

Microsoft.SC-400.vMar-2024.by.Utany.93q

Website: www.VCEplus.io

Twitter: https://twitter.com/VCE_Plus

Exam Code: SC-400

Exam Name: Microsoft Information Protection Administrator



02 - Implement Information Protection

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

Cloud Environment

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

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

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

Human Resources (HR) Management System

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

On-Premises Environment

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

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

Business Processes

Sales Contracts

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

Employment Applications

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

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

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

Requirements

HR Requirements

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

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

Resumes must be identified automatically based on similarities to other resumes received in the past.

Employment applications and resumes must be deleted automatically two years after the applications are received.

Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements

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

Compliance Requirements

Fabrikam identifies the following compliance requirements:

All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.

Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.

If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.

The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.

Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.

Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels

and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements

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

QUESTION 1

You need to recommend a solution that meets the Data Loss Prevention requirements for the HR department. Which three actions should you perform? Each correct answer presents part of the solution. (Choose three.)

NOTE: Each correct selection is worth one point.

- A. Schedule EdmUploadAgent.exe to hash and upload a data file that contains employee information.
- B. Create a sensitive info type rule package that contains the EDM classification.
- C. Define the sensitive information database schema in the XML format.

- D. Create a sensitive info type rule package that contains regular expressions.
- E. Define the sensitive information database schema in the CSV format.

Correct Answer: A, B, C

Section:

Explanation:

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

QUESTION 2

You need to recommend a solution that meets the compliance requirements for protecting the documents in the Data shared folder. What should you recommend?

- A. From the Microsoft 365 compliance center, configure an auto-labeling policy.
- B. From Azure Information Protection, configure a content scan job.
- C. From the Microsoft 365 compliance center, configure a Content Search query.
- D. From the Microsoft 365 compliance center, configure a DLP policy.

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner>

QUESTION 3

DRAG DROP

You need to recommend a solution that meets the sales requirements. 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. (Choose three.)

Select and Place:

Actions	Answer Area
Create a sensitive info type that contains an EDM classification.	
Upload sample contract documents to a seed content folder in SharePoint Online.	
Create a sensitive info type that contains a keywords classification.	
Create a sensitive info type that contains a document fingerprint.	
Create an auto-labeling policy for sensitivity labels.	
Create a trainable classifier.	

Correct Answer:

Actions

Create a sensitive info type that contains an EDM classification.

Create a sensitive info type that contains a keywords classification.

Create a sensitive info type that contains a document fingerprint.

Answer Area

Upload sample contract documents to a seed content folder in SharePoint Online.

Create a trainable classifier.

Create an auto-labeling policy for sensitivity labels.

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide>

QUESTION 4

HOTSPOT

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

What should you create in the Exchange admin center and the Microsoft 365 compliance center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Exchange admin center:

	▼
A connector	
A DLP policy	
A mail flow rule	
An organization sharing relationship	

Microsoft 365 compliance center:

	▼
An auto-labeling policy	
A DLP policy	
A custom sensitive info type	
A sensitivity label	

Answer Area:

Answer Area

Exchange admin center:

	▼
A connector	
A DLP policy	
A mail flow rule	
An organization sharing relationship	

Microsoft 365 compliance center:

	▼
An auto-labeling policy	
A DLP policy	
A custom sensitive info type	
A sensitivity label	

Section:

Explanation:

Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-sensitive-info-types?view=o365-worldwide>

03 - Implement Information Protection

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click 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

You need to meet the technical requirements for the Site3 documents.

What should you create?

- A. a retention policy that has Only delete items when they reach a certain age selected
- B. a retention label policy and a retention label that uses an event
- C. a sensitive info type that uses a regular expression and a sensitivity label
- D. a sensitive info type that uses a dictionary and a sensitivity label

Correct Answer: A

Section:

Explanation:

QUESTION 2

You need to meet the technical requirements for the creation of the sensitivity labels.

To which user or users must you grant the Sensitivity label administrator role?

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

- C. Admin1 only
- D. Admin1 and Admin4 only
- E. Admin1 and Admin5 only

Correct Answer: D

Section:

Explanation:

Compliance Data Administrator, Compliance Administrator, and Security Administrator already have the required permissions to create the labels.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide#permissions-required-to-create-and-manage-sensitivity-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.

Hot Area:

Answer Area

Create first:

<input type="text"/>	▼
A Compliance Manager assessment	
A content search	
A DLP policy	
A sensitive info type	
A sensitivity label	

Use for detection method:

<input type="text"/>	▼
Dictionary	
File type	
Keywords	
Regular expression	

Answer Area:

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

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide>

QUESTION 4

DRAG DROP

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

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

Select and Place:

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

Correct Answer:

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

Section:

Explanation:

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for-sharepoint-onedrive-and-exchange>

01 - Implement Data Loss Prevention

QUESTION 1

You have a Microsoft 365 tenant that uses 100 data loss prevention (DLP) policies.

A Microsoft Exchange administrator frequently investigates emails that were blocked due to DLP policy violations.

You need recommend which DLP report the Exchange administrator can use to identify how many messages were blocked based on each DLP policy.

Which report should you recommend?

A. Third-party DLP policy matches

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

Correct Answer: B

Section:

