SC-400$^{Q\&As}$

Microsoft Information Protection Administrator

Pass Microsoft SC-400 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have a Microsoft 365 E5 tenant that uses Microsoft Teams and contains two users named User1 and User2.

You create a data loss prevention (DLP) policy that is applied to the Teams chat and channel messages location for User1 and User2.

Which Teams entities will have DLP protection?

A. 1:1/n chats and private channels only

B. 1:1/n chats and general channels only

C. 1:1/n chats, general channels, and private channels

Correct Answer: A

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams

QUESTION 2

You need to recommend a solution that meets the compliance requirements for viewing DLP tooltip justifications. What should you recommend?

A. Instruct the compliance department users to review the False positive and override report.

B. Configure a Microsoft Power Automate workflow to route DLP notification emails to the compliance department.

C. Instruct the compliance department users to review the DLP incidents report.

D. Configure an Azure logic app to route DLP notification emails to the compliance department.

Correct Answer: A

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

QUESTION 3

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 user2@fabrikam.com.

You need to prevent user2@fabrikam.com from accessing the email.

What should you do?

A. Run the Get-MessageTracecmdlet.

B. Run the Set-OMEMessageRevocationcmdlet.

C. Instruct User1 to delete the email from her Sent Items folder from Microsoft Outlook.

D. Run the New-ComplianceSearchActioncmdlet.

E. Instruct User1 to select Remove external access from Microsoft Outlook on the web.

Correct Answer: B

QUESTION 4

HOTSPOT

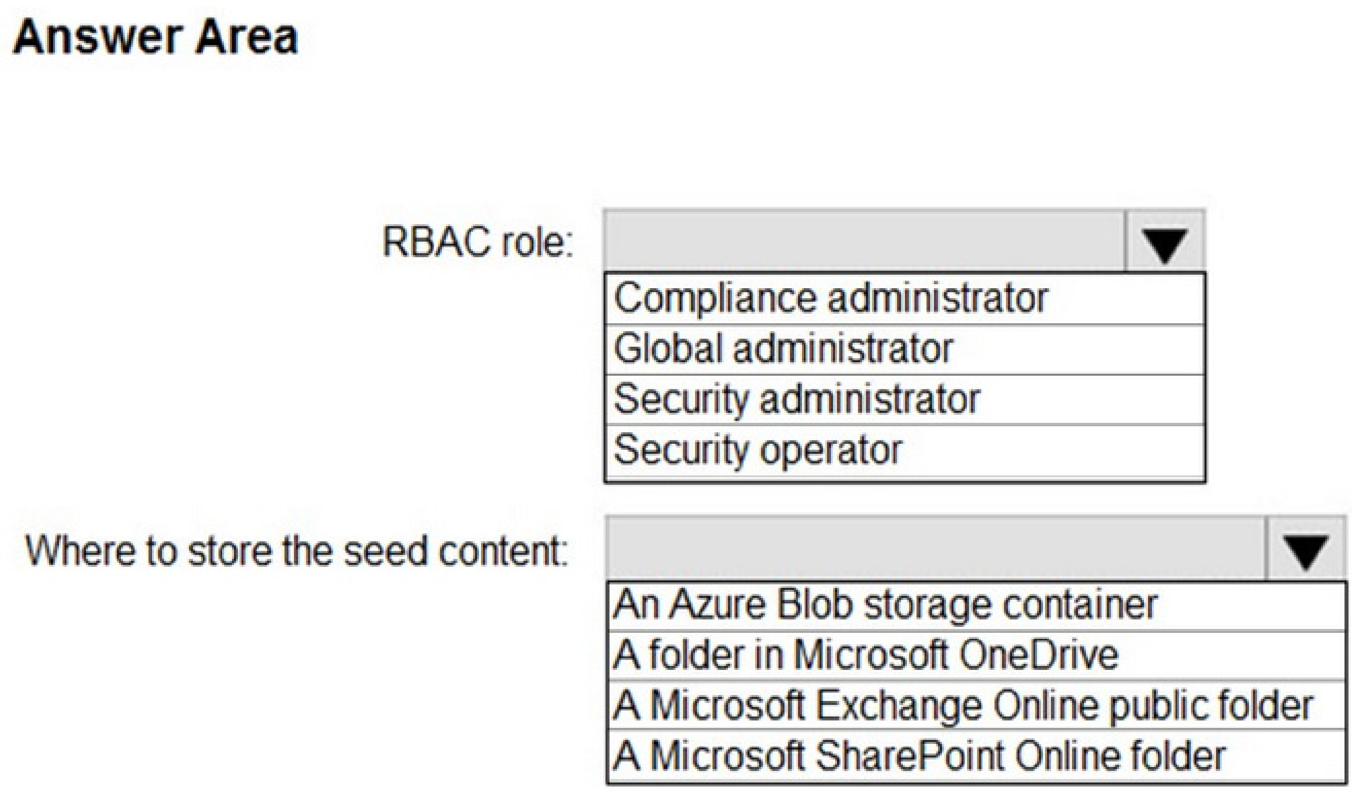
You plan to create a custom trainable classifier based on an organizational from template.

