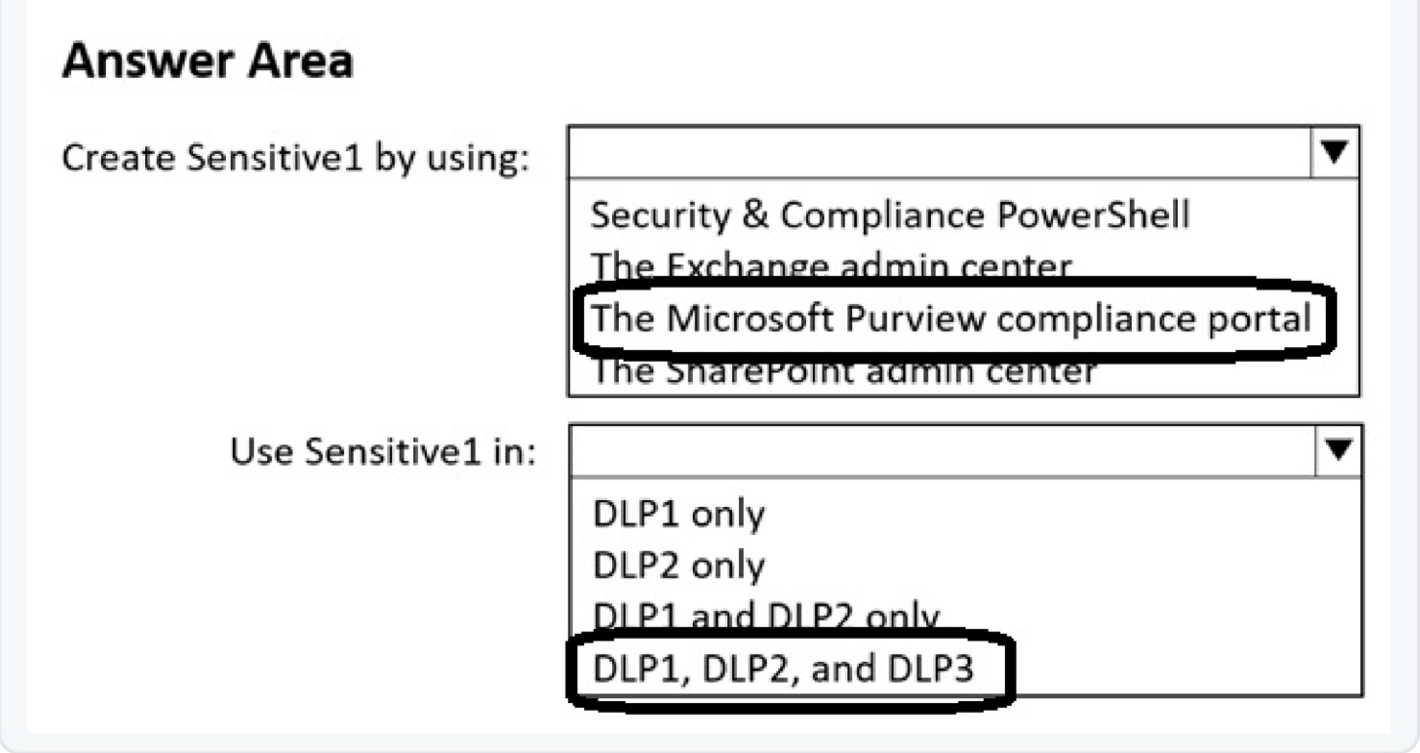
Create Sensitive1 by using: ▼

Security & Compliance PowerShell
The Exchange admin center
The Microsoft Purview compliance portal
The SharePoint admin center

Use Sensitive1 in: ▼

DLP1 only
DLP2 only
DLP1 and DLP2 only
DLP1, DLP2, and DLP3

Answer:



Answer Area

Create Sensitive1 by using:

- Security & Compliance PowerShell
- The Exchange admin center
- [✓ The Microsoft Purview compliance portal]
- The SharePoint admin center

Use Sensitive1 in:

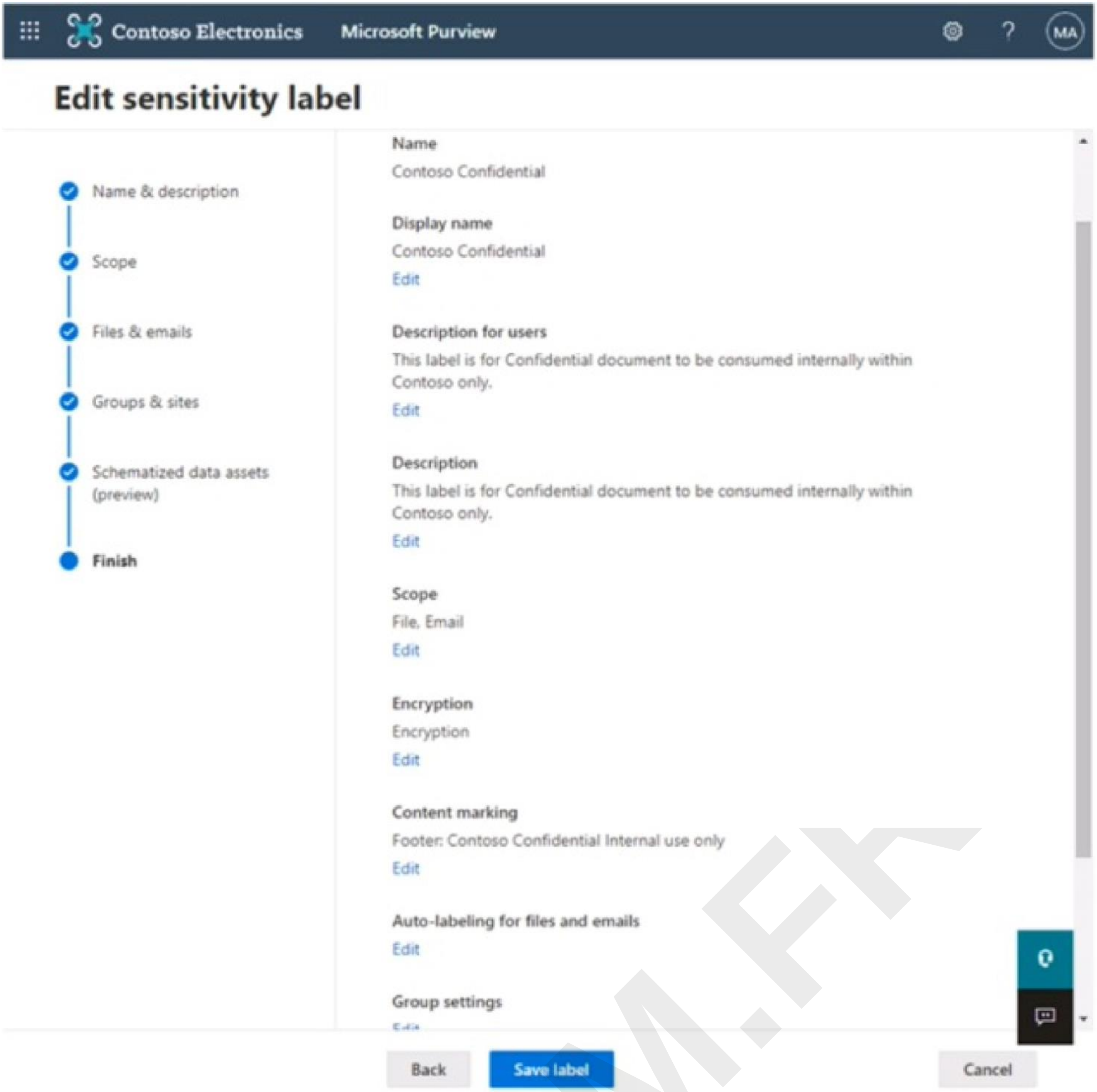
- DLP1 only
- DLP2 only
- DLP1 and DLP2 only
- [✓ DLP1, DLP2, and DLP3]

Question: 79 HOTSPOT

-

You have a Microsoft 365 subscription that contains a sensitivity label named Contoso Confidential.
You publish Contoso Confidential to all users.

Contoso Confidential is configured as shown in the Configuration exhibit. (Click the Configuration tab.)



Edit sensitivity label

Name
Contoso Confidential

Display name
Contoso Confidential
Edit

Description for users
This label is for Confidential document to be consumed internally within Contoso only.
Edit

Description
This label is for Confidential document to be consumed internally within Contoso only.
Edit

Scope
File, Email
Edit

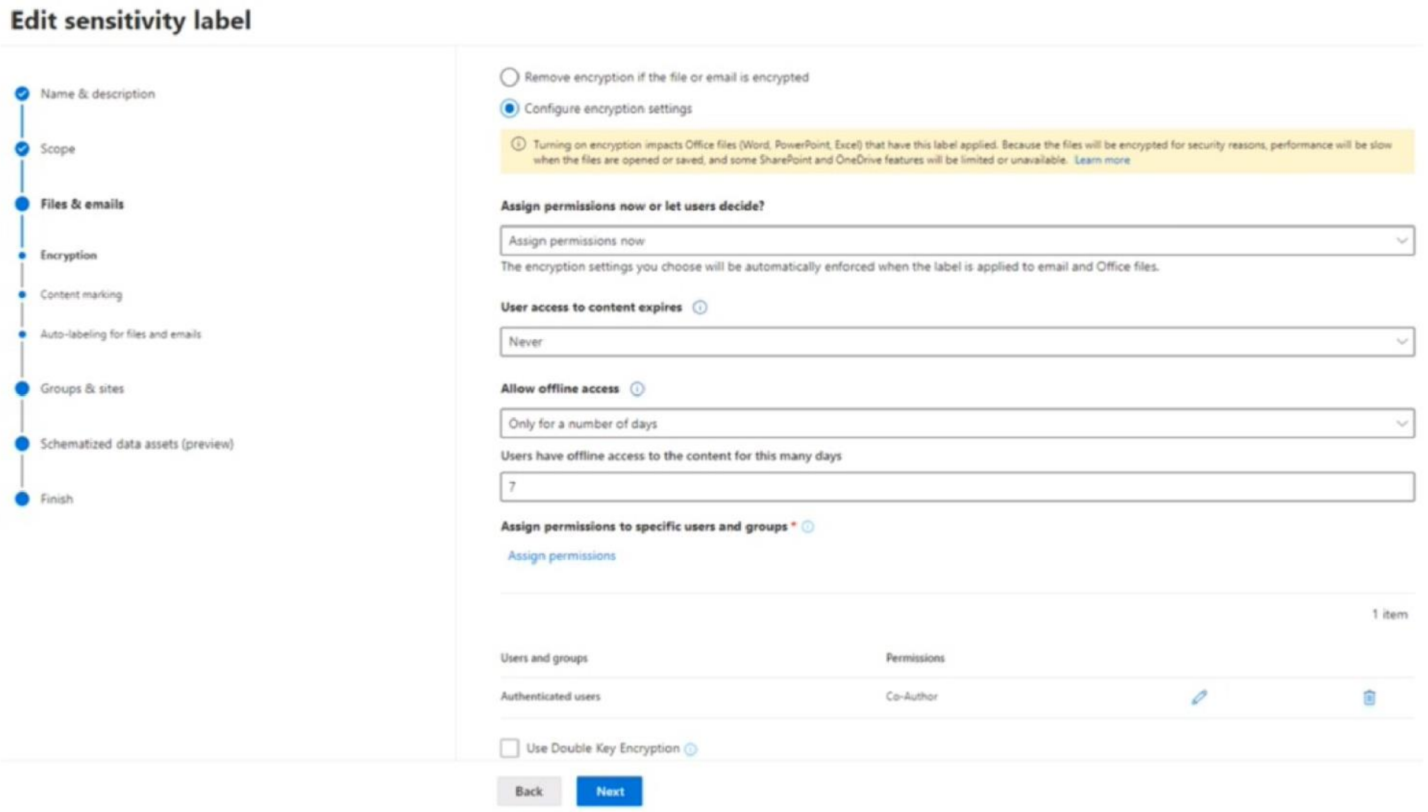
Encryption
Encryption
Edit

Content marking
Footer: Contoso Confidential Internal use only
Edit

Auto-labeling for files and emails
Edit

Group settings

The Encryption settings of Contoso Confidential are configured as shown in the Encryption exhibit. (Click the Encryption tab.)



Edit sensitivity label

- Name & description
- Scope
- **Files & emails**
  - **Encryption**
  - Content marking
  - Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

○ Remove encryption if the file or email is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

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

7

Assign permissions to specific users and groups * ⓘ

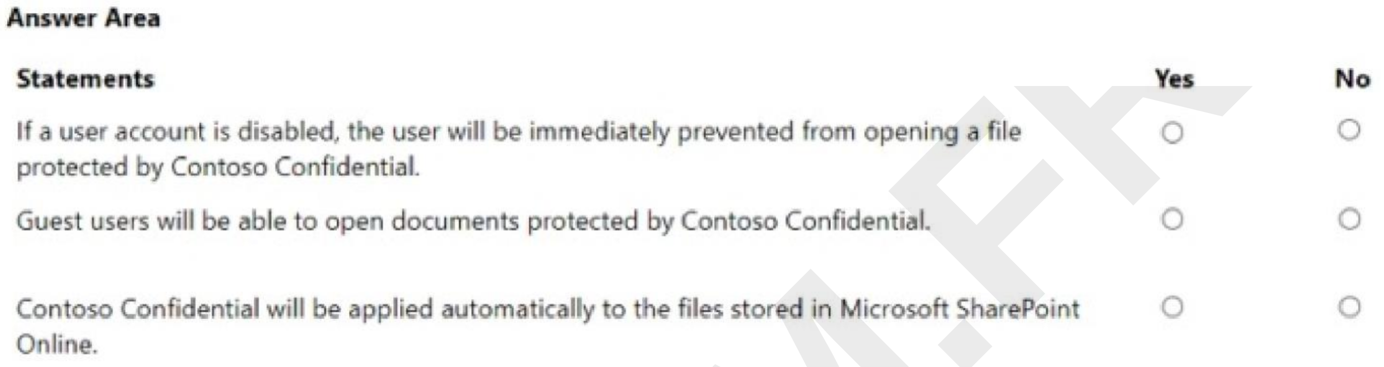
Assign permissions

1 item

Users and groups	Permissions
Authenticated users	Co-Author

□ Use Double Key Encryption ⓘ

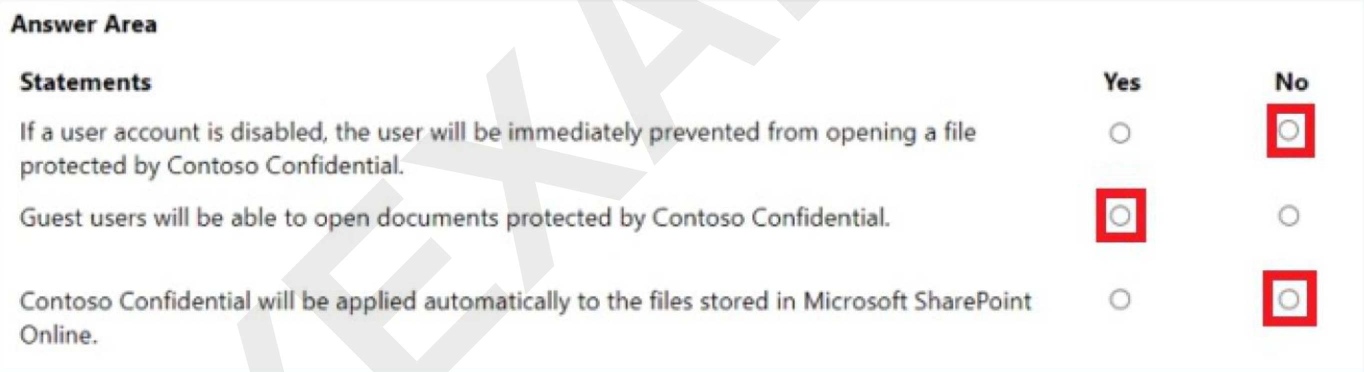
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	○	○
Guest users will be able to open documents protected by Contoso Confidential.	○	○
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.	○	○

Answer:



Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	○	[✓ ○]
Guest users will be able to open documents protected by Contoso Confidential.	[✓ ○]	○
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.	○	[✓ ○]

Explanation:

No

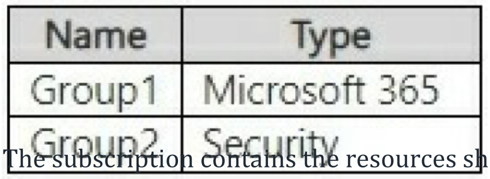
Yes

No

Question: 80 HOTSPOT

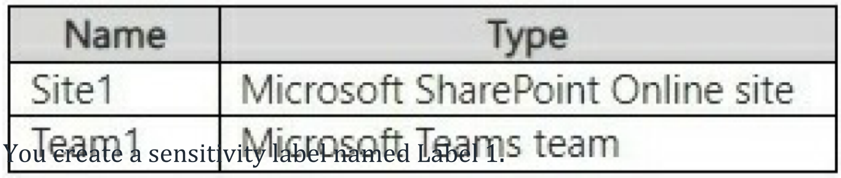
-

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.



Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.



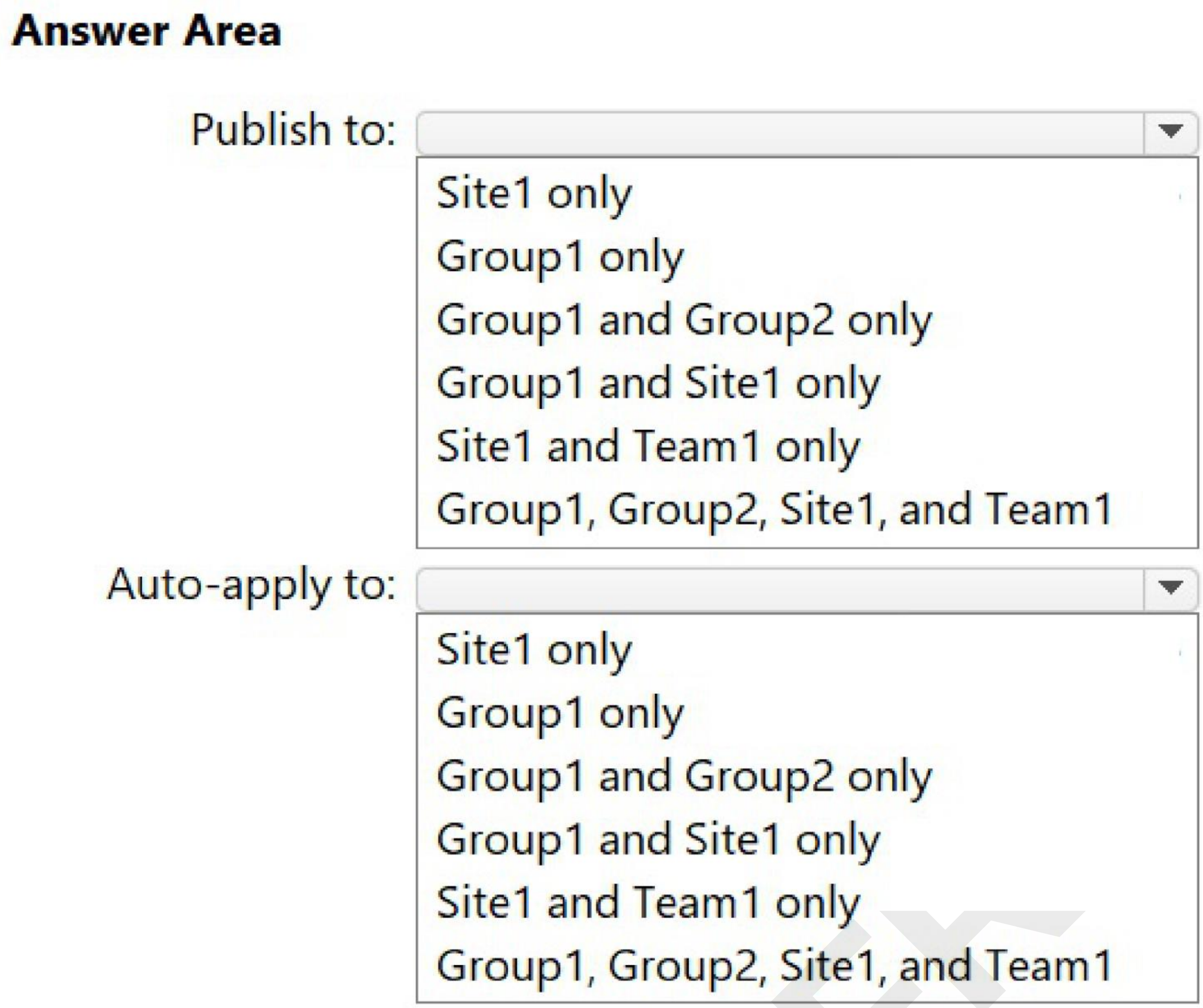
Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label 1.

You need to publish Label1 and have the label apply automatically.

To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

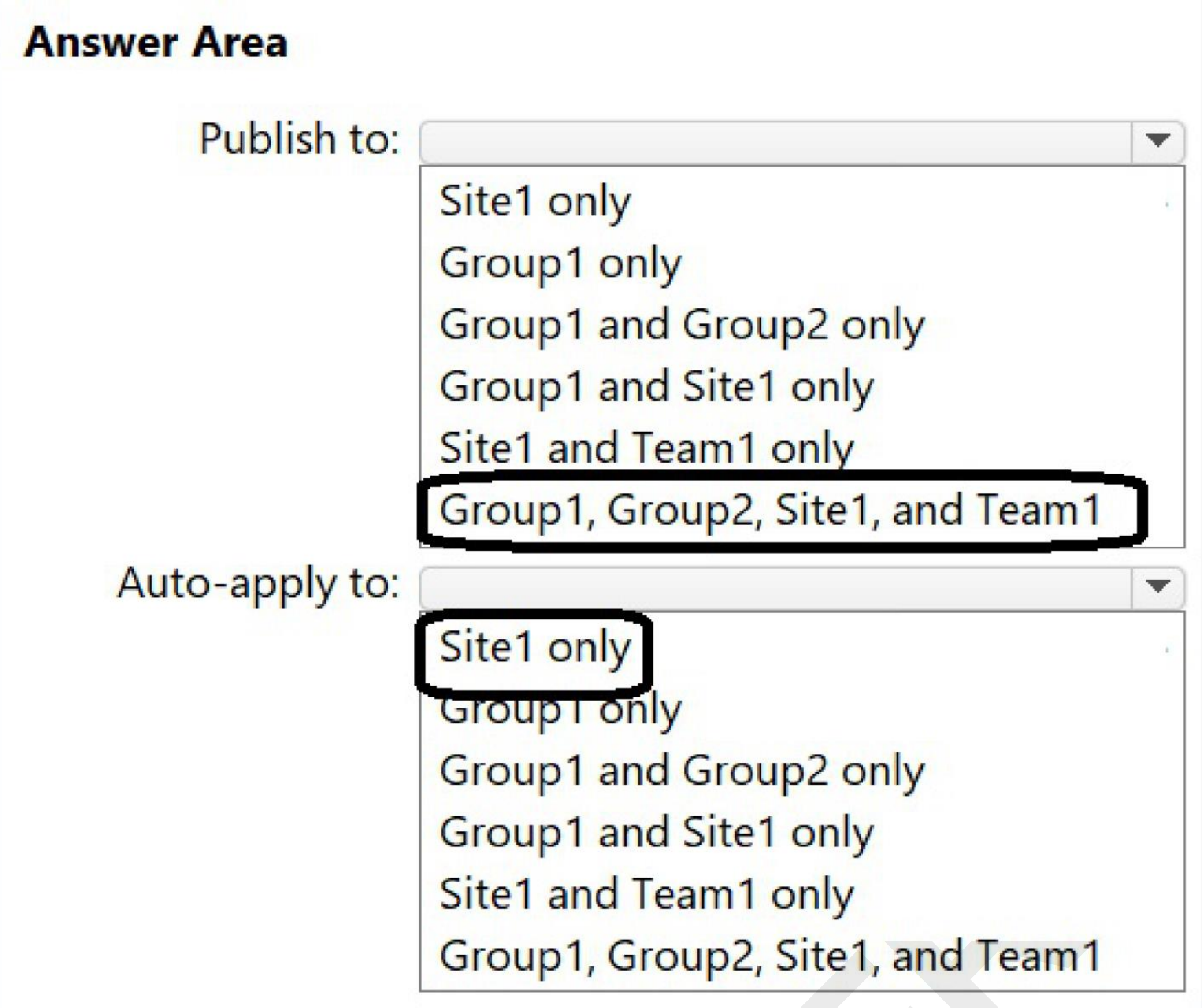
Publish to:

- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Auto-apply to:

- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Answer:



Answer Area

Publish to:

- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- [✓ Group1, Group2, Site1, and Team1]

Auto-apply to:

- [✓ Site1 only]
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

Explanation:

Group 1,Group 2,Site 1,and Team1 .

Site 1 only.