

## 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 retention requirement for the users' Microsoft 365 data. What is the minimum number of retention policies required to achieve the goal?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 6

**Answer:** B

#### Explanation:

The requirement states that all Microsoft 365 data for users must be retained for at least one year. In Microsoft 365, retention policies must be configured for each type of data storage.

Step 1: Identifying Where Data is Stored

From the case study, users store data in the following locations: SharePoint Online sites

OneDrive accounts Exchange email Exchange public folders Teams chats

Teams channel messages

Since these locations fall under two broad categories: Microsoft Exchange data (Emails, Public folders)

SharePoint, OneDrive, and Teams data

Step 2: Required Retention Policies

\* 1. A single retention policy can cover: SharePoint Online

OneDrive Microsoft Teams

\* 2. A second retention policy is required for: Exchange (Emails & Public Folders)

Thus, the minimum number of retention policies required to meet the requirement is 2.

Microsoft 365 retention policies can be applied broadly across multiple services with just two policies:

One for Exchange & Public Folders

One for SharePoint, OneDrive, and Teams

There's no need for separate policies for each individual workload unless different retention durations are required, which is not stated in the requirement.

### NEW QUESTION 2

- (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 3

- (Topic 2)

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

Name	Description
User1	<ul style="list-style-type: none"> <li>User 1 is a regional manager.</li> <li>User1 is assigned the Reader role.</li> <li>Three department managers report to User1.</li> </ul>
User2	<ul style="list-style-type: none"> <li>User2 is the human resources (HR) department manager.</li> <li>User2 has no Microsoft Entra roles assigned.</li> <li>Five HR department users report to User2.</li> </ul>
User3	<ul style="list-style-type: none"> <li>User3 is a developer.</li> <li>User3 reports to User2.</li> <li>User3 is the only user in the compliance department.</li> <li>User3 is assigned the Compliance Administrator role.</li> </ul>
User4	<ul style="list-style-type: none"> <li>User4 is the assistant of User1.</li> <li>User4 has no Microsoft Entra roles assigned.</li> <li>User4 handles a high volume of confidential data on behalf of User1.</li> </ul>

Which users will Microsoft Purview insider risk management flag as potential high-impact users?

- A. User1 and User2 only
- B. User2 and User3 only
- C. User1, User2, and User3 only
- D. User1, User2, User3, and User4

**Answer: D**

**Explanation:**

Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:

User1 (Regional Manager, assigned Reader role, manages department managers) Risk Factors:

Holds a managerial position (regional manager).

Manages multiple department managers, indicating organizational influence. Access to critical business information.

Flagged? -Yes (Managerial role and access to confidential data).

User2 (HR department manager, no Microsoft Entra roles, manages HR department users) Risk Factors:

Manages HR department users, meaning they likely handle sensitive employee data. HR roles are often considered high-risk due to access to personal and payroll data.

Flagged? -Yes (HR role and access to sensitive employee data).

User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role)

Risk Factors:

Compliance Administrator role grants access to sensitive security and regulatory data. Only person in the compliance department, meaning they hold a critical role.

Potentially high impact on compliance and security settings.

Flagged? -Yes (Privileged Compliance Administrator role).

User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1)

Risk Factors:

Handles a high volume of confidential data on behalf of a regional manager. Assistants with access to sensitive data are considered insider risk candidates.

Flagged? -Yes (High access to sensitive information).

Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

**NEW QUESTION 4**

- (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 5

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI). You need to ensure that User1 can perform the following actions:

View recommendations from the Recommendations page. View the user risk level for all events by using Activity explorer. The solution must follow the principle of least privilege.

To which role group should you add User1 for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

View the recommendations:

<input type="checkbox"/>	Compliance Administrator	<input type="checkbox"/>
<input type="checkbox"/>	Insider Risk Management Investigators	<input type="checkbox"/>
<input type="checkbox"/>	Security Reader	<input type="checkbox"/>

View the user risk level:

<input type="checkbox"/>	Compliance Administrator
<input type="checkbox"/>	Insider Risk Management Analysts
<input type="checkbox"/>	Insider Risk Management Investigators
<input type="checkbox"/>	Security Reader

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: The Insider Risk Management Investigators role allows users to view recommendations related to insider risk cases and Microsoft Purview DSPM for AI insights. This role is appropriate because it grants access to review AI-related risk recommendations without unnecessary administrative privileges.

Box 2: The Insider Risk Management Analysts role allows users to analyze user risk levels and events using Activity Explorer. This follows the principle of least privilege, ensuring that User1 can only view risk levels and investigate but does not gain full administrative control over insider risk policies.

#### NEW QUESTION 6

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

You have a file named Customer.csv that contains a list of 1,000 customer names. You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint

Online library.

What should you create in the Microsoft Purview portal, and which type of element should you select? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



## Answer Area

Create:

☐ A sensitive info type
 ☐ A trainable classifier
 ☐ An adaptive scope

Element:

☐ Functions
 ☐ Keyword dictionary
 ☐ Regular expression

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

## Answer Area

Create:

☒ A sensitive info type
 ☐ A trainable classifier
 ☐ An adaptive scope

Element:

☐ Functions
 ☒ Keyword dictionary
 ☐ Regular expression

### 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 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 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 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 configure a mail flow rule that matches the text patterns. Does this meet the goal?

A. Yes

B. No

**Answer:** B

**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.

Text patterns in mail flow rules are not as reliable as sensitive information types in DLP. Mail flow rules lack advanced content detection and machine learning-based classification, making them less effective than DLP.

**NEW QUESTION 9**

- (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to create static retention policies for the following locations:

Teams chats Exchange email SharePoint sites Microsoft 365 Groups

Teams channel messages

What is the minimum number of retention policies required?

A. 1

B. 2

C. 3

D. 4

E. 5

**Answer:** C

**Explanation:**

In Microsoft Purview Data Lifecycle Management, different Microsoft 365 locations require separate retention policies because they fall under different storage and compliance models.

Teams Chats & Teams Channel Messages (1 Policy) require a separate retention policy because Teams messages are stored differently than Exchange and SharePoint content. One policy can cover both Teams chats and Teams channel messages. Exchange Email (1 Policy) requires its own separate policy since emails are managed differently than Teams or SharePoint content. SharePoint Sites & Microsoft 365 Groups (1 Policy) are both stored in SharePoint Online, so they can be managed under one policy.

**NEW QUESTION 10**

- (Topic 2)

You have Microsoft 365 E5 subscription.

You create two alert policies named Policy1 and Policy2 that will be triggered at the times shown in the following table.

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

How many alerts will be added to the Microsoft Purview portal?

A. 2

- B. 3
- C. 4
- D. 5
- E. 6

**Answer:** D

**Explanation:**

In Microsoft Purview, when multiple alert policies trigger alerts, duplicate alerts within a short period (typically 5 minutes) may be suppressed to avoid redundancy. Step-by-step Analysis:

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policy1	10:00:00	Yes
Policy2	10:00:03	Yes
Policy1	10:00:04	No (Duplicate within 5 min)
Policy2	10:00:31	No (Duplicate within 5 min)
Policy1	10:01:01	Yes
Policy1	10:04:45	Yes

Policy1 at 10:00:04 is ignored because Policy1 already triggered at 10:00:00, and it's within 5 minutes.

Policy2 at 10:00:31 is ignored because Policy2 already triggered at 10:00:03, and it's within 5 minutes.

Policy1 at 10:01:01 is a new alert because it's over 1 minute after the previous Policy1 alert.

Policy1 at 10:04:45 is a new alert because it's over 3 minutes after the previous Policy1 alert.

**NEW QUESTION 10**

- (Topic 2)

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 sensitivity label
- D. a Conditional Access policy

**Answer:** C

**Explanation:**

To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection. A sensitivity label allows you to encrypt emails and documents, set expiration policies (e.g., emails expire after 7 days), and enable email revocation

How to configure it?

Go to Microsoft Purview compliance portal Information Protection Create a sensitivity label

Enable encryption and configure the content expiration policy Publish the label to users

**NEW QUESTION 11**

- (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 configure a mail flow rule that matches a sensitive info type. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**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.

Mail flow rules (transport rules) can detect sensitive info, but they are limited in encryption capabilities.

DLP policies provide more advanced protection and integration with Microsoft Purview for sensitive info detection.

**NEW QUESTION 15**



- (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-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets \*Mailbox\* command. Does that meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

The Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets

\*Mailbox\* command is incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

**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 20**

HOTSPOT - (Topic 2)

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.

## Answer Area

Upload:

<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Data hashes
<input checked="" type="checkbox"/>	Data in the XML format
<input type="checkbox"/>	Digitally signed data

Use:

<input checked="" type="checkbox"/>	Azure Storage Explorer
<input checked="" type="checkbox"/>	EDM upload agent
<input type="checkbox"/>	Microsoft Purview portal
<input type="checkbox"/>	The Set-DlpKeywordDictionary cmdlet

- A. Mastered
- B. Not Mastered



**Answer:** A

**Explanation:**

EDM does not store raw data; instead, it requires hashed versions of sensitive data for privacy and security. To upload the hashed data, Microsoft provides the EDM upload agent. This ensures that the data is securely processed and recognized by the EDM service in Microsoft 365.

**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