

# Microsoft

## Exam Questions SC-401

Administering Information Security in Microsoft 365



NEW QUESTION 1

HOTSPOT - (Topic 1)

You are reviewing policies for the SharePoint Online environment.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	<input type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

AI-generated content may be incorrect. Understanding Site4's Retention Policies:  
Site4RetentionPolicy1 deletes items older than 2 years from creation. If a file was created on January 1, 2021, it would be deleted after January 1, 2023.  
Site4RetentionPolicy2 retains files for 4 years from creation. If a file was created on January 1, 2021, it will be kept until January 1, 2025, but not deleted after that (policy states "Do nothing").  
Statement 1 - Yes, because Site4RetentionPolicy2 ensures files are retained for 4 years. Statement 2 - Yes, because Site4RetentionPolicy2 retains the file for 4 years (until January 1, 2025).  
Statement 3 - No, because retention is only for 4 years (until January 1, 2025). After that, the policy does "nothing," meaning the file is no longer recoverable after that period.

NEW QUESTION 2

HOTSPOT - (Topic 1)

You need to meet the technical requirements for the confidential documents.

What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create first:

A Compliance Manager assessment

A content search

A DLP policy

A sensitive info type

A sensitivity label

Use for detection method:

Dictionary

File type

Keywords

Regular expression

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To detect and protect confidential documents, we need a custom rule to identify project codes that start with 999 (since they are classified as confidential).  
Box 1: A Sensitive Info Type (SIT) allows Microsoft Purview DLP policies to recognize structured data (e.g., project codes). DLP policies require a sensitive info type to detect content based on patterns, keywords, or dictionary terms. A sensitivity label alone does not define detection logic—it is used for classification and protection after content is identified.  
Box 2: Since project codes follow a structured 10-digit pattern, we should use a Regular Expression (Regex) to match project codes that start with 999.  
Example Regex pattern: 999\d{7}  
This pattern detects a 10-digit number starting with "999".

NEW QUESTION 3

- (Topic 2)  
You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP). Which devices support Endpoint DLP?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device4 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

Answer: B

Explanation:

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) is supported only on Windows 10 and Windows 11 devices. It does not support macOS or iOS at this time.  
From the provided table:  
Device1 (Windows 11) - Supported Device2 (Windows 10) - Supported Device3 (iOS) - Not supported Device4 (macOS) - Not supported  
Thus, only Device1 and Device2 support Endpoint DLP.

NEW QUESTION 4

HOTSPOT - (Topic 2)  
You have a Microsoft 365 E5 subscription that contains the device configurations shown in the following table.

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

Each configuration uses either Google Chrome or Firefox as a default browser.  
You need to implement Microsoft Purview and deploy the Microsoft Purview browser extension to the configurations.  
To which configuration can each extension be deployed? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Google Chrome:

▼

☐

Config1 only

☐

Config2 only

☐

Config1 and Config2 only

☐

Config2 and Config3 only

☐

Config1, Config2, and Config3

Firefox:

▼

☐

Config1 only

☐

Config2 only

☐

Config1 and Config2 only

☐

Config2 and Config3 only

☐

Config1, Config2, and Config3

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Microsoft Purview browser extensions for Endpoint DLP are supported on: Windows 10/11 (Config1)  
macOS (Config2)  
Not supported on Android (Config3)  
Since Microsoft Purview does not support browser extensions on Android, Config3 is excluded from both Google Chrome and Firefox.

**NEW QUESTION 5**  
HOTSPOT - (Topic 2)  
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 (DLP) 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:

Adaptive scopes

Classifiers

Forensic evidence

Search

Integrates DLP capabilities with insider risk management:

Adaptive Protection

eDiscovery (Premium)

Records management

Trainable classifiers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Captures clips of key security-related user activities:

Adaptive scopes

Classifiers

Forensic evidence

Search

Integrates DLP capabilities with insider risk management:

Adaptive Protection

eDiscovery (Premium)

Records management

Trainable classifiers

**NEW QUESTION 6**  
HOTSPOT - (Topic 2)  
You have a new 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

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

To create a custom trainable classifier in Microsoft Purview (formerly Microsoft Compliance Center), you must first opt into the trainable classifier feature. Before using custom trainable classifiers, Microsoft requires manual opt-in through the Microsoft Purview compliance portal. Without this step, you cannot create a new classifier. The Compliance Administrator role has the necessary permissions to configure data classification, DLP policies, and trainable classifiers. Global Administrator has higher privileges but is not required for this task, violating the principle of least privilege. Security Administrator is focused on security-related settings but does not manage compliance features like classifiers.

