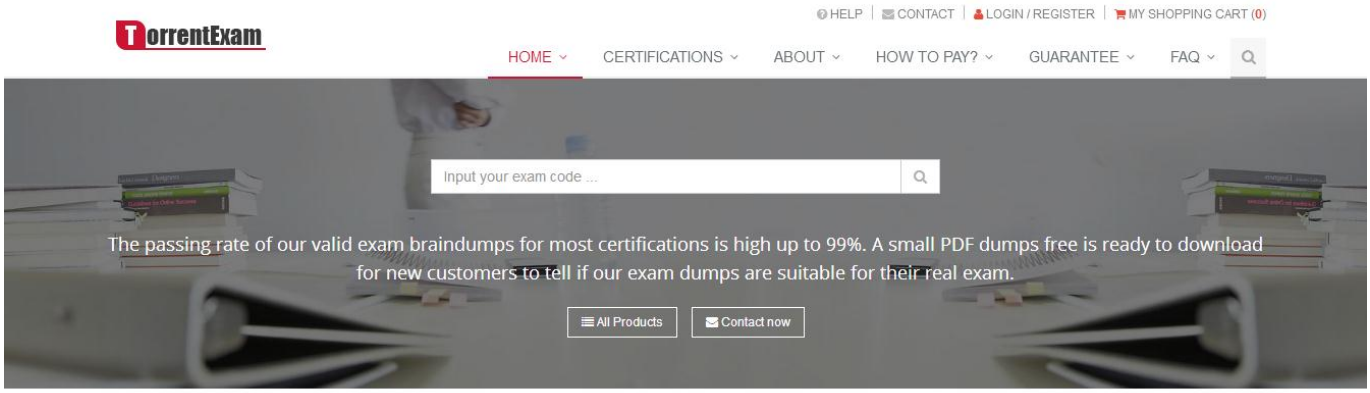
TorrentExam



Why Choose Us

QUALITY AND VALUE

RealExamFree Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.

TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

EASY TO PASS

If you prepare for the exams using our RealExamFree testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

TRY BEFORE BUY

RealExamFree offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

Customer Reviews

I wasted a lot of money and failed twice. Thanks to HPE0-J78 exam collection I pass now.

Noel

realexamfree is a reliable company. I pass exam at first shot. Many thanks

Julie

Pass BIMF.EN successfully. Really good dumps. It saves me a lot of time. Wonderful!

Ahern

online test engine is very useful for me,because i could practice the C-TERP10-67 question dumps in my phone when i was waititng or on the bus even without internet,i could make the most of my time.Last week,i passed the C-TERP10-67. so i want to share the realexamfree with you guys,hope you will get a good result in test.

Carl

http://www.torrentexam.com

Best Exam Bootcamp & Excellent VCE Torrent & Satisfying Dumps Torrent

Exam : **SC-401**

Title : Administering Information Security in Microsoft 365

Vendor : Microsoft

Version : DEMO

NO.1 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.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

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.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

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.
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: B

Explanation:
Permissions required to create and manage sensitivity labels:
"Another option is to add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group."
https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels

NO.2 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.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

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.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

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.
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:
If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Yammer locations.
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide#create-and-configure-a-retention-policy

NO.3 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.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

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.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

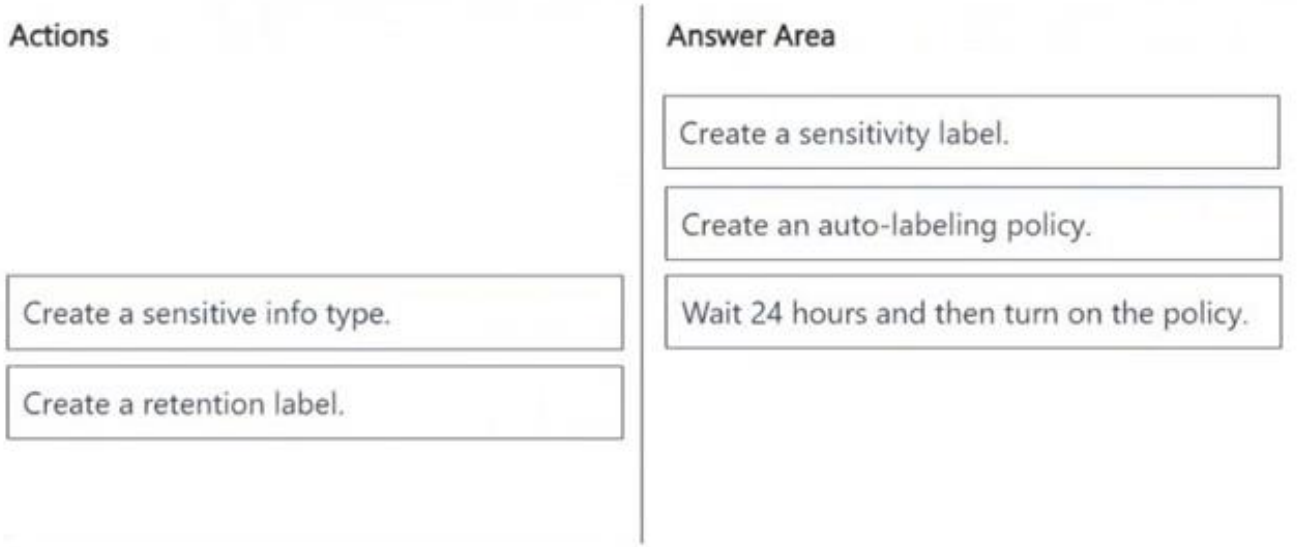
User	Role
User1	Site owner
User2	Site visitor

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:
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.

NO.4 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.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

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.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

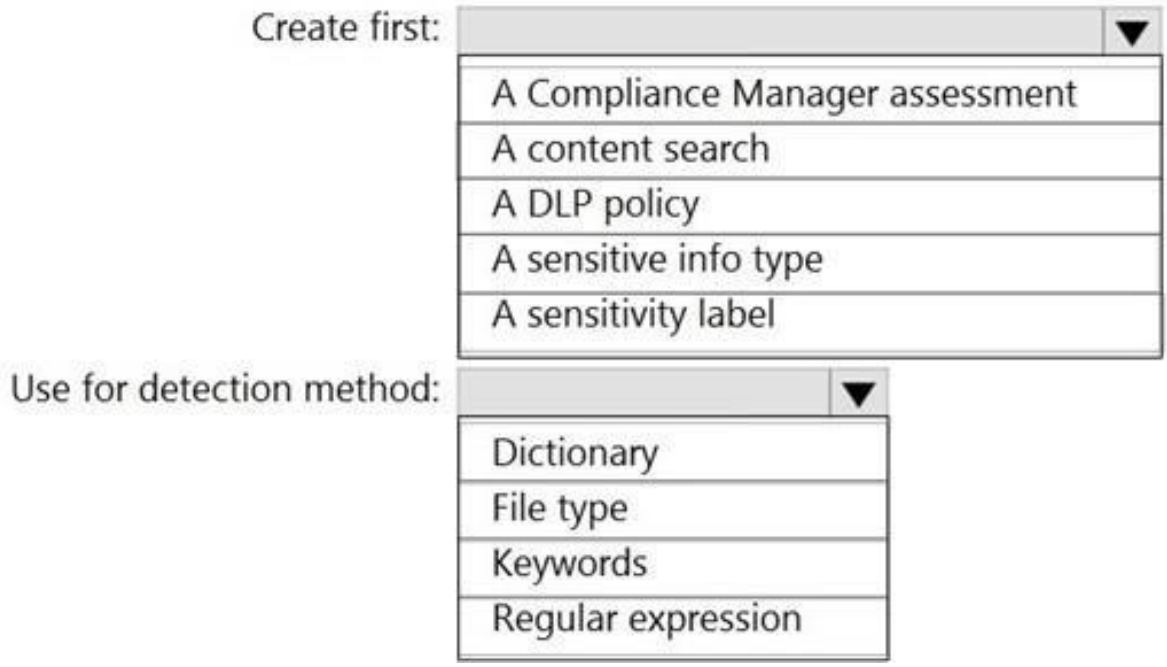
Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder

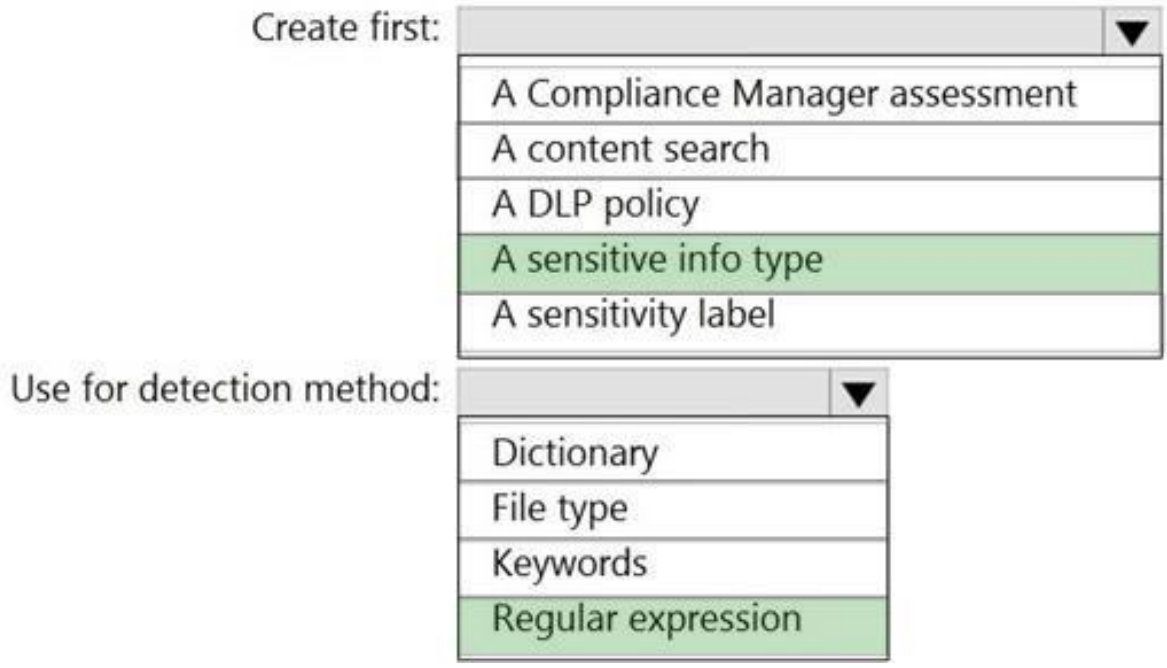
hierarchy based on the project.
Site4 has the following two retention policies applied:
- Name: Site4RetentionPolicy1
Locations to apply the policy: Site4
Delete items older than: 2 years
Delete content based on: When items were created
- Name: Site4RetentionPolicy2
Locations to apply the policy: Site4
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.
Hotspot Question
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.

Answer Area



Answer:

Answer Area



Explanation:
Sensitive information types :
Identifies sensitive data by using built-in or custom regular expressions or a function.
Corroborative evidence includes keywords, confidence levels, and proximity.
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

NO.5 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.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

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.

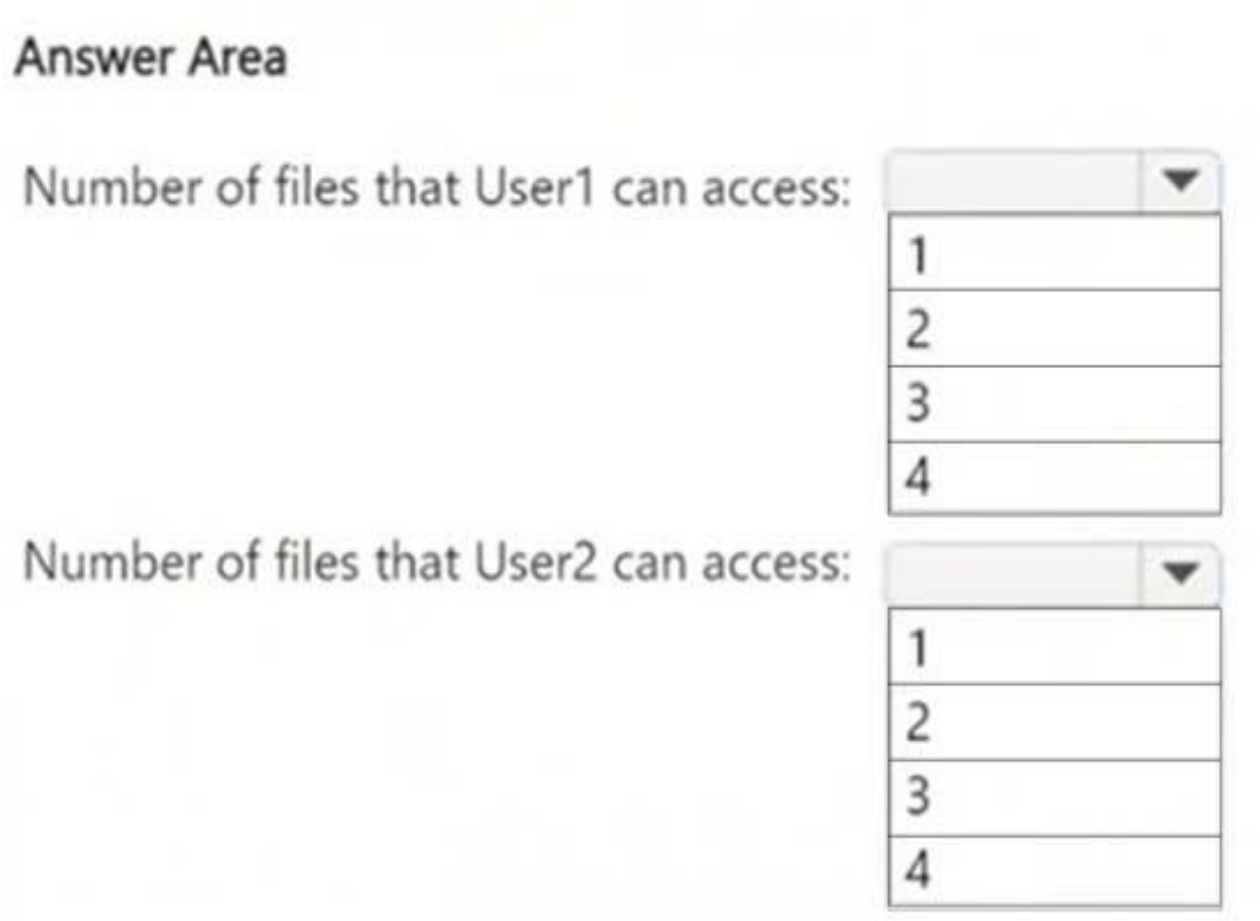
Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

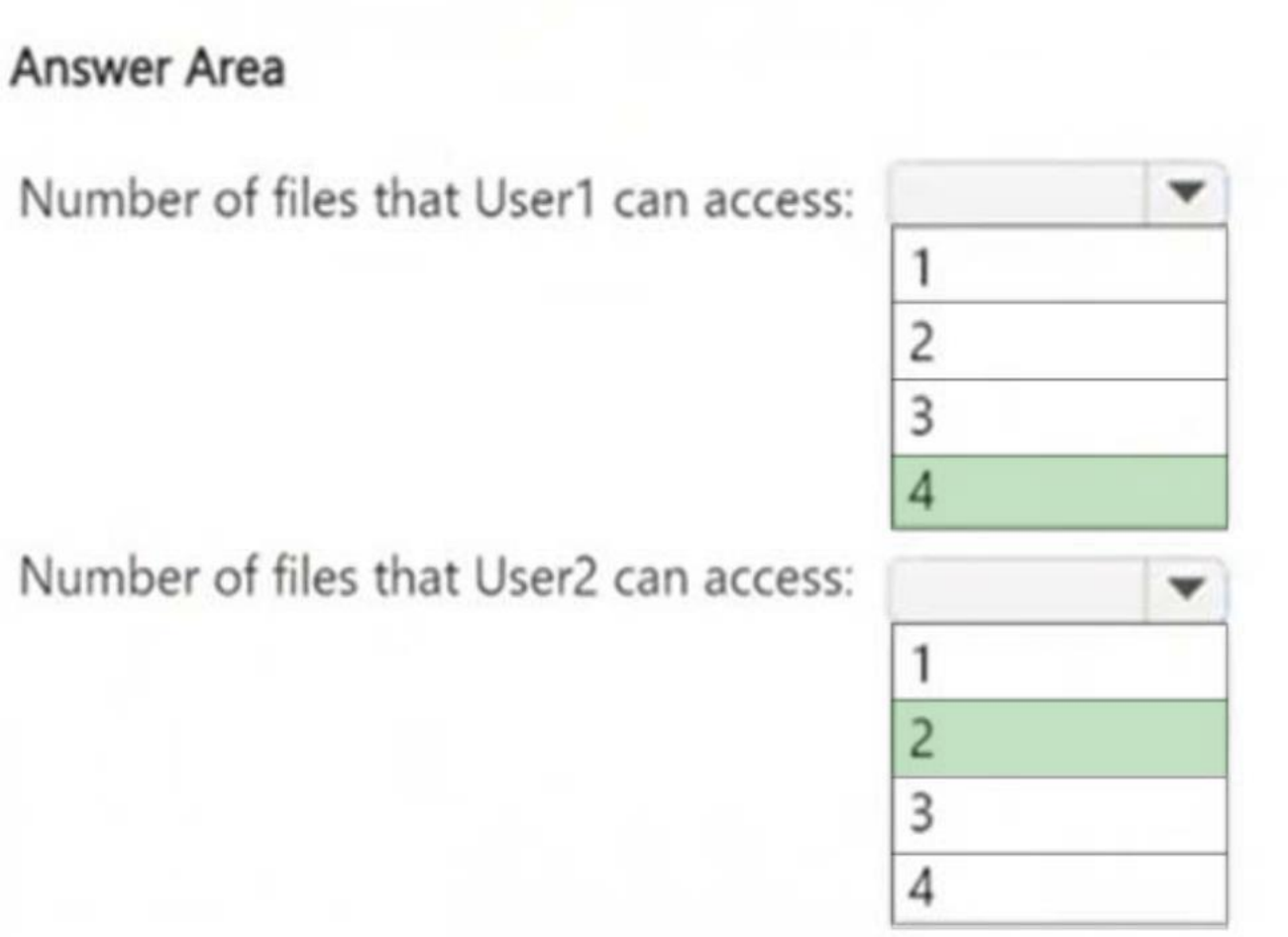
User	Role
User1	Site owner
User2	Site visitor

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.
Hotspot Question
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:
User 1 (Site Owner) - 4 Files
User 2 (Site Visitor) 2 Files
Any item that makes it through the conditions filter has any actions that are defined in the rule applied to it. You have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action, you need to choose from these options:
Block users from accessing shared SharePoint, OneDrive, and Teams content Block everyone. Only the content owner, last modifier, and site admin will continue to have access Block only people from outside your organization. Users inside your organization continue to have access.
Encrypt email messages (applies only to content in Exchange)
The actions that are available in a rule depend on the locations that have been selected. The available actions for each individual location are listed below.
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions

NO.6 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.

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

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.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

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.
Hotspot Question
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:

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.	○	●

Explanation:
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").
Box 1 - Yes, because Site4RetentionPolicy2 ensures files are retained for 4 years.
Box 2 - Yes, because Site4RetentionPolicy2 retains the file for 4 years (until January 1, 2025).
Box 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.

NO.7 You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents.
You plan to implement Microsoft 365 Copilot for the subscription.
You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users.
What should you use?
A. data loss prevention (DLP)
B. Microsoft Purview insider risk management
C. Microsoft Purview Information Barriers (IBs)
D. sensitivity labels
Answer: D
Explanation:

To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels.
Sensitivity labels allow you to classify, protect, and restrict access to sensitive files. You can configure label-based encryption and access control policies to ensure that only authorized users can access or interact with the files in Channel1. Microsoft 365 Copilot respects sensitivity labels, meaning if a file is labeled with restricted permissions, Copilot will not use it in generated responses for unauthorized users.

NO.8 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:
If content grants a user VIEW usage rights but not EXTRACT:
Copilot won't summarize this content but can reference it with a link so the user can then open and view the content outside Copilot.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

NO.9 You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online.
What should you use?
A. the Microsoft Purview portal
B. the Microsoft Entra admin center
C. the SharePoint admin center
D. the Microsoft 365 admin center
Answer: C
Explanation:
To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center Settings Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

NO.10 You have a Microsoft 365 subscription.
You need to customize encrypted email for the subscription. The solution must meet the following requirements.
- Ensure that when an encrypted email is sent, the email includes the company logo.
- Minimize administrative effort.

Which PowerShell cmdlet should you run?

A. Set-IRMConfiguration

B. Set-OMEConfiguration

C. Set-RMSTemplate

D. New-OMEConfiguration

Answer: B

Explanation:

To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set-OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as:

- Company logo
- Custom text
- Background color

This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

NO.11 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

NO.12 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.

NO.13 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:
With 1 policy you cannot choose both Audit and Block.
You need 1 policy for all users with block rule, and exclude group1 and 1 policy that includes group1 only and the rule set to Audit only.

NO.14 You have a Microsoft 365 subscription.
You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From Microsoft Defender for Cloud Apps, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint ad min center, modify the records management settings.
D. From the Microsoft Purview portal, publish a label.
E. From the Microsoft Purview portal, create a label.
Answer: DE
Explanation:

To allow users to apply retention labels to individual documents in Microsoft SharePoint libraries, you need to create a retention label and publish the label.
In Microsoft Purview, retention labels define how long content should be retained or deleted. You must first create a label that specifies the retention rules. After creating the label, you must publish it so that it becomes available for users in SharePoint document libraries. Once published, users can manually apply the retention label to individual documents.

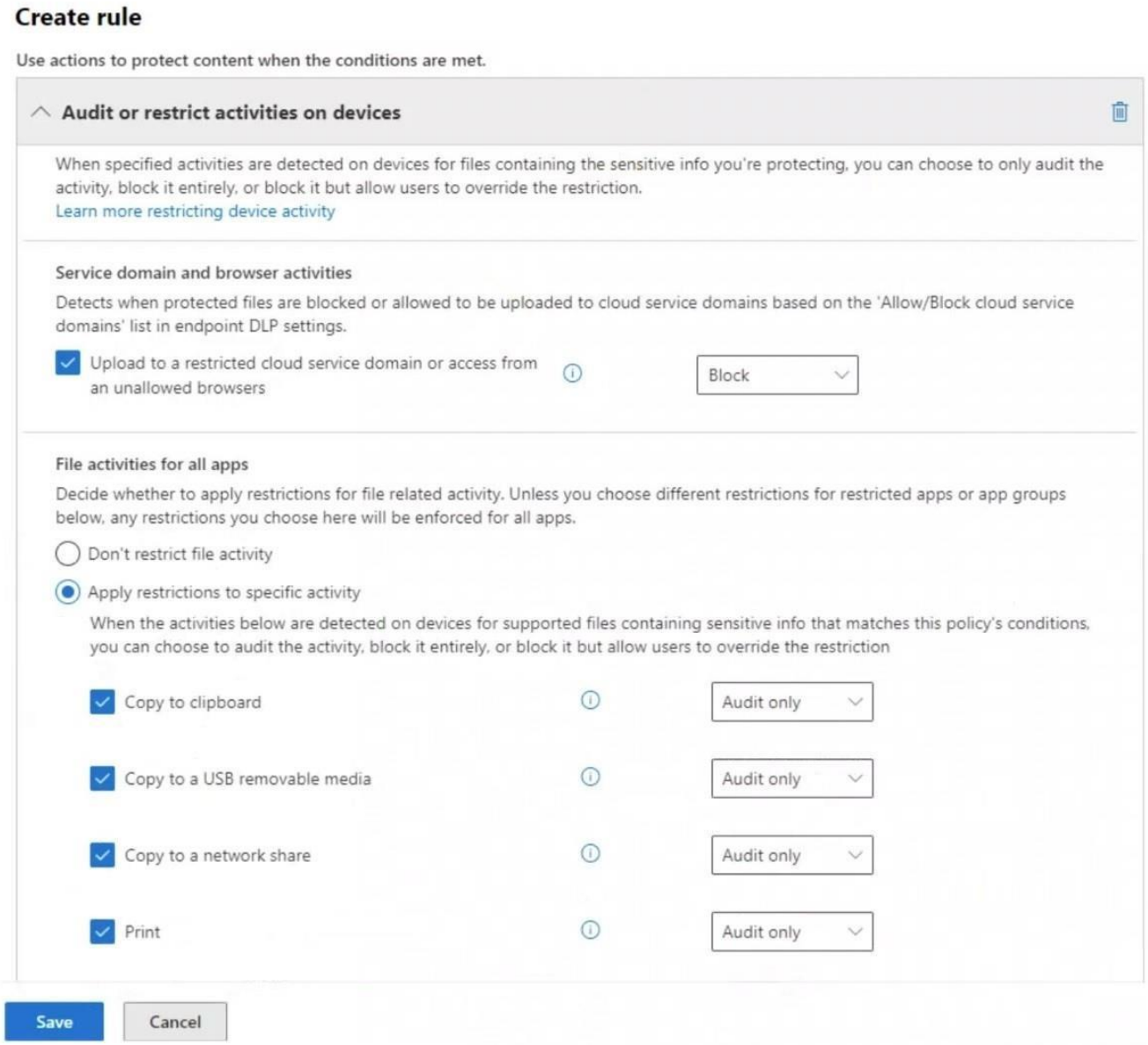
NO.15 You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to implement Microsoft Purview data lifecycle management.
What should you create first?
A. a sensitivity label policy
B. a data loss prevention (DLP) policy
C. an auto-labeling policy
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.

NO.16 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: B
Explanation:
If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Yammer locations.
https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention#create-and-configure-a-retention-policy

NO.17 You have a data loss prevention (DLP) policy configured for endpoints as shown in the

following exhibit.



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:

Detects when a user attempts to upload an item to a restricted service domain or access an item

through a browser. If they are using a browser that is listed in DLP as an unallowed browser, the upload activity will be blocked and the user is redirected to use Microsoft Edge . Microsoft Edge will then either allow or block the upload or access based on the DLP policy configuration So if unallowed browser is NOT configured you can use chrome/etc with impugnity anc won't be kicked over to edge which observes the DLP policy, in other words, sometimes can upload (chrome), sometimes can not (edge).

NO.18 You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	• Exchange email (All recipients) • SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1.
You need to modify RP1.
Which two modifications can you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add locations to the policy.

B. Delete the policy.

C. Remove locations from the policy.

D. Decrease the retention period of the policy.

E. Disable the policy.

F. Increase the retention period of the policy.

Answer: AF

Explanation:
A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.
When a Preservation Lock is applied:
1. You cannot disable or delete the policy.
2. You cannot remove locations from the policy.
3. You cannot decrease the retention period.
4. You can add locations to the policy.
5. You can increase the retention period.
You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

NO.19 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: D
Explanation:
https://learn.microsoft.com/es-es/purview/endpoint-dlp-getting-started
https://learn.microsoft.com/en-us/purview/device-onboarding-macos-overview#before-you-begin

NO.20 You have a Microsoft 365 tenant.
You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.
You need to implement a data loss prevention (DLP) solution that meets the following requirements:
- Email messages that contain a single customer identifier can be sent outside your company.
- Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a sensitivity label
B. a sensitive information type
C. a DLP policy
D. a retention label
E. a mail flow rule

Answer: BC
Explanation:
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

NO.21 You have a Microsoft 365 E5 subscription.
You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:
- web1.contoso.com
- web2.contoso.com
The solution must minimize administrative effort.
To what should you set the Service domains setting for Endpoint DLP?

A. *.contoso.com

B. contoso.com

C. web1.contoso.com and web2.contoso.com

D. web*.contoso.com

Answer: C
Explanation:
The Service domains setting in Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) allows administrators to block or allow specific domains for file uploads. The goal is to prevent users from uploading DLP-protected documents to web1.contoso.com and web2.contoso.com.
Setting the Service domains to "web1.contoso.com and web2.contoso.com" precisely targets the two specific third-party websites, minimizing administrative effort while ensuring strict control.

NO.22 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.

NO.23 You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.
You have a document named Form.docx.
You plan to use PowerShell to create a document fingerprint based on Form.docx.
You need to first connect to the subscription.
Which cmdlet should you run?

A. Connect-IPPSSession

B. Connect-SPOService

C. Connect-ExchangeOnline

D. Connect-MgGraph

Answer: A
Explanation:
Currently, you can create a document fingerprint only in Security & Compliance PowerShell, and Connect-IPPSSession is how you connect to it.
https://learn.microsoft.com/en-us/purview/document-fingerprinting#create-a-custom-sensitive-information-type-based-on-document-fingerprinting-using-powershell
https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

NO.24 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:
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. a CSV file that contains words separated by commas
2. a text file that has one word on each line
Other incorrect answer options you may see on the exam include the following:
- a TSV file that contains words separated by tabs
- an XLSX file that contains one word in each cell of the first row
- a DOCX file that has one word on each line
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide

NO.25 Your company has a Microsoft 365 tenant.
The company performs annual employee assessments. The assessment results are recorded in a document named AssessmentTemplate.docx that is created by using a Microsoft Word template.
Copies of the employee assessments are sent to employees and their managers.
The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive folders. A copy of each assessment is also stored in a SharePoint Online folder named Assessments.
You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.
What should you include in the solution?
A. Create a fingerprint of AssessmentTemplate.docx.

B. Create a sensitive info type that uses Exact Data Match (EDM).
C. Import 100 sample documents from the Assessments folder to a seed folder.
D. Create a fingerprint of 100 sample documents in the Assessments folder.
Answer: A
Explanation:
It is just created document fingerprint using the template, this will be used as "Sensitive Info Type" to discover any employee assessment and apply the control over this file as required.

NO.26 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.

NO.27 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.

NO.28 You have a Microsoft 365 E5 tenant.

You need to add a new keyword dictionary.

What should you create?

A. a trainable classifier

B. a retention policy

C. a sensitivity label

D. a sensitive info type

Answer: D

Explanation:

Connect to the Microsoft Purview compliance portal.

Navigate to Classifications > Sensitive info types.

Select Create and enter a Name and Description for your sensitive info type, then select Next.

https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide