- **Vendor:** Microsoft
- **Exam Code:** SC-400
- **Exam Name:** Microsoft Information Protection Administrator
- **New Updated Questions from Braindump2go (Updated in October/2021)**

QUESTION 82
Case Study 1 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and Vancouver.
Existing Environment
Cloud Environment
Fabrikam has a Microsoft 365 tenant that contains the following resources:

- An Azure Active Directory (Azure AD) tenant that syncs to an on-premises Active Directory domain named corp.fabrikam.com
- Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.
Compliance Configuration
Fabrikam has the following in the Microsoft 365 compliance center:

- A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.
- The Azure Information Protection unified labeling scanner is installed and configured.
- A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.
Human Resources (HR) Management System
The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.
On-Premises Environment
You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.
All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.
Business Processes
Sales Contracts
Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.
Employment Applications
Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for Business folders, or Microsoft Teams channels.
The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.
Requirements
HR Requirements
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.

The HR department identifies the following requirements for handling employment applications:

- Resumes must be identified automatically based on similarities to other resumes received in the past.
- Employment applications and resumes must be deleted automatically two years after the applications are received.
- Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements

A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements

Fabrikam identifies the following compliance requirements:

- All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
- Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
- If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
- The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
- Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
- Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements

You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

You need to recommend a solution to configuration the Microsoft 365 Records management settings by using the CSV file must meet the compliance requirements.

What should you recommend?

A. From the Microsoft 365 compliance center, import the CSV file to a file plan.
B. Use EdmUploadAgent.exe to upload a hash of the CSV to a datastore.
C. Use a PowerShell command that pipes the import csv cmdlet to the New-RetentionPolicy cmdlet.
D. Use a PowerShell command that pipes the import-csv cmdlet to the New-Label cmdlet.

Answer: B

QUESTION 83

Case Study 1 - Fabrikam, Inc

Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and Vancouver.

Existing Environment

Cloud Environment

Fabrikam has a Microsoft 365 tenant that contains the following resources:

- An Azure Active Directory (Azure AD) tenant that syncs to an on-premises Active Directory domain named corp.fabrikam.com
- Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration

Fabrikam has the following in the Microsoft 365 compliance center:

- A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.
- The Azure Information Protection unified labeling scanner is installed and configured.
- A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes

Sales Contracts

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.

The resumes are written by the applicants and are in any format.

Requirements

HR Requirements

You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.

The HR department identifies the following requirements for handling employment applications:

- Resumes must be identified automatically based on similarities to other resumes received in the past.
- Employment applications and resumes must be deleted automatically two years after the applications are received.
- Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements

A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements

Fabrikam identifies the following compliance requirements:

- All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
- Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
- If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
- The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
- Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
- Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements

You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

You need to recommend a solution that meets the executive requirements. What should you recommend?

A. From the Microsoft 365 compliance center, create a retention policy.
B. From the Exchange admin center, enable archive mailboxes.
C. From the Microsoft 365 compliance center, create a retention label.
D. From the Microsoft 365 compliance center, create a DLP policy.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

QUESTION 84
Case Study 1 - Fabrikam, Inc
Overview
Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and Vancouver.
Existing Environment
Cloud Environment
Fabrikam has a Microsoft 365 tenant that contains the following resources:
- An Azure Active Directory (Azure AD) tenant that syncs to an on-premises Active Directory domain named corp.fabrikam.com
- Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.
Compliance Configuration
Fabrikam has the following in the Microsoft 365 compliance center:
- A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.
- The Azure Information Protection unified labeling scanner is installed and configured.
- A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.
Human Resources (HR) Management System
The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.
On-Premises Environment
You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.
All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.
Business Processes
Sales Contracts
Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.
Employment Applications
Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for Business folders, or Microsoft Teams channels.
The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.
Requirements
HR Requirements
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
- Resumes must be identified automatically based on similarities to other resumes received in the past.
- Employment applications and resumes must be deleted automatically two years after the applications are received.
- Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.
Compliance Requirements
Fabrikam identifies the following compliance requirements:
- All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.

- Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
- If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
- The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
- Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
- Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements

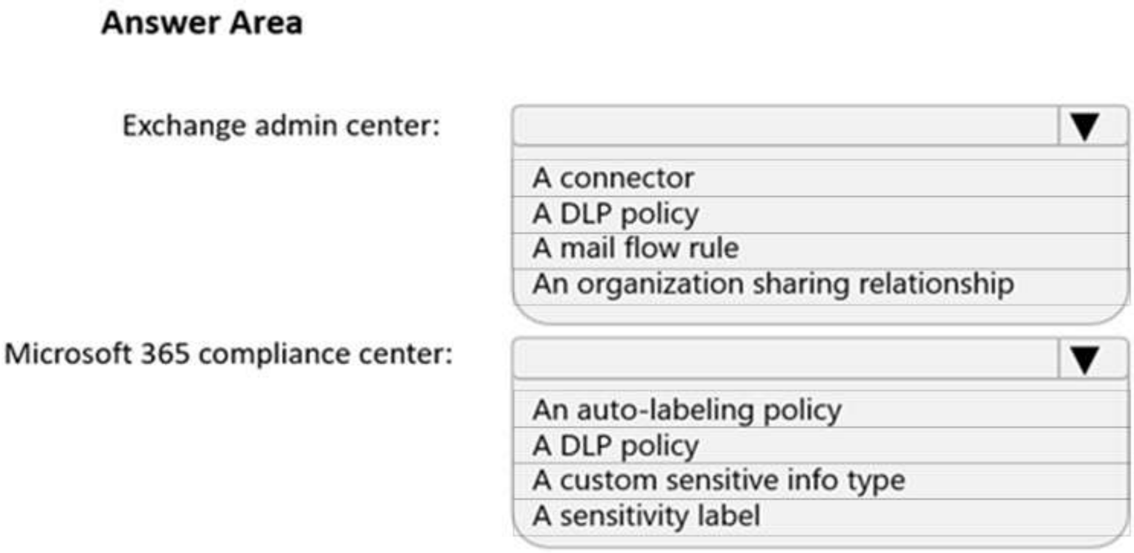
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Hotspot Question

You need to implement a solution to encrypt email. The solution must meet the compliance requirements.

