

# Microsoft SC-401

## Administering Information Security in Microsoft 365

For More Information – Visit link below:

<https://www.examsempire.com/>

**Product Version**

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/sc-401>

# Total Questions: 223

## Latest Version: 10.6

### Topic 1, Contoso, Ltd

#### Instructions

This is a case study. Case studies are not timed separately from other exam sections. You can use as much exam time as you would like to complete each case study. However, there might be additional case studies or other exam sections. Manage your time to ensure that you can complete all the exam sections in the time provided. Pay attention to the Exam Progress at the top of the screen so you have sufficient time to complete any exam sections that follow this case study.

To answer the case study questions, you will need to reference information that is provided in the case. Case studies and associated questions might contain exhibits or other resources that provide more information about the scenario described in the case. Information provided in an individual question does not apply to the other questions in the case study. A Review Screen will appear at the end of this case study. From the Review Screen, you can review and change your answers before you move to the next exam section. After you leave this case study, you will NOT be able to return to it.

#### To start the case study

To display the first question in this case study, select the "Next" button. To the left of the question, a menu provides links to information such as business requirements, the existing environment, and problem statements. Please read through all this information before answering any questions. When you are ready to answer a question, select the "Question" button to return to the question.

#### Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

#### Existing Environment

##### Microsoft 365 Environment

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

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

Users store data in the following locations:

- SharePoint sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

**SharePoint Online Environment**

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4. Site2 contains the files shown in the following table.

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

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

User	Role
User1	Site owner
User2	Site visitor

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

Site4 has the following two retention policies applied:

- Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
- Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

#### **Problem Statements**

Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

#### **Requirements**

##### **Planned Changes**

Contoso plans to create the following data loss prevention (DLP) policy:

- Name: DLPpolicy1
- Locations to apply the policy: Site2
- Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
- Actions: Restrict access to the content

##### **Technical Requirements**

Contoso must meet the following technical requirements:

- All administrative users must be able to review DLP reports.
- Whenever possible, the principle of least privilege must be used.
- For all users, all Microsoft 365 data must be retained for at least one year.
- Confidential documents must be detected and protected by using Microsoft 365.

- Site1 documents that include credit card numbers must be labeled automatically.
- All administrative users must be able to create Microsoft 365 sensitivity labels.
- After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

## Question: 1

DRAGDROP

You need to meet the technical requirements for the Site1 documents.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a sensitivity label.	
Wait 24 hours and then turn on the policy.	
Create a sensitive info type.	
Create a retention label.	
Create an auto-labeling policy.	

**Answer:**

Actions	Answer Area
Create a sensitivity label.	Create a sensitive info type.
Wait 24 hours and then turn on the policy.	Create a retention label.
Create a sensitive info type.	Create an auto-labeling policy.
Create a retention label.	
Create an auto-labeling policy.	

Explanation:

## Question: 2

You need to meet the technical requirements for the creation of the sensitivity labels. To which user or users must you assign the Sensitivity Label Administrator role?

- A. Admin1 only
- B. Admin1 and Admin4 only
- C. Admin1 and Admin5 only
- D. Admin1, Admin2, and Admin3 only
- E. Admin1, Admin2, Admin4, and Admin5 only

**Answer: D**

Explanation:

To meet the requirement that all administrative users must be able to create Microsoft 365 sensitivity labels, we need to assign the Sensitivity Label Administrator role to the correct users. Sensitivity Label Administrator Role Responsibilities

This role allows users to:

- Create and manage sensitivity labels in Microsoft Purview.
- Publish and configure auto-labeling policies.
- Modify label encryption and content marking settings.

Review of Admin Roles from the Table:

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	<input type="checkbox"/> No, read-only permissions.
Admin2	Compliance Data Administrator	<input type="checkbox"/> Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	<input type="checkbox"/> Yes, has full compliance management, including labels.
Admin4	Security Operator	<input type="checkbox"/> No, this role is focused on security alerts and response.
Admin5	Security Administrator	<input type="checkbox"/> No, primarily focused on security policies and threat management.

Users that must be assigned the Sensitivity Label Administrator role:

- Admin2 (Compliance Data Administrator)
- Admin3 (Compliance Administrator)
- Admin1 (Global Reader) (should be assigned this role to fulfill the requirement that all admins can create labels).

**Question: 3**

HOTSPOT

You need to meet the technical requirements for the confidential documents.  
What should you create first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

### Answer Area

Create first:

- A Compliance Manager assessment
- A content search
- A DLP policy
- A sensitive info type
- A sensitivity label

Use for detection method:

- Dictionary
- File type
- Keywords
- Regular expression

**Answer:**

### Answer Area

Create first:

- A Compliance Manager assessment
- A content search
- A DLP policy
- A sensitive info type
- A sensitivity label

Use for detection method:

- Dictionary
- File type
- Keywords
- Regular expression

Explanation:

**Question: 4**

HOTSPOT

How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Number of files that User1 can access:

	▼
1	
2	
3	
4	

Number of files that User2 can access:

	▼
1	
2	
3	
4	

**Answer:**

## Answer Area

Number of files that User1 can access:

	▼
1	
2	
3	
4	

Number of files that User2 can access:

	▼
1	
2	
3	
4	

Explanation:

## Question: 5

HOTSPOT

You are reviewing policies for the SharePoint Online environment.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	<input type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	<input type="checkbox"/>	<input type="checkbox"/>

**Answer:**

## Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	<input type="checkbox"/>	<input type="checkbox"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Explanation:

## Question: 6

You need to meet the retention requirement for the users' Microsoft 365 data. What is the minimum number of retention policies required to achieve the goal?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 6

**Answer: B**

Explanation:

The requirement states that all Microsoft 365 data for users must be retained for at least one year. In Microsoft 365, retention policies must be configured for each type of data storage.

Step 1: Identifying Where Data is Stored

From the case study, users store data in the following locations:

- SharePoint Online sites
- OneDrive accounts
- Exchange email
- Exchange public folders
- Teams chats
- Teams channel messages

Since these locations fall under two broad categories:

- Microsoft Exchange data (Emails, Public folders)
- SharePoint, OneDrive, and Teams data

Step 2: Required Retention Policies

1. A single retention policy can cover:

- SharePoint Online
- OneDrive
- Microsoft Teams

2. A second retention policy is required for:

- Exchange (Emails & Public Folders)

Thus, the minimum number of retention policies required to meet the requirement is 2. Microsoft 365 retention policies can be applied broadly across multiple services with just two policies:

- One for Exchange & Public Folders
- One for SharePoint, OneDrive, and Teams

There's no need for separate policies for each individual workload unless different retention durations are required, which is not stated in the requirement.

## Topic 2, Mix Questions

### Mix Questions

#### SC-401 Mix Questions IN THIS CASE STUDY

### Question: 7

You have a Microsoft 365 E5 subscription that contains a Microsoft Teams channel named Channel1. Channel1 contains research and development documents. You plan to implement Microsoft 365 Copilot for the subscription. You need to prevent the contents of files stored in Channel1 from being included in answers generated by Copilot and shown to unauthorized users. What should you use?

- A. data loss prevention (DLP)
- B. Microsoft Purview insider risk management
- C. Microsoft Purview Information Barriers
- D. sensitivity labels

**Answer: D**

Explanation:

To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels.

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

### Question: 8

DRAGDROP

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:

- A file is shared externally.
- A file is labeled as internal only.

Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter 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.

Filters	Answer Area	Filter
<input type="checkbox"/> Access level	When a file is shared externally.	<input type="text"/>
<input type="checkbox"/> Collaborators	When a file is labelled as Internal only.	<input type="text"/>
<input type="checkbox"/> Matched policy		
<input type="checkbox"/> Sensitivity label		

**Answer:**

Filters	Answer Area	Filter
<input type="checkbox"/> Access level	When a file is shared externally.	<input type="text" value="Access level"/>
<input type="checkbox"/> Collaborators	When a file is labelled as Internal only.	<input type="text" value="Sensitivity label"/>
<input type="checkbox"/> Matched policy		
<input type="checkbox"/> Sensitivity label		

Explanation:

## Question: 9

HOTSPOT

You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.

You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	None	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File1	<i>None</i>
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

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

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



**Answer:**

## Answer Area

### Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



Explanation:

## Question: 10

You have a Microsoft 365 E5 subscription.

You need to create a sensitivity label named Label1. The solution must ensure that users can use Microsoft 365 Copilot to summarize files that have Label1 applied.

Which permission should you select for Label1?

- A. Export content(EXPORT)
- B. Copy and extract content(EXTRACT)
- C. Edit content(DOCEDIT)
- D. View rights(VIEW)

**Answer: B**

Explanation:

To allow Microsoft 365 Copilot to summarize files that have Label1 applied, the label must grant permission to extract content from the document. The correct permission for this is Copy and extract content (EXTRACT).

Microsoft 365 Copilot requires access to read and process content in documents to generate summaries. The EXTRACT permission allows users (and AI tools like Copilot) to copy and extract content for processing while still maintaining the protection applied by the sensitivity label.

## Question: 11

HOTSPOT

You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.

<b>Label name</b>	<a href="#">Edit</a>
Rebranding	
<b>Tooltip</b>	<a href="#">Edit</a>
Used for all documents containing information about the rebranding effort	
<b>Description</b>	<a href="#">Edit</a>
<b>Encryption</b>	<a href="#">Edit</a>
Advanced protection for content with this label	
<b>Content marking</b>	<a href="#">Edit</a>
Watermark: INTERNAL	
<b>Endpoint data loss prevention</b>	<a href="#">Edit</a>
<b>Auto labeling</b>	<a href="#">Edit</a>

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input checked="" type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

**Question: 12**

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1. You plan to enable co-authoring for encrypted files. You need to ensure that files that have label1 applied support co-authoring. Which two settings should you modify? To answer, select the settings in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

## Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings

 Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

Assign permissions now or let users decide?

Assign permissions now


The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires 

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access 

Always

Assign permissions to specific users and groups \* 

Assign permissions

0 items


Users and groups


Permissions

Edit

Delete

No data available

Use dynamic watermarking 

 Customize text (optional)

Use Double Key Encryption 

https://sts.contoso.com

**Answer:**

Answer Area

## Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings

 Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires 

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access 

Always

Assign permissions to specific users and groups \* 

[Assign permissions](#)

0 items

Users and groups


Permissions

Edit

Delete

No data available

Use dynamic watermarking 

 Customize text (optional)

Use Double Key Encryption 

https://sts.contoso.com

Explanation:

## Question: 13

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.

Answer Area

Action to perform:

- Create an Exact Data Match (EDM) schema.
- Import a data loss prevention (DLP) rule package.
- Start the opt-in process.

To perform the action, assign the role of:

- Compliance Administrator
- Global Administrator
- Security Administrator

**Answer:**

Answer Area

Action to perform:

- Create an Exact Data Match (EDM) schema.
- Import a data loss prevention (DLP) rule package.
- Start the opt-in process.

To perform the action, assign the role of:

- Compliance Administrator
- Global Administrator
- Security Administrator

Explanation:

## Question: 14

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.

## Answer Area

Create:

  
 A sensitive info type  
 A trainable classifier  
 An adaptive scope

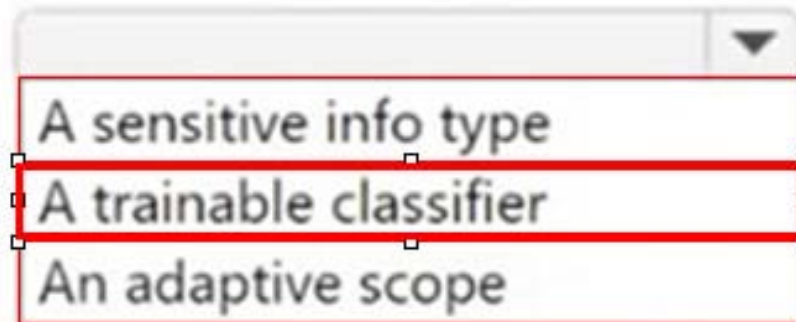
Element:

  
 Functions  
 Keyword dictionary  
 Regular expression

**Answer:**

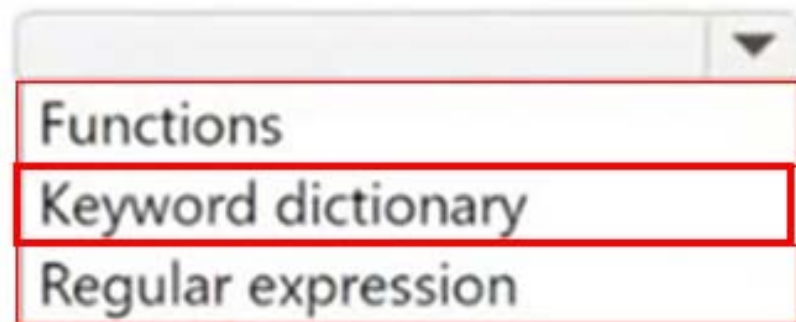
## Answer Area

Create:



A sensitive info type  
A trainable classifier  
An adaptive scope

Element:



Functions  
Keyword dictionary  
Regular expression

Explanation:

### Question: 15

You have a Microsoft 365 E5 subscription.  
You need to enable support for sensitivity labels in Microsoft SharePoint Online.  
What should you use?

- A. the Microsoft Purview portal
- B. the Microsoft Entra admin center
- C. the SharePoint admin center
- D. the Microsoft 365 admin center

**Answer: C**

Explanation:

To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.  
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center → Settings → Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

## Question: 16

You have a Microsoft 365 subscription.

You need to customize encrypted email for the subscription. The solution must meet the following requirements.

- Ensure that when an encrypted email is sent, the email includes the company logo.
- Minimize administrative effort.

Which PowerShell cmdlet should you run?

- A. Set-IRMConfiguration
- B. Set-OMEConfiguration
- C. Set-RMSTemplate
- D. New-OMEConfiguration

**Answer: B**

Explanation:

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

- Company logo
- Custom text
- Background color

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

## Question: 17

You have a Microsoft 365 E5 subscription.

You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.

What should you configure first?

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

**Answer: C**

Explanation:

To ensure that encrypted email messages sent to external recipients can be revoked or expire within seven days, you need to configure a sensitivity label with encryption settings in Microsoft Purview Information Protection. A sensitivity label allows you to encrypt emails and documents, set expiration policies (e.g., emails expire after 7 days), and enable email revocation  
How to configure it?

- Go to Microsoft Purview compliance portal → Information Protection
- Create a sensitivity label
- Enable encryption and configure the content expiration policy
- Publish the label to users

## Question: 18

### HOTSPOT

You have a Microsoft 365 E5 subscription.

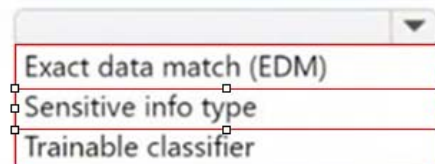
You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

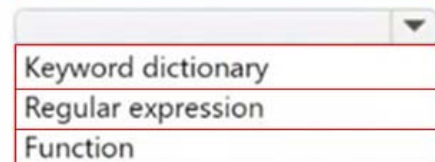
### Answer Area

To identify the documents, use a data classification of:



A screenshot of a dropdown menu with three options: "Exact data match (EDM)", "Sensitive info type", and "Trainable classifier". The "Sensitive info type" option is highlighted with a red border.

Configure data classifications by using a:

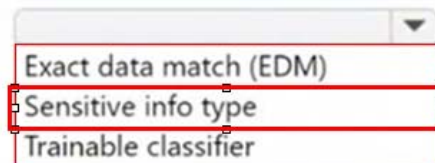


A screenshot of a dropdown menu with three options: "Keyword dictionary", "Regular expression", and "Function". The "Regular expression" option is highlighted with a red border.

**Answer:**

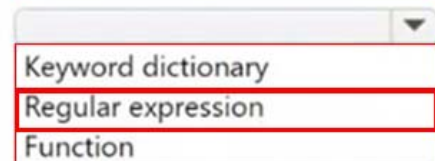
### Answer Area

To identify the documents, use a data classification of:



A screenshot of a dropdown menu with three options: "Exact data match (EDM)", "Sensitive info type", and "Trainable classifier". The "Sensitive info type" option is highlighted with a red border.

Configure data classifications by using a:



A screenshot of a dropdown menu with three options: "Keyword dictionary", "Regular expression", and "Function". The "Regular expression" option is highlighted with a red border.

Explanation:

## Question: 19

You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.

You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.

You need to identify and categorize the resumes. The solution must minimize administrative effort.

What should you include in the solution?

- A. a trainable classifier
- B. a keyword dictionary
- C. a function
- D. an exact data match (EDM) classifier

**Answer: A**

Explanation:

Since you need to automatically apply a sensitivity label to resumes based on their content and structure (work experience, education, accomplishments), a trainable classifier is the best choice.

Trainable classifiers use machine learning to identify unstructured data, such as resumes, contracts, or legal documents. Instead of relying on predefined patterns (like keywords or regular expressions), a trainable classifier learns from sample documents and can accurately identify resumes even if they are formatted differently.

Final Approach:

- Train a trainable classifier using sample resumes.
- Deploy the classifier in Microsoft Purview.
- Configure a sensitivity label to be automatically applied when a document matches the classifier.

## Question: 20

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.

## 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:**

## 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

Explanation:

### Question: 21

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.

### Answer Area

User1:

  
 File1.docx only  
 File1.docx and File2.docx only  
 File1.docx, File2.docx, and File3.docx

User2:

  
 File1.docx only  
 File1.docx and File2.docx only  
 File1.docx, File2.docx, and File3.docx

**Answer:**

## Answer Area

User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx**

User2:

- File1.docx only
- File1.docx and File2.docx only**
- File1.docx, File2.docx, and File3.docx

Explanation:

### Question: 22

You are planning a data loss prevention (DLP) solution that will apply to Windows Client computers.

You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:

- If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.
- All other users must be blocked from copying the file.

What should you create?

- A. one DLP policy that contains one DLP rule
- B. one DLP policy that contains two DLP rules
- C. two DLP policies that each contains one DLP rule

**Answer: B**

Explanation:

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: 23

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 admin center, modify the records management settings.
- D. From the Microsoft Purview portal, publish a label.
- E. From the Microsoft Purview portal, create a label.

**Answer: D, E**

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: 24

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management.

What should you create first?

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

**Answer: D**

Explanation:

To implement Microsoft Purview Data Lifecycle Management for SharePoint Online (Site1), you need to create a retention label first. Retention labels define how long content should be retained or deleted based on compliance requirements. Once a retention label is created, it can be manually or automatically applied to content in SharePoint Online, Exchange, OneDrive, and Teams. After creating a retention label, you can configure label policies to apply them to Site1 and other locations.

### Question: 25

You have a Microsoft 365 E5 subscription.

You need to create static retention policies for the following locations:

- Teams chats
- Exchange email
- SharePoint sites
- Microsoft 365 Groups
- Teams channel messages

What is the minimum number of retention policies required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Answer: C**

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: 26

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.

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

<input checked="" type="checkbox"/> Copy to clipboard	ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Copy to a USB removable media	ⓘ	Audit only ▾
<input checked="" type="checkbox"/> Copy to a network share	ⓘ	Audit only ▾
<input checked="" type="checkbox"/> 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.

**Answer: A, B**

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: 27

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	<ul style="list-style-type: none"><li>Exchange email (All recipients)</li><li>SharePoint sites (All sites)</li></ul>
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1.

You need to modify RP1.

Which two modifications can you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add locations to the policy.
- B. Delete the policy.
- C. Remove locations from the policy.
- D. Decrease the retention period of the policy.
- E. Disable the policy.
- F. Increase the retention period of the policy.

**Answer: A, F**

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: 28

You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

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

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device4 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Answer: B**

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: 29

## 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	<i>None</i>
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.

### 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:**

### 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

Explanation:

### Question: 30

#### 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.

## Answer Area

Google Chrome:

Config1 only
Config2 only
Config1 and Config2 only
Config2 and Config3 only
Config1, Config2, and Config3

Firefox:

Config1 only
Config2 only
Config1 and Config2 only
Config2 and Config3 only
Config1, Config2, and Config3

**Answer:**

## Answer Area

Google Chrome:

Config1 only
Config2 only
Config1 and Config2 only
Config2 and Config3 only
Config1, Config2, and Config3

Firefox:

Config1 only
Config2 only
Config1 and Config2 only
Config2 and Config3 only
Config1, Config2, and Config3

Explanation:

## Question: 31

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.

You need to implement a data loss prevention (DLP) solution that meets the following requirements:

- Email messages that contain a single customer identifier can be sent outside your company.
- Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

**Answer: B, C**

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: 32

DRAGDROP

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.

Settings	Answer Area	Setting
<input type="checkbox"/> Additional checks	Match product serial numbers that contain a 10-character alphanumeric string:	<input type="text"/>
<input type="checkbox"/> Character proximity	Ensure that the abbreviation of SN appears within six characters of each product serial number:	<input type="text"/>
<input type="checkbox"/> Confidence level	Exclude a test serial number of 1111111111 from a match:	<input type="text"/>
<input type="checkbox"/> Primary element		
<input type="checkbox"/> Supporting elements		

**Answer:**

Settings	Answer Area	Setting
<input type="checkbox"/> Additional checks	Match product serial numbers that contain a 10-character alphanumeric string:	<input type="checkbox"/> Primary element
<input type="checkbox"/> Character proximity	Ensure that the abbreviation of SN appears within six characters of each product serial number:	<input type="checkbox"/> Character proximity
<input type="checkbox"/> Confidence level	Exclude a test serial number of 1111111111 from a match:	<input type="checkbox"/> Additional checks
<input type="checkbox"/> Primary element		
<input type="checkbox"/> Supporting elements		

Explanation:

### Question: 33

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:

- web1.contoso.com
- web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

- A. \*.contoso.com
- B. contoso.com
- C. web1.contoso.com and web2.contoso.com
- D. web\*.contoso.com

**Answer: C**

Explanation:

The Service domains setting in Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) allows administrators to block or allow specific domains for file uploads. The goal is to prevent users from uploading DLP-protected documents to web1.contoso.com and web2.contoso.com.

Setting the Service domains to "web1.contoso.com and web2.contoso.com" precisely targets the two specific third-party websites, minimizing administrative effort while ensuring strict control.

### Question: 34

You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.

You configure an advanced DLP rule in the policy.

Which type of condition can you use in the rule?

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

**Answer: A**

Explanation:

When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns. This allows you to apply protection and trigger actions based on the identified content.

### Question: 35

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.

## Answer Area

Upload:

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

Use:

- Azure Storage Explorer
- EDM upload agent
- Microsoft Purview portal
- 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
- Microsoft Purview portal
- The Set-DlpKeywordDictionary cmdlet

Explanation:

## Question: 36

DRAGDROP

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.

Actions

- 0 Publish the trainable classifier.
- 0 Retrain the trainable classifier.
- 0 Create the trainable classifier.
- 0 Test the trainable classifier.
- 0 Create a terms of use (ToU) policy.

Answer Area

0

0

0

**Answer:**

Actions

- 0 Publish the trainable classifier.
- 0 Retrain the trainable classifier.
- 0 Create the trainable classifier.
- 0 Test the trainable classifier.
- 0 Create a terms of use (ToU) policy.

Answer Area

0 Create the trainable classifier.

0 Test the trainable classifier.

0 Publish the trainable classifier.

Explanation:

## Question: 37

You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.

You have a document named Form.docx.

You plan to use PowerShell to create a document fingerprint based on Form.docx.

You need to first connect to the subscription.

Which cmdlet should you run?

- A. Connect-IPPSSession
- B. Connect-SPOService
- C. Connect-ExchangeOnline
- D. Connect-MgGraph

**Answer: A**

Explanation:

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: 38

You receive an email that contains a list of words that will be used for a sensitive information type.

You need to create a file that can be used as the source of a keyword dictionary.

In which format should you save the list?

- A. an XLSX file that contains one word in each cell of the first row
- B. an XML file that contains a keyword tag for each word
- C. an ACCDB database file that contains a table named Dictionary
- D. a text file that has one word on each line

**Answer: D**

Explanation:

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: 39

Your company has a Microsoft 365 tenant.

The company performs annual employee assessments. The assessment results are recorded in a document named AssessmentTemplate.docx that is created by using a Microsoft Word template. Copies of the employee assessments are sent to employees and their managers.

The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive folders. A copy of each assessment is also stored in a SharePoint Online folder named Assessments.

You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.

What should you include in the solution?

- A. Create a fingerprint of AssessmentTemplate.docx.
- B. Create a sensitive info type that uses Exact Data Match (EDM).
- C. Import 100 sample documents from the Assessments folder to a seed folder.
- D. Create a fingerprint of 100 sample documents in the Assessments folder.

**Answer: A**

Explanation:

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: 40

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You are creating an exact data match (EDM) classifier named EDM1.

For EDM1, you upload a schema file that contains the fields shown in the following table.

Column name	Match mode
PP	EU Passport Number
Name	All Full Names
DateOfBirth	Single-token
AccountNumber	Multi-token

What is the maximum number of primary elements that EDM1 can have?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: B**

Explanation:

In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.

From the provided table, the Match mode indicates how data is analyzed:

- PP (EU Passport Number) → Likely a primary element because it's unique.
- Name (All Full Names) → Typically not a primary element as names are common.
- DateOfBirth (Single-token) → Usually a secondary element, not unique.
- AccountNumber (Multi-token) → Can be a primary element, as it's a unique identifier.
- Since EDM supports a maximum of two primary elements, the correct answer is 2.

## Question: 41

You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1.

You plan to create the items shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Which items can use Trainable 1?

- A. Label2 only
- B. Label1 and Label2 only
- C. Label1 and Policy1 only
- D. Label2, Policy1, and DLP1 only
- E. Label1, Label2, Policy1, and DLP1

**Answer: D**

Explanation:

A trainable classifier in Microsoft Purview is used to automatically identify and classify unstructured data based on content patterns. The classifier can be used in:

1. Retention Labels (Label2) → Supported

- Trainable classifiers can be linked to retention labels to automatically classify and apply retention policies to documents.

2. Retention Label Policies (Policy1) → Supported

- Retention label policies define how and where retention labels are applied, including automatically using trainable classifiers.

3. Data Loss Prevention (DLP) Policies (DLP1) → Supported

- Trainable classifiers can be used in DLP policies to detect and protect sensitive content automatically.

## Question: 42

You have a Microsoft 365 E5 tenant.  
You need to add a new keyword dictionary.  
What should you create?

- A. a trainable classifier
- B. a retention policy
- C. a sensitivity label
- D. a sensitive info type

**Answer: D**

Explanation:

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: 43

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

**Answer: B**

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: 44

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

**Answer: B**

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: 45

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

**Answer: B**

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: 46

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

**Answer: B**

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: 47

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

**Answer: A**

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: 48

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

**Answer: B**

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: 49

HOTSPOT

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DLP) alert shown in the following exhibit.



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

 Megan Bowen

Email recipients

 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

Document1.docx

Actions



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.

**Answer Area**

The email was [answer choice].

- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager [answer choice].

- approved the email by using a workflow
- overrode Rule1
- was uninvolved in the override process

**Answer:**

**Answer Area**

The email was [answer choice].

- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager [answer choice].

- approved the email by using a workflow
- overrode Rule1
- was uninvolved in the override process

Explanation:

**Question: 50**

**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.

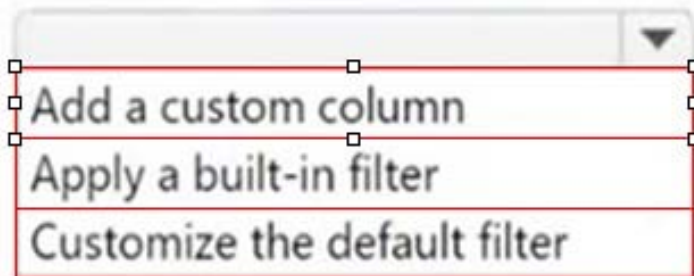
The exported file needs to display the sensitive info type detected for each DLP rule match.

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.

## Answer Area

In Activity explorer:



Add a custom column  
Apply a built-in filter  
Customize the default filter

File type:

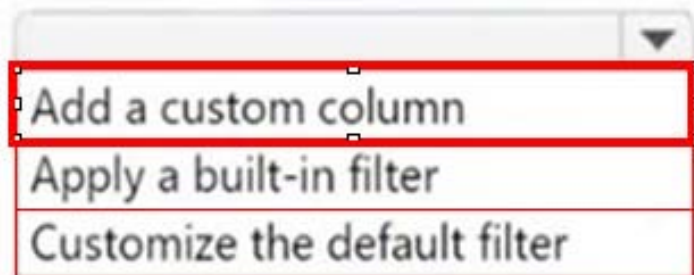


CSV  
JSON  
TXT  
XML

**Answer:**

## Answer Area

In Activity explorer:



Add a custom column  
Apply a built-in filter  
Customize the default filter

File type:



CSV  
JSON  
TXT  
XML

Explanation:

## Question: 51

### DRAGDROP

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies.

You need to identify the following:

- Rules that are applied without triggering a policy alert
- The top 10 files that have matched DLP policies
- Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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.

Reports	Answer Area	Report
DLP policy matches	Rules that are applied without triggering a policy alert:	
False positive and override	The top 10 files that have matched DLP policies:	
Incident reports	Alerts that are miscategorized:	

**Answer:**

Reports	Answer Area	Report
DLP policy matches	Rules that are applied without triggering a policy alert:	False positive and override
False positive and override	The top 10 files that have matched DLP policies:	DLP policy matches
Incident reports	Alerts that are miscategorized:	Incident reports

Explanation:

## Question: 52

### HOTSPOT

You have a Microsoft 365 E5 subscription. The subscription contains devices that are onboarded to Microsoft Purview and configured as shown in the following table.

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Device3	macOS	Installed

The subscription contains the users shown in the following table.

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

You need to review the activities.

What should you use for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)   
 Audit log search   
 Insider risk audit log   
 Unified Catalog

User2:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

User3:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

**Answer:**

**Answer Area**

User1:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)   
 Audit log search   
 Insider risk audit log   
 Unified Catalog

User2:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

User3:  Activity explorer in Data Security Posture Management for AI (DSPM for AI)  
 Audit log search  
 Insider risk audit log  
 Unified Catalog

Explanation:

**Question: 53**

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	None	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccessed	User1	9 Months
30	AuditRetention3	Sharepoint	None	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	None	10 Years

The users perform the following actions:

- User1 renames a Microsoft SharePoint Online site.
- User2 sends an email message.

How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

User1 renames a SharePoint site:

  
▼  
90 days  
6 months  
9 months  
1 year  
10 years

User2 sends an email message:

  
▼  
90 days  
6 months  
9 months  
1 year  
10 years

**Answer:**

## Answer Area

User1 renames a SharePoint site:

- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

User2 sends an email message:

- 90 days
- 6 months
- 9 months
- 1 year
- 10 years

Explanation:

### Question: 54

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Description
User1	<ul style="list-style-type: none"> <li>• User 1 is a regional manager.</li> <li>• User1 is assigned the Reader role.</li> <li>• Three department managers report to User1.</li> </ul>
User2	<ul style="list-style-type: none"> <li>• User2 is the human resources (HR) department manager.</li> <li>• User2 has no Microsoft Entra roles assigned.</li> <li>• Five HR department users report to User2.</li> </ul>
User3	<ul style="list-style-type: none"> <li>• User3 is a developer.</li> <li>• User3 reports to User2.</li> <li>• User3 is the only user in the compliance department.</li> <li>• User3 is assigned the Compliance Administrator role.</li> </ul>
User4	<ul style="list-style-type: none"> <li>• User4 is the assistant of User1.</li> <li>• User4 has no Microsoft Entra roles assigned.</li> <li>• User4 handles a high volume of confidential data on behalf of User1.</li> </ul>

Which users will Microsoft Purview insider risk management flag as potential high-impact users?

- A. User1 and User2 only
- B. User2 and User3 only
- C. User1, User2, and User3 only
- D. User1, User2, User3, and User4

**Answer: D**

Explanation:

Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:

User1 (Regional Manager, assigned Reader role, manages department managers)

Risk Factors:

- Holds a managerial position (regional manager).
- Manages multiple department managers, indicating organizational influence.
- Access to critical business information.

Flagged? -Yes (Managerial role and access to confidential data).

User2 (HR department manager, no Microsoft Entra roles, manages HR department users)

Risk Factors:

- Manages HR department users, meaning they likely handle sensitive employee data.
- HR roles are often considered high-risk due to access to personal and payroll data.

Flagged? -Yes (HR role and access to sensitive employee data).

User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role)

Risk Factors:

- Compliance Administrator role grants access to sensitive security and regulatory data.
- Only person in the compliance department, meaning they hold a critical role.
- Potentially high impact on compliance and security settings.

Flagged? -Yes (Privileged Compliance Administrator role).

User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1)

Risk Factors:

- Handles a high volume of confidential data on behalf of a regional manager.
- Assistants with access to sensitive data are considered insider risk candidates.

Flagged? -Yes (High access to sensitive information).

Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

## Question: 55

You have a Microsoft 365 E5 subscription.

You need to review a Microsoft 365 Copilot usage report.

From where should you review the report?

- A. Information Protection in the Microsoft Purview portal
- B. the Microsoft 365 admin center
- C. DSPM for AI in the Microsoft Purview portal
- D. the Microsoft Defender portal

**Answer: C**

Explanation:

To review a Microsoft 365 Copilot usage report, you need to use Data Security Posture Management for AI (DSPM for AI) in the Microsoft Purview portal. DSPM for AI provides insights into AI-related activities, including Copilot usage, risk assessments, and data security posture related to AI interactions within Microsoft 365.

## Question: 56

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management.

You implement the HR data connector.

You need to prepare the data that will be imported by the data connector.

In which format should you prepare the data?

- A. JSON
- B. CSV
- C. TSV

- D. XML
- E. PRN

**Answer: B**

Explanation:

When implementing Microsoft Purview Insider Risk Management and using the HR data connector, you must prepare HR data in CSV (Comma-Separated Values) format. This format is required because Microsoft Purview supports CSV files for importing user employment details, termination dates, role changes, and other HR-related attributes.

### Question: 57

You have a Microsoft 365 E5 subscription.

You plan to implement insider risk management for users that manage sensitive data associated with a project.

You need to create a protection policy for the users. The solution must meet the following requirements:

- Minimize the impact on users who are NOT part of the project.
- Minimize administrative effort.

What should you do first?

- A. From the Microsoft Purview portal, create an insider risk management policy.
- B. From the Microsoft Entra admin center, create a security group.

**Answer: B**

Explanation:

To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative effort, you should first create a security group in Microsoft Entra ID (formerly Azure AD).

Security groups allow you to scope insider risk management policies to specific users instead of applying policies to all users, which helps in minimizing unnecessary alerts and reducing administrative overhead. After creating the security group, you can assign this group to a Microsoft Purview Insider Risk Management policy, ensuring that only project-related users are affected.

### Question: 58

You have a Microsoft 365 E5 subscription. The subscription contains 500 devices that are onboarded to Microsoft Purview.

You select Activate Microsoft Purview Audit.

You need to ensure that you can track interactions between users and generative AI websites. What should you deploy to the devices?

- A. the Microsoft Purview extension
- B. the Microsoft Purview Information Protection client
- C. the Microsoft Defender Browser Protection extension
- D. Endpoint analytics

**Answer: A**

Explanation:

To track interactions between users and generative AI websites in Microsoft Purview Audit, you need to deploy the Microsoft Purview browser extension to the devices. This extension enables tracking of user activities on web-based applications, including AI-related tools like ChatGPT, Microsoft Copilot, and other generative AI platforms.

Microsoft Purview extension provides visibility into browser-based activities, including AI tool usage, ensuring compliance and risk management within Microsoft Purview. This extension works with Microsoft Edge and Google Chrome to track and log user interactions.

## Question: 59

HOTSPOT

You have a Microsoft 365 subscription.

You plan to deploy an audit log retention policy.


You need to perform a search to validate whether the policy will be applied to the intended entries.







Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area


# Search









 [Learn about audit](#)

Searches completed <b>0</b>	Active searches <b>0</b>	Active unfiltered searches <b>0</b>
<b>Date and time range (UTC) *</b> Start: Aug  00:00  End: Aug  00:00 	<b>Activities - friendly names</b> Choose which activities to search ... 	<b>Users</b> Add the users whose audit logs you ...
<b>Keyword Search</b> Enter the keyword to search for	<b>Activities - operation names</b> ⓘ Enter operation values, separated by ...	<b>File, folder, or site</b> ⓘ Enter all or a part of the name of a fil...
<b>Admin Units</b> Choose which Admin Units to se... 	<b>Record types</b> Select the record types to search f... 	<b>Workloads</b> Enter the workloads to search for 
	<b>Search name</b> Give the search a name	

Answer Area

# Search

 [Learn about audit](#)

Searches completed <b>0</b>	Active searches <b>0</b>	Active unfiltered searches <b>0</b>
<b>Date and time range (UTC) *</b> Start: Aug  00:00  End: Aug  00:00 	<b>Activities - friendly names</b> Choose which activities to search ... 	<b>Users</b> Add the users whose audit logs you ...
<b>Keyword Search</b> Enter the keyword to search for	<b>Activities - operation names</b> ⓘ Enter operation values, separated by ...	<b>File, folder, or site</b> ⓘ Enter all or a part of the name of a fil...
<b>Admin Units</b> Choose which Admin Units to se... 	<b>Record types</b> Select the record types to search f... 	<b>Workloads</b> Enter the workloads to search for 
	<b>Search name</b> Give the search a name	

**Answer:**

# Search

[Learn about audit](#)

Searches completed: 0 | Active searches: 0 | Active unfiltered searches: 0

Date and time range (UTC) \*

Start: Aug 00:00 | Choose which activities to search ...

End: Aug 00:00

Activities - friendly names

Activities - operation names ⓘ

Record types

Search name

Users

File, folder, or site ⓘ

Workloads

Keyword Search

Admin Units

Explanation:

## Question: 60

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You create a communication compliance policy named Policy1 and select Detect Microsoft Copilot interactions.

Which two trainable classifiers will be added to Policy1 automatically? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Unauthorized disclosure
- B. Prompt Shields
- C. Threat
- D. Corporate Sabotage
- E. Protected Materials

**Answer: A, E**

Explanation:

When you create a communication compliance policy in Microsoft Purview and select "Detect Microsoft Copilot interactions," certain trainable classifiers are automatically added to help detect sensitive or inappropriate AI usage.

The "Unauthorized disclosure" classifier helps detect cases where users might share confidential or sensitive information via Copilot interactions, preventing unintended data leaks. The "Protected Materials" classifier is used to identify sensitive or restricted content that should not be shared through Copilot, ensuring compliance with organizational policies.

## Question: 61

Your company has offices in multiple countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management.

You plan to perform the following actions:

- In a new country, open an office named Office1.
- Create a new user named User1.
- Deploy insider risk management to Office1.
- Add User1 to the Insider Risk Management Admins role group.

You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.

What should you create first?

- A. a dynamic device group
- B. a dynamic user group
- C. an administrative unit
- D. a management group

**Answer: C**

Explanation:

To ensure User1 can perform insider risk management tasks only for the users and devices in Office1, the first step is to create an administrative unit in Microsoft Entra ID (formerly Azure AD).

Administrative units allow you to scope permissions to specific users, devices, and locations. By creating an administrative unit for Office1 and assigning User1 to the Insider Risk Management Admins role group within that unit, User1 will only have access to users and devices in Office1.

## Question: 62

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

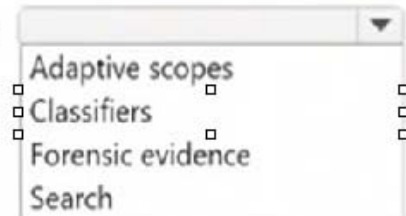
- Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.
- Integrates data loss prevention (DLP) capabilities with insider risk management.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

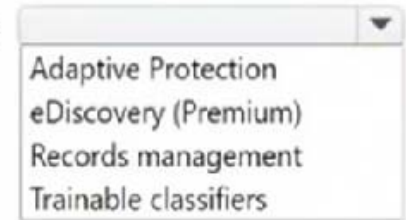
NOTE: Each correct selection is worth one point.

## Answer Area

Captures clips of key security-related user activities:



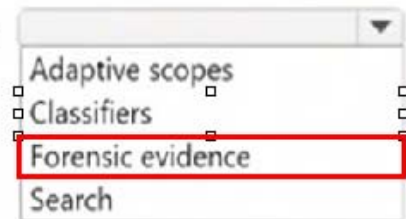
Integrates DLP capabilities with insider risk management:



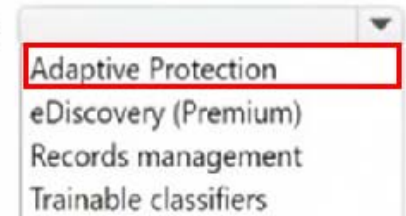
**Answer:**

## Answer Area

Captures clips of key security-related user activities:



Integrates DLP capabilities with insider risk management:



Explanation:

## Question: 63

You have a Microsoft 365 subscription.  
Users have devices that run Windows 11.

You plan to create a Microsoft Purview insider risk management policy that will detect when a user performs the following actions:

- Deletes files that contain a sensitive information type (SIT) from their device
- Copies files that contain a SIT to a USB drive
- Prints files that contain a SIT

You need to prepare the environment to support the policy.

What should you do?

A. Configure the physical badging connector.

- B. Configure the HR data connector.
- C. Create a Microsoft Purview communication compliance policy.
- D. Onboard the devices to Microsoft Purview.

**Answer: D**

Explanation:

To ensure that Microsoft Purview Insider Risk Management can detect file deletions, USB copies, and print actions on sensitive information, you must onboard the Windows 11 devices to Microsoft Purview.

Device onboarding enables endpoint activity monitoring, allowing Purview to track and log user activities such as file deletions, USB transfers, and printing of sensitive files. Once onboarded, the Insider Risk Management policy can analyze these activities and generate risk alerts when sensitive information types (SITs) are involved.

### Question: 64

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to ensure that User1 can perform the following actions:

- View recommendations from the Recommendations page.
- View the user risk level for all events by using Activity explorer.

The solution must follow the principle of least privilege.

To which role group should you add User1 for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

View the recommendations:

Compliance Administrator
Insider Risk Management Investigators
Security Reader

View the user risk level:

Compliance Administrator
Insider Risk Management Analysts
Insider Risk Management Investigators
Security Reader

**Answer:**

## Answer Area

View the recommendations:

- Compliance Administrator
- Insider Risk Management Investigators
- Security Reader

View the user risk level:

- Compliance Administrator
- Insider Risk Management Analysts
- Insider Risk Management Investigators
- Security Reader

Explanation:

## Question: 65

### HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need ensure that an incident will be generated when a user visits a phishing website.

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

NOTE: Each correct selection is worth one point.

### Answer Area

Type of policy to create:

- a Communication compliance
- a Data loss prevention (DLP)
- an Insider risk management

Prerequisite to complete:

- Create a sensitive service domain group.
- Deploy the Microsoft Defender Browser Protection extension.
- Deploy the Microsoft Purview extension.
- From Data Loss Prevention, configure the Service domains settings.

**Answer:**

**Answer Area**

Type of policy to create:

- a Communication compliance
- a Data loss prevention (DLP)
- an Insider risk management

Prerequisite to complete:

- Create a sensitive service domain group.
- Deploy the Microsoft Defender Browser Protection extension.
- Deploy the Microsoft Purview extension.
- From Data Loss Prevention, configure the Service domains settings.

Explanation:

**Question: 66**

You have Microsoft 365 E5 subscription.

You create two alert policies named Policy1 and Policy2 that will be triggered at the times shown in the following table.

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

How many alerts will be added to the Microsoft Purview portal?

- A. 2
- B. 3
- C. 4

- D. 5
- E. 6

**Answer: D**

Explanation:

In Microsoft Purview, when multiple alert policies trigger alerts, duplicate alerts within a short period (typically 5 minutes) may be suppressed to avoid redundancy.

Step-by-step Analysis:

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policy1	10:00:00	Yes
Policy2	10:00:03	Yes
Policy1	10:00:04	No (Duplicate within 5 min)
Policy2	10:00:31	No (Duplicate within 5 min)
Policy1	10:01:01	Yes
Policy1	10:04:45	Yes

- Policy1 at 10:00:04 is ignored because Policy1 already triggered at 10:00:00, and it's within 5 minutes.
- Policy2 at 10:00:31 is ignored because Policy2 already triggered at 10:00:03, and it's within 5 minutes.
- Policy1 at 10:01:01 is a new alert because it's over 1 minute after the previous Policy1 alert.
- Policy1 at 10:04:45 is a new alert because it's over 3 minutes after the previous Policy1 alert.

**Question: 67**

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role group
Admin1	Insider Risk Management Admins
Admin2	Insider Risk Management Analysts
Admin3	Risk Management Investigators
Admin4	Insider Risk Management Auditors

You plan to create a Microsoft Purview insider risk management case named Case1.

Which insider risk management object should you select first, and which users will be added as contributors for Case1 by default?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Object:

▼

- An alert
- A policy
- A risky user
- A notice template
- Forensic evidence

Users:

▼

- Admin1 and Admin2 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

**Answer:**

## Answer Area

Object:

▼

- An alert
- A policy
- A risky user**
- A notice template
- Forensic evidence

Users:

▼

- Admin1 and Admin2 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4**

Explanation:

### Question: 68

#### HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and just-in-time (JIT) protection. The subscription contains the users shown in the following table.

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

The subscription contains the devices shown in the following table.

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

The devices contain the files shown in the following table.

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

- |   | Yes                                 | No                       |
|---|-------------------------------------|--------------------------|
| If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.             | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action. | <input type="checkbox"/>            | <input type="checkbox"/> |
| If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.            | <input type="checkbox"/>            | <input type="checkbox"/> |

**Answer:**

Answer Area

Statements

- |   | Yes                                 | No                                  |
|---|-------------------------------------|-------------------------------------|
| If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.             | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action. | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

Explanation:

## Question: 69

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 Purview portal create an insider risk policy
- B. From the Microsoft Defender portal create a file policy
- C. From the Microsoft Defender portal, create an activity policy.
- D. From the Microsoft Purview portal, start a data investigation.

**Answer: B**

Explanation:

An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.

### Question: 70

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

Solution: You run the Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.

Does that meet the goal?

- A. Yes
- B. No

**Answer: B**

Explanation:

The Set-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command is incorrect. This assigns folder permissions but does not enable auditing. It does not track who accessed the mailbox or deleted emails.

## Question: 71

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

Solution: You run the `Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox*` command.

Does that meet the goal?

A. Yes

B. No

**Answer: B**

Explanation:

The `Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox*` command is incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

## Question: 72

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.  
Solution: You run the Set-Mailbox -Identity "User1" -AuditEnabled \$true command.  
Does that meet the goal?

- A. Yes
- B. No

**Answer: A**

Explanation:

To track who accesses User1's mailbox, you need to enable mailbox auditing for User1. By default, Exchange mailbox auditing is not enabled per mailbox (even though it is enabled tenant-wide).

The Set-Mailbox -Identity "User1" -AuditEnabled \$true command enables audit logging for mailbox actions like:

- Read emails
- Delete emails
- Send emails as User1
- Access by delegated users

Once enabled, you can search for future sign-ins and actions in the Microsoft Purview audit logs.

### Question: 73

You have a data loss prevention (DIP) policy that applies to the Devices location. The policy protects documents that contain United States passport numbers  
Users report that they cannot upload documents to a travel management website because of the pokey.

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 DIP) setting should you configure?

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

**Answer: A**

Explanation:

### Question: 74

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the data loss prevention (DLP) policies shown in the following table.

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown in the following table.

Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

All the policies are assigned to Site1.

You need to ensure that if a user uploads a document to Site1 that matches all the rules, the user will be shown the Tip 2 policy tip. What should you do?

- A. Change the priority of DLP2 to 0.
- B. Prevent additional processing of the policies if there is a match for Rule2
- C. Change the priority of DLP2 to 3.
- D. Enable additional processing of the policies if there is a match for Rule1.

**Answer: B**

Explanation:

**Question: 75**

HOTSPOT

You have a data loss prevention (DIP) policy that has the advanced DIP rules shown in the following table.

Name	Priority	Actions
Rule1	0	<ul style="list-style-type: none"><li>• Notify users with email and policy tips</li><li>• User overrides: Off</li></ul>
Rule2	1	<ul style="list-style-type: none"><li>• Notify users with email and policy tips</li><li>• Restrict access to the content</li><li>• User overrides: Off</li></ul>
Rule3	2	<ul style="list-style-type: none"><li>• Notify users with email and policy tips</li><li>• Restrict access to the content</li><li>• User overrides: On</li></ul>
Rule4	3	<ul style="list-style-type: none"><li>• Notify users with email and policy tips</li><li>• Restrict access to the content</li><li>• User overrides: Off</li></ul>

You need to identify which rules will apply when content matches multiple advanced DIP rules. Which rules should you identify? To answer, select the appropriate options in the answer area.

If content matches Rule2, Rule3, and Rule4:

Dropdown menu options:

- Only Rule2 takes effect
- Only Rule3 takes effect
- Only Rule4 takes effect
- Rule2, Rule3, and Rule4 take effect

If content matches Rule2, Rule3, and Rule4:

Dropdown menu options:

- Only Rule2 takes effect
- Only Rule3 takes effect
- Only Rule4 takes effect
- Rule2, Rule3, and Rule4 take effect

**Answer:**

If content matches Rule2, Rule3, and Rule4:

▼

Only Rule2 takes effect

Only Rule3 takes effect

Only Rule4 takes effect

Rule2, Rule3, and Rule4 take effect

If content matches Rule2, Rule3, and Rule4:

▼

Only Rule2 takes effect

Only Rule3 takes effect

Only Rule4 takes effect

Rule2, Rule3, and Rule4 take effect

Explanation:

## Question: 76

HOTSPOT

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

You create the data loss prevention (DLP) policies shown in the following table.

Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	None	Send an incident report to the administrator.	None

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.	<input type="radio"/>	<input type="radio"/>
If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	<input type="radio"/>	<input type="radio"/>
If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	<input type="radio"/>	<input type="radio"/>

### Answer:

Answer Area

Statements

If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.

Yes

No

If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

Explanation:

## Question: 77

You have 4 Microsoft 565 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2. You plan to configure a retention label named Labe1 and apply label1 to all the files in Site1 You need to ensure that two years after a file is created in Site1. the file moves automatically to Site2. How should you configure the Choose what happens after the retention period setting for Label1?

- A. Deactivate retention settings
- B. Start a disposition review
- C. Change the label
- D. Run a Power Automate flow

**Answer: D**

Explanation:

## Question: 78

### HOTSPOT

You have a Microsoft 365 ES subscription

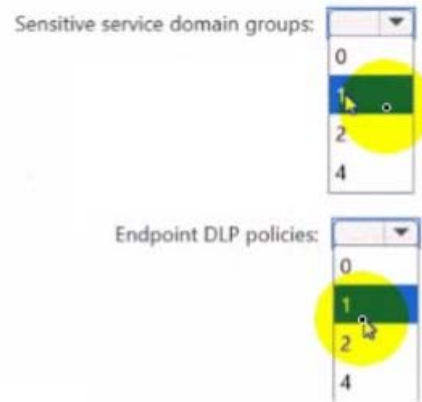
You need to implement Endpoint data loss prevention (Endpoint DLP) to meet the following requirements:

- Ensure that users can upload data to only two sites named Site1 and Site2.
- Prevent users from pasting data to two search engines named Search1 and Search2.
- Minimize the number of policies and groups.

What If the minimum number of sensitive service domain groups and Endpoint DIP policies required? To answer, select the appropriate options in the answer area.

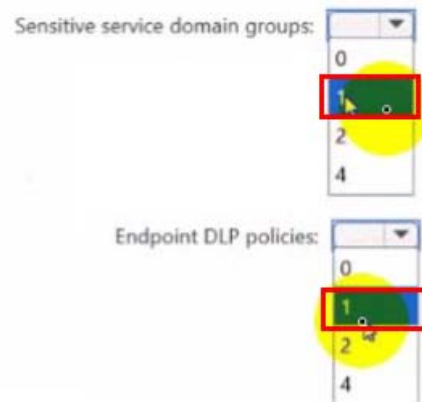
NOTE: Each correct selection is worth one point.

Answer Area



**Answer:**

Answer Area



Explanation:

### Question: 79

You have a Microsoft 565 E5 tenant that uses Microsoft Teams and contains two users named User1 and User2. You create a data loss prevention (DLP) policy that is applied to the Teams chat and channel messages location for User1 and User2. Which Teams entities will have DLP protection?

- A. 1:1/n chats and general channels only
- B. 1:1/n chats and private channels only
- C. 1:1/n chats, general channels, and private channels

**Answer: C**

Explanation:

## Question: 80

### HOTSPOT

You create a data loss prevention (DIP) policy that meets the following requirements:

- Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat
- Prevents guest users from accessing a sensitive document stored in a Microsoft Team? channel

Which location should you select for each requirement? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat:

Exchange email  
OneDrive accounts  
SharePoint sites  
Teams chat and channel messages

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel:

Exchange email  
OneDrive accounts  
SharePoint sites  
Teams chat and channel messages

**Answer:**

Answer Area

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat:

Exchange email  
OneDrive accounts  
SharePoint sites  
Teams chat and channel messages

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel:

Exchange email  
OneDrive accounts  
SharePoint sites  
Teams chat and channel messages

Explanation:

## Question: 81

### HOTSPOT

You have a Microsoft 365 ES subscription that uses Microsoft Teams and contains the users shown in the following table.

Name	Team membership
User1	Team1, Team2
User2	Team2

You have the retention policies shown in the following table.

Name	Location	Included	Retain items for	Start retention period	At the end of retention period
Policy1	Microsoft Teams channel messages	All teams	7 years	When items are created	Delete items automatically
	Microsoft Teams chats	User1			
Policy2	Microsoft Teams channel messages	Team1	5 years	When items are created	Delete items automatically
	Microsoft Teams chats	User2			

The users perform the actions shown in the following table.

User	Location	Action
User1	Team1 channel	Edits a message
User2	Private 1:1 chat with User1	Sends a message to User1
User1	Team2 channel	Deletes a message

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
The message edited by User1 will be deleted after five years.	<input type="radio"/>	<input type="radio"/>
User1 can see the message sent by User2 for up to seven years.	<input type="radio"/>	<input type="radio"/>
The message deleted by User1 will be moved to the SubstrateHolds folder.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
The message edited by User1 will be deleted after five years.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can see the message sent by User2 for up to seven years.	<input checked="" type="radio"/>	<input type="radio"/>
The message deleted by User1 will be moved to the SubstrateHolds folder.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 82

You have a Microsoft 365 E5 subscription.  
Users access their mailbox by using the following apps.

- Outlook for Microsoft 365
- Outlook on the web
- Outlook Mobile (iOS, Android)

You create a data loss prevention (DLP) policy named DLP1 that has the following settings:

- Location; Exchange email
- Status: On
- User notifications: On
- Notify users with a policy tip: Enabled

Which apps display a policy tip when content is matched by using DIP1 ?

- A. Outlook for Microsoft 365 only
- B. Outlook on the web only
- C. Outlook for Microsoft 365 and Outlook on the web only
- D. Outlook for Microsoft 365 and Outlook Mobile (iOS. Android) only
- E. Outlook for Microsoft 365. Outlook on the web, and Outlook Mobile (iOS. Android)

**Answer: C**

Explanation:

## Question: 83

HOTSPOT

You have the files shown in the following table.

Name	Location	Date modified	Date created
File1	Microsoft SharePoint Online site	June 01, 2022	December 28, 2015
File2	Microsoft OneDrive account	February 02, 2021	January 02, 2015
File3	Microsoft Exchange Online public folder	May 01, 2010	May 01, 2010

You configure a retention policy as shown >n the exhibit. (Click the Exhibit lab.)

The start of the retention period is based on when items are created. The current date is January 01. 207S.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
File1 will be deleted after you turn on the policy.	<input type="radio"/>	<input type="radio"/>
File2 will be deleted after you turn on the policy.	<input type="radio"/>	<input type="radio"/>
File3 will be deleted after you turn on the policy.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
File1 will be deleted after you turn on the policy.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File2 will be deleted after you turn on the policy.	<input type="checkbox"/>	<input type="checkbox"/>
File3 will be deleted after you turn on the policy.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Explanation:

### Question: 84

You have a Microsoft J65 ES subscription. You need to create a Microsoft Defender for Cloud Apps policy that will detect data loss prevention (DIP) violations. What should you create?

- A. a file policy
- B. an activity policy
- C. a session policy
- D. an access policy

**Answer: A**

Explanation:

### Question: 85

HOTSPOT

You have Microsoft 365 E5 tenant that has a domain name of 86s40q.ofimicrosoft.com. The tenant contains the users shown in the following table.

Name	User type
User1	Member
User2	Guest


You have a published sensitivity label.

The Access control settings for the sensitivity label are configured as shown in the exhibit (Click the Exhibit tab.)

## Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings

 Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires 

Never

Allow offline access 

Always

**Assign permissions to specific users and groups \*** 

[Assign permissions](#)

2 items

Users and groups	Permissions	Edit	Delete
LegalTeam@86s40q.onmicrosoft.com	Co-Author		
USSales@86s40q.onmicrosoft.com	Reviewer		

Use dynamic watermarking 

Use Double Key Encryption 

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied.	<input type="radio"/>	<input type="radio"/>
The owner of an email can assign permissions when applying the sensitivity label.	<input type="radio"/>	<input type="radio"/>
USSales@86s40q.onmicrosoft.com can print an email that has the sensitivity label applied.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied.	<input type="radio"/>	<input checked="" type="radio"/>
The owner of an email can assign permissions when applying the sensitivity label.	<input type="radio"/>	<input checked="" type="radio"/>
USSales@86s40q.onmicrosoft.com can print an email that has the sensitivity label applied.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 86

You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Platform	Microsoft Purview	Microsoft Purview client
Device1	Windows 11	Not onboarded	Installed
Device2	Windows 10	Onboarded	Installed
Device3	macOS	Onboarded	Not installed

From which devices can Microsoft Purview Insider Risk Management capture forensic evidence?

- A. Device only
- B. Device2 only
- C. Device1 and Device2 only
- D. Device2 and Device3 only
- E. Device1, Device2 and Device3

**Answer: B**

Explanation:

## Question: 87

HOTSPOT

You have a Microsoft 365 ES subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	macOS
Device4	Android

You plan to implement inside' risk management and capture forensic evidence  
Which devices support the collection of forensic evidence, and what should you do to prepare each supported device? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Device:

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4

To prepare:

- Install the Microsoft Purview client only.
- Onboard the devices to Microsoft Purview only.
- Onboard the devices to Microsoft Purview and install the Microsoft Purview client.

**Answer:**

Answer Area

Device: Device1 only  
Device1 and Device2 only  
Device1, Device2, and Device3 only  
Device1, Device2, and Device4 only  
Device1, Device2, Device3, and Device4

To prepare: Install the Microsoft Purview client only.  
Onboard the devices to Microsoft Purview only.  
Onboard the devices to Microsoft Purview and install the Microsoft Purview client.

Explanation:

### Question: 88

You have a Microsoft 365 ES subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs. You need to limit alert notifications to actionable DLP events. What should you do?

- A. From the Microsoft Defender portal, apply a filter to the alerts.
- B. From the Microsoft Purview portal, modify the Policy Tips settings of a DLP policy.
- C. From the Microsoft Purview portal, modify the matched activities threshold of an alert policy.
- D. From the Microsoft Purview portal, modify the User overrides settings of a DLP policy.

**Answer: C**

Explanation:

### Question: 89

DRAGDROP

You have a Microsoft 365 ES subscription.

You need to create the Microsoft Purview insider risk management policies shown in the following table.

Name	Description
Policy1	Monitors the printing of files by users that submitted their resignation
Policy2	Monitors the accidental sharing of data outside of an organization by users in a priority user group
Policy3	Monitors the downloading of files from Microsoft SharePoint Online to personal cloud storage services

Which policy template should you use for each policy? To answer, drag the appropriate policy templates to the correct policies

Each template may be used once more than once or not at all. You may need to drag the split bar between panes or scroll to view..

**Answer:**

Explanation:

## Question: 90

**HOTSPOT**

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

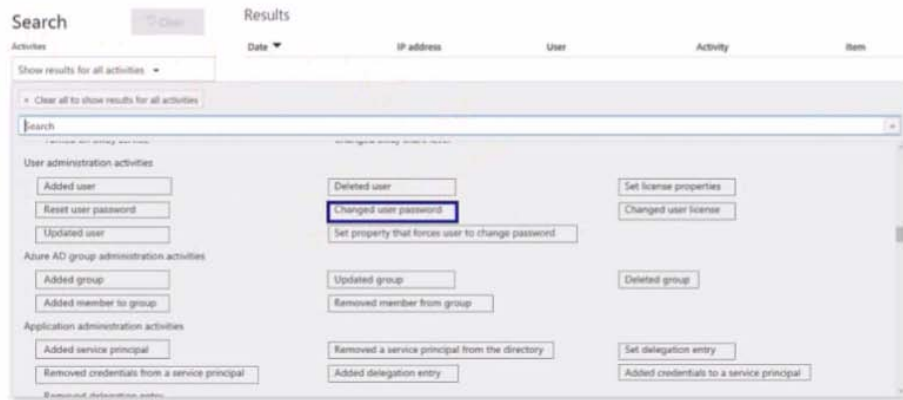
You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.

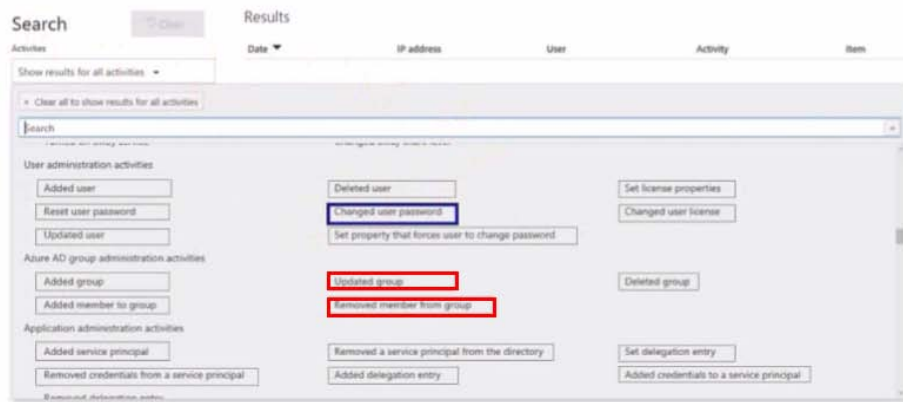
NOTE: Each correct selection is worth one point.

Answer Area



**Answer:**

Answer Area



Explanation:

## Question: 91

You need to provide a user with the ability to view data loss prevention (DIP) alerts in the Microsoft Purview portal. The solution must use the principle of least privilege. Which role should you assign to the user?

- A. Compliance Administrator
- B. Security Reader
- C. Security Operator
- D. Compliance Data Administrator

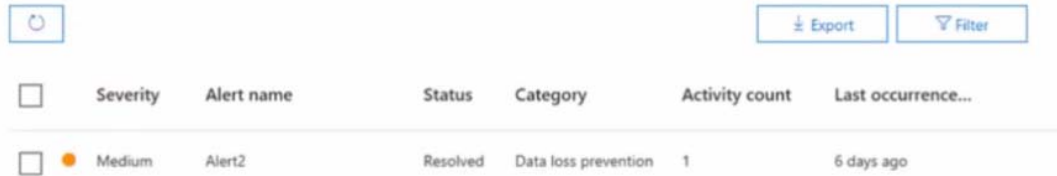
**Answer: A**

Explanation:

## Question: 92

You have a Microsoft 365 alert named Alert2 as shown in the following exhibit.

View alerts



<input type="checkbox"/>	Severity	Alert name	Status	Category	Activity count	Last occurrence...
<input type="checkbox"/>	Medium	Alert2	Resolved	Data loss prevention	1	6 days ago

You need to manage the status of Alert? To which status can you change Alette?

- A. The status cannot be changed.
- B. Dismissed only
- C. Investigating only
- D. Active or Investigating only
- E. Investigating. Active, or Dismissed

**Answer: D**

Explanation:

## Question: 93

You have a Microsoft \$65 subscription.

You plan to retain the following audit log record types and activities for the next three years.

- CopilotInteraction: All activities selected (1/1)
  - o Interacted with Copilot
- Compliance DLP endpoint: All activities selected {2/2}
  - o Matched DIP rule
  - o Removed DI P rule from document
- AzureActiveDirectory 2 of 25 activities selected (2/25)
  - o Reset user password
  - o Changed user password

What is the minimum number of audit retention policies you should create to retain only the selected record types and activities?

- A. 1
- B. 2
- C. 3
- D. 5

**Answer: C**

Explanation:

### Question: 94

You have a Microsoft 565 E5 subscription.

You plan to use Microsoft Purview insider risk management.

You need to create an insider risk management policy that will detect data theft from Microsoft SharePoint Online by users that submitted their resignation or are near their employment termination date.

What should you do first?

- A. Configure a HR data connector.
- B. Configure Office indicators.
- C. Configure a Physical badging connector.
- D. Onboard devices to Microsoft Defender for Endpoint.

**Answer: A**

Explanation:

### Question: 95

You have a Microsoft J65 subscription linked to a Microsoft Entra tenant that contains a user named User1. You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. the Security Reader role in the Microsoft Entra admin center
- B. the Compliance Management role in the Exchange admin center
- C. the View Only Audit Logs role in the Exchange admin center
- D. the Reviewer role in the Microsoft Purview portal

**Answer: C**

Explanation:

### Question: 96

HOTSPOT

You have a Microsoft 365 E5 subscription.  
From the Microsoft Purview Data Security Posture Management for AI portal, you review the recommendations for AI data security.  
You plan to create a one-click policy to block elevated risk users from pasting or uploading sensitive data to AI websites.  
How will the policy be configured? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

The policy mode will be configured to use:

- Test it out first
- Turn it on right away
- Keep it off

The policy will apply to:

- Devices only
- SharePoint sites only
- Instances only
- Devices and SharePoint sites
- Devices, Instances, and SharePoint sites

**Answer:**

Answer Area

The policy mode will be configured to use:

- Test it out first
- Turn it on right away
- Keep it off

The policy will apply to:

- Devices only
- SharePoint sites only
- Instances only
- Devices and SharePoint sites
- Devices, Instances, and SharePoint sites

Explanation:

## Question: 97

You have a Microsoft J65 E5 subscription that contains a user named User1.  
All users are assigned Microsoft 365 Copilot licenses.  
You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).  
You need to ensure that User1 can analyze prompts and responses for AI interaction events. The solution must follow the principle of least privilege.  
To which two role groups should you add User1? Each correct answer presents part of the solution.  
NOTE; Each correct selection is worth one point.

- A. Information Protection Analysts
- B. Security Reader
- C. Content Explorer Content Viewer

- D. Insider Risk Management Investigators
- E. Content Explorer list Viewer

**Answer: C, E**

Explanation:

**Question: 98**

**HOTSPOT**

You have a Microsoft 365 ES subscription that contains two Windows devices named Device1 and Device2. Device1 has the default browser set to Microsoft Edge. Device2 has the default browser set to Google Chrome.

You need to ensure that Microsoft Purview insider risk management can collect signals when a user copies files to a USB device by using their default browser.

What should you deploy to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- The Microsoft Defender Browser Protection extension
- The Microsoft Purview extension
- The Microsoft Purview Information Protection client

Device2:

- The Microsoft Defender Browser Protection extension
- The Microsoft Purview extension
- The Microsoft Purview Information Protection client

**Answer:**

Answer Area

Device1:

- The Microsoft Defender Browser Protection extension
- The Microsoft Purview extension
- The Microsoft Purview Information Protection client**

Device2:

- The Microsoft Defender Browser Protection extension
- The Microsoft Purview extension**
- The Microsoft Purview Information Protection client

Explanation:

## Question: 99

You have a Microsoft S65 E5 subscription that contains two users named User1 and Admin1. Admin1 manages audit retention policies for the subscription.

You need to ensure that the audit logs of User1 will be retained for 10 years.

What should you do first?

- A. Assign a Microsoft Purview Audit (Premium) add-on license to User1.
- B. Assign a 10-year audit log retention add-on license to Admin1.
- C. Assign a 10-year audit log retention add-on license to User1.
- D. Assign a Microsoft Purview Audit (Premium) add-on license to Admin1.

**Answer: C**

Explanation:

## Question: 100

HOTSPOT

You have a Microsoft 365 ES subscription.

You plan to use the Microsoft Purview portal to map human resources (HR) data for use with insider risk management policies.

You need to add a data connector to import the HR data.

What should you do first and in which format should you import the data? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The screenshot shows two dropdown menus. The 'First' dropdown menu is open, showing four options: 'Configure the Insider risk management settings.', 'Create a new import job in the Data lifecycle management settings.', 'Create a subject rights request.', and 'Register an app in Microsoft Entra ID.'. The 'Import as' dropdown menu is also open, showing four options: 'CSV', 'XLSX', 'XML', and 'ODS'.

**Answer:**

Answer Area

First:   
Create a new import job in the Data lifecycle management settings.  
Create a subject rights request.  
Register an app in Microsoft Entra ID.

Import as:   
XLSX  
XML  
ODS

Explanation:

## Question: 101

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If match, stop processing	Priority
Rule1	1 or more IP addresses	Tip1	No	0
Rule2	3 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tips will appear for File2?

- A. Tip1 only
- B. Tip2 only
- C. Tip3 only
- D. Tip1 and Tip2 only

**Answer: B**

Explanation:

## Question: 102

You have a Microsoft J65 E5 subscription. You plan to implement retention policies for Microsoft Teams. Which item types can be retained?

- A. voice memos from the Teams mobile client
- B. embedded images
- C. code snippets

**Answer: B**

Explanation:

## Question: 103

HOTSPOT

You have a Microsoft 365 tenant

You need to create a new sensitive info type for items that contain the following:

- An employee ID number that consists of the hire date of the employee followed by a three digit number
- The words "Employee", "ID", or "Identification" within 300 characters of the employee ID number

What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point

Answer Area

Primary element:

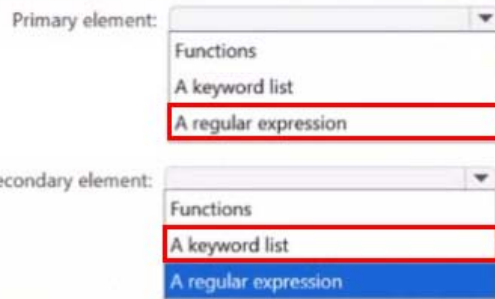
- Functions
- A keyword list
- A regular expression

Secondary element:

- Functions
- A keyword list
- A regular expression

**Answer:**

Answer Area



Explanation:

### Question: 104

You have a Microsoft 565 subscription that contains 100 users and a Microsoft 365 group named Group1. All users have Windows 11 devices and use Microsoft SharePoint Online and Exchange Online. A sensitivity label named Label1 is published as the default label for Group1. You add two sublabels named Sublabel1 and Sublabel2 to Label1. You need to ensure that the settings in Sublabel 1 are applied by default to Group 1. What should you do?

- A. Change the order of Sublabel1
- B. Duplicate all the settings from Sublabel1 to Label1.
- C. Modify the policy of Label1.
- D. Delete the policy of Label1 and publish Sublabel1.

**Answer: C**

Explanation:

### Question: 105

HOTSPOT

You have a Microsoft 365 subscription that contains the sensitive information types (SITs) shown in the following exhibit.

# Classifiers

Trainable classifiers Sensitive info types EDM classifiers

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

+ Create sensitive info type + Create Fingerprint based SIT Refresh 315 items Search

Name ↑	Type	Publisher
<input type="checkbox"/> ABA Routing Number	Entity	Microsoft Corporation
<input type="checkbox"/> ASPNET Machine Key	Credential	Microsoft Corporation
<input type="checkbox"/> Adatum document patterns	Fingerprint	111923cdkContoso.onmicrosoft.com
<input type="checkbox"/> Adatum numbers	Entity	Contoso
<input type="checkbox"/> All Credential Types	BundledCredential	Microsoft Corporation
<input type="checkbox"/> All Full Names	BundledEntity	Microsoft Corporation

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 flection is worth one point.

Answer Area

To create a new SIT, you can copy [answer choice].

- ABA Routing Number and Adatum numbers only
- ABA Routing Number, Adatum numbers, and All Full Names only
- Adatum document patterns and Adatum numbers only
- Adatum numbers only
- all of the SITs

You can edit [answer choice] directly without creating a copy first.

- ABA Routing Number and Adatum numbers only
- ABA Routing Number, Adatum numbers, and All Full Names only
- Adatum document patterns and Adatum numbers only
- Adatum numbers only
- all of the SITs

**Answer:**

Answer Area

To create a new SIT, you can copy [answer choice].

ABA Routing Number and Adatum numbers only  
ABA Routing Number, Adatum numbers, and All Full Names only  
Adatum document patterns and Adatum numbers only  
Adatum numbers only  
all of the SITs

You can edit [answer choice] directly without creating a copy first.

ABA Routing Number and Adatum numbers only  
ABA Routing Number, Adatum numbers, and All Full Names only  
Adatum document patterns and Adatum numbers only  
Adatum numbers only  
all of the SITs

Explanation:

## Question: 106

HOTSPOT

You have two Microsoft 365 subscriptions named Contoso and Fabrikam. The subscriptions contain the users shown in the following table.

Name	Subscription	Email address
User1	Contoso	user1@contoso.com
User2	Contoso	user2@contoso.com
User3	Fabrikam	user3@fabrikam.com
User4	Fabrikam	user4@fabrikam.com

You have a sensitivity label named Sensitivity1 as shown in the exhibit. (Click the Exhibit tab) you have the files shown in the following table.

Name	Sensitivity1
File1	Automatically applied by using an auto-labeling policy
File2	Applied by User2
File3	Applied by User1

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
User1 can edit rights for File1.	<input type="radio"/>	<input type="radio"/>
User2 can edit rights for File3.	<input type="radio"/>	<input type="radio"/>
User3 can print File2.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can edit rights for File1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can edit rights for File3.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can print File2.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 107

HOTSPOT

You have a Microsoft 365 ES subscription that contains the devices shown in the following table.

Name	Platform	Chipset
Device1	Windows 11	x64
Device2	Windows 11	ARM64
Device3	Windows 10	x86

You publish Microsoft Purview Information Protection sensitivity labels.

You plan to deploy the information protection client to the devices. The solution must ensure that the labels can be applied to sensitive images and documents

On which devices can you install the information protection client, and what should users use to apply labels? To answer, select the appropriate options in the answer area.

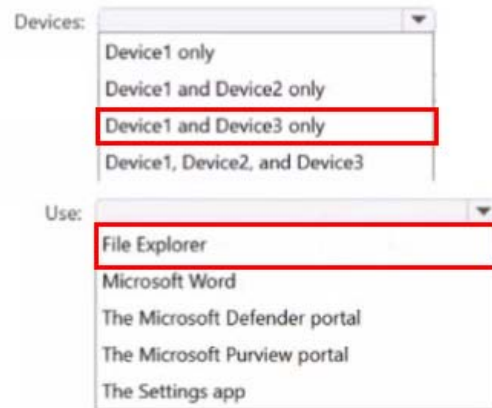
Answer Area

Devices:

Use:

**Answer:**

Answer Area



Explanation:

### Question: 108

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com. A user named User 1 sends link based, branded emails that are encrypted by using Microsoft Purview Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients Can User1 revoke the emails?

- A. Recipient1 only
- B. Recipient4 only
- C. Recipient1 and Recipient^ only
- D. Recipient3 and Recipients only
- E. Recipient1, Recipient2. Recipient3, and Recipient4

**Answer: D**

Explanation:

## Question: 109

### HOTSPOT

You are implementing Microsoft Purview Advanced Message Encryption for a Microsoft 365 tenant named contoso.com. You need to meet the following requirements:

- All email to a domain named fabrikam.com must be encrypted automatically.
- Encrypted emails must expire seven days after they are sent.

What should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically:

- A data connector in the Microsoft Purview portal
- A data loss prevention (DLP) policy in the Microsoft Purview portal
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:

- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft Purview portal
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft Purview portal

**Answer:**

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically:

- A data connector in the Microsoft Purview portal
- A data loss prevention (DLP) policy in the Microsoft Purview portal
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:

- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft Purview portal
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft Purview portal

Explanation:

## Question: 110

You have a Microsoft 365 E5 tenant that contains a user named User1. User1 is assigned the Compliance Administrator role. User1 cannot view the regular expression in the IP Address sensitive info type. You need to ensure that User1 can view the regular expression. What should you do?

- A. Assign User1 to the Reviewer role group
- B. Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.
- C. Instruct User1 to use the Test function on the sensitive info type.
- D. Assign User1 the Global Reader role.

**Answer: B**

Explanation:

## Question: 111

HOTSPOT

You have a Microsoft 365 subscription.

In Microsoft Exchange Online, you configure the mail flow rule shown in the following exhibit.

### Protect with OMEv2

 Edit rule conditions  Edit rule settings

Status: Enabled

Enable or disable rule

Enabled

Rule settings

Rule name

Protect with OMEv2

Mode

Enforce

Severity

Not Specified

Set date range

Specific date range is not set

Senders address

Matching Header 

Priority

0

For rule processing errors

Ignore

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.

Answer Area

Recipients who use Gmail [answer choice]

must sign in to the Office 365 Message Encryption (OME) portal to read messages  
will be unable to read messages  
will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription [answer choice]

must sign in to the Office 365 Message Encryption (OME) portal to read messages  
will be unable to read messages  
will have messages decrypted automatically

**Answer:**

Answer Area

Recipients who use Gmail [answer choice]

must sign in to the Office 365 Message Encryption (OME) portal to read messages  
will be unable to read messages  
will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription [answer choice]

must sign in to the Office 365 Message Encryption (OME) portal to read messages  
will be unable to read messages  
will have messages decrypted automatically

Explanation:

## Question: 112

You have a Microsoft 365 ES subscription  
You plan to create an met data match (EDM) classifier named EDM1.  
You need to grant permissions to hash and upload the sensitive information source table for EDM1. What should you create first?

- A. a Microsoft Entra enterprise application named EDM.DataUploaders
- B. a Microsoft Purview role group named EDM.DataUploaders
- C. a security group named EDM.DataUploaders
- D. a Microsoft Entra app registration named EDM.DataUploaders
- D. a Microsoft 365 group named EDM.Datauploaders

**Answer: C**

Explanation:

## Question: 113

HOTSPOT

You have a Microsoft 365 IS subscription that contains the resources shown in the following table.

Name	Type	Member of
User1	User	None
User2	User	Group1
Group1	Group	None

The subscription contains a Windows 11 device named Device 1 and has the Microsoft Purview Information Protection client installed. Device 1 contains the resources shown in the following table.

Name	Type	Path
File1.png	File	C:\Temp
File2.docx	File	D:\Folder1
Folder2	Folder	D:\

You publish a sensitivity label named Label1 to User1 and Group1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	<input type="radio"/>	<input type="radio"/>
User1 can apply Label1 to Folder2 by using the information protection client.	<input type="radio"/>	<input type="radio"/>
User2 can apply Label1 to File2.docx by using the information protection client.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can apply Label1 to Folder2 by using the information protection client.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can apply Label1 to File2.docx by using the information protection client.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 114

You are creating a custom trainable classifier to identify organizational product codes referenced in Microsoft 365 content. You identify 300 files to use as seed content. When should you store the seed content?

- A. a Microsoft OneDrive folder
- B. a Microsoft Exchange Online shared mailbox
- C. an Azure file share
- D. a Microsoft SharePoint Online folder

**Answer: D**

Explanation:

## Question: 115

You have a Microsoft 365 ES subscription.

You have a Microsoft SharePoint Online document library that contains Microsoft Word and Excel documents. The documents contain the following types of information:

- Credit card numbers
- Physical addresses in the UK
- National health service numbers from the UK
- Sensitive projects that contain the following words: Project Tailspin, Project Contoso, and Project Falcon

You have email messages in Microsoft Exchange Online that contain the following information types:

- Credit card numbers
- User sign-in credentials
- National health service numbers from the UK

You plan to use sensitive information types (SITs) for compliance policies.

What is the minimum number of SITs required to classify all the information types?

- A. 2
- B. 5
- C. 7
- D. 10

**Answer: B**

Explanation:

## Question: 116

You have a Microsoft 365 ES subscription that contains a Windows 11 device named Device 1 and three users named User 1, User2, and User3.

You plan to deploy Azure Information Protection (AIP) and the Microsoft Purview Information Protection client to Device 1.

You need to ensure that the users can perform the following actions on Device1 as part of the planned deployment

- User 1 will test the functionality of the client.
- User2 will install and configure the Microsoft Rights Management connector.
- User3 will be configured as the service account for the information protection scanner.

The solution must maximize the security of the sign-in process for the users What should you do?

- A. Exclude User2 and User3 from multifactor authentication (MfA).
- B. Enable User? and User3 for passwordless authentication.
- C. Exclude User1 and User? from multifactor authentication (Mf A}
- D. Enable User1, User I and User 3 for passkey (FIDO2) authentication

**Answer: B**

Explanation:

## Question: 117

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains three tiles named File1, File2, and File3.

You create the data loss prevention (DIP) policies shown in the following table.

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

The DIP rule matches for each tile are shown in the following table.

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

How many DIP policy matches events will be added to Activity explorer, and how many policy matches will be added to the DLP incidents report? To answer, select the appropriate options in the answer area.

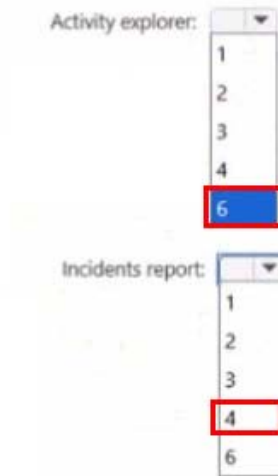
Answer Area

Activity explorer:

Incidents report:

**Answer:**

Answer Area



Explanation:

### Question: 118

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User 1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User 1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

Solution: You run the Set-AuditConfig -Workload Exchange command.

Does that meet the goal?

A. Yes

B. No

**Answer: A**

Explanation:

### Question: 119

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You onboard the computers to Microsoft Defender for Endpoint Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

Explanation:

### Question: 120

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).  
You have computers that run Windows 11 and have Microsoft 365 Apps instated. The computers are joined to a Microsoft Entra tenant  
You need to ensure that Endpoint DLP policies can protect content on the computers.  
Solution: You deploy the Endpoint DLP configuration package to the computers.  
Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

Explanation:

### Question: 121

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).  
You have computer that run Windows 11 and have Microsoft 365 Apps instated The computers are joined to a Microsoft Entra tenant  
You need to ensure that endpoint DLP policies can protect content on the computers.  
Solution: You deploy the Microsoft Purview Information Protection client to the computers.  
Does this meet the goal?

- A. Yes
- B. Yes

**Answer: B**

Explanation:

## Question: 122

You have a Microsoft 365 E5 subscription. The subscription contains a user named User1 and the sensitivity labels shown in the following table.

Name	Authenticated users: View content(VIEW)	Authenticated users: Copy and extract content(EXTRACT)	Authenticated users: Export content(EXPORT)
Label1	Granted	Not granted	Not granted
Label2	Granted	Granted	Not granted
Label3	Granted	Not granted	Granted

You publish the labels to User1.

The subscription contains the files shown in the following table.

Name	Label
File1	Label1
File2	Label2
File3	Label3

Which files can Microsoft 365 Copilot summarize for User1?

- A. File2only
- B. File3 only
- C. File2 and File3 only
- D. File1, File2. and File3

**Answer: A**

Explanation:

## Question: 123

You have a Microsoft 365 E5 subscription. The subscription contains 500 Windows devices that are onboarded to Microsoft Purview.

You need to prevent users from sharing sensitive information with third-party generative AI websites. Which Microsoft Purview solution should you use?

- A. Information Protection
- B. Information Barriers
- C. Insider Risk Management
- D. Data Loss Prevention

**Answer: D**

Explanation:

### Question: 124

You have a Microsoft 365 E5 subscription that contains a user named User1.

You deploy Microsoft Purview insider risk management.

You need ensure that insider risk management events related to User1 are visible only to specific users.

What should you create?

- A. a global exclusion
- B. an indicator variant
- C. a priority user group
- D. a detection group

**Answer: D**

Explanation:

### Question: 125

You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx. File1 has a sensitivity label applied. The label is configured as shown in the following table.

User	Permission
User1	Owner
User2	Editor
User3	Restricted Editor
User4	Viewer

Which users can summarize File1 by using Microsoft 365 Copilot?

- A. User1 only
- B. User1 and User2 only
- C. User1, User2, and User3 only
- D. User1, User2, User3, and User4

**Answer: B**

Explanation:

### Question: 126

#### HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to ensure that users are prevented from uploading sensitive data to ChatGPT and Google Gemini. The solution must meet the following requirements:

- Prevent credit card numbers from being pasted into ChatGPT and Gemini.
- Prevent documents that contain classified data from being uploaded to ChatGPT and Gemini.

Which Microsoft Purview solution should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Credit card numbers:

- Communication Compliance
- Data Loss Prevention**
- Information Barriers
- Insider Risk Management

Documents:

- Communication Compliance
- Data Loss Prevention**
- Information Barriers
- Insider Risk Management

**Answer:**

Answer Area

Credit card numbers:

- Communication Compliance
- Data Loss Prevention**
- Information Barriers
- Insider Risk Management

Documents:

- Communication Compliance
- Data Loss Prevention**
- Information Barriers
- Insider Risk Management

Explanation:

### Question: 127

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. You are evaluating the use of custom data assessment scans to identify the potential oversharing of data in the subscription. What is the maximum number of items the data assessments can support per location?

- A. 50.000
- B. 100.000
- C. 200.000
- D. 500.000

**Answer: C**

Explanation:

### Question: 128

You have a Microsoft 365 subscription. You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

- A. From Exchange Online PowerShell, run Start-ManagedFolderAssistant.
- B. From the Microsoft Purview portal, create a data loss prevention (DLP) policy.
- C. From the Microsoft Purview portal, create a label policy.
- D. From Exchange Online PowerShell, run start -RetentionAutoTagLearning.

**Answer: A**

Explanation:

### Question: 129

You have a Microsoft 365 E5 subscription that has a sensitivity label named Sensitivity1. You plan to create an auto-labeling policy that will apply Sensitivity1 to Microsoft Exchange Online mailboxes.

On February 1, you create the auto-labeling policy and enable simulation mode by using the default settings. No modifications are made to the policy in simulation mode.

When will the policy first be turned on?

- A. February 2
- B. February 6
- C. February 15
- D. never

**Answer: C**

Explanation:

### Question: 130

You have a Microsoft 365 E5 subscription that has a Microsoft Purview exact data match (EDM) classifier named EDM1.

You plan to create the Microsoft Purview policies shown in the following table.

Name	Type
DLP1	Data loss prevention (DLP)
Insider1	Insider risk management
Retention1	Retention

Which policies can use EDM1?

- A. DLP1 only
- B. Retention 1 only
- C. DLP1 and Insider1 only
- D. Insider1 and Retention1 only
- E. DLP1, Insider1, and Retention1

**Answer: A**

Explanation:

### Question: 131

You have a Microsoft 365 E5 subscriptions.

You deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).

You need to edit the default policies created as part of the deployment.

Which two Microsoft Purview solutions should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Insider Risk Management
- B. Information Protection
- C. Compliance Manager
- D. DSPMforAI
- E. Information Barriers
- F. Data Lifecycle Management
- G. Data Loss Prevention

**Answer: B, G**

Explanation:

### Question: 132

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Author
File1.docx	User1
File2.docx	User2
File3.docx	USER1

In the Microsoft Purview portal, you create a content search named Content1 and configure the search conditions as shown in the following exhibit.

# Define your search conditions

Query language-country/region: None 

Query builder

KQL editor

```
-Author:USER1
```

0 errors detected

Which files will be returned by Content1?

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

**Answer: B**

Explanation:

## Question: 133







You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a file named File1.docx.

You create a sensitivity label named Label1 as shown in the following exhibit.

**Assign permissions to specific users and groups** \* ⓘ

Assign permissions

3 items

Users and groups	Permissions	Edit	Delete
User1@86s40q.onmicrosoft.com	Co-Author		
User2@86s40q.onmicrosoft.com	Reviewer		
User3@86s40q.onmicrosoft.com	Viewer		

Use dynamic watermarking ⓘ

Use Double Key Encryption ⓘ

You apply Label1 to File1.

For which users can Microsoft 365 Copilot summarize File1?

- A. No user
- B. User 1 only
- C. User1 and User2 only
- D. User1, User2, and User3

**Answer: D**

Explanation:

## Question: 134

HOTSPOT









You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4 and a file named File1.docx.

To File1, you apply a sensitivity label that has the permissions shown in the following exhibit.

### Assign permissions to specific users and groups

Assign permissions

4 items

Users and groups	Permissions	Edit	Delete
User1@86s40q.onmicrosoft.com	Co-Owner		
User2@86s40q.onmicrosoft.com	Co-Author		
User3@86s40q.onmicrosoft.com	Reviewer		
User4@86s40q.onmicrosoft.com	Viewer		

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.

Answer Area

Microsoft 365 Copilot can summarize File1 for [answer choice].

- User1, User2, User3, and User4
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

For [answer choice], Microsoft 365 Copilot can reference File1 by using a link.

- User1, User2, User3, and User4
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

**Answer:**

Answer Area

Microsoft 365 Copilot can summarize File1 for [answer choice].

User1, User2, User3, and User4  
User1 only  
User1 and User2 only  
User1, User2, and User3 only  
**User1, User2, User3, and User4**

For [answer choice], Microsoft 365 Copilot can reference File1 by using a link.

User1, User2, User3, and User4  
**User1 only**  
User1 and User2 only  
User1, User2, and User3 only  
User1, User2, User3, and User4

Explanation:

## Question: 135

### HOTSPOT

You have a Microsoft 365 £5 subscription.

You are implementing insider risk management.

You need to create an insider risk management notice template and format the message body of the notice template.

How should you configure the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use the: Microsoft Purview portal  
Microsoft 365 admin center  
Microsoft Defender portal  
Microsoft Entra admin center  
**Microsoft Purview portal**

Format in: HTML  
**HTML**  
Markdown  
RTF  
XML

**Answer:**

## Answer Area

Use the: Microsoft Purview portal

- Microsoft 365 admin center
- Microsoft Defender portal
- Microsoft Entra admin center
- Microsoft Purview portal**

Format in: HTML

- HTML**
- Markdown
- RTF
- XML

Explanation:

## Question: 136

### HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. The subscription contains an Endpoint data loss prevention (Endpoint DLP) policy as shown in the Actions exhibit. (Click the Actions tab.)

^ **Actions**

Use actions to protect content when the conditions are met.

^ **Audit or restrict activities on devices**

When specific activities are detected on devices with protected files containing sensitive information, you can choose whether to only audit the activity, block it entirely, or block it and 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.

<input checked="" type="checkbox"/> Upload to a restricted cloud service domain or access from an unallowed browsers	ⓘ	Audit only
Sensitive service domain group restriction(s) configured. <a href="#">Edit</a>		
<input checked="" type="checkbox"/> Paste to supported browsers	ⓘ	Audit only
Sensitive service domain group restriction(s) configured. <a href="#">Edit</a>		

You configure the Upload to a restricted cloud service domain or access from an unallowed browsers settings as shown in the Upload restrictions exhibit. (Click the Upload restrictions tab.)

### Sensitive service domain restrictions

Enforce different restrictions for sensitive service domains that are defined by the sensitive service domain groups set up in endpoint DLP settings.

+ Add group   ↑↓ Reorder   ✕ Clear selection

Group	Priority	Action
<input type="checkbox"/> Mail Services	1	Block with ov...
<input type="checkbox"/> File Services	2	Block
<input type="checkbox"/> Generative AI Websites	3	Block

You configure the Paste to supported browsers settings as shown in the Paste restrictions exhibit. (Click the Paste restrictions tab.)

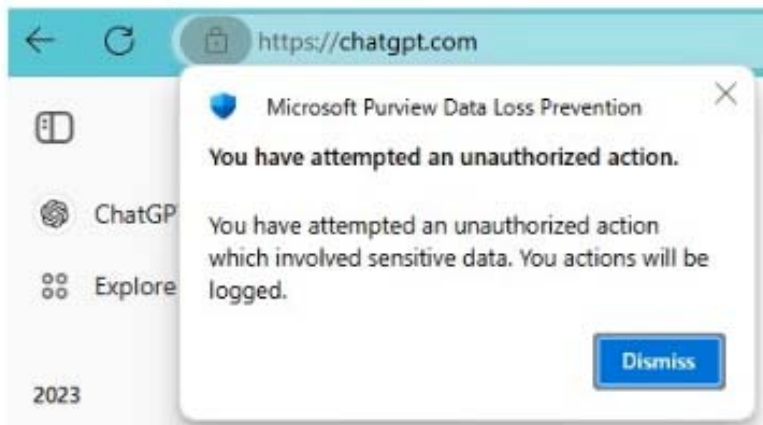
### Sensitive service domain restrictions

Enforce different restrictions for sensitive service domains that are defined by the sensitive service domain groups set up in endpoint DLP settings.

+ Add group   ↑↓ Reorder   ✕ Clear selection

Group	Priority	Action
<input type="checkbox"/> Mail Services	1	Block
<input type="checkbox"/> Generative AI Websites	2	Block with ov...

When User1 pastes content into ChatGPT, the user receives the error message shown in the Error exhibit. (Click the Error tab.)



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
User1 can paste sensitive data from an email to ChatGPT after selecting <b>Dismiss</b> .	<input type="radio"/>	<input type="radio"/>
User1 can upload emails that contain sensitive data to ChatGPT after selecting <b>Dismiss</b> .	<input type="radio"/>	<input type="radio"/>
User1 can paste sensitive data from a Microsoft Word document to ChatGPT after selecting <b>Dismiss</b> .	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can paste sensitive data from an email to ChatGPT after selecting <b>Dismiss</b> .	<input type="radio"/>	<input checked="" type="radio"/>
User1 can upload emails that contain sensitive data to ChatGPT after selecting <b>Dismiss</b> .	<input type="radio"/>	<input checked="" type="radio"/>
User1 can paste sensitive data from a Microsoft Word document to ChatGPT after selecting <b>Dismiss</b> .	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 137

**HOTSPOT**

You have a Microsoft 365 E5 subscription that uses Microsoft Purview Audit (Premium) with the 10-Year Audit Log Retention add-on license.

The subscription contains the audit retention policies shown in the following table.

Name	Users	Record type	Activities	Duration	Priority
RP1	User1	SharePoint	Created site collection	1 Year	30
RP2	User1	SharePoint	None	3 Years	20
RP3	User1	SharePoint	Created site collection	3 Years	40
RP4	User1	SharePoint	Renamed site	6 Months	10

From the SharePoint Online admin center, User1 performs the actions shown in the following table.

Name	Description
Action1	Archives a site
Action2	Creates a site collection
Action3	Renames a site

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
Action1 will be retained for one year.	<input type="radio"/>	<input type="radio"/>
Action2 will be retained for three years.	<input type="radio"/>	<input type="radio"/>
Action3 will be retained for six months.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
Action1 will be retained for one year.	<input type="radio"/>	<input checked="" type="radio"/>
Action2 will be retained for three years.	<input type="radio"/>	<input checked="" type="radio"/>
Action3 will be retained for six months.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

### Question: 138

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps. You need to ensure that you receive an alert when a user uploads a document to a third-party cloud storage service.

What should you use?

- A. an activity policy
- B. a sensitivity label
- C. a file policy

D. an insider risk policy

**Answer: C**

Explanation:

### Question: 139

You have a Microsoft 365 E5 subscription.  
You plan to use insider risk management to collect and investigate forensic evidence.  
You need to enable forensic evidence capturing.  
What should you do first?

- A. Configure the information protection scanner.
- B. Claim capacity.
- C. Enable Adaptive Protection.
- D. Create priority user groups.

**Answer: B**

Explanation:

### Question: 140

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.  
You need to deploy a Microsoft Purview insider risk management solution that will generate an alert when users share sensitive information on Site1 with external recipients.  
Which two actions should you perform? Each correct answer presents part of the solution.  
NOTE: Each correct answer is worth one point.

- A. Create a data loss prevention (DLP) policy.
- B. Turn on Indicators.
- C. Configure adaptive protection.
- D. Turn on analytics.
- E. Create an insider risk policy.

**Answer: B, E**

Explanation:

## Question: 141

You have a Microsoft 365 subscription.  
You create and run a content search from the Microsoft Purview portal.  
You need to download the results of the content search.  
What should you obtain first?

- A. a certificate
- B. a password
- C. a pin
- D. an export key

**Answer: D**

Explanation:

## Question: 142

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 that has the users shown in the following table.

Name	Role
User1	Owner
User2	Member

You create the retention labels shown in the following table.

Name	Retention period	Retention action	Based on
Retention1	4 years	Retain only	When a file was labeled
Retention2	2 years	Retain and delete	When a file was labeled

You publish the retention labels to Site1.

On March 1,2023, you assign the retention labels to the files shown in the following table.

Name	Modified by	Retention label
File1	User1	Retention1
File2	User1	Retention2

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
User1 can delete File1 on March 10, 2023.	<input type="radio"/>	<input type="radio"/>
User2 can delete File1 on March 10, 2027.	<input type="radio"/>	<input type="radio"/>
User2 can edit File2 on March 15, 2025.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2023.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete File1 on March 10, 2027.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can edit File2 on March 15, 2025.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 143

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.

Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

You have a custom employee information form named Template1 .docx.  
 You plan to create a sensitive info type named Sensitive1 that will use the document fingerprint from Template1.docx.

What should you use to create Sensitive1, and in which DLP policies can you use Sensitive1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create Sensitive1 by using:

- The Microsoft Purview portal
- Security & Compliance PowerShell
- The Exchange admin center
- The Microsoft Purview portal**
- The SharePoint admin center

Use Sensitive1 in:

- DLP1, DLP2, and DLP3
- DLP1 only
- DLP2 only
- DLP1 and DLP2 only
- DLP1, DLP2, and DLP3**

**Answer:**

Answer Area

Create Sensitive1 by using:

- The Microsoft Purview portal
- Security & Compliance PowerShell
- The Exchange admin center
- The Microsoft Purview portal**
- The SharePoint admin center

Use Sensitive1 in:

- DLP1, DLP2, and DLP3
- DLP1 only
- DLP2 only
- DLP1 and DLP2 only
- DLP1, DLP2, and DLP3**

Explanation:

**Question: 144**

HOTSPOT

You have a Microsoft 365 E5 tenant.

You have sensitivity labels as shown in the Sensitivity Labels exhibit. (Click the Sensitivity Labels tab.)

+ Create a label   Publish labels   Refresh

Name	Order	Scope
Public	0 - lowest	File, Email
General	1	File, Email
Confidential	2	File, Email
Internal	3	File, Email
External	4 - highest	File, Email

The Confidential/External sensitivity label is configured to encrypt files and emails when applied to content.

The sensitivity labels are published as shown in the Published exhibit. (Click the Published tab.)

## Sensitivity Policy1

[Edit policy](#)   [Delete policy](#)

### Name

Sensitivity Policy1

### Description

### Published labels

Public  
General  
Confidential  
Confidential/Internal  
Confidential/External

### Published to

All

### Policy settings

Users must provide justification to remove a label or lower its classification

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
The Internal sensitivity label inherits all the settings from the Confidential label.	<input type="radio"/>	<input type="radio"/>
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	<input type="radio"/>	<input type="radio"/>
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	<input type="radio"/>	<input checked="" type="radio"/>
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	<input type="radio"/>	<input checked="" type="radio"/>
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

### Question: 145

You have a Microsoft 365 subscription.  
You create a new trainable classifier.  
You need to train the classifier.  
Which source can you use to train the classifier?

- A. an on-premises Microsoft SharePoint Server site
- B. an Azure Files share
- C. a Microsoft SharePoint Online site
- D. an NFS file share

**Answer: C**

Explanation:

### Question: 146

You have a Microsoft 365 tenant that uses Microsoft Purview Message Encryption.  
You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using Microsoft Purview Message Encryption.

What should you do?

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

**Answer: A**

Explanation:

## Question: 147

HOTSPOT

You have a Microsoft 365 subscription that contains a sensitivity label named Contoso Confidential.

You publish Contoso Confidential to all users.

Contoso Confidential is configured as shown in the Configuration exhibit. (Click the Configuration tab.)

## Edit sensitivity label

- ✓ Label details
- ✓ Scope
- ✓ Items
- ✓ Groups & sites
- ✓ Schematized data assets (preview)
- Finish**

### Review your settings and finish

**Name**  
Contoso Confidential

**Display name**  
Contoso Confidential  
[Edit](#)

**Description for users**  
Contoso Confidential  
[Edit](#)

**Scope**  
Files & other data assets, Email  
[Edit](#)

**Access control**  
[Edit](#)

**Content marking**  
Footer: Contoso Confidential Internal use only  
[Edit](#)

**Auto-labeling for files and emails**  
None  
[Edit](#)

**Auto-labeling for schematized data assets (preview)**  
None  
[Edit](#)

[Back](#) [Save label](#)

The Access control settings of Contoso Confidential are configured as shown in the Access control exhibit. (Click the Access control tab.)

# Edit sensitivity label

- ✓ Label details
- ✓ Scope
- ✓ Items
- ✓ Groups & sites
- ✓ Schematized data assets (preview)
- Finish**

## Review your settings and finish

### Name

Contoso Confidential

### Display name

Contoso Confidential

[Edit](#)

### Description for users

Contoso Confidential

[Edit](#)

### Scope

Files & other data assets, Email

[Edit](#)

### Access control

Access control

[Edit](#)

### Content marking

Footer: Contoso Confidential Internal use only

[Edit](#)

### Auto-labeling for files and emails

None

[Edit](#)

### Auto-labeling for schematized data assets (preview)

None

[Edit](#)

[Back](#)

[Save label](#)

[Cancel](#)

# Edit sensitivity label

- Label details
- Scope
- Items**
- Access control
- Content marking
- Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

## Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings

*i* Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. [Learn more about this setting](#)

[Go to co-authoring setting](#)

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires *i*

Never

Allow offline access *i*

Only for a number of days

Users have offline access to the content for this many days

7

**Assign permissions to specific users and groups** \* *i*

[Assign permissions](#)

1 item

Users and groups	Permissions	Edit	Delete
AuthenticatedUsers	Co-Author		

Use dynamic watermarking *i*

Use Double Key Encryption *i*

[Back](#)

[Next](#)

[Cancel](#)

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

Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	<input type="radio"/>	<input type="radio"/>
Guest users will be able to open documents protected by Contoso Confidential.	<input type="radio"/>	<input type="radio"/>
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	<input checked="" type="radio"/>	<input type="radio"/>
Guest users will be able to open documents protected by Contoso Confidential.	<input type="radio"/>	<input checked="" type="radio"/>
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

**Question: 148**

**HOTSPOT**

You have a Microsoft 365 £5 subscription.

You have a Microsoft Purview Advanced Message Encryption branding template named OME1.

You need to create a Microsoft Exchange Online mail flow rule to apply OME1 to email.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Apply this rule if:

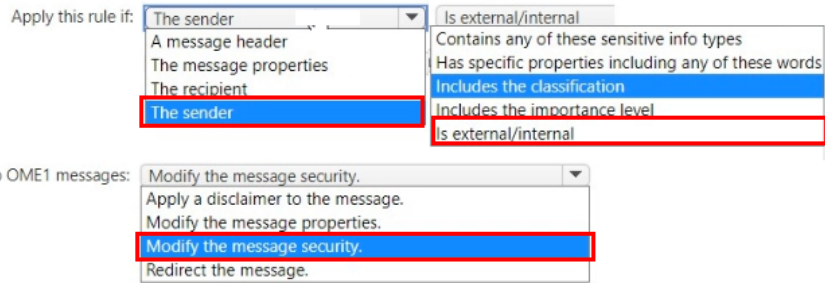
The sender	Is external/internal
A message header	Contains any of these sensitive info types
The message properties	Has specific properties including any of these words
The recipient	Includes the classification
The sender	Includes the importance level
	Is external/internal

To apply custom branding to OME1 messages:

Modify the message security.
Apply a disclaimer to the message.
Modify the message properties.
Modify the message security.
Redirect the message.

**Answer:**

Answer Area



Explanation:

### Question: 149

You have a sensitive information type based on a trainable classifier. You are unsatisfied with the result of the trainable classifier. You need to retrain the classifier. What should you use in the Microsoft Purview portal?

- A. Content explorer from Data classification
- B. Labels from Information protection
- C. Labels from Information governance
- D. Content search

**Answer: A**

Explanation:

### Question: 150

HOTSPOT

You have a Microsoft 365 £5 subscription that contains the groups shown in the following table.

Name	Type	Primary email address
Group1	Microsoft 365	Group1@contoso.com
Dist1	Distribution	Dist1@contoso.com

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Dist1
User3	None

You create the mail flow rules shown in the following table.

Name	Apply this rule if	Do the following
Rule1	The recipient is a member of group1@contoso.com	Apply Office 365 Message Encryption and rights protection
Rule2	The sender is dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

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

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	<input type="radio"/>	<input type="radio"/>
If User2 sends an email message to User1, the message is encrypted automatically.	<input type="radio"/>	<input type="radio"/>
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 sends an email message to User1, the message is encrypted automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 151

You have a Microsoft 365 tenant that is opt-in for trainable classifiers. You need to ensure that a user named User1 can create custom trainable classifiers. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. Security Administrator
- B. Compliance Administrator
- C. Global Administrator
- D. Security Operator

**Answer: C**

Explanation:

## Question: 152

You have a Microsoft 365 E5 subscription. You create a sensitivity label named Label1 and publish Label1 to all users and groups. You have the following files in a SharePoint site:

- File1.doc
- File2.docx
- File3.xlsx
- File4.txt

You need to identify which files can have Label1 applied. Which files should you identify?

- A. File2.docx only
- B. File2.docx and File3.xlsx only
- C. File1.doc File2-docx, and File3.xlsx only
- D. File1.doc File2-docx, File3.xlsx, and File4.txt

**Answer: B**

Explanation:

## Question: 153

You have a Microsoft 365 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2. You plan to use policies to meet the following requirements:

- Add a watermark of Confidential to a document if the document contains the words Project1 or Project2.
- Retain a document for seven years if the document contains credit card information.
- Add a watermark of Internal Use Only to all the documents stored on Site2.
- Add a watermark of Confidential to all the documents stored on Site1.

You need to recommend the minimum number of sensitive info types required.  
How many sensitive info types should you recommend?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: C**

Explanation:

### Question: 154

You need to test Microsoft Purview Advanced Message Encryption capabilities for your company. The test must verify the following information:

- The acquired default template names
- The encryption and decryption verification status

Which PowerShell cmdlet should you run?

- A. Test-OAuthConnectivity
- B. Test-ClientAccessRule
- C. Test-IRMConfiguration
- D. Test-Mailflow

**Answer: C**

Explanation:

### Question: 155

You have a Microsoft 365 E5 subscription that contains the adaptive scopes shown in the following table.

Name	Type	Query
Scope1	Users	FirstName starts with User
Scope2	SharePoint Online sites	SiteTitle starts with Site

You create the retention policies shown in the following table.

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

Which retention policies support a preservation lock?

- A. RPolicy2only
- B. RPolicy3on1y
- C. RPolicy1 and RPolicy2 only
- D. RPolicy1 and RPolicy3 only
- E. RPolicy1, RPolicy2, and RPolicy3

<b>Answer: B</b>
------------------

Explanation:

## Question: 156

At the end of a project, you upload project documents to a Microsoft SharePoint Online library that contains many files. The following is a sample of the project document file names:

- aei\_AA989.docx
- bd\_WS098.docx
- cei\_DF112.docx
- ebc\_QQ454.docx
- ecc\_BB565.docx

All documents that use this naming format must be labeled as Project Documents:

You need to create an auto-apply retention label policy.

What should you use to identify the files?

- A. A retention label
- B. A trainable classifier
- C. A sensitive info type

**Answer: C**

Explanation:

## Question: 157

DRAGDROP

You have a Microsoft 365 £5 subscription.

You need to prevent the sharing of sensitive information in Microsoft Teams.

Which entities can you protect by applying a data loss prevention (DLP) policy to each resource? To answer, drag the appropriate activities to the correct entity. Each activity 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.

Activities	Answer Area
<input type="checkbox"/> 1:1/n chats only	User accounts: <input type="text"/>
<input type="checkbox"/> Private channels only	Microsoft 365 groups: <input type="text"/>
<input type="checkbox"/> General chats only	Security groups or distribution lists: <input type="text"/>
<input type="checkbox"/> 1:1/n chats and private channels only	
<input type="checkbox"/> 1:1/n chats and general chats only	
<input type="checkbox"/> Private channels and general chats only	
<input type="checkbox"/> 1:1/n chats, private channels, and general	

**Answer:**

Activities	Answer Area
<input type="checkbox"/> 1:1/n chats only	User accounts: <input type="checkbox"/> 1:1/n chats and private channels only
<input type="checkbox"/> Private channels only	Microsoft 365 groups: <input type="checkbox"/> General chats only
<input type="checkbox"/> General chats only	Security groups or distribution lists: <input type="checkbox"/> 1:1/n chats and private channels only
<input type="checkbox"/> 1:1/n chats and private channels only	
<input type="checkbox"/> 1:1/n chats and general chats only	
<input type="checkbox"/> Private channels and general chats only	
<input type="checkbox"/> 1:1/n chats, private channels, and general	

Explanation:

## Question: 158

You have a Microsoft 365 E5 subscription.

You create a data loss prevention (DLP) policy and select. Use Notifications to inform your users and help educate them on the proper use of sensitive info.

Which apps will show the policy tip?

- A. Outlook on the web only
- B. Outlook Win32 only
- C. Outlook for iOS and Android only
- D. Outlook on the web and Outlook Win32 only
- E. Outlook Win32 and Outlook for iOS and Android only
- F. Outlook on the web. Outlook Win32, and Outlook for iOS and Android

**Answer: D**

Explanation:








### Question: 159

You are creating a DLP policy named Policy1 that will be applied to the locations as shown in the following exhibit.

# Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

 Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

	Location	Scope	Actions
<input checked="" type="checkbox"/>	 Exchange email	All groups	Edit
<input checked="" type="checkbox"/>	 SharePoint sites	All sites	Edit
<input checked="" type="checkbox"/>	 OneDrive accounts	All users & groups	Edit
<input checked="" type="checkbox"/>	 Teams chat and channel messages	All users & groups	Edit
<input checked="" type="checkbox"/>	 Instances	All instances	Edit
<input checked="" type="checkbox"/>	 On-premises repositories	All repositories	Edit
<input type="checkbox"/>	 Fabric and Power BI workspaces	Turn on location to scope	

Policy1 contains an advanced data loss prevention (DLP) rule named Rule1.

Which two conditions can you use in Rule1? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Document property is
- B. Attachment's file extension is
- C. Document size equals or is greater than
- D. Content is shared from Microsoft 365
- E. Content contains

**Answer: D, E**

Explanation:

### Question: 160

You have a Microsoft 365 E5 subscription that contains a device named Device1. You need to enable Endpoint data loss prevention (Endpoint DLP) for Device1. What should you do first in the Microsoft Purview portal?

- A. Turn on device onboarding.
- B. Enable Microsoft Privacy Risk Management.
- C. Create a Microsoft Purview Information Barriers (IBs) segment.
- D. Add a Microsoft Purview Information Protection scanner cluster.
- E. Onboard Device1 to Microsoft Purview.

**Answer: A**

Explanation:

### Question: 161

You have a Microsoft 365 E5 tenant. You create a data loss prevention (DLP) policy. You need to ensure that the policy protects documents in Microsoft Teams chat sessions. Which location should you enable in the policy?

- A. SharePoint sites
- B. Exchange email
- C. Teams chat and channel messages
- D. OneDrive accounts

**Answer: D**

Explanation:

### Question: 162

**DRAGDROP**

You have a Microsoft 365 tenant.

A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years, and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.

You need to implement the regulatory requirement.

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**

- Add a management lock.
- Create a retention policy.
- Create a retention label.
- Create a retention label policy.
- Add a preservation lock.

**Answer Area**

**Answer:**

**Actions**

- Add a management lock.
- Create a retention policy.
- Create a retention label.
- Create a retention label policy.
- Add a preservation lock.

**Answer Area**

- Create a retention label.
- Create a retention label policy.
- Add a preservation lock.

Explanation:

**Question: 163**

You need to create a retention policy to delete content after seven years from the following locations:

- Exchange Online email
- SharePoint Online sites
- OneDrive accounts
- Microsoft 365 Groups
- Teams channel messages
- Teams chats

What is the minimum number of retention policies that you should create?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer: B**

Explanation:

**Question: 164**

**HOTSPOT**

You create a retention label policy named Contoso\_Policy that contains the following labels:

- 10 years then delete
- 5 years then delete
- Do not retain

Contoso.Policy is applied to content in Microsoft SharePoint Online sites.

After a couple of days, you discover the following messages on the Properties page of the label policy:

- Status: Off (Error)
- It's taking longer than expected to deploy the policy

You need to reinitiate the policy.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Set-RetentionCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Start-EdgeSynchronization

Start-RetentionAutoTagLearning

-id Contoso\_Policy

-RetryDistribution

-ForceFullSync

-FullCrawl

-RetryDistribution

-Train

**Answer:**

Answer Area

Set-RetentionCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Start-EdgeSynchronization

Start-RetentionAutoTagLearning

-id Contoso\_Policy

-RetryDistribution

-ForceFullSync

-FullCrawl

-RetryDistribution

-Train

Explanation:

## Question: 165

### HOTSPOT


You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of
User1	Members group of Site1
User2	Owners group of Site1
Admin1	SharePoint Administrator role

You have a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

^ **Actions**

Use actions to protect content when the conditions are met.

^ **Restrict access or encrypt the content in Microsoft 365 locations** 

**Restrict access or encrypt the content in Microsoft 365 locations**

Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.  
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

Block everyone. ⓘ

Block only people outside your organization. ⓘ

Block only people who were given access to the content through the "Anyone with the link" option. ⓘ

+ Add an action v

You apply DLP1 to Site1.

User1 uploads a file named File1 to Site1. File1 does NOT match any of the DLP1 rules. User2 updates File1 to contain data that matches the DLP1 rules.  
 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
User1 can access File1 on Site1.	<input type="radio"/>	<input type="radio"/>
User2 can access File1 on Site1.	<input type="radio"/>	<input type="radio"/>
Admin1 can access File1 on Site1.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access File1 on Site1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can access File1 on Site1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 166

HOTSPOT

You have a Microsoft 365 subscription that has a retention label named Retention1. The subscription contains the files shown in the following table.

Name	Stored in	Number of sensitive information types (SITs)		
		IP address	SWIFT code	Shared access signature (SAS)
File1	Microsoft Exchange Online	1	2	4
File2	Microsoft SharePoint Online	3	5	1
File3	Microsoft OneDrive	3	3	2

You create an auto-labeling policy named Policy1 that will automatically apply Retention1 as shown in the Auto-labeling policy

Exhibit. (Click the Auto-labeling policy tab.)

You configure Policy1 to apply Retention1 as shown in the Locations exhibit. (Click the Locations tab.)

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
Retention1 is applied to File1.	<input type="radio"/>	<input type="radio"/>
Retention1 is applied to File2.	<input type="radio"/>	<input type="radio"/>
Retention1 is applied to File3.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
Retention1 is applied to File1.	<input checked="" type="radio"/>	<input type="radio"/>
Retention1 is applied to File2.	<input checked="" type="radio"/>	<input type="radio"/>
Retention1 is applied to File3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 167

You have a Microsoft 365 E5 subscription that contains a data loss prevention (DLP) policy named DLP1. DLP1 contains the DLP rules shown in the table.

Name	Priority	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules.
Rule1	0	On	Tip 1	Enabled
Rule2	1	On	Tip 2	Enabled
Rule3	2	On	Tip 3	Disabled
Rule4	3	On	Tip 4	Enabled

You need to ensure that when a document matches all the rules, users will see Tip 2. What should you change?

- A. the priority setting of Rule2 to 0
- B. the priority setting of Rule2 to 2
- C. the priority setting of Rule3 and Rule4 to 0
- D. the If there's a match for this rule, stop processing additional DLP policies and rules setting for Rule3 to Enabled

**Answer: A**

Explanation:

## Question: 168

You have a Microsoft 365 E5 subscription that contains a user named User1. You deploy Microsoft Purview Data Security Posture Management for AD (DSPM for AD). You need to ensure that User1 can verify the auditing status of the subscription. The solution must follow the principle of least privilege. To which role group should you add User1?

- A. Insider Risk Management Analysts
- B. Security Reader
- C. Insider Risk Management Investigators
- D. View-Only Organization Management for Microsoft Exchange Online

**Answer: B**

Explanation:

## Question: 169

DRAGDROP

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview Insider Risk Management.

You obtain a file named File1.csv that contains employee resignation data.

You need to implement the HR data connector and upload File1.csv by using the connector.

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

- From the Microsoft Purview portal, add the data connector.
- Run a sample script to upload File1.csv.
- From the Microsoft Entra admin center, create an app registration.
- Configure the Insider Risk Management settings.
- Implement Microsoft Entra Connect sync.

Answer Area

**Answer:**

Actions

- From the Microsoft Purview portal, add the data connector.
- Run a sample script to upload File1.csv.
- From the Microsoft Entra admin center, create an app registration.
- Configure the Insider Risk Management settings.
- Implement Microsoft Entra Connect sync.

Answer Area

- From the Microsoft Entra admin center, create an app registration.
- From the Microsoft Purview portal, add the data connector.
- Run a sample script to upload File1.csv.

Explanation:

## Question: 170

### HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need to deploy a compliance solution that will detect the accidental oversharing of information outside of an organization.

The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Policy template:

Policy template prerequisite:

Policy template prerequisite:

**Answer:**



Explanation:

### Question: 171

You have a Microsoft 365 E5 subscription.  
You are implementing insider risk management.  
You need to maximize the amount of historical data that is collected when an event is triggered.  
What is the maximum number of days that historical data can be collected?

- A. 30
- B. 60
- C. 90
- D. 180

**Answer: C**

Explanation:

### Question: 172

You have a Microsoft 365 E5 subscription that contains 500 Windows devices.  
You plan to deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI).  
You need to ensure that you can monitor user activities on third-party generative AI websites.

Which two prerequisites should you complete for DSPM for AI? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Install the Microsoft Purview extension on the devices.
- B. Create a data leaks policy.
- C. Onboard the devices to Microsoft Purview.
- D. Create a communication compliance policy.
- E. Create an Endpoint data loss prevention (Endpoint DLP) policy.
- F. Enroll the devices in Microsoft Intune.

**Answer: A, C**

Explanation:

### Question: 173

You have a Microsoft 365 E5 subscription that uses retention label policies. You need to identify all the changes made to retention labels during the last 30 days. What should you use in the Microsoft Purview portal?

- A. Reports
- B. Activity explorer
- C. User data search
- D. Content search

**Answer: B**

Explanation:

### Question: 174

DRAGDROP

You have a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management and contains three users named User1, User2, and User3.

All insider risk management policies have adaptive protection enabled and the default conditions for insider risk levels configured.

The users perform the following activities, which trigger insider risk policy alerts:

User1 performs at least one data exfiltration activity that results in a high severity risk score.

User2 performs at least three risky user activities within seven days, that each results in a high severity risk score.

User3 performs at least two data exfiltration activities within seven days, that each results in a high severity risk score.

Which insider risk level is assigned to each user? To answer, drag the appropriate levels to the correct users. Each level 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.

**Answer:**

Explanation:

## Question: 175

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Microsoft Purview role group	Microsoft 365 role
User1	None	Global Administrator
User2	Insider Risk Management Analysts	None
User3	Insider Risk Management Investigators	None

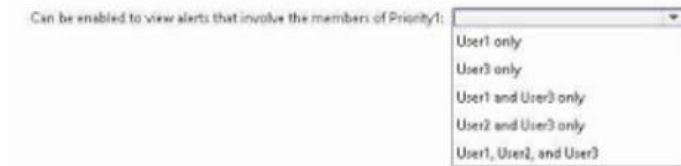
The subscription contains the groups shown in the following table.

You plan to create a priority user group named Priority1.

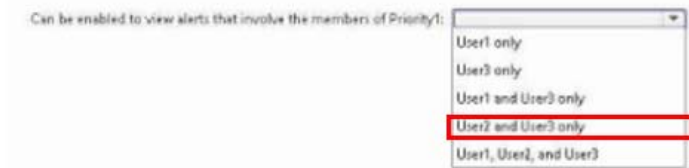
You need to identify the following:

- . Which users and groups can be added to Priority1?
- . Which users can be enabled to view alerts that involve the members of Priority1?

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



**Answer:**



Explanation:

## Question: 176

HOTSPOT

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. Site1 has a document library that contains the files shown in the following table.

Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

From the Microsoft Purview compliance portal, for Site1 you create a content search named Search1 that has the date in the YYYY-MM-DD format as shown in the following exhibit.

**Define your search conditions**

Query language-country/region: None

Query builder  
 KQL editor

**Created**

Before

2024-01-31

**AND**

**File type**

Equals name of

docx

Back Next Cancel

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
File1 is included in the Search1 results.	<input type="radio"/>	<input type="radio"/>
File2 is included in the Search1 results.	<input type="radio"/>	<input type="radio"/>
File3 is included in the Search1 results.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
File1 is included in the Search1 results.	<input type="radio"/>	<input checked="" type="radio"/>
File2 is included in the Search1 results.	<input checked="" type="radio"/>	<input type="radio"/>
File3 is included in the Search1 results.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

### Question: 177

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains three files named File1, File2, and File3.

You create the data loss prevention (DLP) policies shown in the following table.

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

The DLP rule matches for each file are shown in the following table.

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

How many DLP policy matches events will be added to Activity explorer, and how many policy matches will be added to the DLP incidents report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Activity explorer:

Incidents report:

Incidents report:

**Answer:**

Answer Area

Activity explorer:

Incidents report:

Incidents report:

Explanation:

## Question: 178

Nate: 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 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant.

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You onboard the computers to Microsoft Defender for Endpoint.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

Explanation:

## Question: 179

You have a Microsoft 365 E5 subscription.

You plan to deploy Microsoft Purview Data Security Posture Management for AI (DSPM for AI) to protect company data that contains Personally Identifiable Information (PII) from being shared with third-party generative AI tools.

You need to complete the prerequisites for the planned deployment.

Which two Microsoft Purview solutions should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Data Loss Prevention
- B. Communication Compliance
- C. Audit
- D. Insider Risk Management
- E. Information Barriers

**Answer: A, C**

Explanation:

## Question: 180

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of security group
User1	Group1, Group2
User2	Group2
User3	Group1, Group3

You have the data loss prevention (DLP) policies shown in the following table.

Name	Location	Included	Number of DLP rules	Rule severity
DLP1	Devices	Group1	1	High
DLP2	Devices	Group2	1	Medium
DLP3	Devices	Group3	1	Medium

From Insider risk management, you configure a priority user group named PriGroup1 that contains User3 as a member. You have the insider risk policies shown in the following table.

Name	Policy template	Trigger	Group
Policy1	Data leaks	DLP1	Group1
Policy2	Data leaks	DLP2	Group2
Policy3	Data leaks by priority users	DLP3	PriGroup1

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
When User3 performs an action that matches the rule for DLP1, Policy1 generates an alert.	<input type="radio"/>	<input type="radio"/>
When User1 performs an action that matches the rule for DLP2, Policy2 generates an alert.	<input type="radio"/>	<input type="radio"/>
When User3 performs an action that matches the rule for DLP3, Policy3 generates an alert.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
When User3 performs an action that matches the rule for DLP1, Policy1 generates an alert.	<input checked="" type="radio"/>	<input type="radio"/>
When User1 performs an action that matches the rule for DLP2, Policy2 generates an alert.	<input type="radio"/>	<input checked="" type="radio"/>
When User3 performs an action that matches the rule for DLP3, Policy3 generates an alert.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 181

DRAGDROP

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You need to implement insider risk management. The solution must meet the following requirements:

- Ensure that User1 can create insider risk management policies.
- Ensure that User2 can use content captured by using insider risk management policies
- Follow the principle of least privilege.

To which role group should you add each user? To answer, drag the appropriate role groups to the correct users. Each role group 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.

Role groups

- Insider Risk Management
- Insider Risk Management Admins
- Insider Risk Management Analysts
- Insider Risk Management Auditors
- Insider Risk Management Investigators

Answer Area

User1:

User2:

**Answer:**

Role groups

- Insider Risk Management
- Insider Risk Management Admins
- Insider Risk Management Analysts
- Insider Risk Management Auditors
- Insider Risk Management Investigators

Answer Area

User1:  Insider Risk Management Admins

User2:  Insider Risk Management Analysts

Explanation:

## Question: 182

You have a Microsoft 365 subscription.

You configure a Microsoft Purview insider risk management policy named Policy1.

You need to ensure that you will receive real-time recommendations on how to configure the indicator thresholds for Policy1. The solution must ensure that the recommendations are based on a user's activity from the past 10 days.

What should you do first?

- A. Configure the Insider Risk Management Data sharing settings.
- B. Create a data loss prevention (DLP) policy.
- C. Enable insider risk management analytics.
- D. Create an Insider Risk Indicators connector.

**Answer: C**

Explanation:

## Question: 183

HOTSPOT

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management.

You need to recommend policy templates that meet the following requirements:

- Contain risk indicators and scoring for when a user receives a poor performance review
- Contain risk indicators and scoring for when a user disables security features on a device.

Which template should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

When a user receives a poor performance review:

- Data leaks
- Data theft by departing users
- Security policy violations
- Security policy violations by risky users

When a user disables security features:

- Data leaks
- Data theft by departing users
- Security policy violations
- Security policy violations by risky users

**Answer:**

Answer Area

When a user receives a poor performance review:

- Data leaks
- Data theft by departing users
- Security policy violations
- Security policy violations by risky users

When a user disables security features:

- Data leaks
- Data theft by departing users
- Security policy violations
- Security policy violations by risky users

Explanation:

## Question: 184

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need to perform a content search for email messages that meet the following requirements:

- Are delivered to both user1@contoso.com and user2@contoso.com
- Are sent from a user account that has a name that starts with the word Compliance

How should you complete the query in the KQL editor? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Recipients:  AND Sender=

("User1@contoso.com" "User2@contoso.com")  
"User1@contoso.com AND User2@contoso.com"  
%"User1@contoso.com" "User2@contoso.com"%  
&"User1@contoso.com" "User2@contoso.com"&

"Compliance"  
"Compliance"  
"Compliance[\*]"  
"Compliance[#]"

**Answer:**

Answer Area

Recipients:  AND Sender=

("User1@contoso.com" "User2@contoso.com")  
**"User1@contoso.com AND User2@contoso.com"**  
%"User1@contoso.com" "User2@contoso.com"%  
&"User1@contoso.com" "User2@contoso.com"&

"Compliance"  
**"Compliance"**  
"Compliance[\*]"  
"Compliance[#]"

Explanation:

### Question: 185

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. The subscription has a data loss prevention (DLP) policy named Policy 1. User2 sends an outbound message that generates a false positive for Policy 1. You need to ensure that User1 can download the message that generated the alert. The solution must follow the principle of least privilege. To which role group should you add User1?

- A. Data Investigator
- B. Global Reader
- C. eDiscovery Manager
- D. Security Operator

**Answer: A**

Explanation:

### Question: 186

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to ensure that all email messages that contain attachments are encrypted automatically by using Microsoft Purview Message Encryption. What should you create?

- A. a mail flow rule

- B. an information barrier segment
- C. a data loss prevention (DLP) policy
- D. a sensitivity label

**Answer: A**

Explanation:

**Question: 187****HOTSPOT**

You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Purview Message Encryption.

User1 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail1	User2@contoso.com	.docx	40 MB
Mail2	User4@outlook.com	.doc	3 MB
Mail3	User3@gmail.com	.xlsx	7 MB

User2 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

For which emails will the attachments be encrypted? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

- Mail1 only
- Mail3 only
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:

- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- Mail4 and Mail6 only
- Mail4, Mail5, and Mail6

**Answer:**

Answer Area

User1:

- Mail1 only
- Mail3 only
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:

- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- Mail4 and Mail6 only
- Mail4, Mail5, and Mail6

Explanation:

## Question: 188

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a trainable classifier named Classifier1. You need to increase the accuracy of Classifier1. The solution must use the principle of least privilege.

Which feature should you use and to which role group should you be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Feature:

Role group:

**Answer:**

Answer Area

Feature:

Role group:

Explanation:

**Question: 189**

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.

Name	Detection method
SIT1	Fingerprint
SIT2	Regular expression

You plan to create the policies shown in the following table and assign them to a Microsoft SharePoint Online site.

Name	Type
DLP1	Data loss prevention (DLP) policy
Retention1	Retention label auto-labeling policy
Sensitivity1	Sensitivity label auto-labeling policy

Which policies can use SIT1. and which policies can use SIT2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

SIT1:

SIT2:

SIT2:

**Answer:**

Answer Area

SIT1:

SIT2:

SIT2:

Explanation:

## Question: 190

HOTSPOT

You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.

<b>Label name</b>	<a href="#">Edit</a>
Rebranding	
<b>Tooltip</b>	<a href="#">Edit</a>
Used for all documents containing information about the rebranding effort	
<b>Description</b>	<a href="#">Edit</a>
<b>Encryption</b>	<a href="#">Edit</a>
Advanced protection for content with this label	
<b>Content marking</b>	<a href="#">Edit</a>
Watermark: INTERNAL	
<b>Endpoint data loss prevention</b>	<a href="#">Edit</a>
<b>Auto labeling</b>	<a href="#">Edit</a>

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
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input checked="" type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 191

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.

Name	Primary element	Character proximity	Supporting elements	Additional checks
SIT1	Regular expression: <code>prd:\d{4}</code>	15	Keyword: <code>product</code>	<i>None</i>
SIT2	Regular expression: <code>(\d{10} \d{12})</code>	<i>None</i>	<i>None</i>	Exclude specific values: <code>111-111-1111</code>
SIT3	Function: <code>Func_credit_card</code>	<i>None</i>	<i>None</i>	<i>None</i>

A user sends the email messages shown in the following table.

Name	Content
Email1	The product code you requested for the bicycle is <code>prd:1234</code> .
Email2	The bank account number is <code>123456789012</code> . Contact your account rep at <code>111-111-1111</code> .
Email3	Please use my credit card that ends with <code>0023</code> and has an expiration date of <code>01/25</code> .

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
SIT1 will identify and match the content in Email1.	<input type="radio"/>	<input type="radio"/>
SIT2 will identify and match the content in Email2.	<input type="radio"/>	<input type="radio"/>
SIT3 will identify and match the content in Email3.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
SIT1 will identify and match the content in Email1.	<input type="radio"/>	<input checked="" type="radio"/>
SIT2 will identify and match the content in Email2.	<input checked="" type="radio"/>	<input type="radio"/>
SIT3 will identify and match the content in Email3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

**Question: 192**

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. On January 1, you create the sensitivity label shown in the following table.

Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish Label1 to User1.  
On January 3, User1 creates a Microsoft Word document named Doc1 and applies Label1 to the document. On January 4, User2 edits Doc1.  
On January 15, you increase the content expiry period for Label1 to 28 days. When will access to Doc1 expire for User2?

- A. January 23
- B. January 24
- C. January 25
- D. January 31

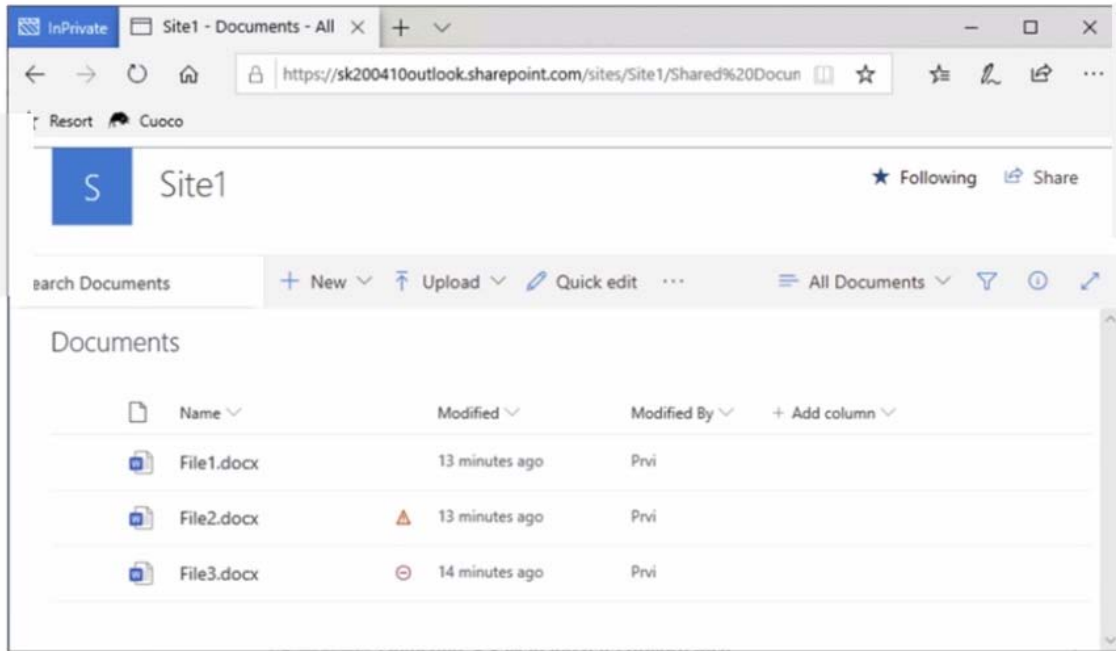
**Answer: B**

Explanation:

**Question: 193**

HOTSPOT

You have a Microsoft 365 E5 tenant that contains two users named User1, and User2 and a Microsoft SharePoint Online site named Site1 as shown in the following exhibit.



For Site1, the users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Member

You publish a retention label named Retention1 to Site1.

To which files can the users apply Retention1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:   
File1.docx only  
File1.docx and File2.docx only  
File1.docx, File2.docx, and File3.docx

User2:   
File1.docx only  
File1.docx and File2.docx only  
File1.docx, File2.docx, and File3.docx

**Answer:**

Answer Area

User1:   
File1.docx only  
File1.docx and File2.docx only  
File1.docx, File2.docx, and File3.docx

User2:   
File1.docx only  
File1.docx and File2.docx only  
File1.docx, File2.docx, and File3.docx

Explanation:

### Question: 194

You create a retention label that has a retention period of seven years. You need to ensure that documents containing a credit card number are retained for seven years. Other documents must not be retained. What should you create?

- A. a retention label policy of type publish
- B. a retention policy that retains files automatically
- C. a retention label policy of type auto-apply
- D. a retention policy that deletes files automatically

**Answer: C**

Explanation:

## Question: 195

### HOTSPOT

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.

## Create retention label

**Review and finish**

Name  
Label1  
[Edit](#)

**Retention settings**

Retention period	Retention action
2 years <a href="#">Edit</a>	Delete only <a href="#">Edit</a>

**Based on**  
Based on when it was created  
[Edit](#)

You publish Label1 to SharePoint sites.

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.

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2025, and apply Label1 to the file, you can [answer choice].

If you create a file in a Microsoft SharePoint library on March 15, 2025, and apply Label1 to the file, the file will [answer choice].

**Answer:**

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2025, and apply Label1 to the file, you can [answer choice].

If you create a file in a Microsoft SharePoint library on March 15, 2025, and apply Label1 to the file, the file will [answer choice].

Explanation:

### Question: 196

HOTSPOT

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain an EU Social Security Number (SSN) or Equivalent ID.
- Prevent any email messages that contain credit card numbers from being sent outside your organization.
- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers.
- Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policies:  ▼

1  
2  
3

Rules:  ▼

1  
2  
3  
4

**Answer:**

Answer Area

Policies:  ▼

1  
**2**  
3

Rules:  ▼

1  
2  
3  
**4**

Explanation:

### Question: 197

You are configuring a data loss prevention (DLP) policy to report when credit card data is found on a Microsoft Entra joined Windows device.

You plan to use information from the policy to restrict the ability to copy the sensitive data to the clipboard.

What should you configure in the policy advanced DLP rule?

- A. an action
- B. the incident report
- C. user notifications
- D. user overrides

**Answer: A**

Explanation:

### Question: 198

You have a Microsoft OneDrive folder that contains the files shown in the following table.

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

In Microsoft Defender for Cloud Apps, you create a file policy to automatically apply a classification. What is the effect of applying the policy?

- A. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.
- B. The policy will apply to only the docx and txt files. The policy will classify the files immediately.
- C. The policy will apply to all the files. The policy will classify only 100 files daily.
- D. The policy will apply to only the .docx files. The policy will classify only 100 files daily.

**Answer: A**

Explanation:

### Question: 199

HOTSPOT

You have a Microsoft 365 E5 subscription that contains three users named U\$er1, User2, and User3. The subscription contains the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, User3
Group3	User1, User2, User3

The subscription contains the devices shown in the following table.

Name	Platform
Device1	Windows
Device2	Android
Device3	macOS

All the devices are onboarded to Microsoft Purview.

You have the data loss prevention (DLP) policies shown in the following table.

Answer Area

Statements	Yes	No
When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device.	<input type="radio"/>	<input type="radio"/>
When User2 signs in to Device2, the user will be restricted from copying data to the clipboard.	<input type="radio"/>	<input type="radio"/>
When User3 signs in to Device3, the user will be restricted from accessing corporate content	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 signs in to Device2, the user will be restricted from copying data to the clipboard.	<input checked="" type="radio"/>	<input type="radio"/>
When User3 signs in to Device3, the user will be restricted from accessing corporate content	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 200

### HOTSPOT

You have a Microsoft 365 tenant that uses Microsoft Teams.

You create a data loss prevention (DLP) policy to prevent Microsoft Teams users from sharing sensitive information. You need to identify which locations must be selected to meet the following requirements:

- Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams.
- If a user attempts to share sensitive information during a Microsoft Teams chat session, the message must be deleted immediately.

Which three locations should you select? To answer, select the appropriate locations in the answer area

NOTE: Each correct selection is worth one point.

Location	Scope	Actions
<input type="checkbox"/> Exchange email	Turn on location to scope	
<input checked="" type="checkbox"/> SharePoint sites	Turn on location to scope	
<input checked="" type="checkbox"/> OneDrive accounts	Turn on location to scope	
<input checked="" type="checkbox"/> Teams chat and channel messages	Turn on location to scope	
<input type="checkbox"/> Instances	Turn on location to scope	
<input type="checkbox"/> On-premises repositories	Turn on location to scope	
<input type="checkbox"/> Fabric and Power BI workspaces	Turn on location to scope	

**Answer:**

Location	Scope	Actions
<input type="checkbox"/> Exchange email		Turn on location to scope
<input checked="" type="checkbox"/> SharePoint sites		Turn on location to scope
<input checked="" type="checkbox"/> OneDrive accounts		Turn on location to scope
<input checked="" type="checkbox"/> Teams chat and channel messages		Turn on location to scope
<input type="checkbox"/> Instances		Turn on location to scope
<input type="checkbox"/> On-premises repositories		Turn on location to scope
<input type="checkbox"/> Fabric and Power BI workspaces		Turn on location to scope

Explanation:

## Question: 201

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 Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages selected.

Does this meet the goal?

- A. Yes
- B. No

**Answer: A**

Explanation:

## Question: 202

### HOTSPOT

You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1. Sensitivity1 adds a watermark and a header to content.

You create a policy to automatically apply Sensitivity1 to emails in Microsoft Exchange Online and Site1.

How will Sensitivity1 mark matching emails and Site1 documents? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

Exchange Online emails:

Site1 documents:

Site1 documents:

**Answer:**

#### Answer Area

Exchange Online emails:

Site1 documents:

Site1 documents:

Explanation:

### Question: 203

You implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP). You have computers that run Windows 11 and have Microsoft 365 Apps installed. The computers are joined to a Microsoft Entra tenant. 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:

### Question: 204

You have a Microsoft 365 tenant that uses Microsoft Purview Information Protection. You create a sensitivity label named Sensitivity1 and configure Sensitivity1 to encrypt files and emails. You publish Sensitivity1. You discover that users are NOT prompted to apply Sensitivity1 to their files and email. You need to ensure that the users must apply Sensitivity1 to their files and email before saving the files or sending the emails. The solution must meet the following requirements:

- Prevent users from removing the label from the files and emails.
- Minimize administrative effort

What should you do?

- A. Select Control access for Sensitivity1.
- B. Create a new auto-labeling policy.
- C. Configure the protection settings of the sensitivity label policy for Sensitivity1.
- D. Publish Sensitivity1 by creating a label policy.

**Answer: C**

Explanation:

### Question: 205

You have a Microsoft 365 E5 tenant and the Windows Client devices shown in the following table.

Name	Joined to Microsoft Entra	Configuration
Device1	Yes	Onboarded to Microsoft Purview
Device2	Yes	Onboarded to Microsoft Defender for Endpoint
Device3	Yes	Enrolled in Microsoft Intune
Device4	No	Enrolled in Microsoft Intune

To which devices can you apply Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device3, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Answer: B**

Explanation:

### Question: 206

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Role
User1	Information Protection Administrator
User2	Information Protection Analyst
User3	Information Protection Investigator

You need to delegate the following tasks:

- Create and manage data loss prevention (DIP) policies.
- Review classified content by using Content explorer.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create and manage DLP policies:

Review classified content by using Content explorer:

**Answer:**

Answer Area

Create and manage DLP policies:

Review classified content by using Content explorer:

Explanation:

## Question: 207

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

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...

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. (Click the Review tab.)

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Locations to apply the policy
- ✓ Policy settings
- ✓ Test or turn on the policy
- Review your settings

## 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:

## Question: 208

### HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online and Teams. You need to ensure that when a user sends a message containing a cloud attachment, a retention label is applied to the cloud attachment by using an auto-labeling policy. How should you configure the retention label to start the retention period, and to which locations should you apply the auto-labeling policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Start the retention period based on when the items were:

- Created
- Labeled
- Last modified

Locations:

- Microsoft 365 Group mailboxes and sites only
- OneDrive accounts and SharePoint classic and communication sites only
- Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

**Answer:**

Answer Area

Start the retention period based on when the items were:

- Created
- Labeled
- Last modified

Locations:

- Microsoft 365 Group mailboxes and sites only
- OneDrive accounts and SharePoint classic and communication sites only
- Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

Explanation:

**Question: 209**

**HOTSPOT**

You plan to implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP). You need to identify which end user activities can be audited on the endpoints, and which activities can be restricted on the end points. What should you identify for each activity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Print a protected document:

- Can be audited only
- Can be restricted only
- Can be audited and restricted

Create a document in a monitored location:

- Can be audited only
- Can be restricted only
- Can be audited and restricted

Copy a protected document to USB removable media:

- Can be audited only
- Can be restricted only
- Can be audited and restricted

**Answer:**

Answer Area

Print a protected document:

- Can be audited only
- Can be restricted only
- Can be audited and restricted

Create a document in a monitored location:

- Can be audited only
- Can be restricted only
- Can be audited and restricted

Copy a protected document to USB removable media:

- Can be audited only
- Can be restricted only
- Can be audited and restricted

Explanation:

### Question: 210

You have a Microsoft 365 E5 tenant that contains the policies shown in the following table.

Name	Type	Retention period	Start the retention period based on	At the end of the retention period
Label1	Label	5 years	When items were created	Delete items automatically
Label2	Retention	7 years	When items were created	Delete items automatically
Label3	Retention	10 years	When items were created	Do nothing

A file named File1 has all the policies applied. How long will File1 be retained?

- A. File1 will be deleted automatically after five years.
- B. File1 will be deleted automatically after 10 years.
- C. File1 will be retained until the file is deleted manually.
- D. File1 will be deleted automatically after seven years.

**Answer: B**

Explanation:

### Question: 211

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Site1. You create the data loss prevention (DLP) policy shown in the following exhibit.

# Review your settings

## Template name

Custom policy

[Edit](#)

## Policy name

Policy1

[Edit](#)

## Description

[Edit](#)

## Applies to content in these locations

[Edit](#)

SharePoint sites

## Policy settings

[Edit](#)

If the content contains these types of sensitive info: IP Address .

If there are at least 2 instances of the same type of sensitive info, block access to the content .

## Turn policy on after it's created?

[Edit](#)

Yes

[Back](#)

[Create](#)

[Cancel](#)

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
User1 can view the contents of File1.txt.	<input type="radio"/>	<input type="radio"/>
User2 can view the contents of File1.txt.	<input type="radio"/>	<input type="radio"/>
User2 can view the contents of File2.docx.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can view the contents of File1.txt.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can view the contents of File1.txt.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can view the contents of File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 212

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	Priority
Rule1	1 or more IP addresses	Tip1	0
Rule2	2 or more IP addresses	Tip2	1
Rule3	6 or more IP addresses	Tip3	2

You apply DLP1 to Site1.

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
File1.txt has the Tip1 policy tip.	<input type="radio"/>	<input type="radio"/>
File2.docx has the Tip3 policy tip.	<input type="radio"/>	<input type="radio"/>
File3.dat has the Tip2 policy tip.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
File1.txt has the Tip1 policy tip.	<input type="radio"/>	<input checked="" type="radio"/>
File2.docx has the Tip3 policy tip.	<input checked="" type="radio"/>	<input type="radio"/>
File3.dat has the Tip2 policy tip.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

## Question: 213

### HOTSPOT

You have a Microsoft 365 subscription.

You have the sensitive files shown in the following table.

You have an Endpoint data loss prevention (Endpoint DLP) policy that contains the actions shown in the Actions exhibit. (Click the Actions tab.)

**Edit rule**

**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.

Upload to a restricted cloud service domain or access from an unallowed browsers ⓘ Block

+ Choose different restrictions for sensitive service domains

Paste to supported browsers ⓘ Audit only

+ Choose different restrictions for sensitive service domains

---

**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

Copy to clipboard ⓘ Audit only

+ Choose different copy to clipboard restrictions

Copy to a removable USB device ⓘ Audit only

+ Choose different removable USB device restrictions

The status of the Endpoint DLP policy is shown in the Status exhibit- (Click the Status tab.)

<input type="checkbox"/>	Name	Priority	Last modified	Status
<input type="checkbox"/>	Endpoint DLP	6	Nov 17, 2024 11:21 AM	On

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
File1 can be uploaded to a restricted cloud service domain.	<input type="radio"/>	<input type="radio"/>
File2 can be uploaded to a restricted cloud service domain.	<input type="radio"/>	<input type="radio"/>
File3 can be uploaded to a restricted cloud service domain.	<input type="radio"/>	<input type="radio"/>

**Answer:**

**Answer Area**

Statements	Yes	No
File1 can be uploaded to a restricted cloud service domain.	<input type="radio"/>	<input checked="" type="radio"/>
File2 can be uploaded to a restricted cloud service domain.	<input checked="" type="radio"/>	<input type="radio"/>
File3 can be uploaded to a restricted cloud service domain.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 214

DRAGDROP

You have a Microsoft 365 E5 subscription.

You need to label Microsoft Exchange Online emails that match the following conditions:

- Contain employment offers
- Contain offensive language
- Contain medical terms and conditions

The solution must minimize administrative effort.

Which type of data classification should you use for each condition? To answer, drag the appropriate data classification types to the correct conditions. Each data classification type 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.

The screenshot shows a drag-and-drop interface. On the left, under 'Data classifications', there are three items: 'Exact data match (EDM)', 'Sensitive info type', and 'Trainable classifier'. On the right, under 'Answer Area', there are three conditions: 'Contain employment offers:', 'Contain offensive language:', and 'Contain medical terms and conditions:'. Each condition has an empty text box next to it. A vertical split bar is between the two panes, and a mouse cursor is visible near the bottom of the split bar.

The screenshot shows the same interface as above, but with the correct assignments. 'Sensitive info type' is assigned to 'Contain employment offers:', 'Trainable classifier' is assigned to 'Contain offensive language:', and 'Exact data match (EDM)' is assigned to 'Contain medical terms and conditions:'. The data classification items on the left are now empty.

**Answer:**

Explanation:

## Question: 215

HOTSPOT

You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abe 123.

You need to create a new sensitive info type for the project codes.

How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

(\s)(  \  )(\s)

[aA]{3}	d{000-999}
[abc]{3}	d{123}
[alpha]{3}	d{3}
(a0zA-Z){3}	

**Answer:**

Answer Area

(\s)(  \  )(\s)

[aA]{3}	d{000-999}
[abc]{3}	d{123}
[alpha]{3}	d{3}
(a0zA-Z){3}	

Explanation:

## Question: 216

HOTSPOT

You create a sensitivity label as shown in the Sensitivity Label exhibit. (Click the Sensitivity Label tab.)

# Review your settings and finish

## Name

Sensitivity1

[Edit](#)

## Display name

Sensitivity1

[Edit](#)

## Description for users

Sensitivity1

[Edit](#)

## Scope

Files & other data assets, Email

[Edit](#)

## Access control

None

[Edit](#)

## Policy name

Auto-labeling policy

## Label and policy settings

Label	Sensitivity1	
Exchange overwrite label		true

## Sensitive Info Type

IP Address

You create an auto-labeling policy as shown in the Auto Labeling Policy exhibit. (Click the Auto Labeling Policy tab.)

**Sensitive Info Type**

IP Address

**Trainable Classifier**

**Admin units**

None

**Apply to content in these locations**

Exchange email      All

**Exclude content from these locations**

Exchange email      None

**Rules for auto-applying this label**

Exchange email      1 rule

**Mode**

On

A user sends the following email:

From: user1@contoso.com  
To: user2@fabrikam.com  
Subject: Address List  
Message Body:

Here are the lists that you requested.

Attachments:  
<<File1.docx>>  
<<File2.xml>>

Both attachments contain lists of IP addresses.  
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
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
Sensitivity1 is applied to the email.	<input checked="" type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 217

Your company has Microsoft 365 E5 subscription and plans to use Microsoft Purview Advanced Message Encryption.

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft 365 logo.

What should you do to create the branding templates?

- A. Create a Transport rule.
- B. Create an RMS template.
- C. Run the New-OMEConfiguration cmdlet.
- D. Run the set-IRMConfiguration cmdlet.

**Answer: C**

Explanation:

## Question: 218

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Compliance Administrator
User2	Security Operator
User3	eDiscovery Manager

You need to implement sensitivity labels.

Which users can create sensitivity labels, and which portal should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User 2 and User3 only
- User1, User2, and User3

Portal:

- Microsoft Entra admin center
- Microsoft 365 admin center
- Microsoft Purview portal
- Microsoft Defender portal

**Answer:**

Answer Area

Users:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User 2 and User3 only
- User1, User2, and User3

Portal:

- Microsoft Entra admin center
- Microsoft 365 admin center
- Microsoft Purview portal
- Microsoft Defender portal

Explanation:

## Question: 219

HOTSPOT

You have a Microsoft 365 E5 subscription.

In Microsoft Exchange Online, you have the mail flow rule shown in the following exhibit.

## Protect with OMEv2

 Edit rule conditions  Edit rule settings

Status: Enabled

Enable or disable rule

Enabled

### Rule settings

Rule name	Mode
Protect with OMEv2	Enforce
Severity	Set date range
Not Specified	Specific date range is not set
Senders address	Priority
Matching Header	0
For rule processing errors	
Ignore	

### Rule description

Apply this rule if

*Is sent to 'Outside the organization'  
and Includes these words in the message subject: '[Encrypt]'*

Do the following

*rights protect message with RMS template: 'Do Not Forward'*

Rule comments

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.

Answer Area

Outbound messages with the [Encrypt] string in the [answer choice] of the message will be encrypted.

- body
- email address
- header
- subject line

The mail flow rule will [answer choice].

- allow recipients to copy and paste message content
- allow recipients to print the message
- restrict recipients from printing the message
- restrict recipients from viewing attachments

**Answer:**

Answer Area

Outbound messages with the [Encrypt] string in the [answer choice] of the message will be encrypted.

- body
- email address
- header
- subject line

The mail flow rule will [answer choice].

- allow recipients to copy and paste message content
- allow recipients to print the message
- restrict recipients from printing the message
- restrict recipients from viewing attachments

Explanation:

## Question: 220

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and a sensitivity label named Label 1.

The external sharing settings for Site1 are configured as shown in the Site1 exhibit. (Click the Site1 tab.)

## Sharing

The sharing settings available for this site depend on your organization-level settings.

[Learn more about the external sharing settings](#)

### External sharing

Site content can be shared with:

- Anyone  
Users can share files and folders using links that don't require sign-in.
- New and existing guests  
Guests must sign in or provide a verification code.
- Existing guests only  
Only guests already in your organization's directory.
- Only people in your organization  
No external sharing allowed.

The external sharing settings for Label! are configured as shown in the Label! exhibit. (Click the Label1 tab.)

## Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

**Control external sharing from labeled SharePoint sites**

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

**Content can be shared with**

Anyone ⓘ

Users can share files and folders using links that don't require sign-in.

New and existing guests ⓘ

Guests must sign in or provide a verification code.

Existing guests ⓘ

Only guests in your organization's directory.

Only people in your organization

No external sharing allowed.

**Use Microsoft Entra Conditional Access to protect labeled SharePoint sites**

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

Label1 is applied to Site1.

Answer Area

Statements	Yes	No
Internal users can share documents on Site1 with external users.	<input type="radio"/>	<input type="radio"/>
External users require an invitation to access Site1.	<input type="radio"/>	<input type="radio"/>
Only users on managed devices can access Site1.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
Internal users can share documents on Site1 with external users.	<input checked="" type="radio"/>	<input type="radio"/>
External users require an invitation to access Site1.	<input type="radio"/>	<input checked="" type="radio"/>
Only users on managed devices can access Site1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

## Question: 221

### HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

You need to create a sensitive information type (SIT) to detect project code content that starts with the letters pjt followed by six digits and ends with the letters set. The following is an example of the project code.

pjt123456set

How should you complete the regular expression? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

pjt [0-9] (6) sct

(0-9) %6%

#0-9# (6)

^0-9^ #6#

:6:

**Answer:**

Answer Area

pjt [0-9] (6) sct

(0-9) %6%

#0-9# (6)

^0-9^ #6#

:6:

Explanation:

## Question: 222

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Purview.

You need to investigate the following events:

- Events that occurred two months ago
- Events in which users accessed encrypted email by using a one-time passcode (OTP)

Which Microsoft Purview solution should you use, and which type of record should you query?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Solution:

Record type:

**Answer:**

Answer Area

Solution:

Record type:

**Question: 223**

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 that has the users shown in the following table.

You create the retention labels shown in the following table.

Name	Retention period	Retention action	Based on
Retention1	4 years	Retain only	When a file was labeled
Retention2	2 years	Retain and delete	When a file was labeled

You publish the retention labels to Site1.

On March 1, 2025, you assign the retention labels to the files shown in the following table.

Name	Modified by	Retention label
File1	User1	Retention1
File2	User1	Retention2

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
User1 can delete File1 on March 10, 2025.	<input type="radio"/>	<input type="radio"/>
User2 can delete File1 on March 10, 2029.	<input type="radio"/>	<input type="radio"/>
User2 can edit File2 on March 15, 2027.	<input type="radio"/>	<input type="radio"/>

**Answer:**

Answer Area

Statements	Yes	No
User1 can delete File1 on March 10, 2025.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete File1 on March 10, 2029.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can edit File2 on March 15, 2027.	<input checked="" type="radio"/>	<input type="radio"/>

**Thank You for Trying Our Product**  
**Special 16 USD Discount Coupon: NSZUBG3X**  
**Email: [support@examsempire.com](mailto:support@examsempire.com)**

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**