

Exam Questions SC-401

Administering Information Security in Microsoft 365

<https://www.2passeasy.com/dumps/SC-401/>



NEW QUESTION 1

- (Topic 1)

You need to meet the technical requirements for the creation of the sensitivity labels. To which user or users must you assign the Sensitivity Label Administrator role?

- A. Admin1 only
- B. Admin1 and Admin4 only
- C. Admin1 and Admin5 only
- D. Admin1, Admin2, and Admin3 only
- E. Admin1, Admin2, Admin4, and Admin5 only

Answer: D

Explanation:

To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users.

Sensitivity Label Administrator Role Responsibilities

This role allows users to:

Create and manage sensitivity labels in Microsoft Purview. Publish and configure auto-labeling policies.

Modify label encryption and content marking settings.

Review of Admin Roles from the Table:

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	☐ No, read-only permissions.
Admin2	Compliance Data Administrator	☐ Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	☐ Yes, has full compliance management, including labels.
Admin4	Security Operator	☐ No, this role is focused on security alerts and response.
Admin5	Security Administrator	☐ No, primarily focused on security policies and threat management.

Users that must be assigned the Sensitivity Label Administrator role: Admin2 (Compliance Data Administrator)

Admin3 (Compliance Administrator)

Admin1 (Global Reader) (should be assigned this role to fulfill the requirement that all admins can create labels).

NEW QUESTION 2

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.

Answer Area

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.	☒	☐
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.	☐	☐
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.	☐	☐

- 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 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 that contains three DOCX files named File1, File2, and File3.
You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	None	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File1	None
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

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

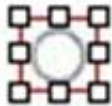
Answer Area

Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



NEW QUESTION 6
- (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 7

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to review a Microsoft 365 Copilot usage report. From where should you review the report?

- A. Information Protection in the Microsoft Purview portal
- B. the Microsoft 365 admin center
- C. DSPM for AI in the Microsoft Purview portal
- D. the Microsoft Defender portal

Answer: C

Explanation:

To review a Microsoft 365 Copilot usage report, you need to use Data Security Posture Management for AI (DSPM for AI) in the Microsoft Purview portal. DSPM for AI provides insights into AI-related activities, including Copilot usage, risk assessments, and data security posture related to AI interactions within Microsoft 365.

NEW QUESTION 8

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
DLP policy matches	Rules that are applied without triggering a policy alert:	
False positive and override	The top 10 files that have matched DLP policies:	
Incident reports	Alerts that are miscategorized:	

- 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 9

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 10

- (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 10

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 13

- (Topic 2)
You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.

Create rule

Use actions to protect content when the conditions are met.

^
Audit or restrict activities on devices

When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.
[Learn more restricting device activity](#)

Service domain and browser activities
Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

☒ Upload to a restricted cloud service domain or access from an unallowed browsers

i

Block

File activities for all apps
Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

☐ Don't restrict file activity
☒ Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

☒ Copy to clipboard

i

Audit only

☒ Copy to a USB removable media

i

Audit only

☒ Copy to a network share

i

Audit only

☒ Print

i

Audit only

Save

Cancel

From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue. What are two possible causes of the issue? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.
- B. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings.
- C. The Access by restricted apps action is set to Audit only.
- D. The Copy to clipboard action is set to Audit only.
- E. The computers are NOT onboarded to Microsoft Purview.

Answer: AB

Explanation:

The issue where users sometimes can upload files to cloud services and sometimes cannot suggests inconsistent enforcement of Endpoint DLP policies. This can be caused by the unallowed browsers in the Microsoft 365 Endpoint DLP settings are NOT configured. Also, there are file path exclusions in the Microsoft 365 Endpoint DLP settings.

Endpoint DLP can block uploads only when using unallowed browsers. If unallowed browsers are not configured, users might be able to bypass restrictions by switching to a different browser. This could explain why uploads sometimes work and sometimes don't, depending on which browser is used.

File path exclusions allow certain files or folders to be exempt from DLP restrictions. If a specific file location is excluded, files stored there won't trigger DLP policies, leading to inconsistent behavior. This could result in some uploads being blocked while others are allowed.

NEW QUESTION 16

- (Topic 2)

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. an XLSX file that contains one word in each cell of the first row
- B. an XML file that contains a keyword tag for each word

- C. an ACCDB database file that contains a table named Dictionary
- D. a text file that has one word on each line

Answer: D

Explanation:

To create a keyword dictionary for a sensitive information type in Microsoft Purview Data Loss Prevention (DLP), you must use a plain text (.txt) file where each keyword is on a separate line.

Format Example (TXT file): confidential sensitive classified top secret

This format is simple, efficient, and directly compatible with Microsoft 365 DLP policies for keyword dictionaries.

How to use the keyword dictionary?

Create a text file with one keyword per line.

Upload it to Microsoft Purview under Data Classification > Sensitive Info Types. Use the dictionary in a DLP policy to identify and protect sensitive information.

NEW QUESTION 18

- (Topic 2)

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 portal create an insider risk policy
- B. From the Microsoft Defender portal create a file policy
- C. From the Microsoft Defender portal, create an activity policy.
- D. From the Microsoft Purview portal, start a data investigation.

Answer: B

Explanation:

An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.

NEW QUESTION 23

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-401 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-401 Product From:

<https://www.2passeasy.com/dumps/SC-401/>

Money Back Guarantee

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