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

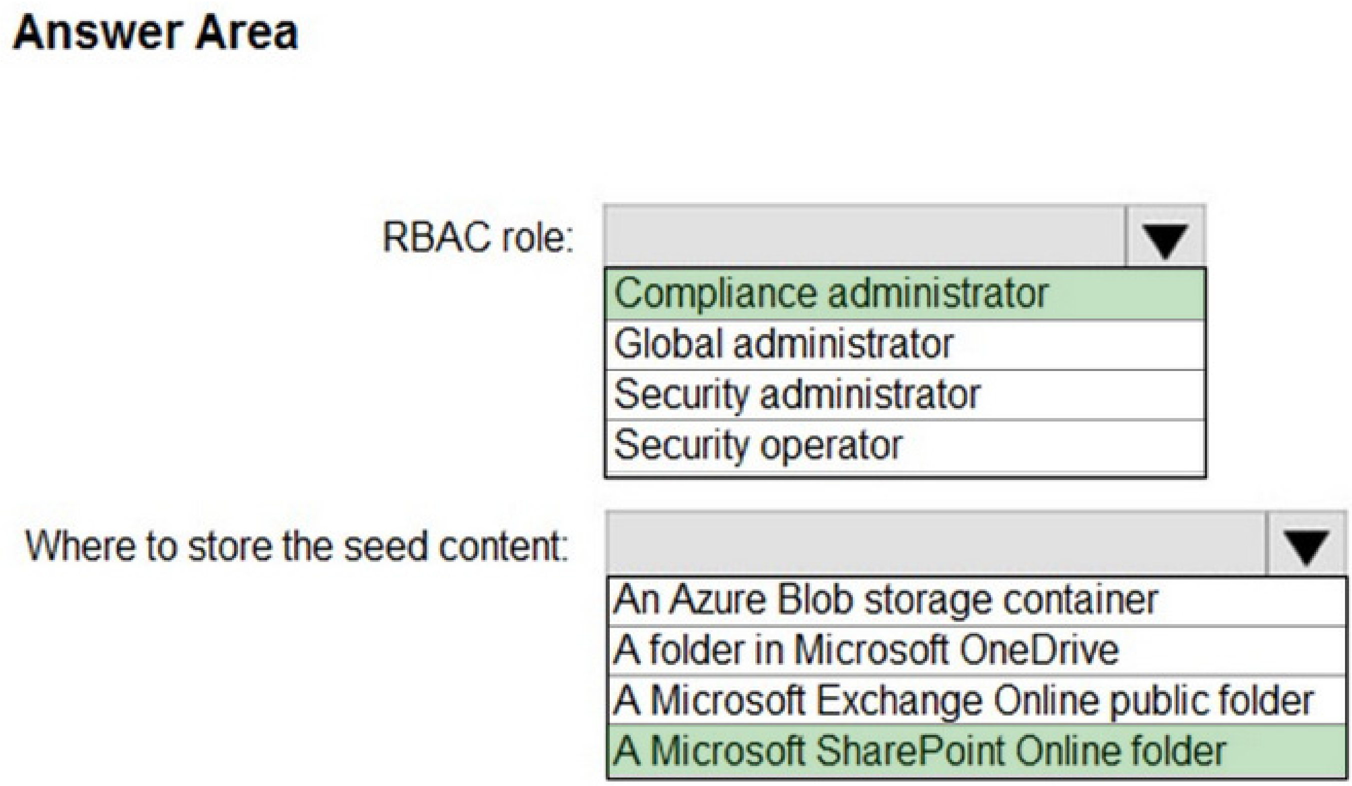
RBAC role:

- 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

Correct 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]

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

QUESTION 5

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 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview compliance portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

Solution: You run the Set-AuditConfig -Workload Exchange command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 6

You plan to implement inside 365 E5 subscription.

You plan to implement insider risk management for users that manage sensitive data associated with a project.

You need to create a protection policy for the users. The solution must meet the following requirements:

1.

Minimize the impact on users who are NOT part of the project.

2.

Minimize administrative effort. What should you do first?

A. From the Microsoft Entra admin center, create a security group.

B. From the Microsoft Purview compliance portal, create an insider risk management policy.

C. From the Microsoft Purview compliance portal, create a priority user group.

D. From the Microsoft Entra admin center, create a risky users policy.

Correct Answer: C

Get started with insider risk management

Configure priority user groups Insider risk management includes support for assigning priority user groups to policies to help identify unique risk activities for user with critical positions, high levels of data and network access, or a past history of risk behavior. Creating a priority user group and assigning users to the group help scope policies to the unique circumstances presented by these users.

You can create a priority user group and assign users to the group to help you scope policies specific to the unique circumstances presented by these identified users. To enable the priority user groups risk score booster, go to the Insider risk management settings page, then select Policy indicators and Risk score boosters. These identified users are more likely to receive alerts, so analysts and investigators can review and prioritize these users\\' risk severity to help triage alerts in accordance with your organization\\'s risk policies and standards.

A priority user group is required when using the following policy templates:

Security policy violations by priority users Data leaks by priority users

Reference:

QUESTION 7

You have a Microsoft 365 E5 subscription that contains a data loss prevention (DLP) policy named DLP1.

DLP1 has a rule that triggers numerous alerts.

You need to reduce the number of alert notifications that are generated. The solution must maintain the sensitivity of DLP1.

What should you do?

A. Change the mode of DLP1 to Test without notifications.

B. Modify the rule and increase the instance count.

C. Modify the rule and configure an alert threshold.

D. Modify the rule and set the priority to the highest value.

Correct Answer: C

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

QUESTION 8

You have a Microsoft 365 tenant that has a retention label policy. You need to configure the policy to meet the following requirements:

1.

Prevent the disabling or deletion of the policy.

2.

Ensure that new labels can be added.

3.

Prevent the removal of labels. What should you do?

A. Import a file plan.

B. Enable insider risk management.

C. Enable the regulatory record option.

D. Create a preservation lock.

Correct Answer: D

QUESTION 9

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.

Correct Answer: A

Global Reader

Members have read-only access to reports, alerts, and can see all the configuration and settings.

The primary difference between Global Reader and Security Reader is that a Global Reader can access configuration and settings.

Note: Compliance Administrator´

View and edit settings and reports for compliance features.

Incorrect:

Not B:

Reviewer

Members can access review sets in eDiscovery (Premium) cases. Members of this role group can see and open the list of cases on the eDiscovery > Advanced page in the Microsoft Purview compliance portal that they\\'re members of. After

the user accesses an eDiscovery (Premium) case, they can select Review sets to access case data. This role doesn\\'t allow the user to preview the results of a collection search that\\'s associated with the case or do other search or case

management tasks. Members of this role group can only access the data in a review set.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions

QUESTION 10

You have a Microsoft 365 E5 subscription that uses Privacy risk management.

You need to recommend which type of policy can evaluate the external sharing of personal data on Microsoft SharePoint Online sites.

Which policy type should you recommend?

A. Data overexposure

B. Data transfers

C. Data theft by departing users

D. Data minimization

E. Security policy violations

Correct Answer: B

QUESTION 11

HOTSPOT

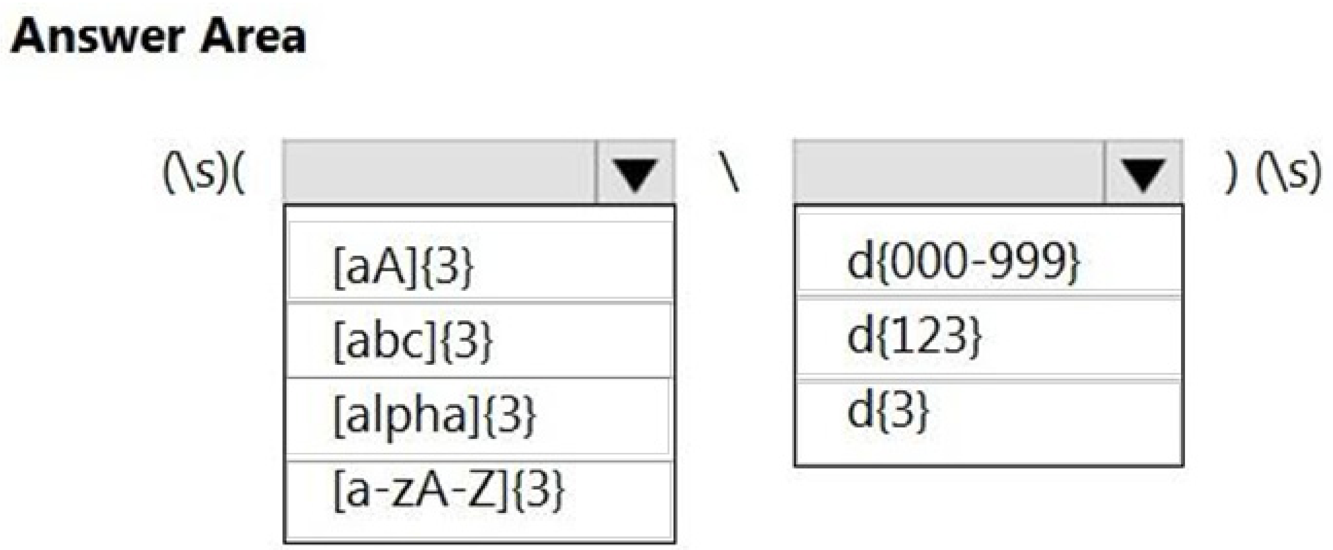
You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

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:



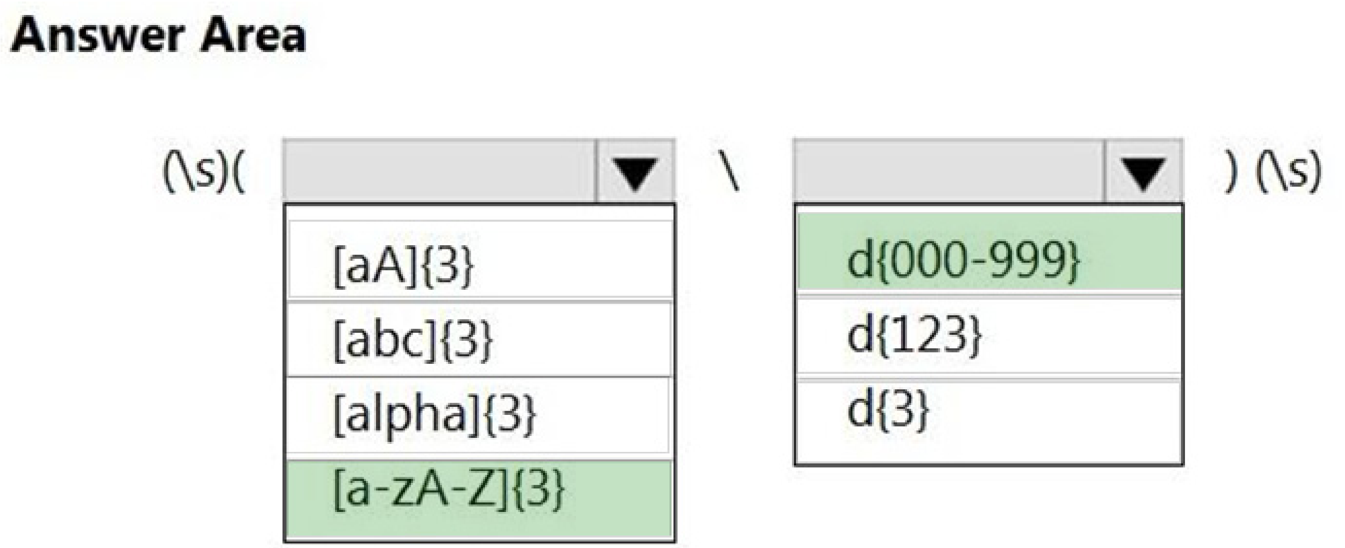
Answer Area

(\s)([▼] \ [▼]) (\s)

