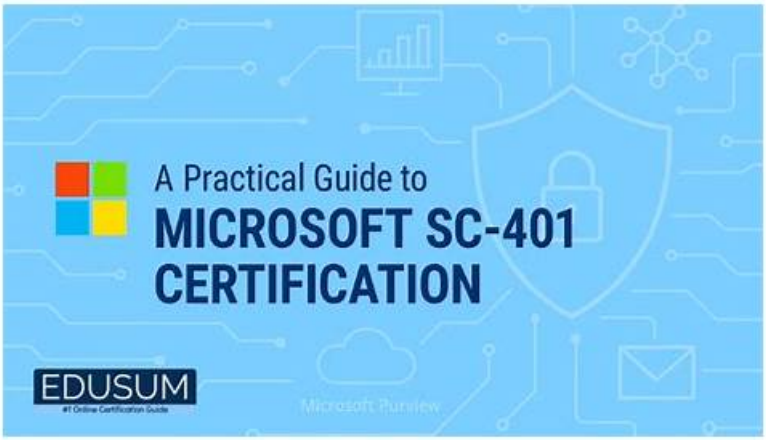
Microsoft SC-401 New Guide Files & Free SC-401 Learning Cram



P.S. Free 2026 Microsoft SC-401 dumps are available on Google Drive shared by PassCollection: https://drive.google.com/open?id=1ChwdkBcYjJI1h9U2DIynWoDbccFm-DmZ

It is similar to the SC-401 desktop-based software, with all the elements of the desktop practice exam. This mock exam can be accessed from any browser and does not require installation. The Microsoft SC-401 questions in the mock test are the same as those in the real exam. And candidates will be able to take the web-based Microsoft SC-401 Practice Test immediately through any operating system and browsers.

If you come to our website to choose our SC-401 real exam, you will enjoy humanized service. Firstly, we have chat windows to wipe out your doubts about our SC-401 exam materials. You can ask any question about our study materials. All of our online workers are going through special training. They are familiar with all details of our SC-401 Practice Guide. If you have any question, you can ask them for help and our services are happy to give you guide on the SC-401 learning quiz.

>> Microsoft SC-401 New Guide Files <<

Free SC-401 Learning Cram | Online SC-401 Tests

If you require any further information about either our SC-401 preparation exam or our corporation, please do not hesitate to let us know. High quality SC-401 practice materials leave a good impression on the exam candidates and bring more business opportunities in the future. And many of our cutomers use our SC-401 Exam Questions as their exam assistant and establish a long cooperation with us.

Microsoft SC-401 Exam Syllabus Topics:

Topic	Details
Topic 1	• Protect Data Used by AI Services: This section evaluates AI Governance Specialists on securing data in AI-driven environments. It includes implementing controls for Microsoft Purview, configuring Data Security Posture Management (DSPM) for AI, and monitoring AI-related security risks to ensure compliance and protection.
Topic 2	• Implement Information Protection: This section measures the skills of Information Security Analysts in classifying and protecting data. It covers identifying and managing sensitive information, creating and applying sensitivity labels, and implementing protection for Windows, file shares, and Exchange. Candidates must also configure document fingerprinting, trainable classifiers, and encryption strategies using Microsoft Purview.

Topic 3	• Implement Data Loss Prevention and Retention: This section evaluates Data Protection Officers on designing and managing data loss prevention (DLP) policies and retention strategies. It includes setting policies for data security, configuring Endpoint DLP, and managing retention labels and policies. Candidates must understand adaptive scopes, policy precedence, and data recovery within Microsoft 365.
Topic 4	• Manage Risks, Alerts, and Activities: This section assesses Security Operations Analysts on insider risk management, monitoring alerts, and investigating security activities. It covers configuring risk policies, handling forensic evidence, and responding to alerts using Microsoft Purview and Defender tools. Candidates must also analyze audit logs and manage security workflows.

Microsoft Administering Information Security in Microsoft 365 Sample Questions (Q210-Q215):

NEW QUESTION # 210
Case Study 1 - Contoso, Ltd
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.
Existing Environment
Microsoft 365 Environment
Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.
Users store data in the following locations:
- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages
When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.
SharePoint Online Environment
Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.
Site2 contains the files shown in the following table.
Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.
Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:
- Name: Site4RetentionPolicy1
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created
- Name: Site4RetentionPolicy2
Locations to apply the policy: Site4
Retain items for a specific period: 4 years
Start the retention period based on: When items were created
At the end of the retention period: Do nothing
Problem Statements
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.
Requirements
Planned Changes
Contoso plans to create the following data loss prevention (DLP) policy:
- Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements
Contoso must meet the following technical requirements:
- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.
- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.
Drag and Drop Question
You need to meet the technical requirements for the Site1 documents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:

Explanation:
Explanation:
Create a retention label. -> Has nothing to do with information protection.
Create a sensitive info type. -> Not needed because for credit cards, there is a built-in one.

NEW QUESTION # 211
You have a Microsoft 365 E5 subscription. The subscription contains a user named User1 and the sensitivity labels shown in the following table.
You publish the labels to User1.
The subscription contains the files shown in the following table.
Which files can Microsoft 365 Copilot summarize for User1?

- A. File3 only
- B. File2 only
- C. File2 and File3 only
- D. File1, File2, and File3

Answer: B

Explanation:
For Microsoft 365 Copilot to summarize data within a file, the user must have both the EXTRACT and VIEW usage rights on the sensitivity label applied to that file, according to Microsoft Learn.
This ensures that Copilot can access and process the file's content for summarization purposes.
If a file is encrypted using Azure Rights Management without a sensitivity label, the same permissions (EXTRACT and VIEW) are still required for Copilot to function.
Reference:
https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data- protection-auditing

NEW QUESTION # 212
You have a Microsoft 36S ES subscription.
You need to create the Microsoft Purview insider risk management policies shown in the following table.
Which policy template should you use for each policy? To answer, drag the appropriate policy templates to the correct polices Each template 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..

Answer:

Explanation:

Explanation:

NEW QUESTION # 213
You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.
You have a custom employee information form named Template1 .docx.
You plan to create a sensitive info type named Sensitive! that will use the document fingerprint from Template1.docx.
What should you use to create Sensitive1, and in which DLP policies can you use Sensitive1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:
Step 1 - Requirement
You want to create a custom sensitive info type named Sensitive1.
This SIT will be created from a document fingerprint of Template1.docx.
You then want to use Sensitive1 in DLP policies.
Step 2 - Where do you create custom Sensitive Info Types?
Custom SITs (including document fingerprinting) can only be created in the Microsoft Purview compliance portal.
They cannot be created in the Exchange admin center, SharePoint admin center, or directly in PowerShell.
Answer for creation: The Microsoft Purview portal
Reference: Create a custom sensitive information type with document fingerprinting Step 3 - Where can custom Sensitive Info Types be used?
Once created, custom SITs are tenant-wide and can be used across all workloads that support DLP:
Exchange email
SharePoint Online sites
OneDrive
Teams chat and channel messages
In the table, the DLP policies are:
DLP1 # Exchange Online email
DLP2 # SharePoint Online sites
DLP3 # Teams chat and channel messages
Since Sensitive1 is a custom SIT, it can be used in all three policies.
Answer for usage: DLP1, DLP2, and DLP3

NEW QUESTION # 214
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 # 215
......