### NEW QUESTION 7

- (Topic 2)

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 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-Mailbox -Identity "User1" -AuditEnabled \$true command. Does that meet the goal?

- A. Yes
- B. No

**Answer:** A

### Explanation:

To track who accesses User1's mailbox, you need to enable mailbox auditing for User1. By default, Exchange mailbox auditing is not enabled per mailbox (even though it is enabled tenant-wide).

The Set-Mailbox -Identity "User1" -AuditEnabled \$true command enables audit logging for mailbox actions like:

Read emails Delete emails

Send emails as User1 Access by delegated users

Once enabled, you can search for future sign-ins and actions in the Microsoft Purview audit logs.

### NEW QUESTION 8

- (Topic 2)

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 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-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.

Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

### Explanation:

The Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com - AccessRights Owner command is incorrect. This assigns folder permissions but does not enable auditing. It does not track who accessed the mailbox or deleted emails.

#### NEW QUESTION 9

DRAG DROP - (Topic 2)

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:

Rules that are applied without triggering a policy alert The top 10 files that have matched DLP policies Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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.

Reports	Answer Area	Report
<div><div>DLP policy matches</div><div>False positive and override</div><div>Incident reports</div></div>	Rules that are applied without triggering a policy alert:  The top 10 files that have matched DLP policies:  Alerts that are miscategorized:	<div></div> <div></div> <div></div>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

The False positive and override report helps identify rules that were applied but did not generate an actual policy alert, which means they were overridden or deemed false positives.

The DLP policy matches report provides details on files that matched DLP policies, including the top 10 files.

The Incident reports report helps analyze and review alerts, including those that may have been miscategorized.

#### NEW QUESTION 10

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management. What should you create first?

- A. a sensitivity label policy
- B. a data loss prevention (DLP) policy
- C. an auto-labeling policy
- D. a retention label

**Answer:** D

#### Explanation:

To implement Microsoft Purview Data Lifecycle Management for SharePoint Online (Site1), you need to create a retention label first. Retention labels define how long content should be retained or deleted based on compliance requirements. Once a retention label is created, it can be manually or automatically applied to content in SharePoint Online, Exchange, OneDrive, and Teams. After creating a retention label, you can configure label policies to apply them to Site1 and other locations.

#### NEW QUESTION 10

- (Topic 2)

You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.

You configure an advanced DLP rule in the policy. Which type of condition can you use in the rule?

- A. Sensitive info type
- B. Content search query
- C. Sensitive label
- D. Keywords

**Answer:** A

#### Explanation:

When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns. This allows you to apply protection and trigger actions based on the identified content.

#### NEW QUESTION 15

HOTSPOT - (Topic 2)

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.

<b>Label name</b>	<b>Edit</b>
Rebranding	
<b>Tooltip</b>	<b>Edit</b>
Used for all documents containing information about the rebranding effort	
<b>Description</b>	<b>Edit</b>
<b>Encryption</b>	<b>Edit</b>
Advanced protection for content with this label	
<b>Content marking</b>	<b>Edit</b>
Watermark: INTERNAL	
<b>Endpoint data loss prevention</b>	<b>Edit</b>
<b>Auto labeling</b>	<b>Edit</b>

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



Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**  
Statement 1 - No. The sensitivity label includes content marking (watermark: INTERNAL), but it only applies to documents where the label is manually or automatically applied, not to all documents by default.  
Statement 2 - No. The sensitivity label only specifies a watermark, not a header. If a header marking was configured, it would explicitly appear in the label settings.  
Statement 3 - No. There is no indication that auto-labeling is configured to apply the label only to documents with the word "rebranding". Auto-labeling is an optional setting that needs explicit configuration.

NEW QUESTION 16

- (Topic 2)  
You have a Microsoft 365 subscription.  
You need to customize encrypted email for the subscription. The solution must meet the following requirements.  
Ensure that when an encrypted email is sent, the email includes the company logo. Minimize administrative effort.  
Which PowerShell cmdlet should you run?

- A. Set-IRMConfiguration
- B. Set-OMEConfiguration
- C. Set-RMSTemplate
- D. New-OMEConfiguration

Answer: B

**Explanation:**  
To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set- OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as: Company logo  
Custom text Background color  
This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

NEW QUESTION 18

HOTSPOT - (Topic 2)  
You have a Microsoft 365 E5 subscription.  
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.  
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the documents, use a data classification of:

Exact data match (EDM)

Sensitive info type

Trainable classifier

Configure data classifications by using a:

Keyword dictionary

Regular expression

Function

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Since you are looking for a specific pattern (PA followed by eight digits, e.g., PA 12345678), the best classification method is Sensitive Info Type. Sensitive Info Types allow pattern-based matching to identify structured data. Exact Data Match (EDM) is not needed because you're not comparing against a fixed dataset. Trainable classifier is not appropriate because this is a structured pattern, not an unstructured document classification.

Box 2: Since PA 12345678 follows a structured pattern, the most effective method is Regular Expression (Regex). A Regular Expression (Regex) can be written to match "PA" followed by exactly eight digits (e.g., PA\s\d{8}). Keyword dictionary is not ideal because it works for predefined words, not number patterns. Function is unnecessary because there is no need for checksum validation or predefined validation rules.

**NEW QUESTION 22**

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	<ul style="list-style-type: none"><li>• Exchange email (All recipients)</li><li>• SharePoint sites (All sites)</li></ul>
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1. You need to modify RP1.  
Which two modifications can you perform? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

- A. Add locations to the policy.
- B. Delete the policy.
- C. Remove locations from the policy.
- D. Decrease the retention period of the policy.
- E. Disable the policy.
- F. Increase the retention period of the policy.

**Answer:** AF

**Explanation:**

A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.

When a Preservation Lock is applied:

- \* 1. You cannot disable or delete the policy.
- \* 2. You cannot remove locations from the policy.
- \* 3. You cannot decrease the retention period.
- \* 4. You can add locations to the policy.
- \* 5. You can increase the retention period.

You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

**NEW QUESTION 23**

- (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. You are creating an exact data match (EDM) classifier named EDM1.  
For EDM1, you upload a schema file that contains the fields shown in the following table.

Column name	Match mode
PP	EU Passport Number
Name	All Full Names
DateOfBirth	Single-token
AccountNumber	Multi-token

What is the maximum number of primary elements that EDM1 can have?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer:** B

**Explanation:**

In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.

From the provided table, the Match mode indicates how data is analyzed: PP (EU Passport Number) Likely a primary element because it's unique. Name (All Full Names) Typically not a primary element as names are common. DateOfBirth (Single-token) Usually a secondary element, not unique. AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier. Since EDM supports a maximum of two primary elements, the correct answer is 2.

**NEW QUESTION 24**

**HOTSPOT - (Topic 2)**

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need ensure that an incident will be generated when a user visits a phishing website. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Type of policy to create:

- a Communication compliance
- a Data loss prevention (DLP)
- an Insider risk management

Prerequisite to complete:

- Create a sensitive service domain group.
- Deploy the Microsoft Defender Browser Protection extension.
- Deploy the Microsoft Purview extension.
- From Data Loss Prevention, configure the Service domains settings.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Insider Risk Management policies in Microsoft Purview can be configured to detect risky behavior, such as accessing phishing websites. These policies monitor user activity, generate alerts, and help organizations investigate potential security threats.

Box 2: Microsoft Defender Browser Protection extension helps in detecting unsafe or phishing websites and integrating this detection with Insider Risk Management policies. This extension works with Microsoft Edge and Google Chrome to identify risky browsing activity and trigger alerts.

**NEW QUESTION 27**

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents.

You plan to implement Microsoft 365 Copilot for the subscription.

You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.

What should you use?

- A. data loss prevention (DLP)
- B. Microsoft Purview insider risk management
- C. Microsoft Purview Information Barriers
- D. sensitivity labels

**Answer:** D

**Explanation:**

To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels.

Sensitivity labels allow you to classify, protect, and restrict access to sensitive files. You can configure label-based encryption and access control policies to ensure that only authorized users can access or interact with the files in Channel1. Microsoft 365 Copilot respects sensitivity labels, meaning if a file is labeled with restricted permissions, Copilot will not use it in generated responses for unauthorized users.

**NEW QUESTION 30**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.

Which permission should you select for Label1?

- A. Export content(EXPORT)
- B. Copy and extract content(EXTRACT)
- C. Edit content(DOCEDIT)
- D. View rights(VIEW)

**Answer:** B

**Explanation:**

To allow Microsoft 365 Copilot to summarize files that have Label1 applied, the label must grant permission to extract content from the document. The correct permission for this is Copy and extract content (EXTRACT).

Microsoft 365 Copilot requires access to read and process content in documents to generate summaries. The EXTRACT permission allows users (and AI tools like Copilot) to copy and extract content for processing while still maintaining the protection applied by the sensitivity label.



**NEW QUESTION 33**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

The subscription contains the users shown in the following table.

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

You need to review the activities.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:

Activity explorer in Data Security Posture Management for AI (DSPM for AI)

☐

Audit log search

☐

Insider risk audit log

☐

Unified Catalog

☐

User2:

Activity explorer in Data Security Posture Management for AI (DSPM for AI)

☐

Audit log search

☐

Insider risk audit log

☐

Unified Catalog

☐

User3:

Activity explorer in Data Security Posture Management for AI (DSPM for AI)

☐

Audit log search

☐

Insider risk audit log

☐

Unified Catalog

☐

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.

User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI- related activity cannot be tracked in DSPM for AI. Instead, Audit log search should be used to review activity such as using Microsoft 365 Copilot.

User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

**NEW QUESTION 34**

HOTSPOT - (Topic 2)

You have a Microsoft SharePoint Online site that contains the following files.



Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	<i>None</i>
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

Users are assigned roles for the site as shown in the following table.

Name	Role
User1	Site owner
User2	Site member

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

### Answer Area

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

### NEW QUESTION 36

- (Topic 2)

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 11. 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 the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

Adding a folder path to the file path exclusions in Microsoft 365 Endpoint DLP does not prevent Tailspin\_scanner.exe from accessing protected sensitive information. Instead, it would exclude those files from DLP protection, which is not the intended outcome.

To block Tailspin\_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin\_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin\_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

### NEW QUESTION 37

- (Topic 2)

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 recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

#### Explanation:

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.

A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

### NEW QUESTION 42

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to enable support for sensitivity labels in Microsoft SharePoint Online. What should you use?

- A. the Microsoft Purview portal
- B. the Microsoft Entra admin center
- C. the SharePoint admin center
- D. the Microsoft 365 admin center

**Answer: C**

**Explanation:**

To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center. Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center Settings Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

**NEW QUESTION 47**

- (Topic 2)

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 11. 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 the Microsoft Defender for Cloud Apps, you mark the application as Unsanctioned.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Marking Tailspin\_scanner.exe as "Unsanctioned" in Microsoft Defender for Cloud Apps only blocks its usage in cloud-based activities (such as accessing SharePoint, OneDrive, or Exchange Online). However, it does not prevent a locally installed application on Windows 11 devices from accessing sensitive files.

To block Tailspin\_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin\_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin\_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

**NEW QUESTION 50**

HOTSPOT - (Topic 2)

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.

## Answer Area

# 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

 Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

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 

A number of days after 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](#)

0 items

Users and groups


Permissions

Edit

Delete

No data available

☒ Use dynamic watermarking 

 Customize text (optional)

☒ Use Double Key Encryption 

<https://sts.contoso.com>



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
 C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

NEW QUESTION 53  
 HOTSPOT - (Topic 2)  
 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 Label1.  
 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

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Box 1: Publishing a Sensitivity Label

Sensitivity labels can be published to Microsoft 365 groups, security groups, SharePoint

Online sites, and Microsoft Teams. Since we have: Group1 (Microsoft 365 group) - Supported Group2 (Security group) - Supported

Site1 (SharePoint Online site) - Supported Team1 (Microsoft Teams team) - Supported

This means we can publish Label1 to Group1, Group2, Site1, and Team1. Box 2: Auto-Applying a Sensitivity Label

Auto-apply policies for sensitivity labels work on: SharePoint Online sites (documents)

OneDrive (documents) Exchange email (messages)

However, labels cannot be auto-applied to Microsoft 365 groups or Teams directly because labels are applied to files and emails, not to groups or Teams as entities. Since Site1 (a SharePoint Online site) supports auto-apply, it is the correct option.

**NEW QUESTION 56**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SC-401 Practice Exam Features:

- \* SC-401 Questions and Answers Updated Frequently
- \* SC-401 Practice Questions Verified by Expert Senior Certified Staff
- \* SC-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SC-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SC-401 Practice Test Here](#)**