MICROSOFT

SC-401

Administering Information Security in Microsoft 365 (SC-401) Exam Questions & Answers

Total Questions: **05**

Click Here to Get All Microsoft Exam Questions →

https://itexamsquiz.com/product/sc-401-practice-tests/

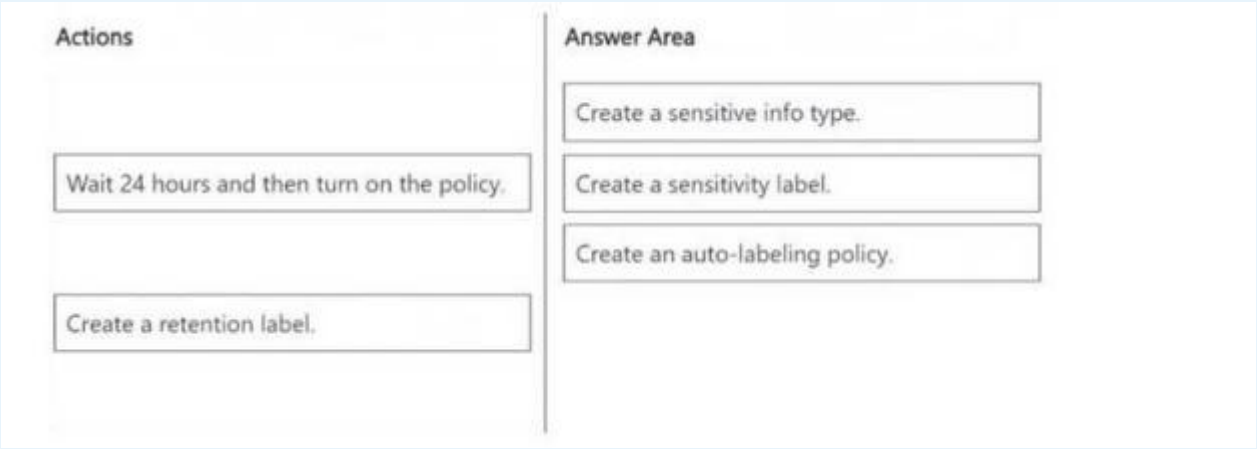
About ITExamsQuiz

Question: 1		ITExamsQuiz

DRAG DROP
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:



The goal is to automatically label documents in Site1 that contain credit card numbers. To achieve this, we need a sensitivity label with an auto-labeling policy based on a sensitive info type that detects credit card numbers.
Step 1: Create a Sensitive Info Type
● A sensitive info type is needed to detect credit card numbers in documents.
● Microsoft Purview includes built-in sensitive info types for credit card numbers, but we can also create a custom one if necessary.
Step 2: Create a Sensitivity Label
● A sensitivity label is required to classify and protect documents containing sensitive information.
● This label can apply encryption, watermarking, or access controls to credit card data.
Step 3: Create an Auto-Labeling Policy
● An auto-labeling policy ensures that the sensitivity label is applied automatically when credit card numbers are detected in Site1.
● This policy is configured to scan files and automatically apply the correct sensitivity label.

Question: 2 ITExamsQuiz

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:

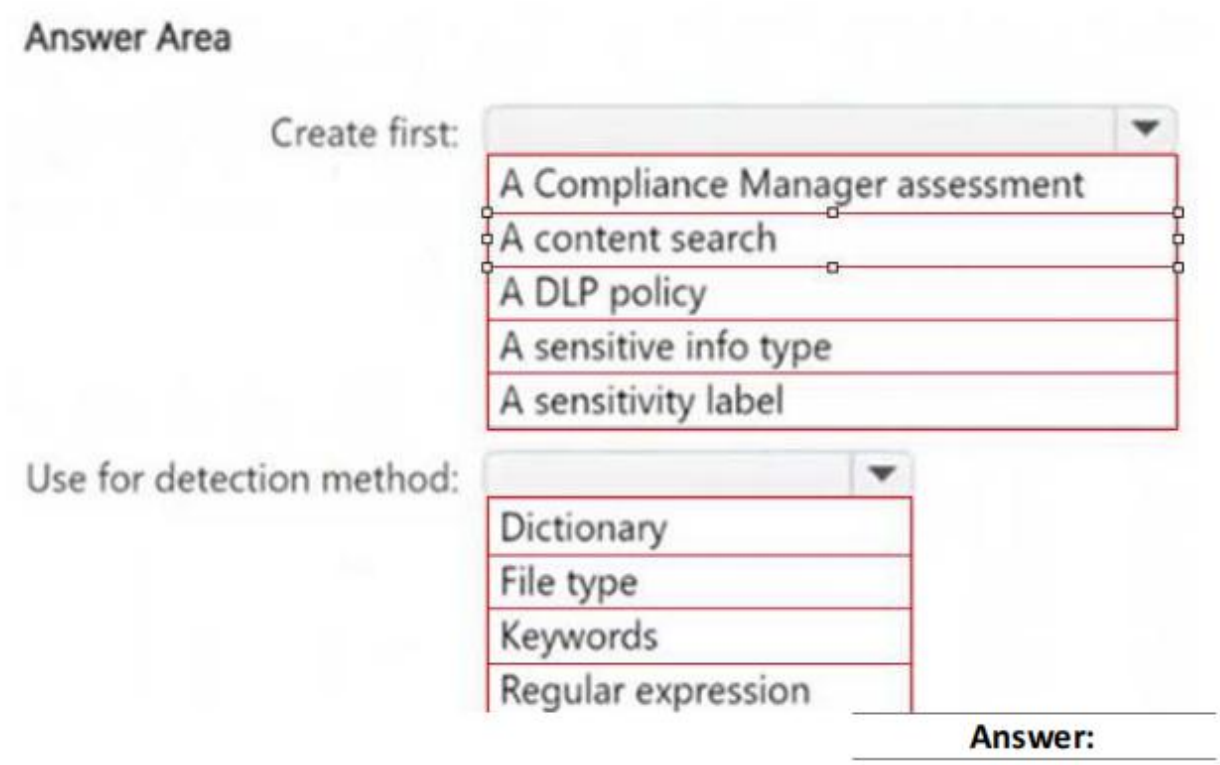
Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	□ No, read-only permissions.
Admin2	Compliance Data Administrator	□ Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	□ Yes, has full compliance management, including labels.
Admin4	Security Operator	□ 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).

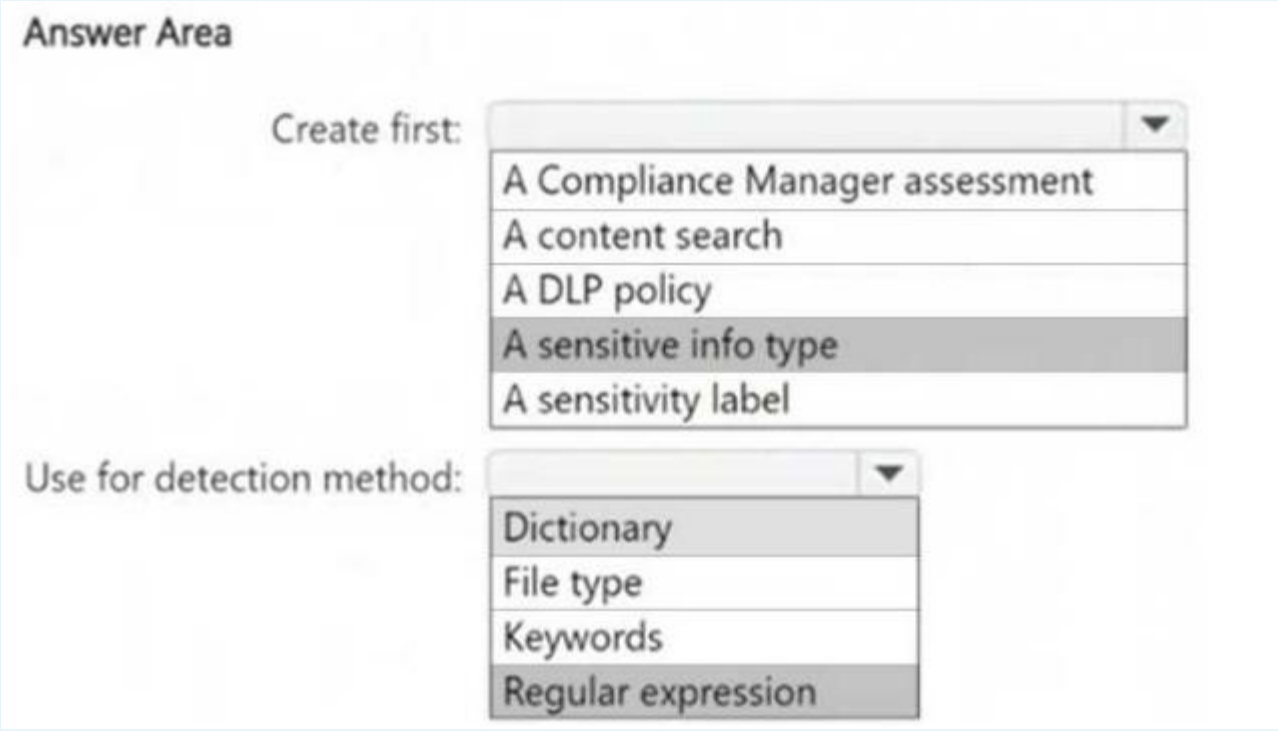
Question: 3 ITExamsQuiz

HOTSPOT

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.



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".

Question: 4 ITExamsQuiz

HOTSPOT
How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

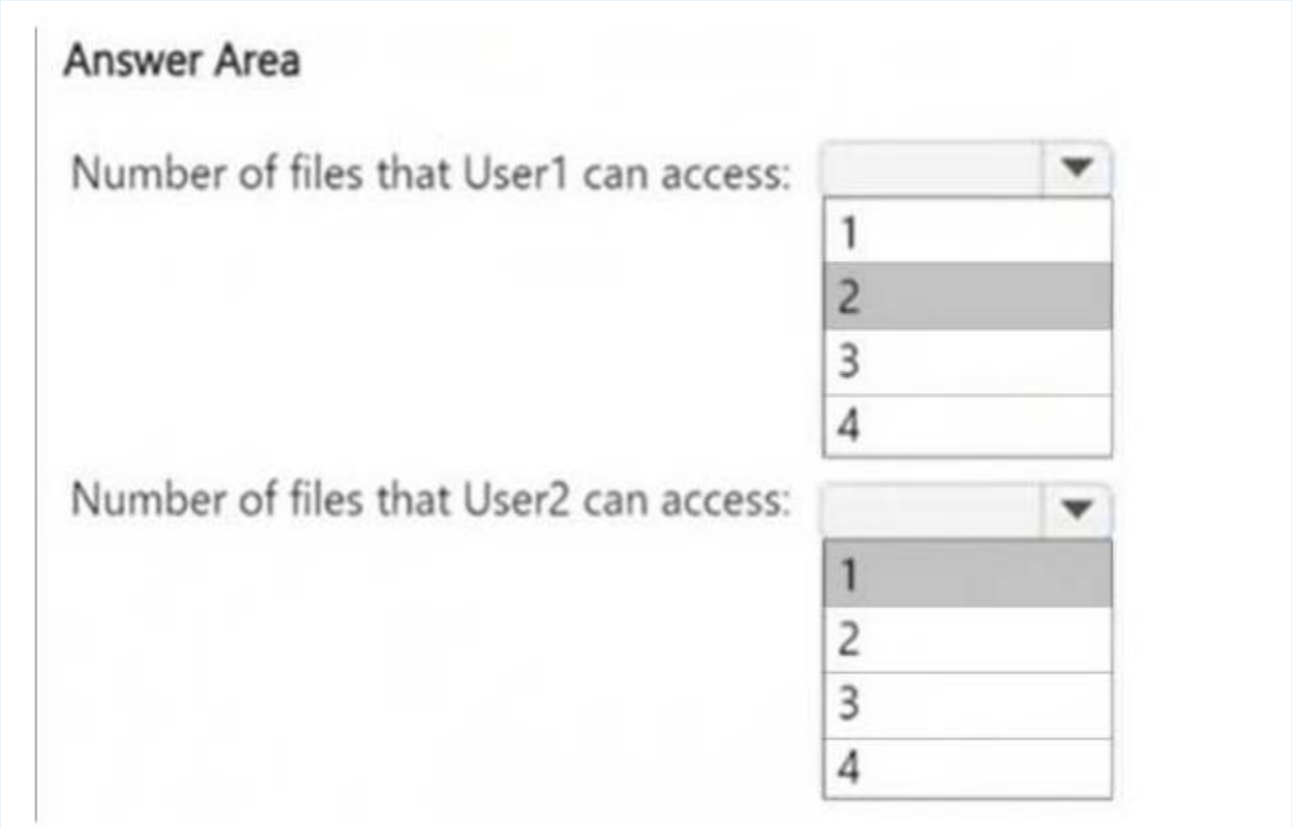
Answer Area

Number of files that User1 can access:
- 1
- 2
- 3
- 4

Number of files that User2 can access:
- 1
- 2
- 3
- 4

Answer:

Explanation:



Understanding DLP Policy Impact on File Access

The DLP policy (DLPpolicy1) applies to Site2 and restricts access when:

- Content contains SWIFT Codes.
- Instance count is 2 or more.

File Analysis (Based on SWIFT Codes Count)

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	□ No restriction (SWIFT codes < 2)
File2.bmp	4	□ Restricted (SWIFT codes ≥ 2)
File3.txt	3	□ Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	□ Restricted (SWIFT codes ≥ 2)

Files that remain accessible (not restricted by DLP):

- File1.docx (Contains only 1 SWIFT Code → Below restriction threshold)

User access after DLP policy is applied:

User	Role in Site2	Access Rights	Can Access Files?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.docx only

User1 (Site Owner):

- Has higher privileges and can override DLP restrictions (through admin intervention).
- Can access 2 files (File1.docx + override access to another file).

User2 (Site Visitor):
- Has read-only access but DLP blocks access to restricted files.
- Can only access 1 file (File1.docx), since all others are restricted.

Question: 5		ITExamsQuiz

HOTSPOT
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.	○	○

Answer:

Explanation:

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.	○	●

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