



## **Free Questions for SC-400 by dumpssheet**

**Shared by Walsh on 24-05-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type:** MultipleChoice

---

Task 2

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.

**Options:**

---

**A-** See the solution below in Explanation

**Answer:**

---

A

**Explanation:**

---

To restrict the Confidential - Finance label to only the members of the Finance Team group, follow these steps:

Create a Sensitivity Label:

Log in to the Microsoft Purview portal or the Microsoft Purview compliance portal as an admin.

Navigate to Sensitivity labels and create a new label called "Confidential - Finance".

[Specify the appropriate settings for this label, including encryption, content markings, and permissions](#)<sup>1</sup>.

Configure Encryption Settings:

When creating the label, ensure that you configure the encryption settings.

[Choose either to assign permissions now \(where you determine exactly which users get which permissions\) or allow users to assign permissions when they apply the label to content](#)<sup>2</sup>.

Assign the Label to the Finance Team Group:

In the Microsoft Purview portal, go to the Groups section.

Select the Finance Team group.

Under Settings, choose Sensitivity labels.

Add the "Confidential - Finance" label to this group.

[Only members of the Finance Team will now have access to this label](#)<sup>3</sup>.

Test the Configuration:

## Question 2

---

**Question Type:** MultipleChoice

---

Task 1

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.

**Options:**

---

**A-** See the solution below in Explanation

**Answer:**

---

A

**Explanation:**

---

Create a Custom Content Type:

Go to your SharePoint Online site.

Click on Settings (gear icon) and select Site settings.

Under Web Designer Galleries, choose Site content types.

Create a new content type (e.g., "Product1 Classification") based on the Document parent content type.

Add a custom column (e.g., "Classification") to this content type.

Apply the Content Type to Document Libraries:

Navigate to the document library where the files are stored.

Click on Library settings.

Under General Settings, select Advanced settings.

Choose Yes for "Allow management of content types."

Add your custom content type ("Product1 Classification") to the library.

Manually Classify Files:

Upload or edit a file in the library.

In the file properties, select the Classification field and set it to "Product1."

Permissions and Encryption:

Ensure that all authenticated users have at least View permissions on the library.

For encryption, SharePoint Online automatically encrypts files at rest using BitLocker disk-level encryption.

Files classified as "Product1" will be encrypted and accessible only to authorized users.

## Question 3

---

**Question Type: MultipleChoice**

---

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?

**Options:**

---

**A-** Yes

**B-** No

**Answer:**

---

B

**Explanation:**

---

Topic 4, Simulations and Labs

## Question 4

---

**Question Type: 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.)

The screenshot shows the Microsoft Purview interface for editing a sensitivity label. The top navigation bar includes the Microsoft Purview logo, the text 'Contoso Electronics Microsoft Purview', and user profile information 'MA'. The main heading is 'Edit sensitivity label'. On the left, a vertical progress bar shows six steps: 'Name & description', 'Scope', 'Files & emails', 'Groups & sites', 'Schematized data assets (preview)', and 'Finish'. The 'Name & description' step is currently active. The main content area displays the following configuration details for the 'Contoso Confidential' 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](#)



# 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 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](#)

Users and groups	Permissions
Authenticated users	Co-Author 

Use Double Key Encryption 

Back

Next

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**

**Answer:**

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

## Question 5

**Question Type: Hotspot**

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

Name	Description
Admin1	Member of the Communication Compliance Investigators role group

Name	Policy template	Status	Time created
Policy1	Detect inappropriate images	Active	11:00 AM
Policy2	Detect financial regulatory compliance	Active	2:30PM
Policy3	Detect sensitive info types	Active	5:45 PM

in the following table.

wise, select No.

## Answer Area

### Statements

Admin2 can review the results of Policy1 at 3:00 PM on August 2, 2023.

Yes

No

**Answer:**

---

Admin3 can review the results of Policy3 at 9:00 PM on August 2, 2023.

Admin1 can review the results of Policy2 at 2:00 PM on August 2, 2023.

## Question 6

---

**Question Type: Hotspot**

---

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

- \* Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.
- \* Integrates data loss prevention (OLP) capabilities with insider risk management.

What should you use for each requirement? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

Captures clips of key security-related user activities:

- Forensic evidence
- Adaptive scopes
- Classifiers
- Forensic evidence
- Search

Answer:

Integrates DLP capabilities with insider risk management:

- eDiscovery (Premium)
- Adaptive Protection
- eDiscovery (Premium)
- Records management
- Trainable classifiers

## Question 7

Question Type: Hotspot

You have a Microsoft 365 E5 tenant that contains the objects shown in the following table.

Name	Type
Project1	Microsoft Teams team
Sales	Microsoft Teams channel
User1	User

That was deleted from the Sales channel by User 1.

How long will the document be retained? To answer, select the appropriate options in

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Restored from:   
Microsoft Teams  
Microsoft OneDrive  
Microsoft Exchange Online  
Microsoft SharePoint Online

Retained for:   
10 days  
30 days  
93 days

## Question 8

Question Type: 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

ate l.docx.

will use the document fingerprint from Template!.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.

## Answer Area

Answer:

---

Create Sensitive1 by using:

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

Use Sensitive1 in:

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

## Question 9

---

Question Type: MultipleChoice

---

You have a Microsoft 365 ES subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement a records management solution for the files stored on Site1. The solution must meet the following requirements:

- \* The files must be retained for seven years.
- \* Files older than seven years must be deleted automatically.

What should you use to manage the files?

### Options:

---

- A- an adaptive scope
- B- a file plan

C- a disposition review

D- a label policy

**Answer:**

---

B

## Question 10

---

**Question Type: MultipleChoice**

---

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 tenant and 500 computers that run Windows 10. The computers are onboarded to Microsoft Purview.

You discover that a third-party application named Tailspin\_scanner.exe accessed protected sensitive information on multiple computers. Tailspin\_scanner.exe is installed locally on the computers.

You need to block Tailspin\_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From Microsoft Defender for Cloud Apps, you create an app discovery policy.

Does this meet the goal?

**Options:**

---

**A-** Yes

**B-** No

**Answer:**

---

B



**To Get Premium Files for SC-400 Visit**

**<https://www.p2pexams.com/products/sc-400>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/microsoft/pdf/sc-400>**