- [aA]{3}
- [abc]{3}
- [alpha]{3}
- [a-zA-Z]{3}

- d{000-999}
- d{123}
- d{3}

Correct Answer:



Answer Area

(\s)([▼] \ [▼]) (\s)

First dropdown:

- [aA]{3}
- [abc]{3}
- [alpha]{3}
- [a-zA-Z]{3} ✓

Second dropdown:

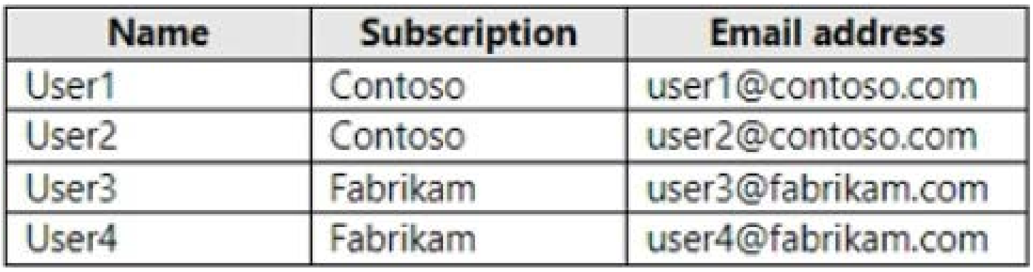
- d{000-999} ✓
- d{123}
- d{3}

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

QUESTION 12

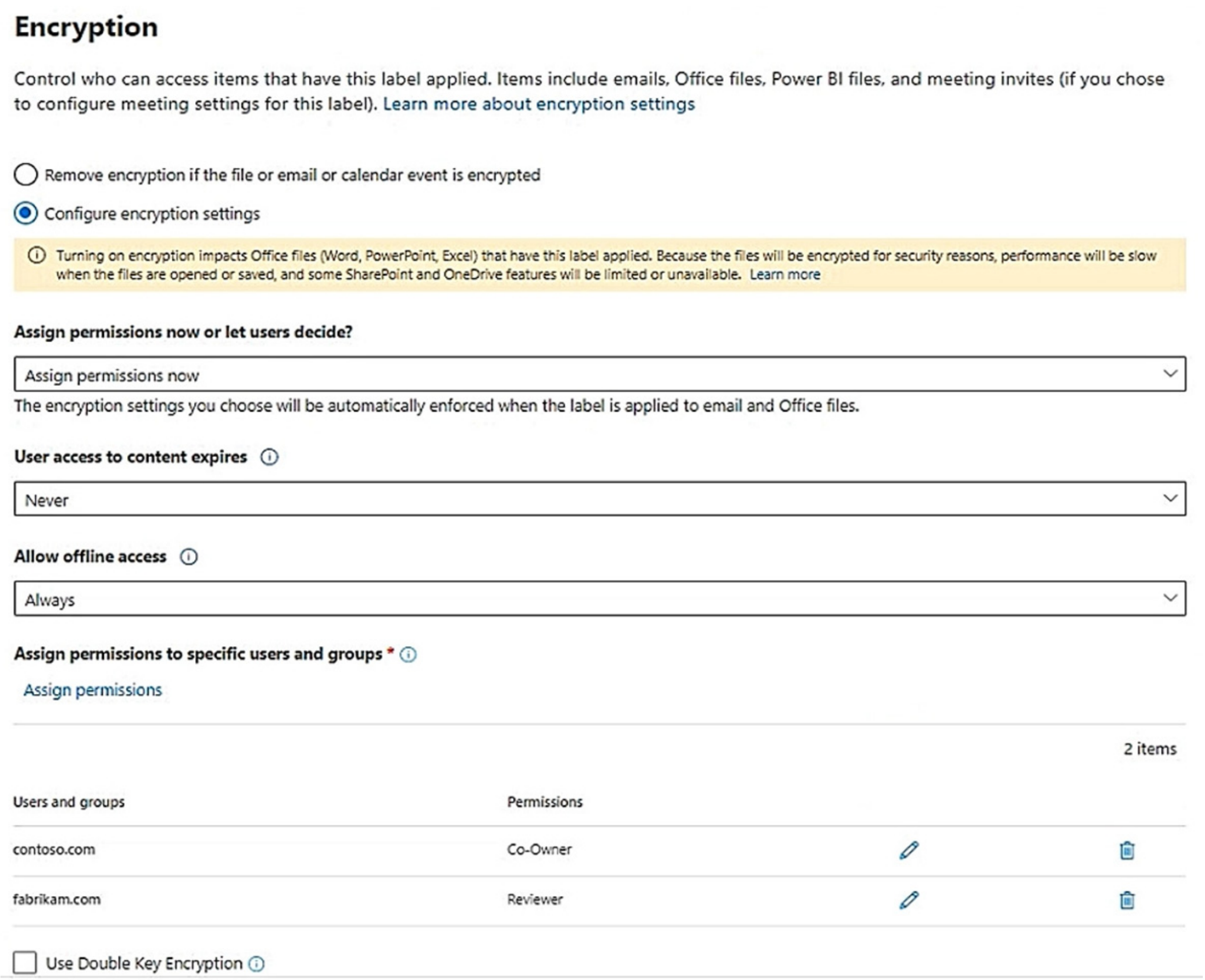
HOTSPOT

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 * ⓘ

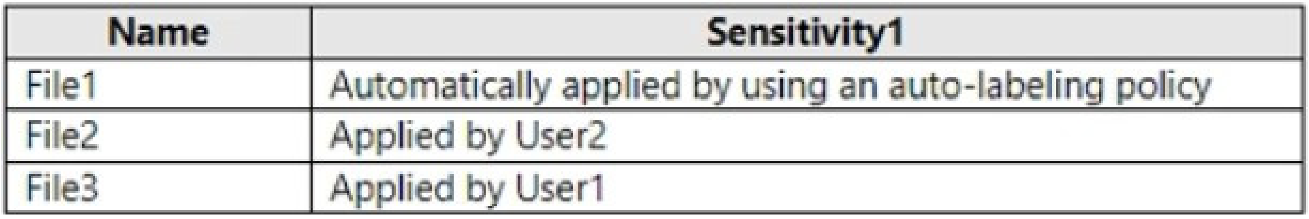
Assign permissions

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.

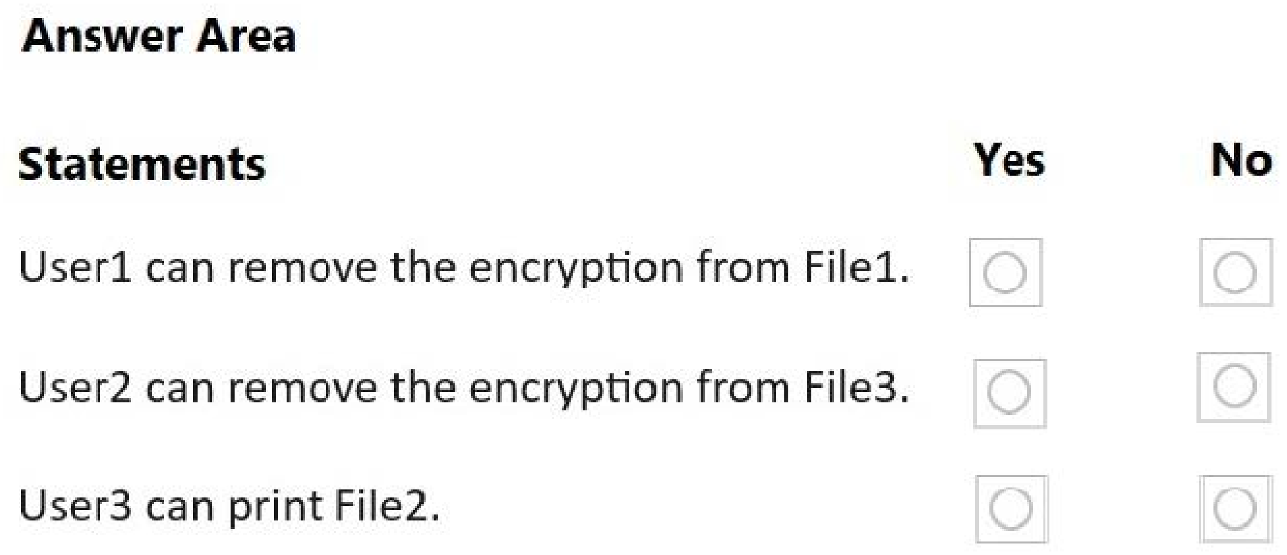


Name	Sensitivity1
File1	Automatically applied by using an auto-labeling policy
File2	Applied by User2
File3	Applied by User1

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

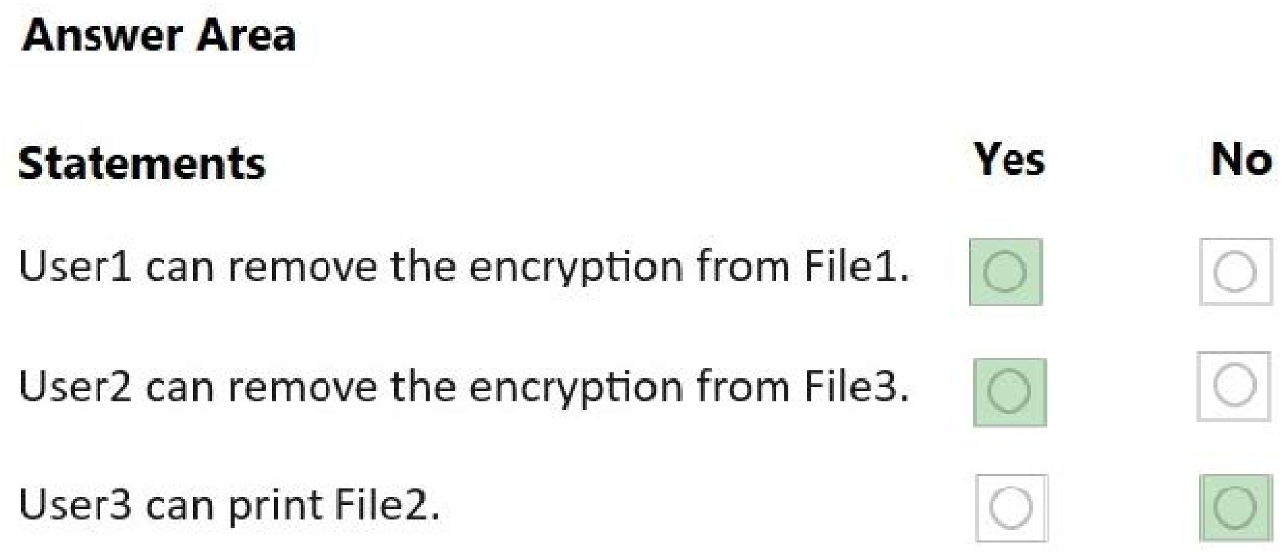
Hot Area:



Answer Area

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

Correct Answer:



Answer Area

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

Box 1: Yes

Yes - User1 can remove the encryption from File1.

User1 is in the Contoso subscription, and has the email address user1@contoso.com

Sensitivity label Sensitiviy1 has assigned contoso.com users Co-owner permissions.

For File1 has Sensitiviy1 been automaticallyapplied by using an auto-labeling policy.

Box 2: Yes

Yes - User2 can remove the encryption from File3.

User2 is in the Contoso subscription, and has the email address user2@contoso.com

Sensitivity label Sensitiviy1 has assigned contoso.com users Co-owner permissions.

For File3 has Sensitiviy1 been applied by User1.

Box 3: No

No - User3 can print File2.

User3 is in the Fabrikam subscription, and has the email address user3@fabrikam.com

Sensitivity label Sensitiviy1 has assigned fabrikam.com users reviewer permissions.

For File2 has Sensitiviy1 been applied by User2.

Reference:

https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels

QUESTION 13

You have a Microsoft 365 E5 subscription.

You are implementing insider risk management.

You need to maximize the amount of historical data that is collected when an event is triggered.

What is the maximum number of days that historical data can be collected?

A. 30

B. 60

C. 90

D. 180

Correct Answer: C