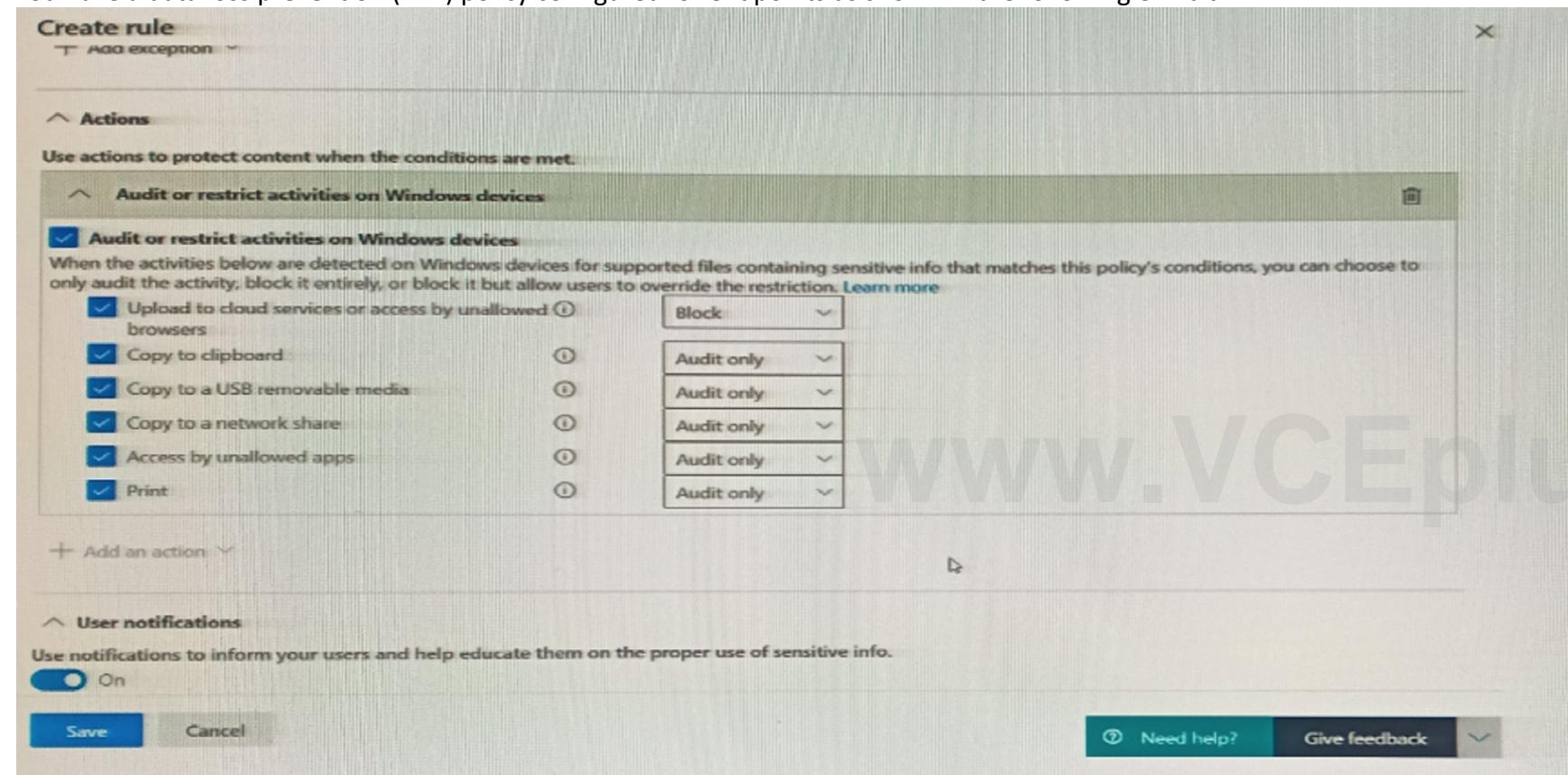
Explanation:

Reference:

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

QUESTION 2

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 Windows devices

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

Activity	Action
<input checked="" type="checkbox"/> Upload to cloud services or access by unallowed browsers	Block
<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"/> Access by unallowed apps	Audit only
<input checked="" type="checkbox"/> Print	Audit only

User notifications

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

☒ On

Buttons: Save, Cancel, Need help?, Give feedback

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

Correct Answer: D, E

Section:

QUESTION 3

You are planning a data loss prevention (DLP) solution that will apply to computers that run Windows 10.

You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:
If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.
All other users must be blocked from copying the file.
What should you create?

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

Correct Answer: A

Section:

QUESTION 4

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

- A. From the Exchange admin center, create a data loss prevention (DLP) policy.
- B. From the Azure portal, create an Azure Active Directory (Azure AD) Identity Protection policy.
- C. From the Microsoft 365 compliance center, create an insider risk policy.
- D. From the Cloud App Security portal, create a file policy.

Correct Answer: D

Section:

Explanation:

File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
2. From the Cloud App Security portal, create a file policy.

Other incorrect answer options you may see on the exam include the following:

From the Microsoft 365 compliance center, start a data investigation.

From the Azure portal, create an Azure Information Protection policy.

Reference:

<https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies>

QUESTION 5

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 keys in plain text to third parties.

You need to ensure that when Azure Storage keys are emailed, the emails are encrypted.

Solution: You configure a mail flow rule that matches a sensitive info type.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

QUESTION 6

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 keys in plain text to third parties.

You need to ensure that when Azure Storage keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has all locations selected.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 7

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 keys in plain text to third parties.

You need to ensure that when Azure Storage keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 8

You are creating an advanced data loss prevention (DLP) rule in a DLP policy named Policy 1 that will have all locations selected.

Which two conditions can you use in the rule? Each correct answer presents a complete solution. (Choose two.)

NOTE: Each correct selection is worth one point.

A. Content contains

B. Content is shared from Microsoft 365

C. Document size equals or is greater than

D. Attachment's file extension is

E. Document property is

Correct Answer: A, B

Section:

QUESTION 9

You need to provide a user with the ability to view data loss prevention (DLP) alerts in the Microsoft 365 compliance center. The solution must use the principle of least privilege. Which role should you assign to the user?

- A. Compliance data administrator
- B. Security operator
- C. Compliance administrator
- D. Security reader

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide>

QUESTION 10

HOTSPOT

You create a data loss prevention (DLP) 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 Teams 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.

Hot Area:

www.VCEplus.io

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 Area:

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

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide>

<https://docs.microsoft.com/en-us/microsoftteams/sharepoint-onedrive-interact>

QUESTION 11

HOTSPOT

You have a Microsoft 365 E5 tenant.

Data loss prevention (DLP) policies are applied to Exchange email, SharePoint sites, and OneDrive accounts locations.

You need to use PowerShell to retrieve a summary of the DLP rule matches from the last seven days.

Which PowerShell module and cmdlet should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Module:

- Azure Active Directory (Azure AD)
- Exchange Online
- SharePoint Online

Cmdlet:

- Get-DlpDetailReport
- Get-DlpDetectionsReport
- Get-DlpPolicy
- Get-DlpSiDetectionsReport

Answer Area:

Answer Area

Module:

- Azure Active Directory (Azure AD)
- Exchange Online
- SharePoint Online

Cmdlet:

- Get-DlpDetailReport
- Get-DlpDetectionsReport
- Get-DlpPolicy
- Get-DlpSiDetectionsReport

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/get-dlpdetectionsreport?view=exchange-ps>

QUESTION 12

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 endpoints.

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.

Hot Area:

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 Area:

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

Section:

Explanation:

Reference:

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

QUESTION 13

You are configuring a data loss prevention (DLP) policy to report when credit card data is found on a Windows 10 device joined to Azure Active Directory (Azure AD).

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 rule?

- A. the incident report
- B. an action
- C. user notifications
- D. user overrides

Correct Answer: D

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 14

You have a Microsoft 365 E5 tenant and the Windows 10 devices shown in the following table.

Name	Azure Active Directory (Azure AD)-joined	Configuration
Device1	Yes	Onboarded to the Microsoft 365 compliance center
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, Device3, and Device4 only
- B. Device1, Device2, Device3, and Device4
- C. Device1 and Device2 only
- D. Device1 and Device3 only
- E. Device1 only

Correct Answer: C

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide>

QUESTION 15

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

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

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

You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).

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

Solution: You enroll the computers in Microsoft Intune.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide>

QUESTION 16

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

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

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

You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).

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

Solution: You deploy the unified labeling client to the computers.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide>

QUESTION 17

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

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

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

You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).

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

Solution: You onboard the computers to Microsoft Defender for Endpoint.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

Reference:

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

QUESTION 18

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Data Classification service inspection method and send alerts to Microsoft Power Automate.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection> <https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

QUESTION 19

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Build-in DLP inspection method and send alerts to Microsoft Power Automate.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection> <https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies>

QUESTION 20

Your company has a Microsoft 365 tenant that uses a domain named contoso.com.

You are implementing data loss prevention (DLP).

The company's default browser is Microsoft Edge.

During a recent audit, you discover that some users use Firefox and Google Chrome browsers to upload files labeled as Confidential to a third-party Microsoft SharePoint Online site that has a URL of <https://m365x076709.sharepoint.com>.

Users are blocked from uploading the confidential files to the site from Microsoft Edge.

You need to ensure that the users cannot upload files labeled as Confidential from Firefox and Google Chrome to any cloud services. Which two actions should you perform? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add m365x076709.sharepoint.com as a blocked service domain.

B. Create a DLP policy that applies to the Devices location.

C. From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, add Firefox and Google Chrome to the unallowed browsers list.

D. From the Microsoft 365 compliance center, onboard the devices.

E. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add contoso.com as an allowed service domain.

Correct Answer: C, D

Section:

Explanation:

Reference:

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

QUESTION 21

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

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

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

You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).

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

Solution: You deploy the Endpoint DLP configuration package to the computers.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

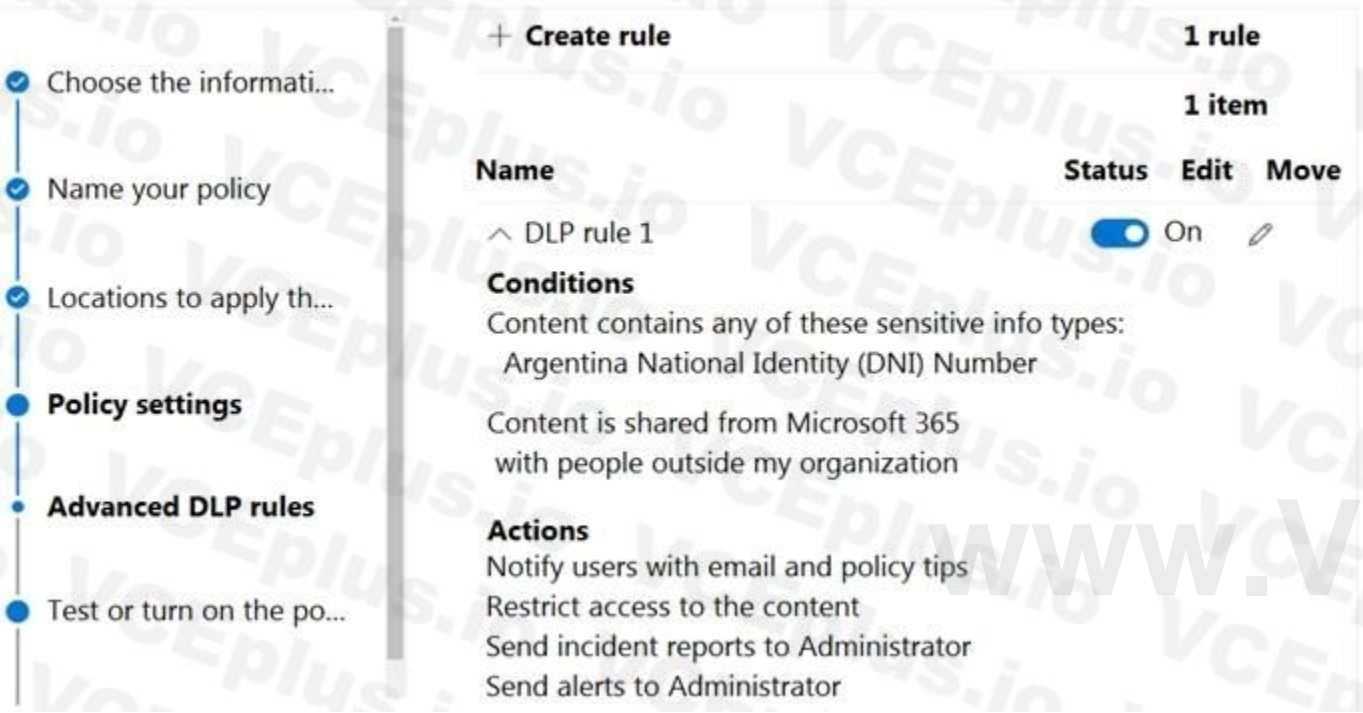
Explanation:


Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide>

QUESTION 22

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

Data loss prevention > **Create policy**



Name	Status	Edit	Move
^ DLP rule 1	<input checked="" type="checkbox"/> On		

Conditions

- Content contains any of these sensitive info types:
 - Argentina National Identity (DNI) Number
- Content is shared from Microsoft 365 with people outside my organization

Actions

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

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

Data loss prevention > **Create policy**

✓ Choose the informati...

✓ Name your policy

✓ Locations to apply th...

✓ Policy settings

✓ Test or turn on the po...

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.

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 23

HOTSPOT

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

Name	Modified by	Data loss prevention (DLP) status
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 view? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

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 Area:

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

Section:

Explanation:

Reference:

<https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx>

QUESTION 24

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. (Choose three.)






NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Choose locations to apply the policy

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






Status	Location	Included
<input type="checkbox"/> Off	 Exchange email	
<input type="checkbox"/> Off	 SharePoint sites	
<input type="checkbox"/> Off	 OneDrive accounts	
<input type="checkbox"/> Off	 Teams chat and channel messages	
<input type="checkbox"/> Off	 Microsoft Cloud App Security	

Answer Area:

Answer Area

Choose locations to apply the policy

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

Status	Location	Included
<input type="checkbox"/> Off	 Exchange email	
<input checked="" type="checkbox"/> On	 SharePoint sites	
<input checked="" type="checkbox"/> On	 OneDrive accounts	
<input checked="" type="checkbox"/> On	 Teams chat and channel messages	
<input type="checkbox"/> Off	 Microsoft Cloud App Security	

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide>

QUESTION 25

HOTSPOT

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

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

You need to identify which rules will apply when content matches multiple advanced DLP rules.
Which rules should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

www.VCEplus.io

Answer Area

If content matches Rule1, Rule2, and Rule3:

	▼
Only Rule1 takes effect	
Only Rule2 takes effect	
Only Rule3 takes effect	
Rule1, Rule2, and Rule3 take effect	

If content matches Rule2, Rule3, and Rule4:

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

Answer Area:

Answer Area

If content matches Rule1, Rule2, and Rule3:

- Only Rule1 takes effect
- Only Rule2 takes effect
- Only Rule3 takes effect
- Rule1, Rule2, and Rule3 take effect

If content matches Rule2, Rule3, and Rule4:

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

Section:**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>

QUESTION 26

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

- A. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
- B. From the Microsoft 365 compliance center, start a data investigation.
- C. From the Microsoft 365 compliance center, create an insider risk policy.
- D. From the Cloud App Security portal, create an activity policy.

Correct Answer: A

Section:**Explanation:**

With a DLP policy, you can identify, monitor, and automatically protect sensitive items.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
2. From the Cloud App Security portal, create a file policy.

Other incorrect answer options you may see on the exam include the following:

From the Exchange admin center, create a data loss prevention (DLP) policy.

From the Microsoft 365 compliance center, create an insider risk policy. From the Azure portal, create an Azure Information Protection policy.

Reference:

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

QUESTION 27

You need to protect documents that contain credit card numbers from being opened by users outside your company. The solution must ensure that users at your company can open the documents.

What should you use?

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

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 28

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

You have the users shown in the following table.

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

You create a data loss prevention (DLP) policy for Site1 that detects credit card number information. You configure the policy to use the following protection action:

When content matches the policy conditions, show policy tips to users and send them an email notification.

You use the default notification settings.

To Site1, User1 uploads a file that contains a credit card number.

Which users receive an email notification?

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

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 29

You have a data loss prevention (DLP) 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 policy.

You need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.

Which Microsoft 365 Endpoint data loss prevention (Endpoint DLP) setting should you configure?

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

Correct Answer: D

Section:

Explanation:

You can control whether sensitive files protected by your policies can be uploaded to specific service domains from Microsoft Edge.

If the list mode is set to Block, then user will not be able to upload sensitive items to those domains. When an upload action is blocked because an item matches a DLP policy, DLP will either generate a warning or block the upload of the sensitive item.

If the list mode is set to Allow, then users will be able to upload sensitive items only to those domains, and upload access to all other domains is not allowed.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 30

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

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

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).

Which devices support Endpoint DLP?

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

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 31

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

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

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 32

HOTSPOT

You have a Microsoft 365 tenant that uses data loss prevention (DLP) to protect sensitive information. You create a new custom sensitive info type that has the matching element shown in the following exhibit.

Matching element

^ Detect content containing

Regular expression v

^(\\d{3}(-)){3}\\d{3}\\d{12}\$

The supporting elements are configured as shown in the following exhibit.

Supporting elements

^ Contains this keyword list

Keyword list

"Employee ID"

Minimum Count

1

The confidence level and character proximity are configured as shown in the following exhibit.

Confidence level ⓘ

Default (60%)

Character proximity ⓘ

Default (300 characters)

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

Hot Area:

Statements	Yes	No
A document that contains the following text will match the sensitive info type: James has an Employee ID of 555-343-111-065.	<input type="radio"/>	<input type="radio"/>
A document that contains the following text will match the sensitive info type: The Employee ID of the employee Ben Smith is 555343123444.	<input type="radio"/>	<input type="radio"/>
A document that contains the following text will match the sensitive info type: The id badge for 555-123 has expired.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area	
Statements	
A document that contains the following text will match the sensitive info type: James has an Employee ID of 555-343-111-065.	Yes <input type="radio"/> No <input checked="" type="radio"/>
A document that contains the following text will match the sensitive info type: The Employee ID of the employee Ben Smith is 555343123444.	Yes <input type="radio"/> No <input checked="" type="radio"/>
A document that contains the following text will match the sensitive info type: The id badge for 555-123 has expired.	Yes <input type="radio"/> No <input checked="" type="radio"/>

Section:**Explanation:**

Note: The regular expression has a starts with (^) and ends with (\$) metacharacter and will not match any of the sentences. Without the starts with (^) metacharacter the first and second sentences would match and the supporting element (Employee ID) would be within 100 character proximity.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide>

QUESTION 33

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

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

You have a Microsoft 365 tenant and 500 computers that run Windows 10. The computers are onboarded to the Microsoft 365 compliance center.

You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.

You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From the Cloud App Security portal, you create an app discovery policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:**Explanation:**

You can create app discovery policies to alert you when new apps are detected within your organization.

Use the unallowed apps list instead.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-policies>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 34

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

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

You have a Microsoft 365 tenant and 500 computers that run Windows 10. The computers are onboarded to the Microsoft 365 compliance center.

You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.

You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

Folder path to the file path exclusions excludes certain paths and files from DLP monitoring.

Use the unallowed apps list instead.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 35

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

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

You have a Microsoft 365 tenant and 500 computers that run Windows 10. The computers are onboarded to the Microsoft 365 compliance center.

You discover that a third-party application named Tailspin_scanner.exe accessed protected sensitive information on multiple computers. Tailspin_scanner.exe is installed locally on the computers.

You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add the application to the unallowed apps list.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

Unallowed apps is a list of applications that you create which will not be allowed to access a DLP protected file.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide>

QUESTION 36

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

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

You are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Data Classification service inspection method and send alerts as email.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Alerts must be sent to the Microsoft Teams site of the affected department. A Microsoft Power Automate playbook should be used.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection>

<https://docs.microsoft.com/en-us/cloud-app-security/flow-integration>

QUESTION 37

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Built-in DLP inspection method and send alerts to Microsoft Power Automate.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/content-inspection-built-in>

<https://docs.microsoft.com/en-us/cloud-app-security/flow-integration>

QUESTION 38

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 are configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected department.

Solution: You use the Built-in DLP inspection method and send alerts as email.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Alerts must be sent to the Microsoft Teams site of the affected department. A Microsoft Power Automate playbook should be used.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/content-inspection-built-in>

<https://docs.microsoft.com/en-us/cloud-app-security/flow-integration>

02 - Implement Data Loss Prevention

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click the Question button to return to the question.

Overview

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

Existing Environment

Cloud Environment

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

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

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

Human Resources (HR) Management System

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

On-Premises Environment

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

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

Business Processes

Sales Contracts

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

Employment Applications

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

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

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

Requirements

HR Requirements

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

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

Resumes must be identified automatically based on similarities to other resumes received in the past.

Employment applications and resumes must be deleted automatically two years after the applications are received.

Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements

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

Compliance Requirements

Fabrikam identifies the following compliance requirements:

All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.

Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.

If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.

The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.

Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.

Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements

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

QUESTION 1

You need to recommend a solution that meets the compliance requirements for viewing DLP tooltip justifications.

What should you recommend?

- A. Instruct the compliance department users to review the False positive and override report.
- B. Configure a Microsoft Power Automate workflow to route DLP notification emails to the compliance department.
- C. Instruct the compliance department users to review the DLP incidents report.
- D. Configure an Azure logic app to route DLP notification emails to the compliance department.

Correct Answer: A

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide>

QUESTION 2

You need to recommend a solution that meets the compliance requirements for Dropbox.

What should you recommend?

- A. Create a file policy in Cloud App Security that uses the built-in DLP inspection method.
- B. Edit an existing retention label that enforces the item deletion settings.
- C. Create a retention label that enforces the item deletion settings.
- D. Create a DLP policy that applies to devices.

Correct Answer: A

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-use-policies-non-microsoft-cloud-apps?view=o365-worldwide>

QUESTION 3

You need to implement a solution that meets the compliance requirements for the Windows 10 computers.

Which two actions should you perform? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

- A. Deploy a Microsoft 365 Endpoint data loss prevention (Endpoint DLP) configuration package to the computers.
- B. Configure the Microsoft Intune device enrollment settings.
- C. Configure hybrid Azure AD join for all the computers.
- D. Configure a compliance policy in Microsoft Intune.
- E. Enroll the computers in Microsoft Defender for Endpoint protection.

Correct Answer: C, E

Section:

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide>

QUESTION 4

You need to recommend a solution to configure the Microsoft 365 Records management settings by using the CSV file. The solution must meet the compliance requirements. What should you recommend?

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

Correct Answer: C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide#import-retention-labels-into-your-file-plan>

03 - Implement Data Loss Prevention

Case study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs.

When you are ready to answer a question, click 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.

www.VCEplus.io

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

You are evaluating the technical requirements for the DLP reports.

Which user can currently view the DLP reports?

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

Correct Answer: E

Section:

QUESTION 2

HOTSPOT

How many files in Site2 will be visible to User1 and User2 after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

www.VCEplus.io

Answer Area

Number of files visible to User1:

	▼
1	
2	
3	
4	

Number of files visible to User2:

	▼
1	
2	
3	
4	

Answer Area:

Answer Area

Number of files visible to User1:

	▼
1	
2	
3	
4	

Number of files visible to User2:

	▼
1	
2	
3	
4	

Section:

Explanation:

Reference:

<https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx>

QUESTION 3

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains a file named File1.

You have a retention policy named Retention1 that has the following settings:

* Retain items for a specific period

o Retention period: 5 years o At the end of the retention period: Delete items automatically

Retention1 is applied to Site.

You need to ensure that File1 is deleted automatically after seven years. The solution must NOT affect the retention of other files on Site1.

What should you do first?

- A. Move File1 to a new folder and list the excluded locations for Retention1.
- B. Create a new retention policy.
- C. Create and publish a new retention label
- D. Move File1 to a new folder and configure the access control list (ACL) entries for File1.

Correct Answer: C

Section:

QUESTION 4

You have a Microsoft 365 E5 subscription.

You need to identify personal data stored in the subscription and control the transfer of personal data between users and groups.

Which type of license should you acquire?

- A. Microsoft Purview Audit (Premium)
- B. Priva Privacy Risk Management
- C. Microsoft 365 E5 Compliance
- D. Priva Subject Rights Requests

Correct Answer: C

Section:

QUESTION 5

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

You create an information barrier segment named Segment1.

You need to add Segment 1 to Site1.

What should you do first?

- A. Run the Set-SPOSite cmdlet.
- B. Run the Set-SPOTenant cmdlet.
- C. Create an information barrier policy.
- D. Modify the permissions of Site1.

Correct Answer: B

Section:

QUESTION 6**HOTSPOT**

You have a Microsoft 365 E5 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.

Hot Area:

Answer Area

Use the:

Format in:

Microsoft Purview compliance portal
Microsoft 365 admin center
Microsoft 365 Defender portal
Microsoft Entra admin center
Microsoft Purview compliance portal

HTML
HTML
Markdown
RTF
XML

Answer Area:

Answer Area

Use the:

Format in:

Microsoft Purview compliance portal
Microsoft 365 admin center
Microsoft 365 Defender portal
Microsoft Entra admin center
Microsoft Purview compliance portal

HTML
HTML
Markdown
RTF
XML

Section:

Explanation:

QUESTION 7

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 sensitivity label
- B. an information barrier segment
- C. a data loss prevention (DLP) policy
- D. a mail flow rule

Correct Answer: D

Section:

QUESTION 8

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

Correct Answer: D

Section:

QUESTION 9

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. Tip2only
- C. Tip3 only
- D. Tip1 and Tip2 only

Correct Answer: D

Section:

QUESTION 10

You have a Microsoft 365 E3 subscription.

You plan to audit all Microsoft Exchange Online user and admin activities.

You need to ensure that all the Exchange audit log records are retained for one year.

What should you do?

- A. Modify the record type of the default audit retention policy.
- B. Modify the retention period of the default audit retention policy.
- C. Create a custom audit retention pol
- D. Assign Microsoft 365 Enterprise E5 licenses to all users.

Correct Answer: D

Section:

QUESTION 11

HOTSPOT

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

Name	Microsoft 365 role	Role group
Admin1	Global Administrator	None
Admin2	Compliance Administrator	None
User3	User	Compliance Manager Contributors
User4	User	Compliance Manager Administrators
User5	User	None

You create an assessment named Assesment1 as shown in the following exhibit.

Assessment1

Status
● In progress

Created
1/15/2021

Generate report

Overview Controls Your improvement actions Microsoft actions

Review details about this assessment and understand your progress toward completion.

49% Assessment progress

1083/2169

Your points achieved ⓘ

0/1086

Microsoft managed points achieved ⓘ

1083/1083

www.VCEplus.io

Which users can update the title of Assessment1, and which users can add User5 to the Compliance Manager Readers role group? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Can update the Assessment1 title:

- User4 only
- Admin2 and User4 only
- Admin1, Admin2, and User4 only
- Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Readers role group:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and User4 only
- Admin1, Admin2, and User4 only

Answer Area:

Answer Area

Can update the Assessment1 title:

- User4 only
- Admin2 and User4 only
- Admin1, Admin2, and User4 only
- Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Readers role group:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and User4 only
- Admin1, Admin2, and User4 only

Section:

Explanation:

QUESTION 12

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. RPolicy3only
- C. RPolicy1l and RPolicy2 only
- D. RPolicy1 and RPolicy3 only
- E. RPolicy1, RPolicy2, and RPolicy3

Correct Answer: D

Section:

QUESTION 13

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 compliance 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.

YOU run the Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminiAuditLogCmdlets 'Mailbox*' command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 14

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 compliance 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.

YOU run the Set-MailboxFolderPernission -Identity 'User1' -User User1fcontoso.com -AccessRights Owner command.

Does that meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 15

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

Correct Answer: C

Section:

QUESTION 16

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. The subscription contains two groups named Group1 and Group2.

You need to implement a policy to detect messages that present a conflict of interest between the users in Group1 and the users in Group2.

What should you use in the Microsoft Purview compliance portal?

- A. Insider risk management
- B. Privacy risk management
- C. Information barriers
- D. Communication compliance

Correct Answer: D

Section:

www.VCEplus.io

QUESTION 17

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a sensitivity label.

Does this meet the goal?

- A. Yes
- B. NO

Correct Answer: A

Section:

QUESTION 18

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create a data loss prevention (DLP) policy.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section:

QUESTION 19

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

Name	Role group
Admin1	eDiscovery Manager
Admin2	eDiscovery Administrator
Admin3	<i>none</i>

You need to ensure that Admin3 can create holds in owing table.
To what should you add Admin3?

- A. the Global Administrator role
- B. the eDiscovery Manager role group
- C. the Compliance Manager Contributors role group
- D. the eDiscovery Administrator role group

Correct Answer: B
Section:

QUESTION 20

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

- * Prevents users from performing data transfers that breach local regulations
- * Minimizes effort to respond to requests for a user's personal data

What should you use in the Microsoft Purview compliance portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

www.VCEplus.io

Answer Area

To prevent users from performing data transfers that breach local regulations:

Information barriers
Communication compliance
Information barriers
Insider risk management
Privacy risk management

To minimize effort to respond to requests for a user's personal data:

Subject rights request
Data loss prevention (DLP)
eDiscovery
Records management
Subject rights request

Answer Area:

Answer Area

To prevent users from performing data transfers that breach local regulations:

Information barriers
Communication compliance
Information barriers
Insider risk management
Privacy risk management

To minimize effort to respond to requests for a user's personal data:

Subject rights request
Data loss prevention (DLP)
eDiscovery
Records management
Subject rights request

Section:

Explanation:

QUESTION 21

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

You configure Microsoft Purview Information Barriers.

You need to identify which information barrier policies apply to User1.

Which cmdlet should you use?

- A. Get-OrganizationSeagent
- B. Get-InformationBarrierPoliciesApplicationStatus
- C. Get-InformationBarrierPolicy
- D. Get-InformationBarrierRecipientStatus

Correct Answer: D

Section:

QUESTION 22

You have a Microsoft 365 E5 subscription. You need to create a subject rights request. What can be configured as a search location?

- A. Microsoft Exchange Online and Teams only
- B. Microsoft Exchange Online, SharePoint Online, and Teams
- C. Microsoft Exchange Online only
- D. Microsoft Exchange Online and SharePoint Online only
- E. Microsoft SharePoint Online only

Correct Answer: B

Section:

QUESTION 23

HOTSPOT

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

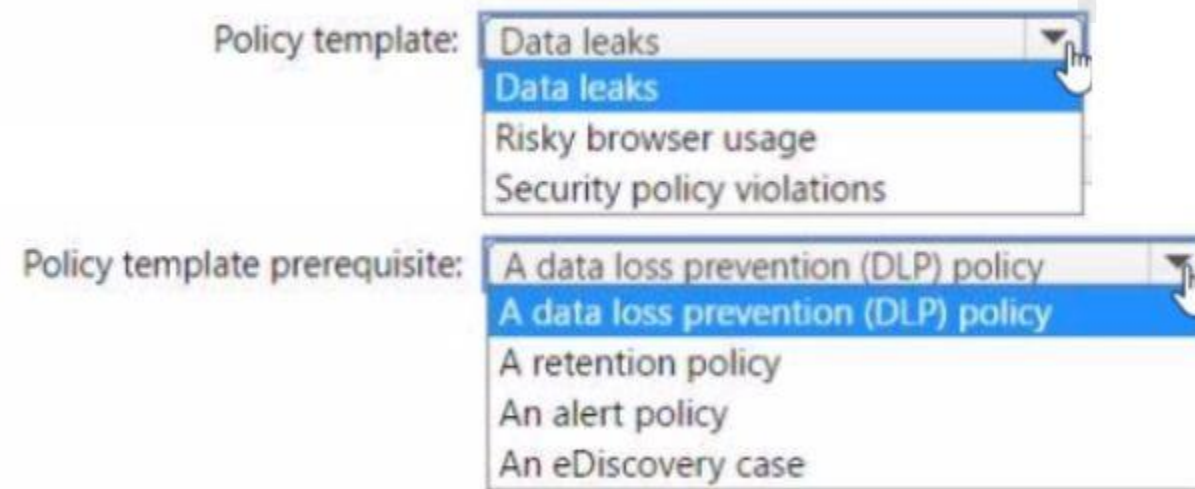
You need to deploy a compliance solution that will detect the accidental oversharing of information outside of an organization. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Answer Area:

Answer Area

Policy template:

Policy template prerequisite:

Section:
Explanation:

QUESTION 24 DRAG DROP

Your company has two departments named department1 and department2 and a Microsoft 365 E5 subscription. You need to prevent communication between the users in department1 and the users in department. How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Values	Answer Area
<input type="text" value="New-InformationBarrierPolicy"/>	<input type="text" value="-Name 'Department1' -UserGroupFilter 'Department -eq 'depar"/>
<input type="text" value="New-OrganizationSegment"/>	<input type="text" value="..."/>
<input type="text" value="Set-InformationBarrierPolicy"/>	<input type="text" value="-Name 'Department1and2' -AssignedSegment 'Department1'"/>
<input type="text" value="Set-OrganizationSegment"/>	<input type="text" value="-SegmentsBlocked 'Department2' -State Active"/>

Correct Answer:

Values

Answer Area

```
New-OrganizationSegment -Name "Department1" -UserGroupFilter "Department -eq 'depar
...
New-InformationBarrierPolicy -Name "Department1and2" -AssignedSegment "Department1"
-SegmentsBlocked "Department2" -State Active
```

Section:

Explanation:

QUESTION 25

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a communication compliance policy named Policy1.

You need to identify whose communications can be monitored by Policy1, and who can be assigned the Reviewer role for Policy1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

www.VCEplus.io

Answer Area

Policy1 can monitor the communications of:

- User1, Group1, Group2, and Group3 only
- User1 only
- User1, Group1, and Group2 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3 only**
- User1, Group1, Group2, Group3, and Group4

The Reviewer role for Policy1 can be assigned to:

- User1, Group1, Group3, and Group4 only
- User1 only
- User1 and Group4 only
- User1, Group3 and Group4 only
- User1, Group1, Group3, and Group4 only**
- User1, Group1, Group2, Group3, and Group4

Answer Area:

Answer Area

Policy1 can monitor the communications of:

- User1, Group1, Group2, and Group3 only
- User1 only
- User1, Group1, and Group2 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3 only**
- User1, Group1, Group2, Group3, and Group4

The Reviewer role for Policy1 can be assigned to:

- User1, Group1, Group3, and Group4 only
- User1 only
- User1 and Group4 only
- User1, Group3 and Group4 only
- User1, Group1, Group3, and Group4 only**
- User1, Group1, Group2, Group3, and Group4

Section:

Explanation:

QUESTION 26

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a security group named Group1 and the users shown in the following table.

Name	Role
User1	Compliance Administrator
User2	None
User3	None

You assign the Compliance Manager roles to the users as shown in the following table.

User	Role
User2	Compliance Manager Contributors
User3	Compliance Manager Administrators

You add two assessments to Compliance Manager as shown in the following exhibit.

Compliance Manager

Overview
Improvement actions
Solutions
Assessments
Assessment templates

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. [Learn how to manage assessments](#)

Add assessment
3 items
Search
Filter
Group

Applied filters:

Assessment ↑
Status

Assessment progress	Your improvement act...	Microsoft actions	Group	Product	Regulation
64%	0 of 227 completed	355 of 355 completed	Group1	Microsoft 365	CSA CCM
64%	1 of 177 completed	195 of 195 completed	Group1	Intune	HIPAA/HITECH

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

Hot Area:

Answer Area

Statements	Yes	No
User1 can edit the title of Assessment1.	<input type="radio"/>	<input type="radio"/>
To Group1, User2 can add an assessment that uses the HIPA/HITECH template.	<input type="radio"/>	<input type="radio"/>
To Group1, User3 can add an assessment that uses the HIPA/HITECH or Microsoft 365	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements	Yes	No
User1 can edit the title of Assessment1.	<input type="radio"/>	<input checked="" type="radio"/>
To Group1, User2 can add an assessment that uses the HIPA/HITECH template.	<input type="radio"/>	<input checked="" type="radio"/>
To Group1, User3 can add an assessment that uses the HIPA/HITECH or Microsoft 365	<input type="radio"/>	<input checked="" type="radio"/>

Section:

Explanation:

QUESTION 27

HOTSPOT

You have a Microsoft 365 E5 subscription.

You are evaluating Data Protection Baseline compliance by using Compliance Manager.

You need to identify improvement actions that meet the following requirements:

* Provide data loss prevention (DLP) policy recommendations.

* Provide Data Protection Baseline recommendations.

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

Hot Area:

Answer Area

DLP policy recommendations:

Solutions
Categories
Regulations
Solutions
Testing Source

Data Protection Baseline recommendations:

Regulations
Categories
Regulations
Solutions
Testing Source

Answer Area:

Answer Area

DLP policy recommendations:

Solutions
Categories
Regulations
Solutions
Testing Source

Data Protection Baseline recommendations:

Regulations
Categories
Regulations
Solutions
Testing Source

Section:

Explanation:

QUESTION 28

You have a Microsoft 365 E5 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site 1. You create the alert policy shown in the following exhibit.

Review your settings

New alert policy

- ☒ Name your alert
- ☒ Create alert settings
- ☒ Set your recipients

Name	AlertPolicy1
Description	Add a description
Severity	● Medium
Category	Others
Filter	Activity is Uploaded file and File extension is Like any of

☒ Review your settings

Aggregation Scope	Trigger an alert when any activity ma
	All users

Recipients	User1@sk220416.onmicrosoft.com
Daily notification limit	Do not send email notifications

[Edit](#)

Do you want to turn the policy on right away?

- ☒ Yes, turn it on right away.
- ☐ No, keep it off. I will turn it on later.

[Back](#)
[Finish](#)
[Cancel](#)

To Site1, User1 uploads the files shown in the following table.

Name	Upload time (hh:mm:ss)
File1.docx	8:00:00
File2.docx	8:00:40
File3.xlsx	8:01:30
File4.docx	8:04:50
File5.docx	8:05:10

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
How many alerts will be generated in response to the file uploads?

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

Correct Answer: C

Section:

Exam F

QUESTION 1

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a retention label.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 2

HOTSPOT

You have a Microsoft 365 subscription that contains two groups named Group1 and Group2.

You have the compliance assessments shown in the following table.

Name	Group
Ca1	Group1
Ca2	Group1
Ca3	Group2

You have the improvement actions shown in the following table.

Action	Compliance assessment	Improvement action	Points	Action type
Action1	Ca1	Create and publish a retention label	5	Technical
Action2	Ca2	Create and publish a retention label	5	Technical
Action3	Ca3	Enable Windows 10 Security baseline	5	Technical
Action4	Ca1	Restrict access to privileged accounts	10	Operational
Action5	Ca2	Update security awareness training	10	Operational
Action6	Ca3	Update security awareness training	10	Operational

You perform the following actions:

- * Create and publish a retention label.
- * Implement security awareness training for all users.
- * For Action4, change Implementation status to Implemented

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The compliance score for Ca1 will increase by 15 points.	<input type="radio"/>	<input type="radio"/>
The compliance score for Ca2 will increase by 15 points.	<input type="radio"/>	<input type="radio"/>
The compliance score for Ca3 will increase by 10 points.	<input type="radio"/>	<input type="radio"/>

Answer Area:

Answer Area

Statements

The compliance score for Ca1 will increase by 15 points.

Yes

☒

No

☐

The compliance score for Ca2 will increase by 15 points.

☐☒

The compliance score for Ca3 will increase by 10 points.

☒☐

Section:

Explanation:

QUESTION 3

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Security

www.VCEplus.io

You have the Compliance Manager improvement action shown in the following exhibit

E Enable self-service password reset

Overview

Details

Implementation Status	Test Status
Not Implemented	Failed high risk
Points achieved	Group
0 / 27	Default Group
Managed by	Action scope
Your organization	Tenant
Action type	Products
Technical	Microsoft 365

Edit implementation details

How to implement

technical

MICROSOFT 365

Documents

0

Assigned to

None

Assign action

Testing Source

Manual

Implementation

Testing

Standards and Regulations

Documents

Implementation status

Not Implemented

Implementation date

Not Available

Implementation notes

This action hasn't been implemented yet. Refer to the implementation instructions for this action.

Edit implementation details

How to implement

Microsoft recommends that your organization enable self-service password reset to allow users who have either forgotten their password or whose account has been locked out as a result of malicious attempts, using an alternate factor to reset their password without the assistance of the help desk.

How to Use Microsoft Solutions to Implement

Your organization can use Azure Active Directory (Azure AD) to give users the ability to change or reset their password with no administrator or help desk involvement. Select **Launch Now** to enable Self-Service Password Reset (SSPR) by selecting "All" or "Selected" on the "Properties" page to determine applicable users.

Launch Now

Learn More

Let users reset their own passwords in Office 365

How it works: Azure Active Directory self-service password reset

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The Enable self-service password reset improvement action can be assigned to **[answer choice]**.

▼

User1 only
Group1 only
User1 and Group1 only
Group1 and Group2 only
User1, Group1, and Group2

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be **[answer choice]**.

▼

0/27
1/27
2/27
5/27
27/27

Answer Area:

Answer Area

The Enable self-service password reset improvement action can be assigned to **[answer choice]**.

▼

User1 only
Group1 only
User1 and Group1 only
Group1 and Group2 only
User1, Group1, and Group2

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be **[answer choice]**.

▼

0/27
1/27
2/27
5/27
27/27

Section:

Explanation:

QUESTION 4

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online document library named Library 1. You need to declare a collection of files that are stored in Library1 as regulatory records. What should you use?

- A. a sensitivity label policy
- B. data loss prevention (DLP) policy

- C. a retention policy
- D. a retention label policy

Correct Answer: D

Section:

QUESTION 5

You have a Microsoft 365 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

Correct Answer: A

Section:

QUESTION 6

You have a Microsoft 365 E5 subscription.

You need to export the details of a retention label. The export must include the following information;

- * Is record
- * Is regulatory
- * Disposition type

What should you do?

- A. From the Microsoft Purview compliance portal, export Compliance Manager assessment actions.
- B. From the Microsoft Purview compliance portal export a file plan.
- C. From the Microsoft Purview compliance portal export a disposition review.
- D. From PowerShell, run the Export-ActivityExplorerData cmdlet.
- E. From PowerShell, run the Get-RetentionEvent cmdlet.

Correct Answer: B

Section:

QUESTION 7

You have a Microsoft 365 E5 subscription that uses Yammer.

You need to create a Microsoft Purview communication compliance policy that will detect inappropriate images in Yammer conversations.

What should you do first?

- A. Configure Hybrid Mode for Yammer.
- B. Configure the Yammer network admin settings.
- C. Assign each user a Yammer license.
- D. Configure Native Mode for Yammer.

Correct Answer: C

Section:

www.VCEplus.io

QUESTION 8

You create a label that encrypts email data.
Users report that they cannot use the label in Outlook on the web to protect the email messages they send.
You need to ensure that the users can use the new label to protect their email.
What should you do?

- A. Wait six hours and ask the users to try again.
- B. Create a label policy.
- C. Create a new sensitive information type.
- D. Modify the priority order of label policies

Correct Answer: D
Section:

QUESTION 9

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group 1 contains 100 users and has dynamic user membership.
All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.
You create a sensitivity label named Label1 and publish Label1 as the default label for Group1.
You need to ensure that the users in Group1 must apply Label1 to their email and documents.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. From the Microsoft Purview compliance portal, modify the settings of the Label1 policy.
- B. From the Azure Active Directory admin center, set Membership type for Group1 to Assigned.
- C. Install the Azure Information Protection unified labeling client on the Windows 10 devices.
- D. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices.
- E. From the Microsoft Purview compliance portal, create an auto-labeling policy.

Correct Answer: A, C
Section:

QUESTION 10

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

Hot Area:
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 Area:
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"/>

Section:
Explanation:

QUESTION 11

You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language. You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically. You need to identify and categorize the resumes. The solution must minimize administrative effort. What should you include in the solution?

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

Correct Answer: A
Section:

QUESTION 12

You have a Microsoft 365 subscription. You create and run a content search from the Microsoft Purview compliance 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

Correct Answer: D
Section:

QUESTION 13

HOTSPOT
You have a Microsoft 365 subscription.

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

Create retention label

✓ Name

✓ File plan descri...

✓ Retention setti...

● Finish

Review and finish

Name

NameLabel1Edit

File plan descriptors

Retention settings

Retention period	Retention action
2 yearsEdit	Retain and DeleteEdit
Based on <div>Based on when it was createdEdit</div>	Use label to classify content as a <div>RecordEdit</div>

Back

Create label

Cancel

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.

Hot Area:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2023, and apply Label1 to the file, you can **[answer choice]**.

If you create a file in a Microsoft SharePoint library on March 15, 2023, and apply Label1 to the file, the file will **[answer choice]**.

Answer Area:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2023, and apply Label1 to the file, you can **[answer choice]**.

If you create a file in a Microsoft SharePoint library on March 15, 2023, and apply Label1 to the file, the file will **[answer choice]**.

Section:

Explanation:

QUESTION 14

You have a Microsoft 365 subscription.
 You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.
 Which two actions should you perform? Each correct answer presents part of the solution.
 NOTE: Each correct selection is worth one point.

- A. From the Microsoft Purview compliance portal, create a label.
- B. From Microsoft Defender for Cloud Apps, create a file policy.
- C. From the Microsoft Purview compliance portal, publish a label.
- D. From the SharePoint admin center, modify the Site Settings.
- E. From the SharePoint admin center, modify the records management settings.

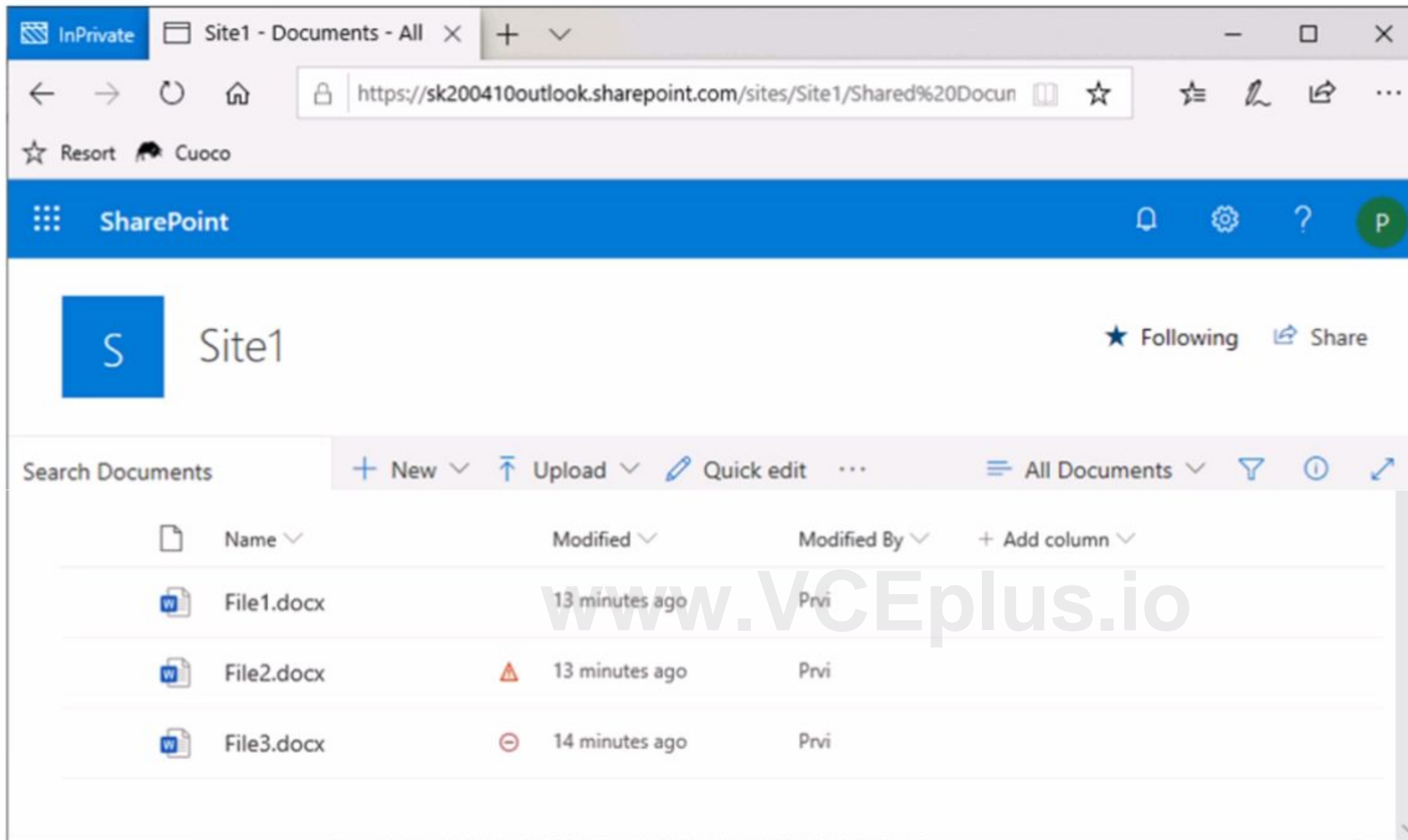
Correct Answer: A, C

Section:

QUESTION 15

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 Retention!? To answer, select the appropriate options in the answer area.

Hot Area:

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 Area:

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

Section:

Explanation: