

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.

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.	<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 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:



A screenshot of a dropdown menu in Google Chrome. The menu is open, showing five options: 'Config1 only', 'Config2 only', 'Config1 and Config2 only', 'Config2 and Config3 only', and 'Config1, Config2, and Config3'. The first three options are highlighted with a red border, indicating they are selected.

Firefox:



A screenshot of a dropdown menu in Firefox. The menu is open, showing five options: 'Config1 only', 'Config2 only', 'Config1 and Config2 only', 'Config2 and Config3 only', and 'Config1, Config2, and Config3'. The first three options are highlighted with a red border, indicating they are selected.

- 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 3

- (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 4

- (Topic 2)

Your company has offices in multiple countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management.

You plan to perform the following actions:

In a new country, open an office named Office1. Create a new user named User1.

Deploy insider risk management to Office1.

Add User1 to the Insider Risk Management Admins role group.

You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.

What should you create first?

- A. a dynamic device group
- B. a dynamic user group
- C. an administrative unit
- D. a management group

Answer: C

Explanation:

To ensure User1 can perform insider risk management tasks only for the users and devices in Office1, the first step is to create an administrative unit in Microsoft Entra ID (formerly Azure AD).

Administrative units allow you to scope permissions to specific users, devices, and locations. By creating an administrative unit for Office1 and assigning User1 to the Insider Risk Management Admins role group within that unit, User1 will only have access to users and devices in Office1.

NEW QUESTION 5

DRAG DROP - (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:

A file is shared externally.

A file is labeled as internal only.

Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter 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.

Filters	Answer Area	Filter
0 Access level	When a file is shared externally.	0
0 Collaborators	When a file is labelled as Internal only.	0
0 Matched policy		
0 Sensitivity label		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Filters	Answer Area	Filter
0 Access level	When a file is shared externally.	0 Access level
0 Collaborators	When a file is labelled as Internal only.	0 Sensitivity label
0 Matched policy		
0 Sensitivity label		

NEW QUESTION 6

- (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 7

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains two Microsoft 365 groups named Group1 and Group2. Both groups use the following resources:

- A group mailbox
- Microsoft Teams channel messages
- A Microsoft SharePoint Online teams site

You create the objects shown in the following table.

Name	Type	Description
RLabel1	Retention label	None
AutoApply1	Auto-labeling policy	Applies RLabel1 to Group1
Retention1	Retention policy	Applied to Group2

To which resources will AutoApply1 and Retention1 be applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

AutoApply1:

▼

The group mailbox only

The SharePoint Online teams site only

The group mailbox and SharePoint Online teams site only

The group mailbox and Teams channel messages only

The group mailbox, SharePoint Online teams site, and Teams channel messages

Retention1:

▼

The group mailbox only

The SharePoint Online teams site only

The group mailbox and SharePoint Online teams site only

The group mailbox and Teams channel messages only

The group mailbox, SharePoint Online teams site, and Teams channel messages

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

AutoApply1 is an auto-labeling policy that applies RLabel1 to Group1. Auto-labeling policies can apply retention labels across group mailboxes, SharePoint Online sites, and Teams channel messages if they are configured for group resources.

Retention1 is a retention policy applied to Group2. Retention policies for Microsoft 365 groups apply to all group resources, including group mailboxes, SharePoint Online teams sites, and Teams channel messages.

Since both AutoApply1 and Retention1 affect entire groups, they apply to all associated resources: group mailbox, SharePoint Online teams site, and Teams channel messages.

NEW QUESTION 8

- (Topic 2)

You have a Microsoft 365 subscription. Users have devices that run Windows 11.

You plan to create a Microsoft Purview insider risk management policy that will detect when a user performs the following actions:

- Deletes files that contain a sensitive information type (SIT) from their device
- Copies files that contain a SIT to a USB drive
- Prints files that contain a SIT

You need to prepare the environment to support the policy.
 What should you do?

- A. Configure the physical badging connector.
- B. Configure the HR data connector.
- C. Create a Microsoft Purview communication compliance policy.
- D. Onboard the devices to Microsoft Purview.

Answer: D

Explanation:

To ensure that Microsoft Purview Insider Risk Management can detect file deletions, USB copies, and print actions on sensitive information, you must onboard the Windows 11 devices to Microsoft Purview.
 Device onboarding enables endpoint activity monitoring, allowing Purview to track and log user activities such as file deletions, USB transfers, and printing of sensitive files. Once onboarded, the Insider Risk Management policy can analyze these activities and generate risk alerts when sensitive information types (SITs) are involved.

NEW QUESTION 9

- (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 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 10

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	Exchangelitem	MailboxLogin	None	90 Days
20	AuditRetention2	Exchangelitem	Send, MailItemsAccessed	User1	9 Months
30	AuditRetention3	Sharepoint	None	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	None	10 Years

The users perform the following actions:

User1 renames a Microsoft SharePoint Online site. User2 sends an email message.

How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1 renames a SharePoint site:

User2 sends an email message:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The action "SiteRenamed" for SharePoint is covered under the AuditRetention4 policy, which applies to User1 and retains logs for 9 months. The action "Send" for ExchangeItem is covered under the AuditRetention2 policy, but this policy applies only to User1. Since User2 is not covered under a specific policy, the default retention period for audit logs in Microsoft Purview is 90 days.

NEW QUESTION 15

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1. You plan to create the items shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Which items can use Trainable 1?

- A. Label2 only
- B. Label1 and Label2 only
- C. Label1 and Policy1 only
- D. Label2, Policy1, and DLP1 only
- E. Label1, Label2, Policy1, and DLP1

Answer: D

Explanation:

A trainable classifier in Microsoft Purview is used to automatically identify and classify unstructured data based on content patterns. The classifier can be used in:

- * 1. Retention Labels (Label2) Supported
Trainable classifiers can be linked to retention labels to automatically classify and apply retention policies to documents.
- * 2. Retention Label Policies (Policy1) Supported
Retention label policies define how and where retention labels are applied, including automatically using trainable classifiers.
- * 3. Data Loss Prevention (DLP) Policies (DLP1) Supported
Trainable classifiers can be used in DLP policies to detect and protect sensitive content automatically.

NEW QUESTION 17

- (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 ⓘ 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

<input checked="" type="checkbox"/>	Copy to clipboard	ⓘ	Audit only ▾
<input checked="" type="checkbox"/>	Copy to a USB removable media	ⓘ	Audit only ▾
<input checked="" type="checkbox"/>	Copy to a network share	ⓘ	Audit only ▾
<input checked="" type="checkbox"/>	Print	ⓘ	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 19

- (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 21

HOTSPOT - (Topic 2)

You have a Microsoft 365 subscription.

You plan to deploy an audit log retention policy.

You need to perform a search to validate whether the policy will be applied to the intended entries.

Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Search

[Learn about audit](#)

The screenshot shows the 'Search' configuration interface with the following sections:

- Searches completed:** 0
- Active searches:** 0
- Active unfiltered searches:** 0
- Date and time range (UTC) *:** Start (Aug 00:00), End (Aug 00:00)
- Activities - friendly names:** Choose which activities to search ...
- Activities - operation names:** Enter operation values, separated by ...
- Users:** Add the users whose audit logs you ...
- File, folder, or site:** Enter all or a part of the name of a fil...
- Keyword Search:** Enter the keyword to search for
- Record types:** Select the record types to search f...
- Workloads:** Enter the workloads to search for
- Admin Units:** Choose which Admin Units to se...
- Search name:** Give the search a name

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To validate whether an audit log retention policy will apply to the intended entries, you should configure the following fields:

Date and time range (UTC) ensures that you are searching for audit logs within the time period when the policy should be applied. Audit logs are time-sensitive, and policies affect logs based on their timestamp.

Record types allows you to filter and search for specific audit log categories (e.g., Exchange, SharePoint, Teams, etc.) that are affected by the retention policy. Selecting the correct record type ensures that the policy is evaluated against the relevant data.

NEW QUESTION 26

- (Topic 2)

You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.

You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.

You need to identify and categorize the resumes. The solution must minimize administrative effort.

What should you include in the solution?

- A. a trainable classifier
- B. a keyword dictionary
- C. a function
- D. an exact data match (EDM) classifier

Answer: A

Explanation:

Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice.

Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.

Final Approach:

Train a trainable classifier using sample resumes. Deploy the classifier in Microsoft Purview.

Configure a sensitivity label to be automatically applied when a document matches the classifier.

NEW QUESTION 31

- (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 33

- (Topic 2)

You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.

You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:

If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.

All other users must be blocked from copying the file. What should you create?

- A. one DLP policy that contains one DLP rule
- B. one DLP policy that contains two DLP rules
- C. two DLP policies that each contains one DLP rule

Answer: B

Explanation:

To meet the requirements, you need one DLP policy with two separate DLP rules to handle the different conditions:

- * 1. First DLP Rule (For Group1 Members): If the user is a member of Group1 and attempts to copy a file with sensitive data to a USB storage device. Allow the file copy but log the event in the audit log.
- * 2. Second DLP Rule (For All Other Users): If any user who is NOT in Group1 attempts to copy a file with sensitive data to a USB storage device. Block the file transfer.

NEW QUESTION 35

- (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 38

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 41

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:

Data hashes
Data in the XML format
Digitally signed data

Use:

Azure Storage Explorer
EDM upload agent
Microsoft Purview portal
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 45

.....

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](#)