What should you create in the Exchange admin center and the Microsoft 36.S compliance center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

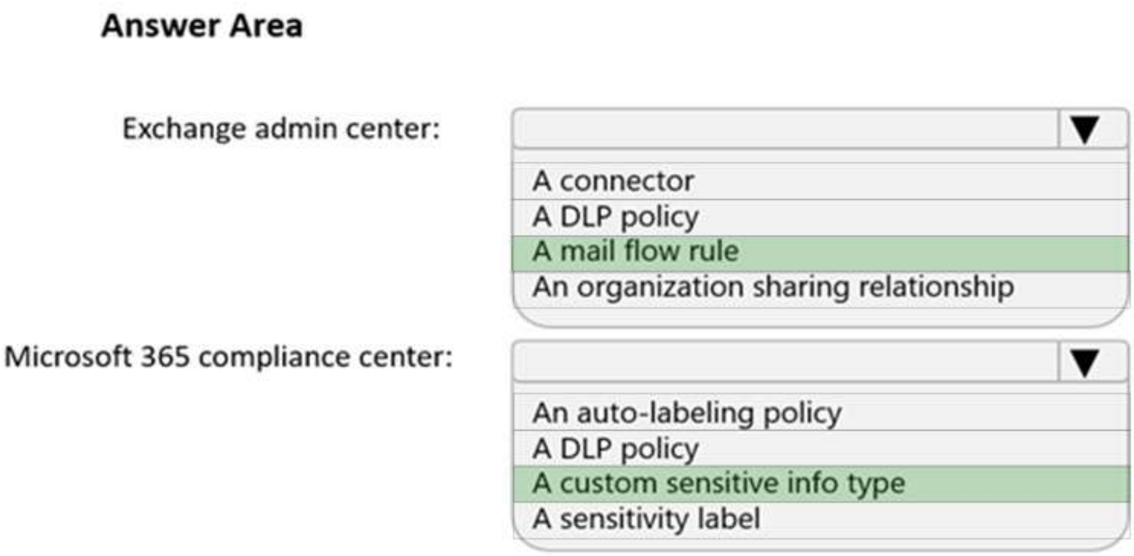


Answer Area

Exchange admin center: ▼
- A connector
- A DLP policy
- A mail flow rule
- An organization sharing relationship

Microsoft 365 compliance center: ▼
- An auto-labeling policy
- A DLP policy
- A custom sensitive info type
- A sensitivity label

Answer:



Answer Area

Exchange admin center:

- A connector
- A DLP policy
- [✓ A mail flow rule]
- An organization sharing relationship

Microsoft 365 compliance center:

- An auto-labeling policy
- A DLP policy
- [✓ A custom sensitive info type]
- A sensitivity label

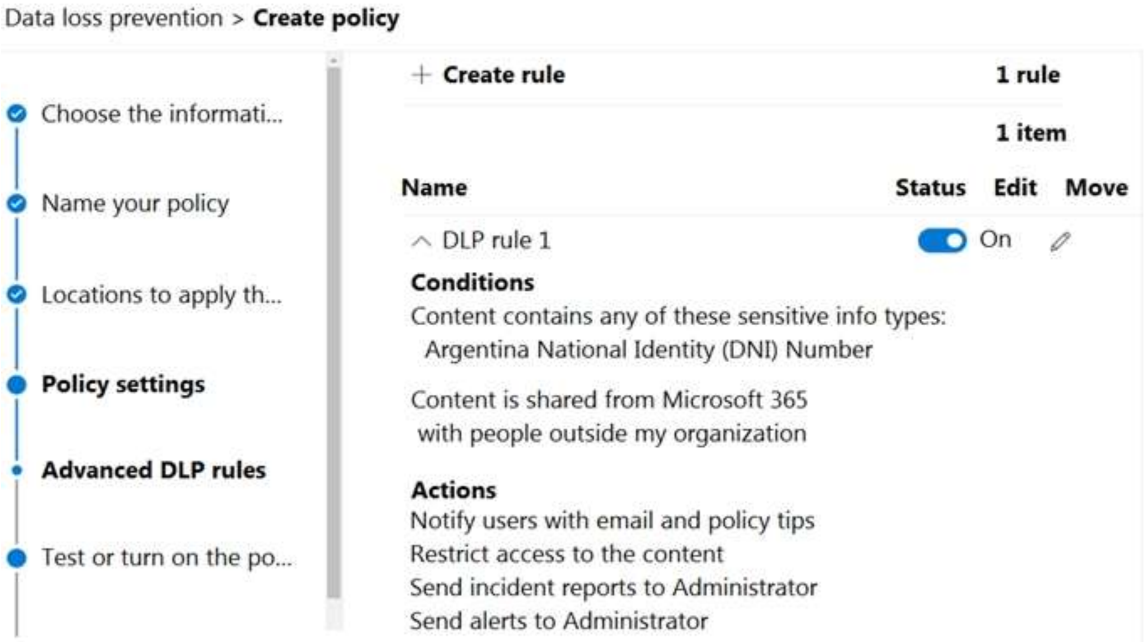
Explanation:
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-sensitive-info-types?view=o365-worldwide

QUESTION 85
You have a data loss prevention (DLP) policy that applies to the Devices location.
The policy protects documents that contain States passport numbers.
Users reports that they cannot upload documents to a travel management website because of the policy.
You need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.
Which Microsoft 365 Endpoint data loss prevention (Endpoint DLP) setting should you configure?

A. Unallowed apps
B. File path exclusions
C. Service domains
D. Unallowed browsers

Answer: C
Explanation:
You can control whether sensitive files protected by your policies can be uploaded to specific service domains from Microsoft Edge.
If the list mode is set to Block, then user will not be able to upload sensitive items to those domains. When an upload action is blocked because an item matches a DLP policy, DLP will either generate a warning or block the upload of the sensitive item.
If the list mode is set to Allow, then users will be able to upload sensitive items only to those domains, and upload access to all other domains is not allowed.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

QUESTION 86
You create a data loss prevention (DLP) policy. The Advanced DLP rules page is shown in the Rules exhibit.



Data loss prevention > Create policy

- Choose the informati...
- Name your policy
- Locations to apply th...
- **Policy settings**
- **Advanced DLP rules**
- Test or turn on the po...

+ **Create rule** **1 rule**

1 item

Name	Status	Edit	Move
DLP rule 1	On		

Conditions

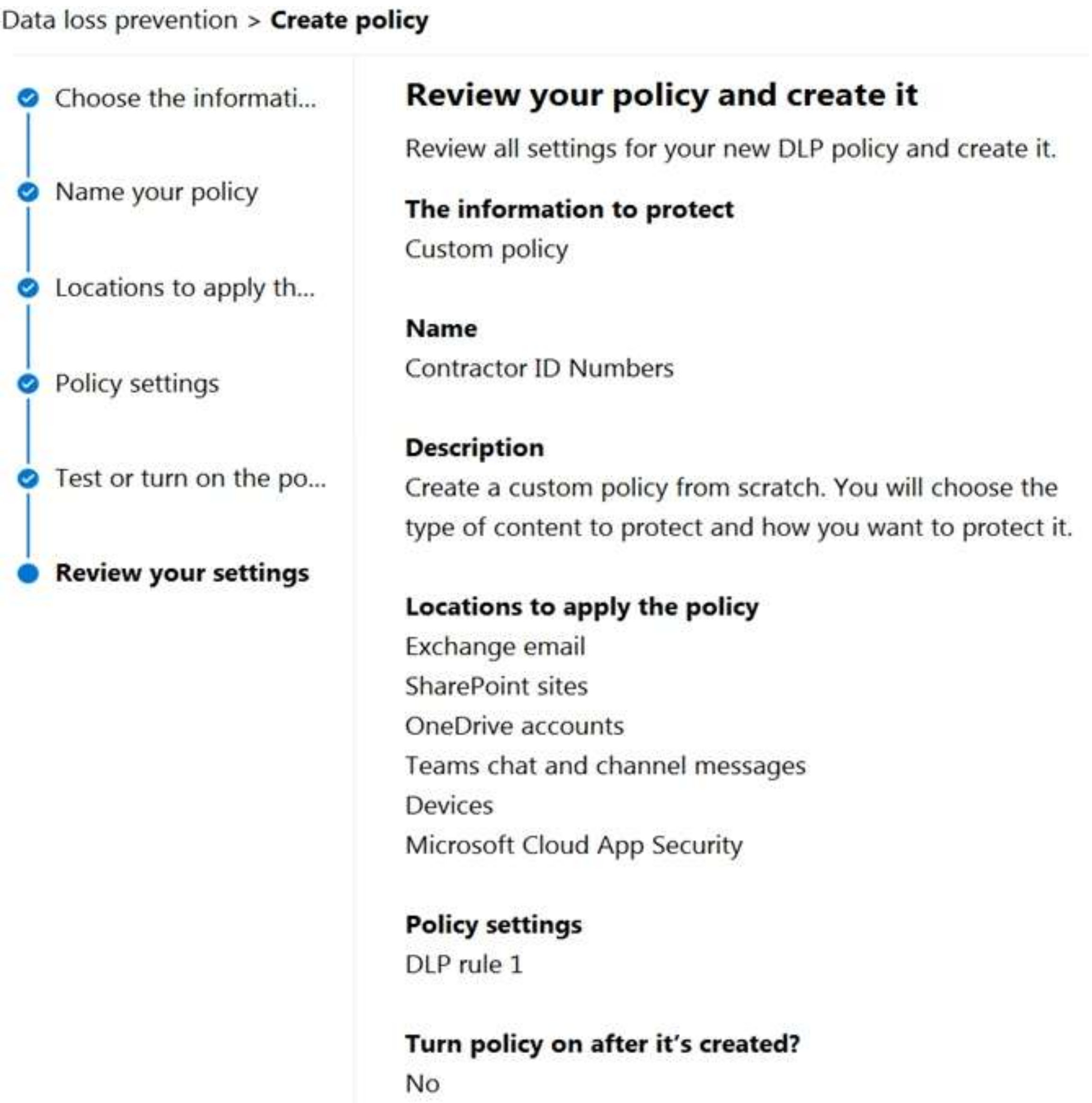
Content contains any of these sensitive info types:
Argentina National Identity (DNI) Number

Content is shared from Microsoft 365
with people outside my organization

Actions

Notify users with email and policy tips
Restrict access to the content
Send incident reports to Administrator
Send alerts to Administrator

The Review your settings page is shown in the review exhibit.



Data loss prevention > **Create policy**

Review your policy and create it

Review all settings for your new DLP policy and create it.

The information to protect
Custom policy

Name
Contractor ID Numbers

Description
Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Locations to apply the policy
Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
Devices
Microsoft Cloud App Security

Policy settings
DLP rule 1

Turn policy on after it's created?
No

You need to review the potential impact of enabling the policy without applying the actions.
What should you do?

A. Edit the policy, remove all the actions in DLP rule 1, and select I'd like to test it out first.
B. Edit the policy, remove the Restrict access to the content and Send incident report to Administrator actions, and then select Yes, turn it on right away.
C. Edit the policy, remove all the actions in DLP rule 1, and select Yes, turn it on right away.
D. Edit the policy, and then select I'd like to test it out first.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template?view=o365-worldwide

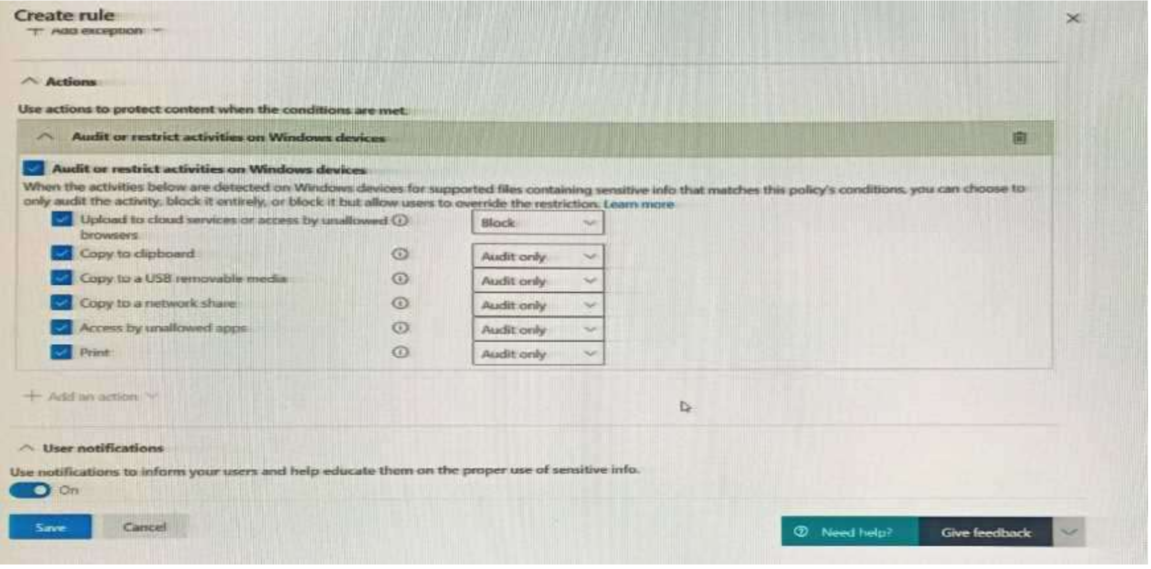
QUESTION 87
You are planning a data loss prevention (DLP) solution that will apply to computers that run Windows 10.
You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:
- If the users are members of 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. two DLP policies that each contains on DLP rule
C. one DLP policy that contains two DLP rules

Answer: B

QUESTION 88
You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.



Create rule

+ Add exception

Actions

Use actions to protect content when the conditions are met.

Audit or restrict activities on Windows devices

☑ Audit or restrict activities on Windows devices

When the activities below are detected on Windows devices for supported files containing sensitive info that matches this policy's conditions, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction. Learn more

☑ Upload to cloud services or access by unallowed browsers	Block
☑ Copy to clipboard	Audit only
☑ Copy to a USB removable media	Audit only
☑ Copy to a network share	Audit only
☑ Access by unallowed apps	Audit only
☑ Print	Audit only

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

From a computer named Computer1, 3 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 Access by unallowed apps action is set to Audit only.
B. The computers are NOT onboarded to the Microsoft 365 compliance center.
C. The Copy to clipboard action is set to Audit only.
D. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DIP) settings.
E. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.

Answer: AD

QUESTION 89
You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.
What should you do?

A. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
B. From the Azure portal, create an Azure Active Directory (Azure Al)) Identity Protection policy.
C. From the Microsoft 36h compliance? center, create an insider risk policy.
D. From the Microsoft 365 compliance center, start a data investigation.

Answer: A
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

QUESTION 90
Your company manufactures parts that are each assigned a unique 12-character alphanumeric serial number. Emails between the company and its customers refer in the serial number.
You need to ensure that ail Microsoft Exchange Online emails containing the serial numbers are retained for five years.
Which three objects should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a trainable classifier
B. a sensitive info type
C. a retention polity
D. a data loss prevention (DLP) policy
E. an auto-labeling policy
F. a retention label
G. a sensitivity label

Answer: BEF
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

QUESTION 91
You receive an email that contains a list of words that will be used few 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. a ISV file that contains words separated by tabs
C. a JSON file that that an element tor each word
D. a text file that has one word on each line

Answer: A

QUESTION 92
You plan to implement sensitivity labels for Microsoft Teams.
You need to ensure that you can view and apply sensitivity labels to new Microsoft Teams sites.
What should you do first?

A. Run the Set-sposite cmdlet.
B. Configure the EnableMTPLabels Azure Active Directory (Azure AD) setting.
C. Create a new sensitivity label scoped to Groups & sites.
D. Run the Execute-AzureAdLabelSync cmdtet.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

QUESTION 93
Your company has a Microsoft 365 tenant that uses a domain named contoso.
The company uses Microsoft Office 365 Message Encryption (OMI) to encrypt email sent to users in fabrikam.com.
A user named User1 erroneously sends an email to user2@fabrikam.
You need to disable user2@fabrikam.com from accessing the email.
What should you do?

A. Run the New-ComplianceSearchAction cmdlet.
B. Instruct User1 to delete the email from her Sent Items folder from Microsoft Outlook.
C. Run the Get-MessageTrace Cmdlet.
D. Run the Set-OMEMessageRevocation Cmdlet.
E. instruct User1 to select Remove external access from Microsoft Outlook on the web.

Answer: C

QUESTION 94
Your company has a Microsoft 365 tenant.
The company performs annual employee assessments. The assessment results are recorded in a document named Assessment I cmplatc.docx that is created by using 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 for Business 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.
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. Create a fingerprint of TOO sample documents in the Assessments folder.
D. Import TOO sample documents from the Assessments folder to a seed folder.

Answer: D

QUESTION 95
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 that uses the following sensitivity labels:
* Confidential
* Internal
* External
The labels are published by using a label policy named Policy1. Users report that Microsoft Office for the wen apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.
You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.
Solution: You modify the publishing settings of Policy1.
Does the meet the goal?

A. Yes
B. No

Answer: B

QUESTION 96
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 that uses the following sensitivity labels:
* Confidential

* Internal
* External
The labels are published by using a label policy named Policy1. Users report that Microsoft Office for the wen apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.
You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.
Solution: You modify the scope of the Confidential label.
Does this meet the goal?

A. Yes
B. No

Answer: B

QUESTION 97
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 that uses the following sensitivity labels:
* Confidential
* Internal
* External
The labels are published by using a label policy named Policy1. Users report that Microsoft Office for the wen apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.
You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.
Solution: You run the Execute-AzureAdLabelSync cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: A

QUESTION 98
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 implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).
You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).
You need to ensure that Endpoint DLP policies can protect content on the computers.
Solution: You onboard the computers to Microsoft Defender fur Endpoint.
Does this meet the goal?

A. Yes
B. No

Answer: A

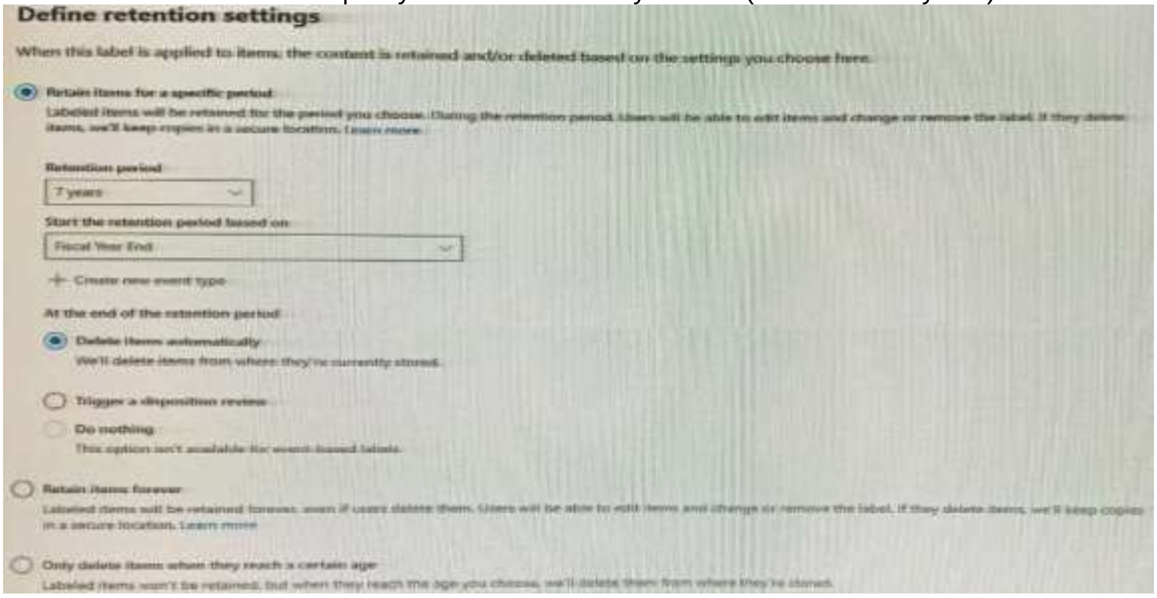
QUESTION 99
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After 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 implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).
You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).
You need to ensure that Endpoint DLP policies can protect content on the computers.
Solution: You enroll the computers in Microsoft intune.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide

QUESTION 100
Hotspot Question
You have the retention label policy shown in the Policy exhibit. (Click the Policy tab.)



Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

● Retain items for a specific period
Labeled items will be retained for the period you choose. During the retention period, users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more

Retention period
7 years

Start the retention period based on
Fiscal Year End

+ Create new event type

At the end of the retention period

● Delete items automatically
We'll delete items from where they're currently stored.

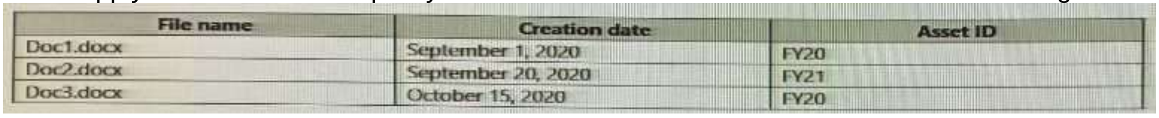
○ Trigger a disposition review

○ Do nothing
This option isn't available for event-based labels.

○ Retain items forever
Labeled items will be retained forever, even if users delete them. Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more

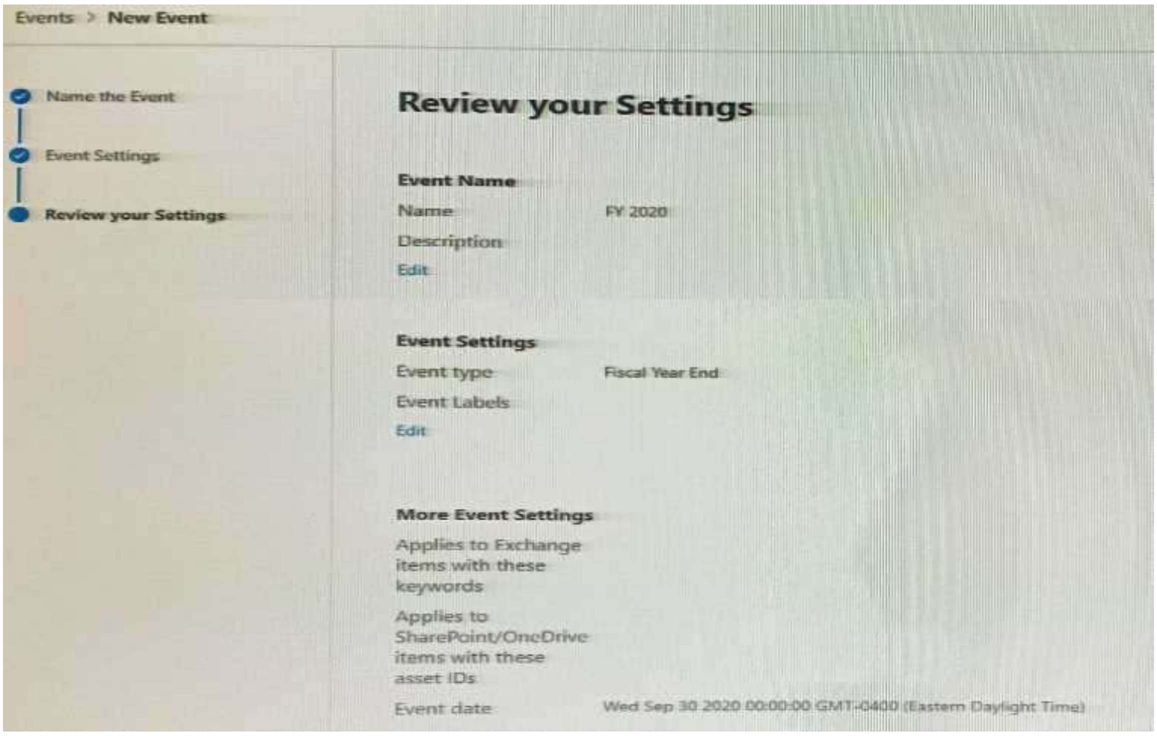
○ Only delete items when they reach a certain age
Labeled items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

Users apply the retention label policy to files and set the asset ID as shown in the following table.



File name	Creation date	Asset ID
Doc1.docx	September 1, 2020	FY20
Doc2.docx	September 20, 2020	FY21
Doc3.docx	October 15, 2020	FY20

On December 1. 2020. you create the event shown in the Event exhibit. (Click the Event tab.):



Events > New Event

- Name the Event
- Event Settings
- Review your Settings

Review your Settings

Event Name

Name FY 2020

Description

Edit

Event Settings

Event type Fiscal Year End

Event Labels

Edit

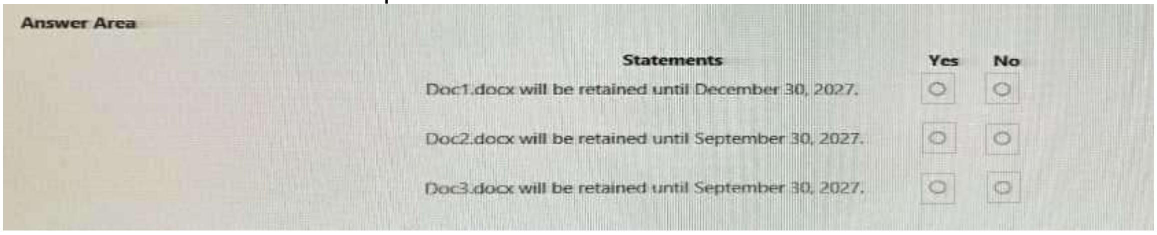
More Event Settings

Applies to Exchange items with these keywords

Applies to SharePoint/OneDrive items with these asset IDs

Event date Wed Sep 30 2020 00:00:00 GMT-0400 (Eastern Daylight Time)

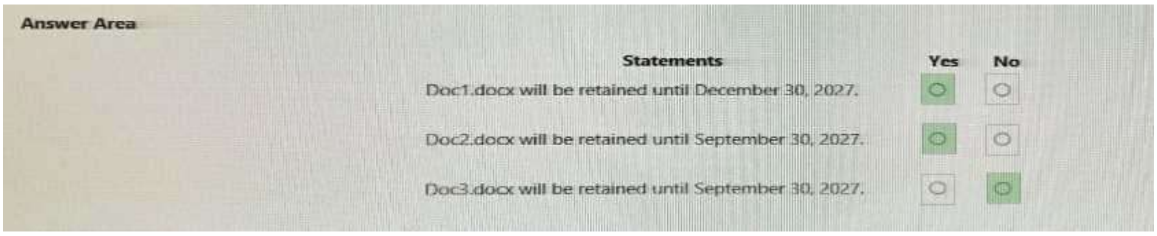
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	○
Doc2.docx will be retained until September 30, 2027.	○	○
Doc3.docx will be retained until September 30, 2027.	○	○

Answer:



Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	●	○
Doc2.docx will be retained until September 30, 2027.	●	○
Doc3.docx will be retained until September 30, 2027.	○	●

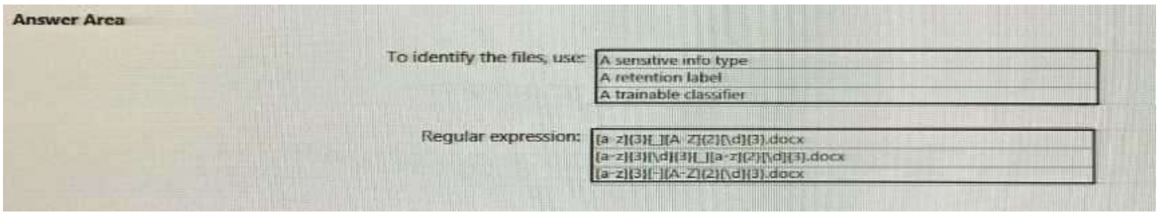
QUESTION 101

Hotspot Question

At the end of a project you upload project documents to a Microsoft SharePoint Online library that contains many fifes.
Files that have the following naming format must be labeled as Project Documents:

```
- aei_AA989.docx
- bci_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx
- ecc_BB565.docx
```

You plan to create an auto-apply retention label policy.
What should you use to identify the files, and which regular expression should you use? To answer, select the appropriate options in the answer area.

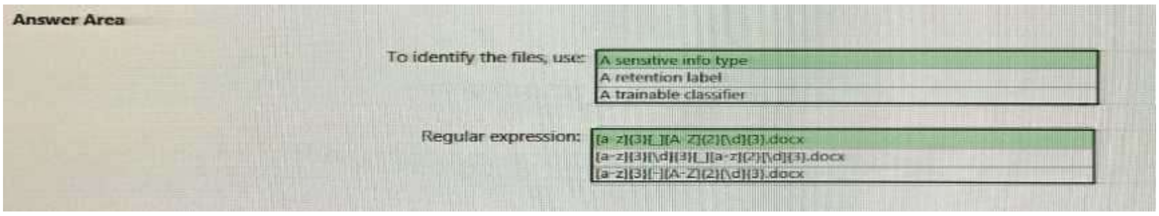


Answer Area

To identify the files, use:
- A sensitive info type
- A retention label
- A trainable classifier

Regular expression:
- [a-z]{3}[_][A-Z]{2}[\d]{3}.docx
- [a-z]{3}[\d]{3}[_][a-z]{2}[\d]{3}.docx
- [a-z]{3}[-][A-Z]{2}[\d]{3}.docx

Answer:



Answer Area

To identify the files, use:
- [✓ A sensitive info type]
- A retention label
- A trainable classifier

Regular expression:
- [✓ [a-z]{3}[_][A-Z]{2}[\d]{3}.docx]
- [a-z]{3}[\d]{3}[_][a-z]{2}[\d]{3}.docx
- [a-z]{3}[-][A-Z]{2}[\d]{3}.docx

QUESTION 102

Hotspot Question

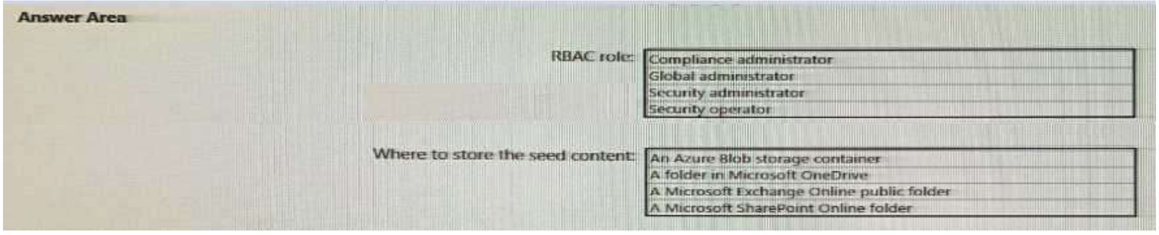
You plan to create a custom trainable classifier based on an organizational form template.

You need to identity which role based access control (RBAC) role is required to create the trainable classifier and where to classifier.

The solution must use the principle of least privilege.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

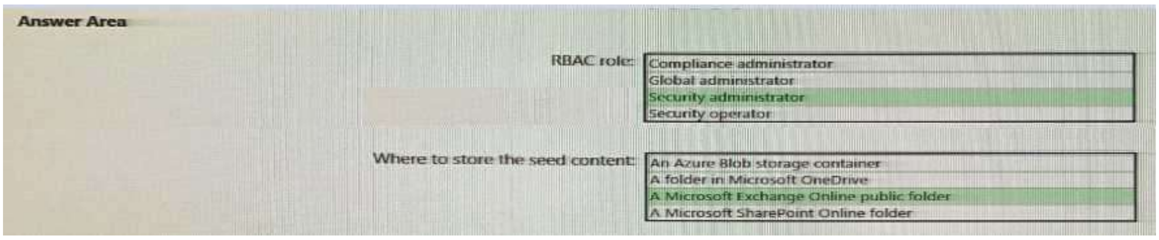


Answer Area

RBAC role:
- Compliance administrator
- Global administrator
- Security administrator
- Security operator

Where to store the seed content:
- An Azure Blob storage container
- A folder in Microsoft OneDrive
- A Microsoft Exchange Online public folder
- A Microsoft SharePoint Online folder

Answer:



Answer Area

RBAC role:
- Compliance administrator
- Global administrator
- [✓ Security administrator]
- Security operator

Where to store the seed content:
- An Azure Blob storage container
- A folder in Microsoft OneDrive
- [✓ A Microsoft Exchange Online public folder]
- A Microsoft SharePoint Online folder

QUESTION 103

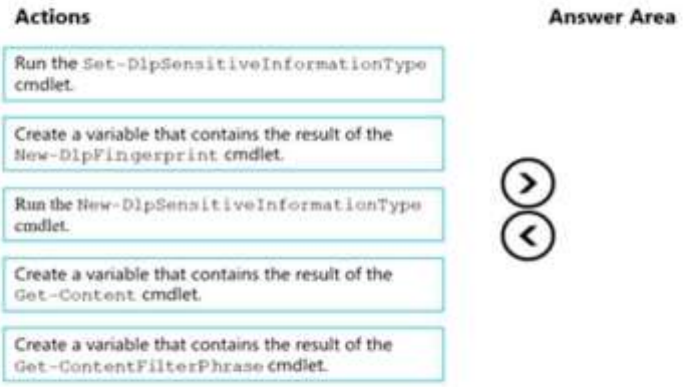
Drag and Drop Question

You have a Microsoft 365 tenant that uses data loss prevention (DLP).

You have a custom employee information form named Template 1.docx.

You need to create a classification rule package based on the document fingerprint of Templatel.docx.

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.



Actions

Run the Set-DlpSensitiveInformationType cmdlet.

Create a variable that contains the result of the New-DlpFingerprint cmdlet.

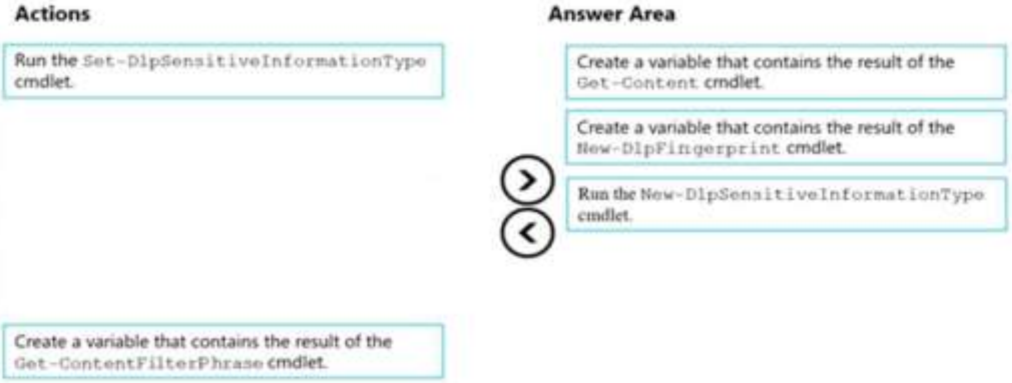
Run the New-DlpSensitiveInformationType cmdlet.

Create a variable that contains the result of the Get-Content cmdlet.

Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.

Answer Area

Answer:



Actions

Run the Set-DlpSensitiveInformationType cmdlet.

Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.

Answer Area

Create a variable that contains the result of the Get-Content cmdlet.

Create a variable that contains the result of the New-DlpFingerprint cmdlet.

Run the New-DlpSensitiveInformationType cmdlet.

QUESTION 104

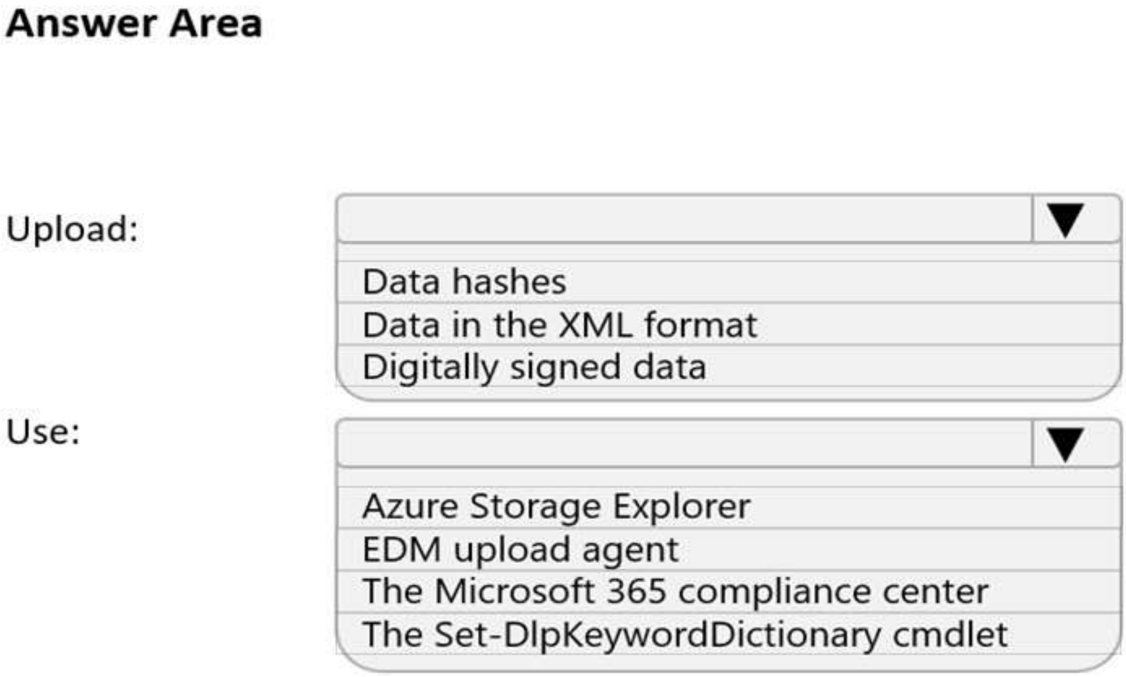
Hotspot Question

You plan to create a custom sensitive information type that will use Exact Data Match (EDM).

You need to identify what to upload to Microsoft 365, and which tool to use for the upload.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

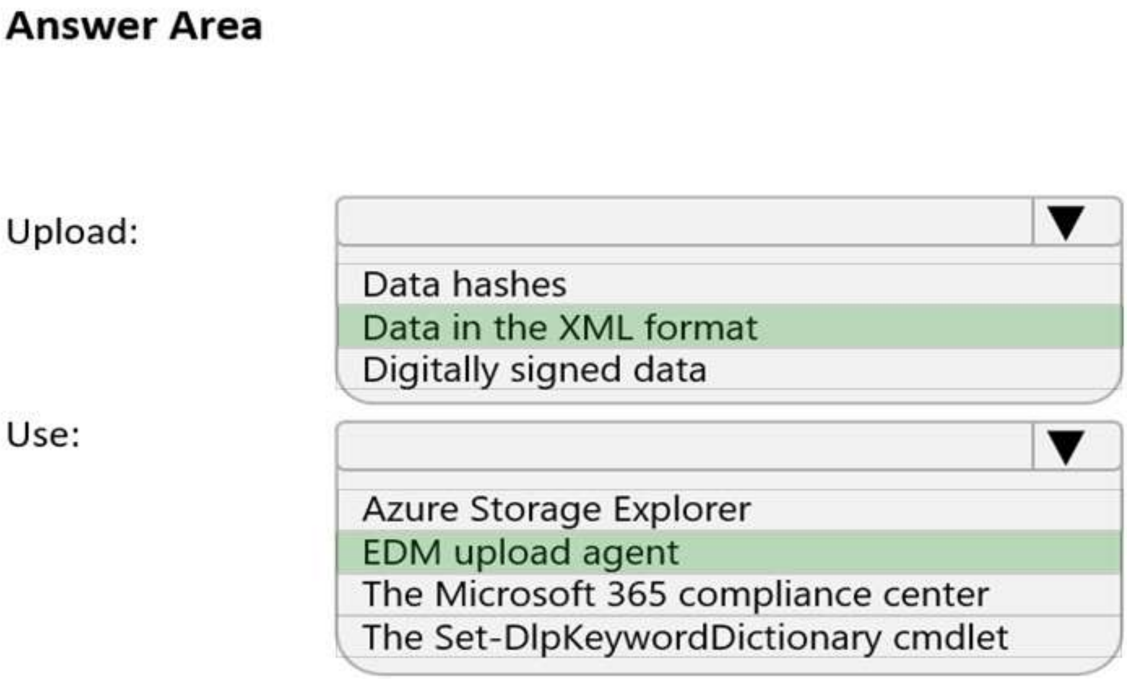


Answer Area

Upload:
- Data hashes
- Data in the XML format
- Digitally signed data

Use:
- Azure Storage Explorer
- EDM upload agent
- The Microsoft 365 compliance center
- The Set-DlpKeywordDictionary cmdlet

Answer:



Answer Area

Upload:

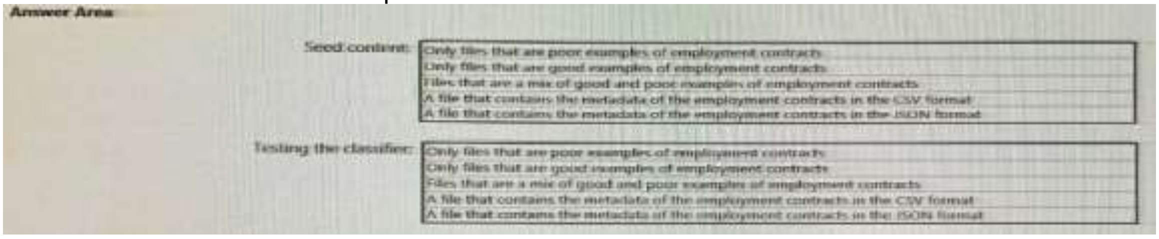
- Data hashes
- Data in the XML format
- Digitally signed data

Use:

- Azure Storage Explorer
- EDM upload agent
- The Microsoft 365 compliance center
- The Set-DlpKeywordDictionary cmdlet

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide

QUESTION 105
Hotspot Question
You plan to implement a sensitive information type based on a trainable classifier.
The sensitive information type will identify employment contracts.
You need to copy the required files to Microsoft SharePoint Online folders to train the classifier.
What should you use to seed content and test the classifier? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

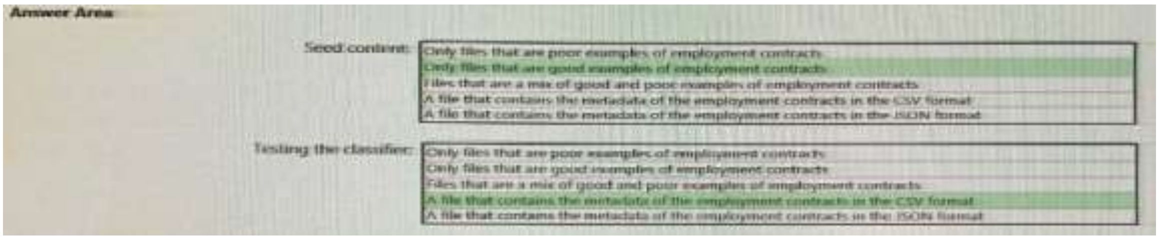
Seed content:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Testing the classifier:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Answer:



Answer Area

Seed content:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Testing the classifier:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

QUESTION 106
You have a Microsoft 365 tenant that uses Microsoft Office 365 Message Encryption (OME).
You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using OME.
What should you do?

A. From the Exchange admin center, create a new sharing policy.
B. From the Microsoft 365 security center, create a Safe Attachments policy.
C. From the Exchange admin center, create a mail flow rule.
D. From the Microsoft 365 compliance center, configure an auto-apply retention label policy.

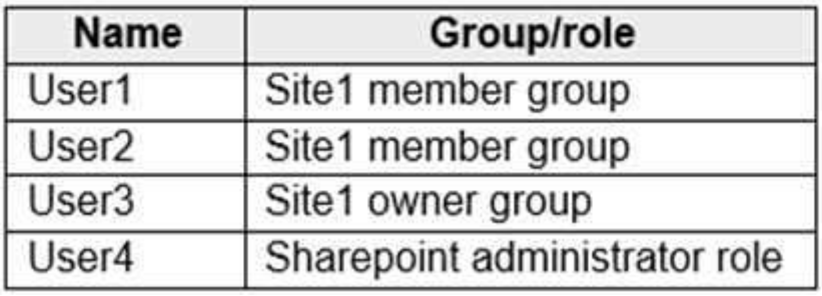
Answer: C
Explanation:
You can create mail flow rules to help protect email messages you send and receive.
You can set up rules to encrypt any outgoing email messages and remove encryption from encrypted messages coming from inside your organization or from replies to encrypted messages sent from your organization.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/define-mail-flow-rules-to-encrypt-email?view=o365-worldwide

QUESTION 107
You need to protect documents that contain credit card numbers from being opened by users outside your company. The solution must ensure that users at your company can open the documents.
What should you use?

A. a sensitivity label policy
B. a sensitivity label
C. a retention policy
D. a data loss prevention (DLP) policy

Answer: D
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

QUESTION 108
You have a Microsoft 365 tenant that contains a Microsoft SharePoint Online site named Site1.
You have the users shown in the following table.



Name	Group/role
User1	Site1 member group
User2	Site1 member group
User3	Site1 owner group
User4	Sharepoint administrator role

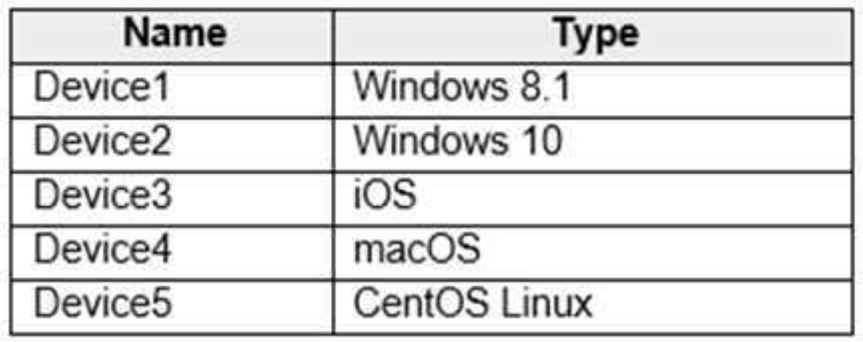
You create a data loss prevention (DLP) policy for Site1 that detects credit card number information. You configure the policy to use the following protection action:
When content matches the policy conditions, show policy tips to users and send them an email notification.
You use the default notification settings.
To Site1, User1 uploads a file that contains a credit card number.
Which users receive an email notification?

A. Used and User2 only
B. Used and User4 only
C. Used, User2, User3, and User4
D. Used only
E. Used and User3 only

Answer: D
Explanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-the-default-dlp-policy?view=o365-worldwide

QUESTION 109
You have a Microsoft 365 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.



Name	Type
Device1	Windows 8.1
Device2	Windows 10
Device3	iOS
Device4	macOS
Device5	CentOS Linux

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).
Which devices support Endpoint DLP?

A. Device5 only
B. Device2 only
C. Device 1, Device2, Device3, Device4, and Device5
D. Device3 and Device4 only
E. Device1 and Device2 only

Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

QUESTION 110
A compliance administrator recently created several data loss prevention (DLP) policies.
After the policies are created, you receive a higher than expected volume of DLP alerts.
You need to identify which rules are generating the alerts.
Which DLP report should you use?

A. Third-party DLP policy matches
B. DLP policy matches
C. DLP incidents
D. False positive and override

Answer: B
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

QUESTION 111
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 10. The computers are onboarded to the Microsoft 365 compliance center.
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 Cloud App Security portal, you create an app discovery policy.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
You can create app discovery policies to alert you when new apps are detected within your organization.
Use the unallowed apps list instead.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-policies
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

QUESTION 112
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 10. The computers are onboarded to the Microsoft 365 compliance center.
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

Answer: B
Explanation:
Folder path to the file path exclusions excludes certain paths and files from DLP monitoring.
Use the unallowed apps list instead.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide