Number: SC-401
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: SC-401

Exam Name: Administering Information Security in Microsoft 365

Exam A

QUESTION 1
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.

Correct Answer: D, E
Section:
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.

QUESTION 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

Correct Answer: D
Section:
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.

QUESTION 3
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

Correct Answer: C
Section:
Explanation:
In Microsoft Purview Data Lifecycle Management, different Microsoft 365 locations require separate retention policies because they fall under different storage and compliance models.
Teams Chats & Teams Channel Messages (1 Policy) require a separate retention policy because Teams messages are stored differently than Exchange and SharePoint content. One policy can cover both Teams chats and Teams channel messages. Exchange Email (1 Policy) requires its own separate policy since emails are managed differently than Teams or SharePoint content. SharePoint Sites & Microsoft 365 Groups (1 Policy) are both stored in SharePoint Online, so they can be managed under one policy.

QUESTION 4
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.

- [x] 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

- [x] Copy to clipboard — Audit only
- [x] Copy to a USB removable media — Audit only
- [x] Copy to a network share — Audit only
- [x] Print — Audit only

Save Cancel

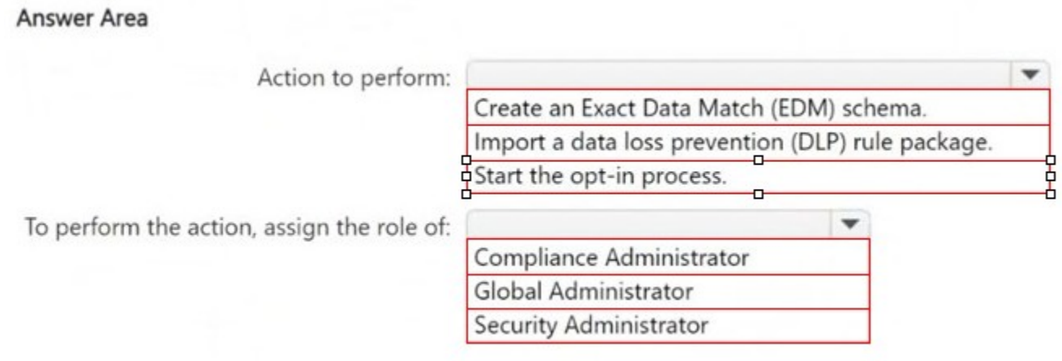
From a computer named Computer1, a user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.
What are two possible causes of the issue? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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.

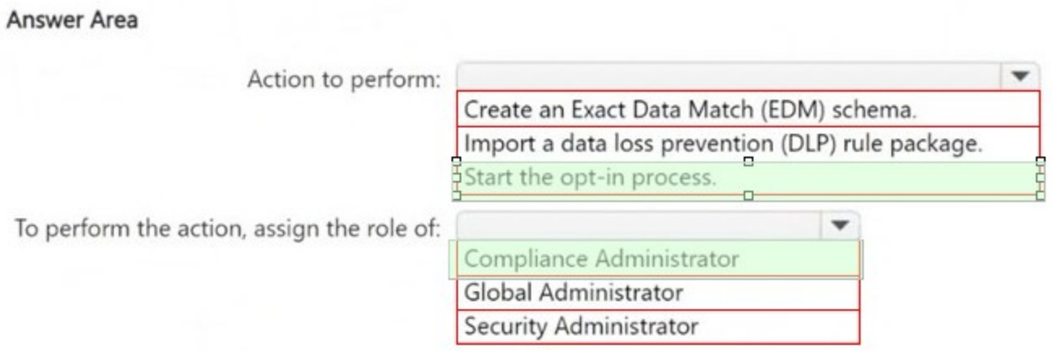
Correct Answer: A, B
Section:
Explanation:
The issue where users sometimes can upload files to cloud services and sometimes cannot suggests inconsistent enforcement of Endpoint DLP policies. This can be caused by the unallowed browsers in the Microsoft 365 Endpoint DLP settings are NOT configured. Also, 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.

QUESTION 5
HOTSPOT
You have a new Microsoft 365 E5 tenant.
You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.
What should you do first? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



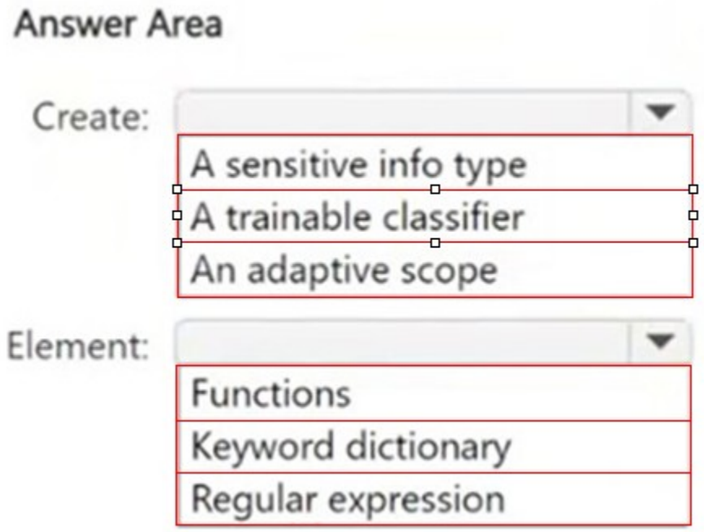
Answer Area:



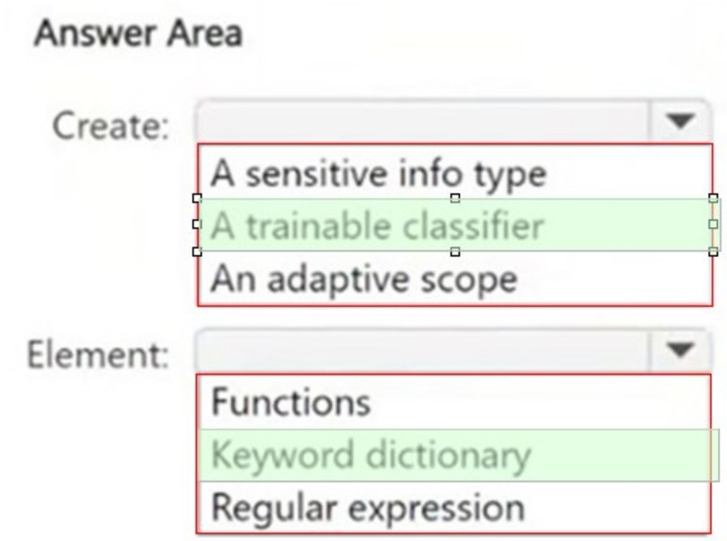
Section:
Explanation:

QUESTION 6
HOTSPOT
You have a Microsoft 365 E5 subscription.
You have a file named Customer.csv that contains a list of 1,000 customer names.
You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint Online library.
What should you create in the Microsoft Purview portal, and which type of element should you select? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:
Explanation:

QUESTION 7
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

Correct Answer: C
Section:
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.

QUESTION 8
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

Correct Answer: B
Section:
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.

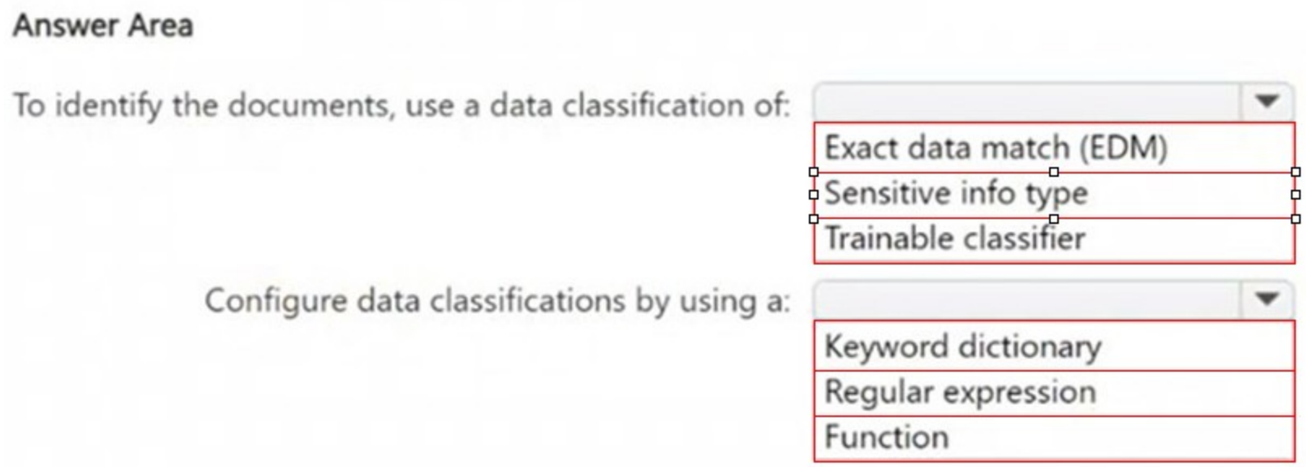
QUESTION 9
You have a Microsoft 365 E5 subscription.
You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.
What should you configure first?

A. a custom branding template
B. a mail flow rule
C. a sensitivity label
D. a Conditional Access policy

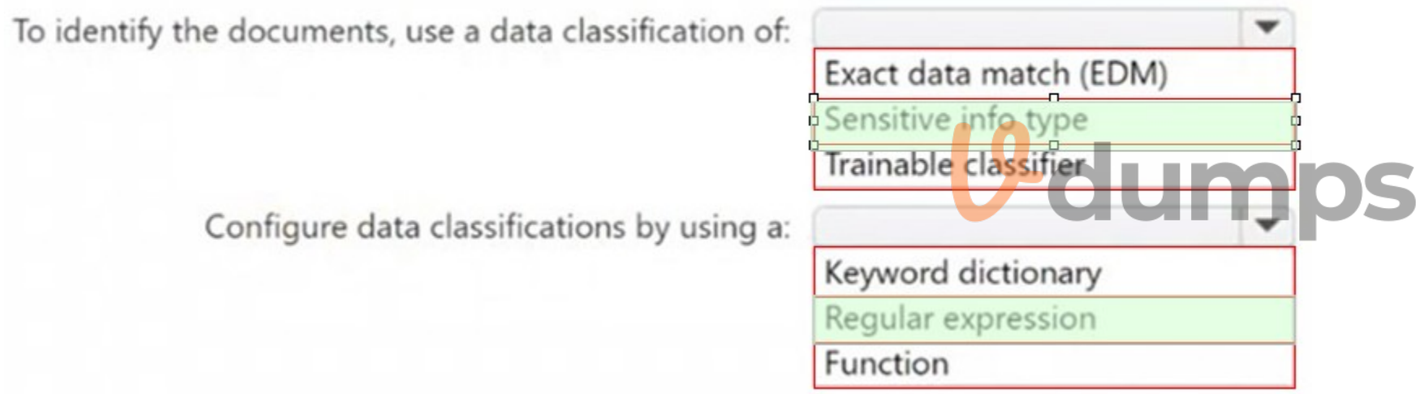
Correct Answer: C
Section:
Explanation:
To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection.
A sensitivity label allows you to encrypt 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

QUESTION 10
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:
Explanation:

QUESTION 11
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

Correct Answer: A
Section:

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.

QUESTION 12
HOTSPOT
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.

Hot Area:

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

Answer Area:

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

Section:
Explanation:

QUESTION 13
HOTSPOT
You have a Microsoft SharePoint Online site that contains the following files.

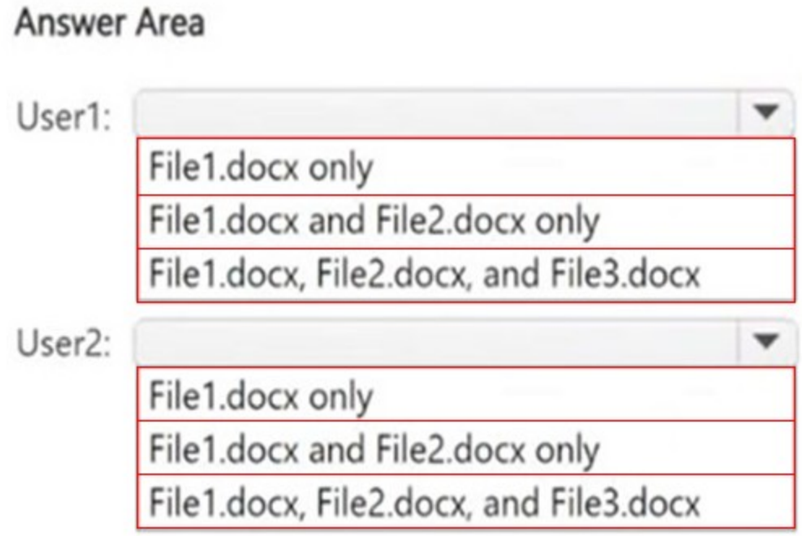
Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	*None*
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

Users are assigned roles for the site as shown in the following table.

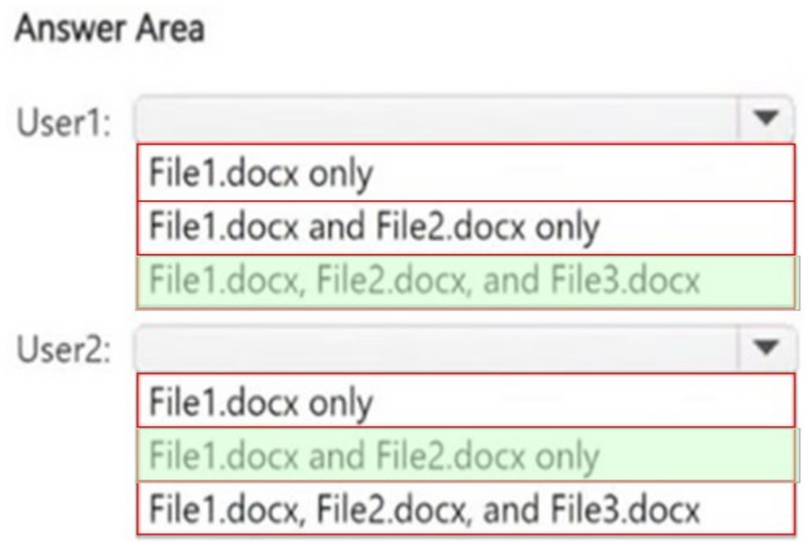
Name	Role
User1	Site owner
User2	Site member

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:
Explanation:

QUESTION 14
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

Correct Answer: B
Section:
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.

QUESTION 15
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.

Correct Answer: A, F
Section:
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.

QUESTION 16
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

Correct Answer: B
Section:
Explanation:
Microsoft 365 Endpoint data loss prevention (Endpoint DLP) is supported only on Windows 10 and Windows 11 devices. It does not support macOS or iOS at this time.
From the provided table:
Device1 (Windows 11) - Supported
Device2 (Windows 10) - Supported
Device3 (iOS) - Not supported
Device4 (macOS) - Not supported
Thus, only Device1 and Device2 support Endpoint DLP.

QUESTION 17
HOTSPOT
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.

Hot Area:

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

Answer Area:

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

Section:
Explanation:

QUESTION 18
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the device configurations shown in the following table.

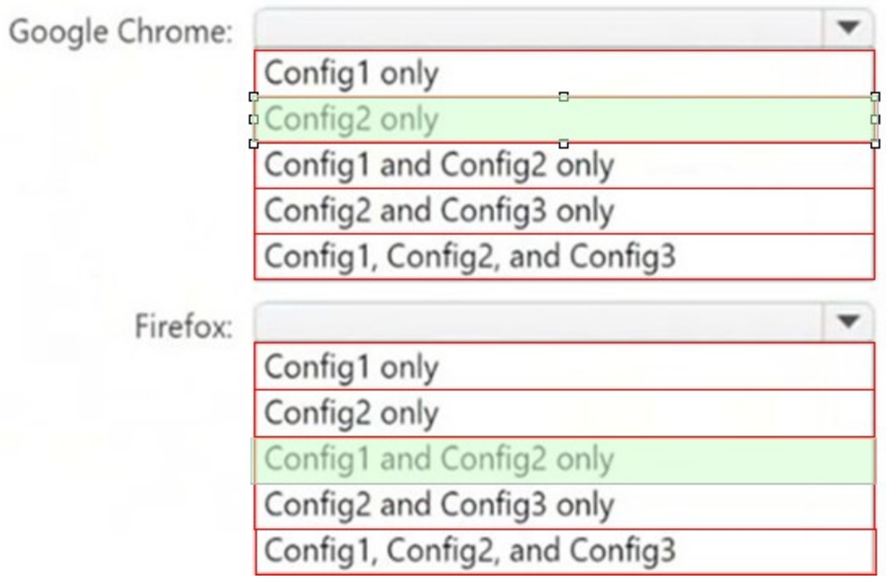
Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

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.

Hot Area:

Answer Area:

Answer Area



Section:
Explanation:

QUESTION 19
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.

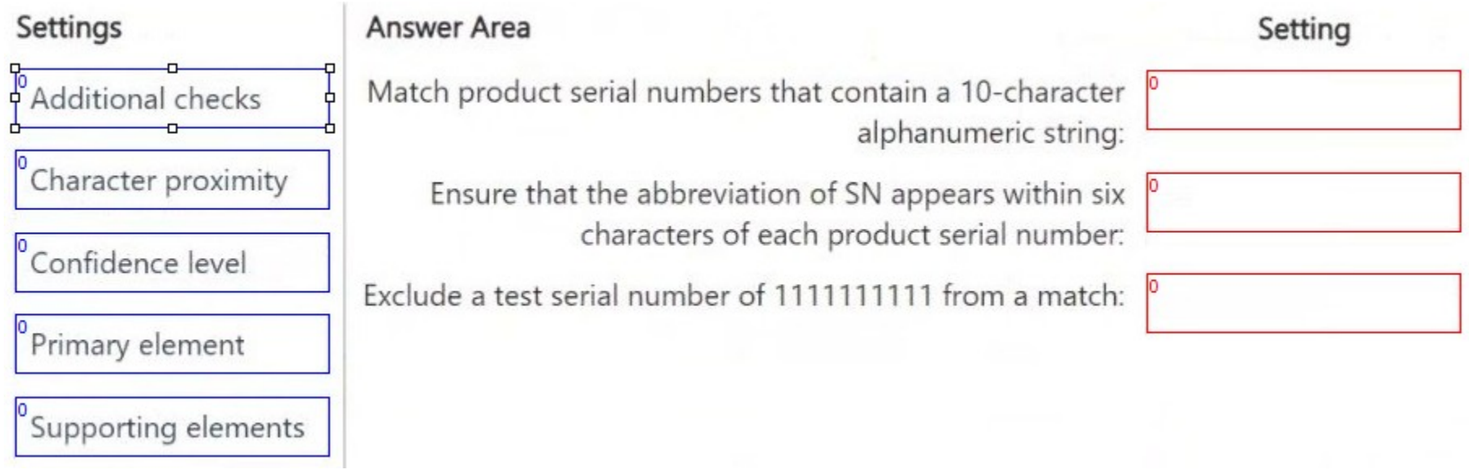
A. a sensitivity label
B. a sensitive information type
C. a DLP policy
D. a retention label
E. a mail flow rule

Correct Answer: B, C
Section:
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.

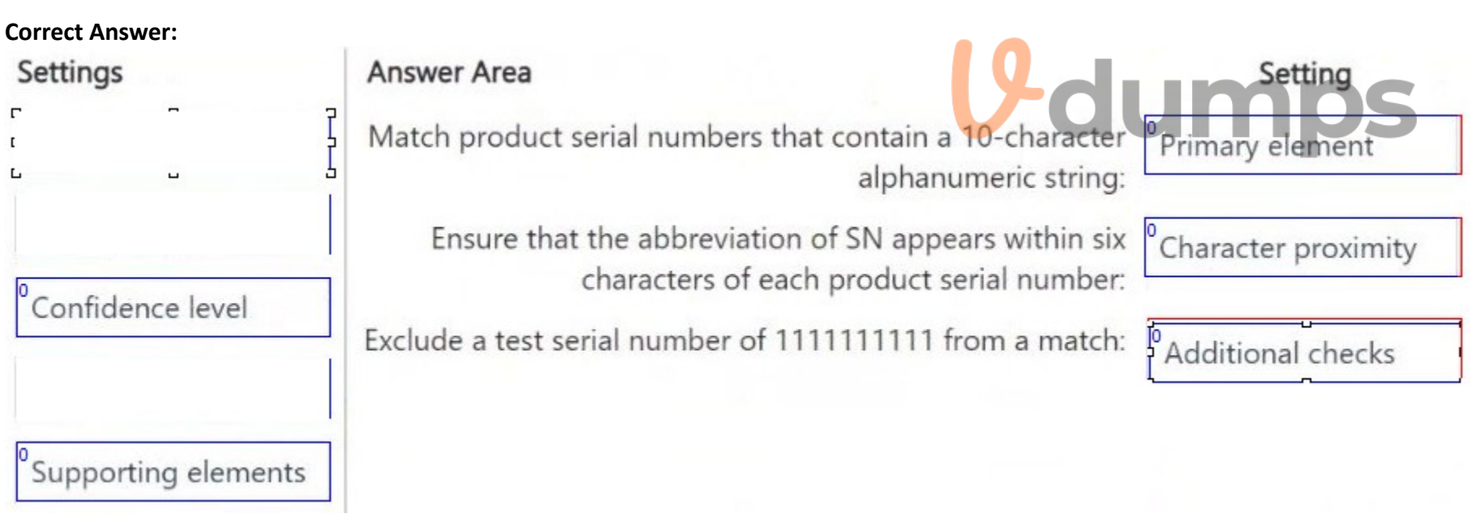
QUESTION 20
DRAG DROP
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You need to create a custom sensitive info type. The solution must meet the following requirements:
Match product serial numbers that contain a 10-character alphanumeric string.

Ensure that the abbreviation of SN appears within six characters of each product serial number.
Exclude a test serial number of 1111111111 from a match.
Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 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

Correct Answer: C
Section:
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.

QUESTION 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?

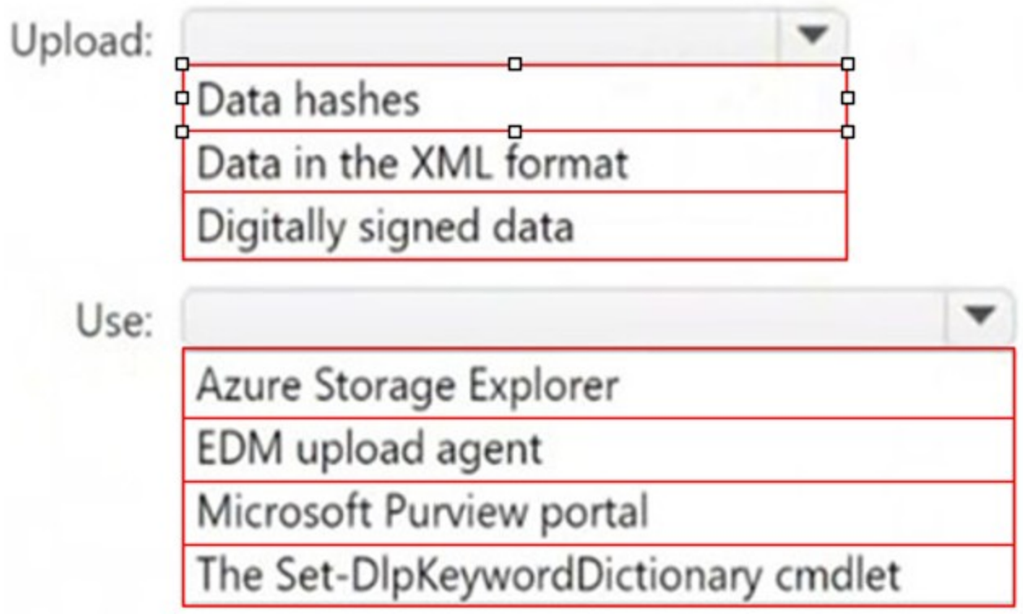
A. Sensitive info type
B. Content search query
C. Sensitive label
D. Keywords

Correct Answer: A
Section:
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.

QUESTION 23
HOTSPOT
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.

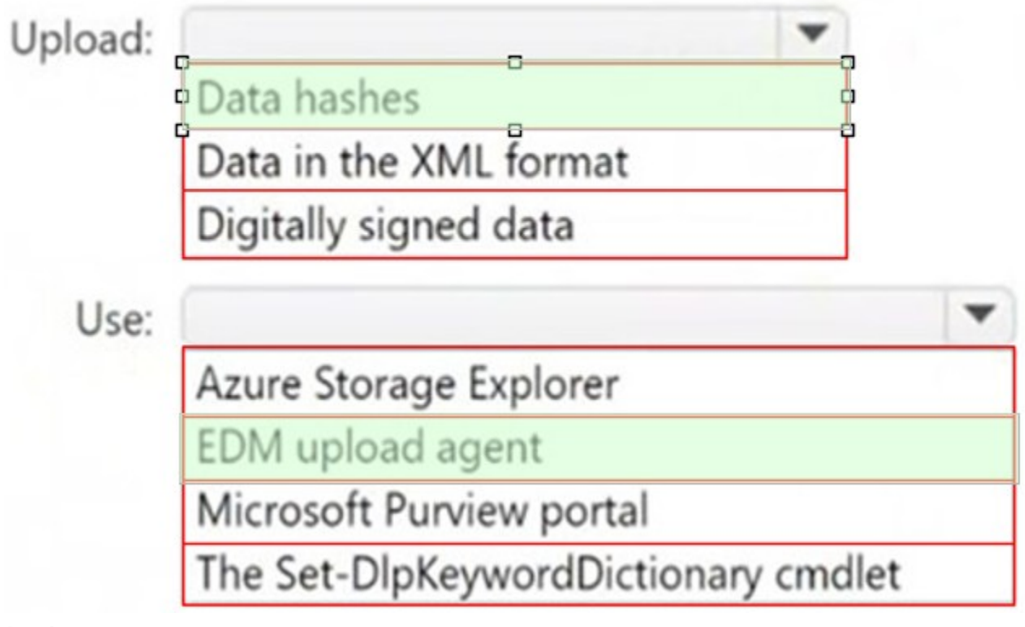
Hot Area:

Answer Area



Answer Area:

Answer Area



Section:
Explanation:

QUESTION 24
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.

Correct Answer: A
Section:
Explanation:
Since all employee assessments follow a specific template (AssessmentTemplate.docx), the best way to identify these documents for Data Loss Prevention (DLP) is to create a document fingerprint of that template.
Document fingerprinting allows Microsoft 365 DLP policies to recognize documents based on their structure and format, even when content inside varies (such as different employee names and results). By creating a fingerprint of AssessmentTemplate.docx, any copy derived from that template will be automatically detected by the DLP policy and blocked from being emailed externally.
Steps to implement:
Create a document fingerprint of AssessmentTemplate.docx using PowerShell and the Microsoft Purview compliance portal.
Apply a DLP policy to prevent external sharing of documents matching this fingerprint.
Test the policy by attempting to email an assessment externally.

QUESTION 25
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

Correct Answer: B
Section:
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.

QUESTION 26
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

Correct Answer: D
Section:
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.

QUESTION 27
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

Correct Answer: D
Section:
Explanation:
To add a new keyword dictionary in Microsoft Purview Data Loss Prevention (DLP), you must create a Sensitive Information Type (SIT).
Sensitive Info Types (SITs) allow you to define custom detection rules, including keyword dictionaries, regular expressions, and functions for identifying sensitive content in emails, documents, and other Microsoft 365

locations. A keyword dictionary is a list of predefined words/phrases that Microsoft Purview can use to identify and classify content for DLP policies.
Steps to add a keyword dictionary:
1. Go to Microsoft Purview compliance portal
2. Navigate to Data classification > Sensitive info types
3. Create a new sensitive info type
4. Add a keyword dictionary
5. Save and use it in a DLP policy

QUESTION 28
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 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
Adding a folder path to the file path exclusions in Microsoft 365 Endpoint DLP does not prevent Tailspin_scanner.exe from accessing protected sensitive information. Instead, it would exclude those files from DLP protection, which is not the intended outcome.
To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.
Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

QUESTION 29
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 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From Microsoft Defender for Cloud Apps, you create an app discovery policy.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
Creating an app discovery policy in Microsoft Defender for Cloud Apps is used for detecting and monitoring cloud application usage, but it does not prevent a locally installed application (Tailspin_scanner.exe) from accessing sensitive files on Windows 11 devices.

To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.
Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

QUESTION 30
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 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.
You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.
You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.
Solution: From the Microsoft Defender for Cloud Apps, you mark the application as Unsanctioned.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
Marking Tailspin_scanner.exe as 'Unsanctioned' in Microsoft Defender for Cloud Apps only blocks its usage in cloud-based activities (such as accessing SharePoint, OneDrive, or Exchange Online). However, it does not prevent a locally installed application on Windows 11 devices from accessing sensitive files.
To block Tailspin_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin_scanner.exe to the Restricted Apps list.
Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

QUESTION 31
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches a sensitive info type.
Does this meet the goal?

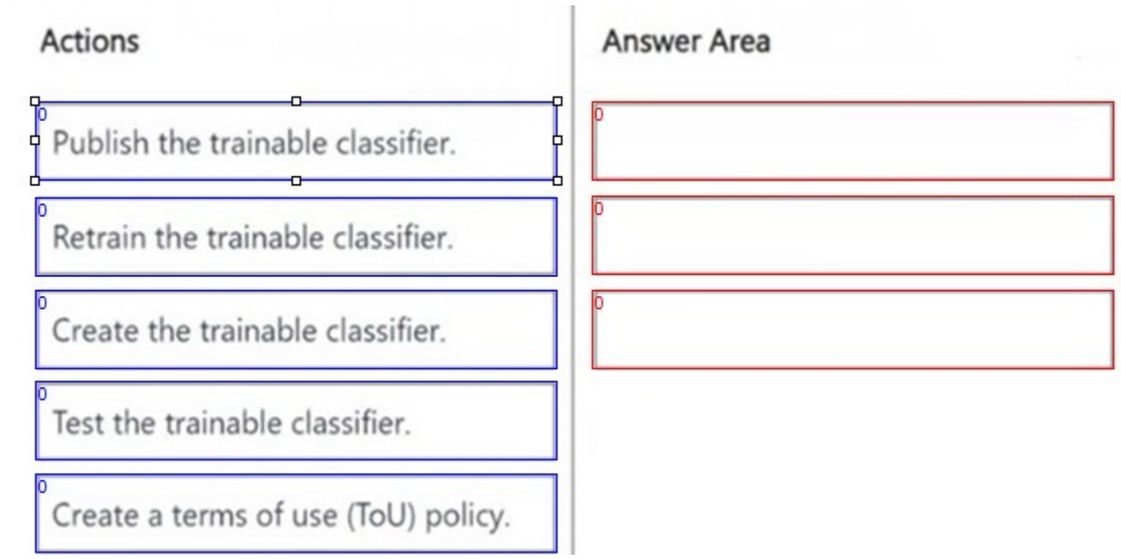
A. Yes
B. No

Correct Answer: B
Section:
Explanation:
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
Mail flow rules (transport rules) can detect sensitive info, but they are limited in encryption capabilities.
DLP policies provide more advanced protection and integration with Microsoft Purview for sensitive info detection.

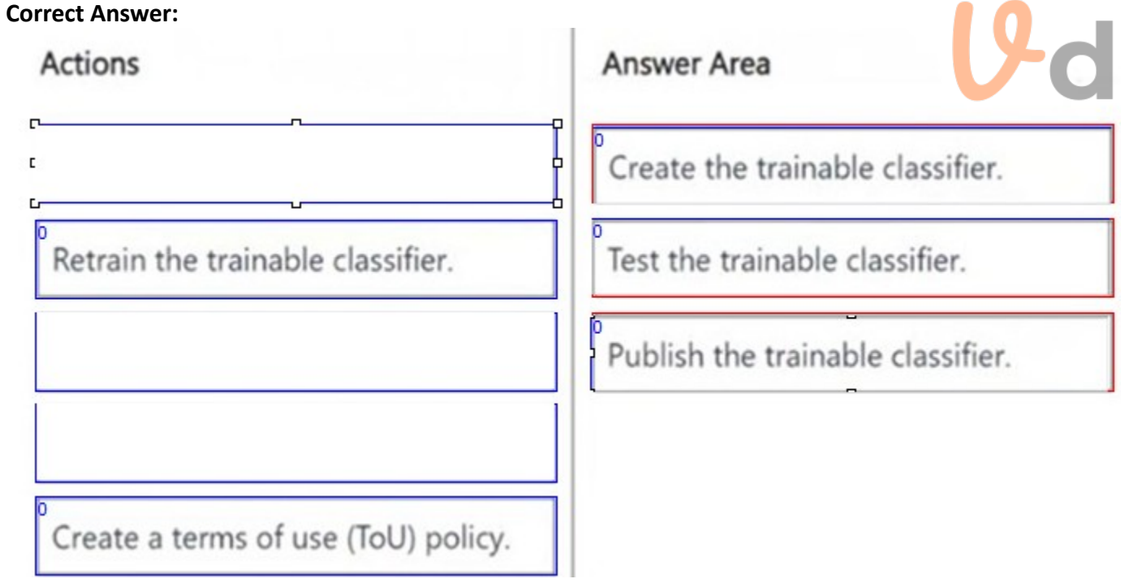
QUESTION 32

DRAG DROP
You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.
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.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 33
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

Correct Answer: A
Section:
Explanation:
To create a document fingerprint in Microsoft 365 Data Loss Prevention (DLP), you need to use PowerShell for Microsoft Purview. The correct cmdlet to connect to the Microsoft 365 Security & Compliance Center (where DLP policies are managed) is Connect-IPPSSession. This cmdlet establishes a PowerShell session to manage DLP policies, compliance settings, and document fingerprinting.

QUESTION 34
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

Correct Answer: D
Section:
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.

QUESTION 35
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.
Does this meet the goal?

A. Yes

B. No

Correct Answer: A
Section:
Explanation:
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

QUESTION 36
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.
You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches the text patterns.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
Text patterns in mail flow rules are not as reliable as sensitive information types in DLP.
Mail flow rules lack advanced content detection and machine learning-based classification, making them less effective than DLP.

QUESTION 37
HOTSPOT
You have a Microsoft 365 E5 subscription.
You receive the data loss prevention (DLP) alert shown in the following exhibit.

Contoso Electronics Microsoft Purview

Sensitive info in email with subject 'Message1'

Details Sensitive info types Metadata

Event details

ID
173fe9ac-3a65-41b0-9914-1db451bba639

Location
Exchange

Time of activity
Jun 6, 2022 8:22 PM

Impacted entities

User
M Megan Bowen

Email recipients
v victoria@fabrikam.com

Email subject
Message1

Policy details

DLP policy matched
Policy1

Rule matched
Rule1

Sensitive info types detected
Credit Card Number (19, 85%)

Actions taken
GenerateAlert

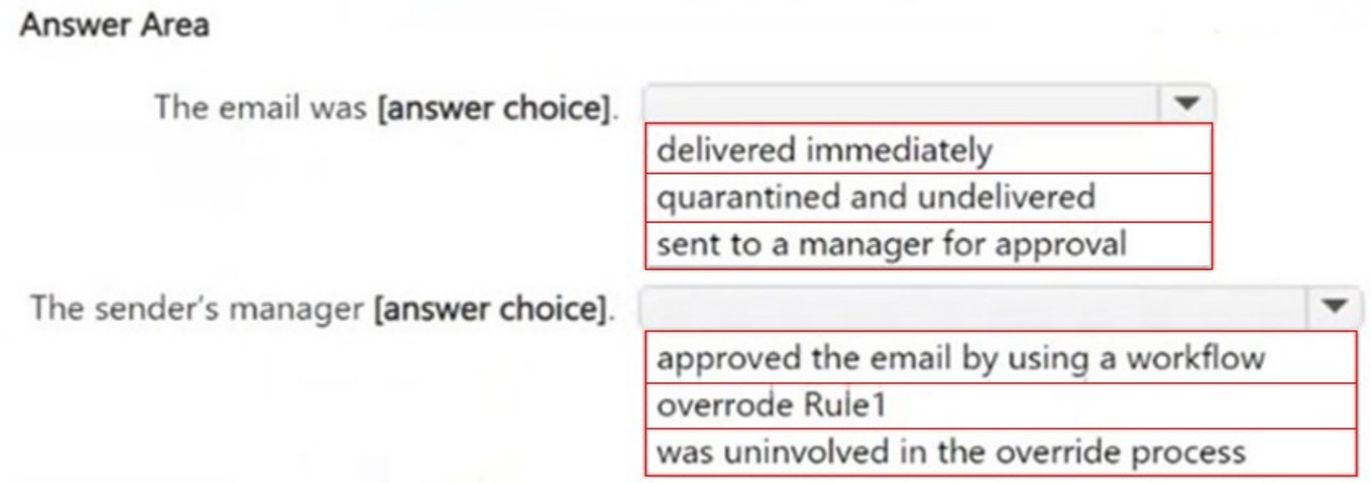
User overrode policy
Yes

Override justification text
Manager approved

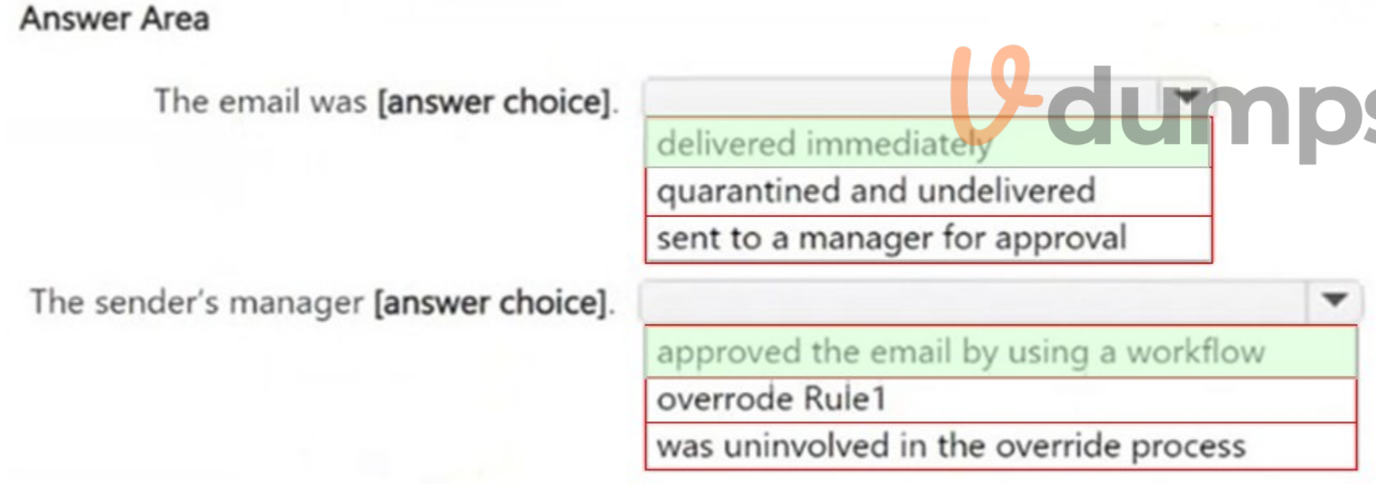
Sensitive info detected in

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Hot Area:



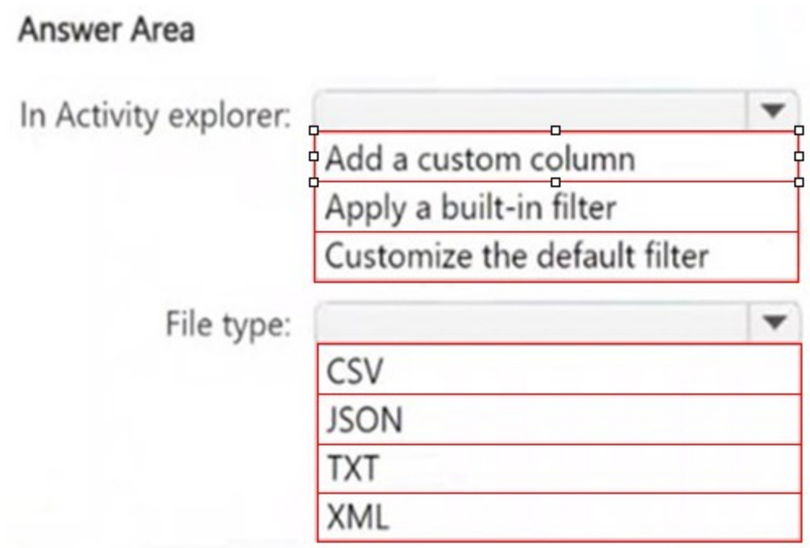
Answer Area:



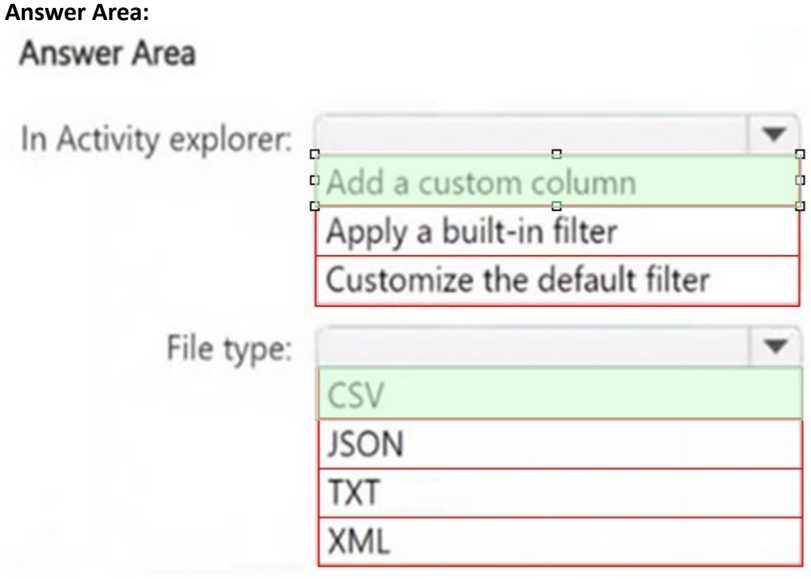
Section:
Explanation:

QUESTION 38
HOTSPOT
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.
You plan to export DLP activity by using Activity explorer.
The exported file needs to display the sensitive info type detected for each DLP rule match.
What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:
Explanation: