

SC-400.VCEplus.premium.exam.44q

Number: SC-400
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



Website: <https://vceplus.com> - <https://vceplus.co>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

SC-400

Microsoft Information Protection Administrator (beta)



Question Set 1

QUESTION 1

You create three sensitivity labels named Sensitivity1, Sensitivity2, and Sensitivity3 and perform the following actions:

- Publish Sensitivity1.
- Create an auto-labeling policy for Sensitivity2.

You plan to create a file policy named Policy1 in Microsoft Cloud App Security.

Which sensitivity labels can you apply to Microsoft SharePoint Online in Policy1?

- A. Sensitivity1 only
- B. Sensitivity1, Sensitivity2, and Sensitivity3
- C. Sensitivity2 only
- D. Sensitivity1 and Sensitivity2 only

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide> <https://docs.microsoft.com/en-us/cloud-app-security/azip-integration>

QUESTION 2

You have a Microsoft OneDrive for Business folder that contains the files shown in the following table.

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20



In Microsoft Cloud App Security, you create a file policy to automatically apply a classification.

What is the effect of applying the policy?

- A. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.
- B. The policy will apply to all the files. The policy will classify only 100 files daily.
- C. The policy will apply to only the .docx files. The policy will classify only 100 files daily.
- D. The policy will apply to only the .docx and .txt files. The policy will classify the files immediately.

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 3

HOTSPOT

You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Office 365 Message Encryption (OME).

User1 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail1	User2@contoso.com	.docx	40 MB
Mail2	User4@outlook.com	.doc	3 MB
Mail3	User3@gmail.com	.xlsx	7 MB

User2 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

For which emails will the attachments be protected? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

- Mail1 only
- Mail3 only
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:

- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- Mail4 and Mail6 only
- Mail1, Mail2, and Mail3

Correct Answer:

Answer Area

User1:

▼
Mail1 only
Mail3 only
Mail1 and Mail2 only
Mail2 and Mail3 only
Mail1, Mail2, and Mail3

User2:

▼
Mail5 only
Mail6 only
Mail4 and Mail5 only
Mail4 and Mail6 only
Mail1, Mail2, and Mail3

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://support.microsoft.com/en-gb/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-us&rs=en-gb&ad=gb#FileTypesforIRM>
<https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide> <https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#message-limits-1>

QUESTION 4

HOTSPOT

You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes.

How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

(\s)(

▼
[aA]{3}
[abc]{3}
[alpha]{3}
[a-zA-Z]{3}

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

Correct Answer:

Answer Area

(\s)(

▼
[aA]{3}
[abc]{3}
[alpha]{3}
[a-zA-Z]{3}

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://joannecklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/>

QUESTION 5

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1. Sensitivity1 adds a watermark and a header to content.

You create a policy to automatically apply Sensitivity1 to emails in Microsoft Exchange Online and Site1.

How will Sensitivity1 mark matching emails and Site1 documents? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Exchange Online emails:

▼
A header only
A watermark only
A watermark and a header

Site1 documents:

▼
A header only
A watermark only
A watermark and a header

Correct Answer:

Answer Area

Exchange Online emails:

	▼
A header only	
A watermark only	
A watermark and a header	

Site1 documents:

	▼
A header only	
A watermark only	
A watermark and a header	

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 6

HOTSPOT

You need to implement an information compliance policy to meet the following requirements:

- Documents that contain passport numbers from the United States, Germany, Australia, and Japan must be identified automatically.
- When a user attempts to send an email or an attachment that contains a passport number, the user must receive a tooltip in Microsoft Outlook.
- Users must be blocked from using Microsoft SharePoint Online or OneDrive for Business to share a document that contains a passport number.

What is the minimum number of sensitivity labels and auto-labeling policies you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Sensitivity labels:

	▼
1	
2	
3	
4	

Auto-labeling policies:

	▼
1	
2	
3	
4	

Correct Answer:

Answer Area

Sensitivity labels: ▼

1
2
3
4

Auto-labeling policies: ▼

1
2
3
4

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 7

HOTSPOT

You have a Microsoft 365 E5 tenant.

You create sensitivity labels as shown in the Sensitivity Labels exhibit.



+ Create a label Publish labels Refresh

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

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

The sensitivity labels are published as shown in the Published exhibit.

Sensitivity Policy1

[Edit policy](#)
[Delete policy](#)

Name

Sensitivity Policy1

Description

Published labels

Public

General

External/External

Internal/Internal

Confidential

Published to

All

Policy settings

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

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

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 8 You are implementing a data classification solution.

The research department at your company requires that documents containing programming code be labeled as Confidential. The department provides samples of the code from its document library. The solution must minimize administrative effort.

What should you do?

- A. Create a custom classifier.
- B. Create a sensitive info type that uses Exact Data Match (EDM).
- C. Use the source code classifier.
- D. Create a sensitive info type that uses a regular expression.

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 9 You have a new Microsoft 365 tenant.

You need to ensure that custom trainable classifiers can be created in the tenant.

To which role should you be assigned to perform the configuration?

- A. Security administrator
- B. Security operator
- C. Global administrator
- D. Compliance administrator

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 10

You need to automatically apply a sensitivity label to documents that contain information about your company's network including computer names, IP addresses, and configuration information.

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

NOTE: Each correct selection is worth one point.

- A. an Information protection auto-labeling policy
- B. a custom trainable classifier
- C. a sensitive info type that uses a regular expression
- D. a data loss prevention (DLP) policy
- E. a sensitive info type that uses keywords
- F. a sensitivity label that has auto-labeling

Correct Answer: AB

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide>
<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide>

QUESTION 11

You are creating a custom trainable classifier to identify organizational product codes referenced in Microsoft 365 content.

You identify 300 files to use as seed content.

Where should you store the seed content?

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

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 12

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft Office 365 logo.

What should you do to create the branding templates?

- A. Create a Transport rule.
- B. Create an RMS template.
- C. Run the `Set-IRMConfiguration` cmdlet.
- D. Run the `New-OMEConfiguration` cmdlet.

Correct Answer: D

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide>



Testlet 2

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

Compliance Configuration

Fabrikam has the following in the Microsoft 365 compliance center:

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

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

Human Resources (HR) Management System

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

On-Premises Environment

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

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

Business Processes

Sales Contracts

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

Employment Applications

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

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

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

Requirements

HR Requirements

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

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

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

Sales Requirements

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

Compliance Requirements

Fabrikam identifies the following compliance requirements:

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

Executive Requirements

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

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: ABC

Section: [none]

Explanation

Explanation/Reference:

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: [none]

Explanation

Explanation/Reference:

Reference:

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



Testlet 3

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	<i>None</i>
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

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: ▼

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

Correct Answer:

Answer Area

Create first: ▼

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

Use for detection method: ▼

Dictionary
File type
Keywords
Regular expression

Section: [none]

Explanation

Explanation/Reference:

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

Question Set 1

QUESTION 1

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:

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	

Correct Answer:

Answer Area

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

	▼
Exchange email	
OneDrive accounts	
SharePoint sites	
Teams chat and channel messages	

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

	▼
Exchange email	
OneDrive accounts	
SharePoint sites	
Teams chat and channel messages	

Section: [none]

Explanation

Explanation/Reference:

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 2

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: [none]

Explanation

Explanation/Reference:

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

QUESTION 3

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:	<div>▼</div> <div>Azure Active Directory (Azure AD)</div> <div>Exchange Online</div> <div>SharePoint Online</div>
Cmdlet:	<div>▼</div> <div>Get-DlpDetailReport</div> <div>Get-DlpDetectionsReport</div> <div>Get-DlpPolicy</div> <div>Get-DlpSiDetectionsReport</div>

Correct Answer:

Answer Area

Module:	<div><div></div><div>Azure Active Directory (Azure AD)</div><div>Exchange Online</div><div>SharePoint Online</div></div>
Cmdlet:	<div><div></div><div>Get-DlpDetailReport</div><div>Get-DlpDetectionsReport</div><div>Get-DlpPolicy</div><div>Get-DlpSiDetectionsReport</div></div>

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 4

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	

Correct Answer:

Answer Area

Print a protected document:

	▼
Can be audited only	
Can be restricted only	
Can be audited and restricted	

Create a document in a monitored location:

	▼
Can be audited only	
Can be restricted only	
Can be audited and restricted	

Copy a protected document to USB removable media:

	▼
Can be audited only	
Can be restricted only	
Can be audited and restricted	

Section: [none]
Explanation

Explanation/Reference:

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

QUESTION 5

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: [none]

Explanation

Explanation/Reference:

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

**QUESTION 6**

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:	<div>▼</div> <div>File1.docx only</div> <div>File1.docx and File2.docx only</div> <div>File1.docx, File2.docx, and File3.docx</div>
User2:	<div>▼</div> <div>File1.docx only</div> <div>File1.docx and File2.docx only</div> <div>File1.docx, File2.docx, and File3.docx</div>

Correct Answer:

Answer Area

User1:	<div>▼</div> <div>File1.docx only</div> <div>File1.docx and File2.docx only</div> <div>File1.docx, File2.docx, and File3.docx</div>
User2:	<div>▼</div> <div>File1.docx only</div> <div>File1.docx and File2.docx only</div> <div>File1.docx, File2.docx, and File3.docx</div>

Section: [none]

Explanation

Explanation/Reference:

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

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 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: [none]

Explanation

Explanation/Reference:

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

QUESTION 8

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: [none]

Explanation

Explanation/Reference:

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

QUESTION 9

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: [none]

Explanation

Explanation/Reference:

Reference:

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

QUESTION 10

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: A

Section: [none]

Explanation

Explanation/Reference:

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 11

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: [none]

Explanation

Explanation/Reference:

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 12

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: [none]

Explanation

Explanation/Reference:

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

Testlet 2

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

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company Some users have company Dropbox accounts.

Compliance Configuration

Fabrikam has the following in the Microsoft 365 compliance center:

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

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

Human Resources (HR) Management System

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

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

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

Business Processes

Sales Contracts

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

Employment Applications

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

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

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

Requirements

HR Requirements

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

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

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

Sales Requirements

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

Compliance Requirements

Fabrikam identifies the following compliance requirements:

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

Executive Requirements

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

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: [none]

Explanation

Explanation/Reference:

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 DLP policy that applies to Cloud App Security.

- 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: [none]

Explanation

Explanation/Reference:

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



Testlet 3

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	None
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

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:

Answer Area

Number of files visible to User1:

▼
1
2
3
4

Number of files visible to User2:

▼
1
2
3
4

Correct Answer:

Answer Area

Number of files visible to User1:

▼
1
2
3
4

Number of files visible to User2:

▼
1
2
3
4

Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx> Question Set 1

QUESTION 1

In Microsoft Exchange Online, you have a retention policy named Policy1 that applies a retention tag named Tag1.

You plan to remove Tag1 from Policy1.

What will occur when you remove the tag from Policy1?

- A. The content will remain tagged and the Managed Folder Assistant will process Tag1.
- B. Tag1 will be removed if Policy1 applied the tag to the content.
- C. The content will remain tagged, but the Managed Folder Assistant will ignore Tag1.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies#removing-or-deleting-a-retention-tag-from-a-retention-policy>

QUESTION 2

DRAG DROP

You have a Microsoft 365 tenant.

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

You need to implement the regulatory requirement.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. (Choose three.) **Select and Place:**

Actions

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

Answer Area

Correct Answer:

Actions

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

Answer Area

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

Section: [none]
Explanation

Explanation/Reference:

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

<https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock?view=o365-worldwide>

QUESTION 3 You have a Microsoft SharePoint Online site that contains employee contracts in a document library named Contracts.

The contracts must be treated as records in accordance with your company's records management policy.

You need to implement a solution to automatically mark all the contracts as records when they are uploaded to Contracts.

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. Create a sensitivity label.
- B. Create a retention label.
- C. Configure a default label on the Contracts document library.
- D. Create a retention policy.
- E. Create a SharePoint Records Center.
- F. Create a retention lock.

Correct Answer: BC

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide>

QUESTION 4 You need to create a retention policy to delete content after seven years from the following locations:

- Exchange email
- SharePoint sites
- OneDrive accounts
- Office 365 groups
- Teams channel messages
- Teams chats



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

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

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 5

HOTSPOT

You create a retention policy as shown in the following exhibit.

Retention Policy 1

Status

Enabled (Pending)

Policy name

Retention Policy 1

Description

Retention Policy for SharePoint Site1 and Exchange

Applies to content in these locations

Exchange email

SharePoint sites

Settings

Retention period

Keep content, and delete it if it's older than 10 years

Preservation lock

No data available

A user named User1 deletes a file named File1.docx from a Microsoft SharePoint Online site named Site1.

A user named User2 deletes an email and empties the Deleted Items folder in Microsoft Outlook.

Where is the content retained one year after deletion? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

File.docx:	<div>▼</div> <div> <div>Preservation Hold</div> <div>Recoverable Items</div> <div>SubstrateHolds</div> <div>The first-stage Recycle Bin</div> </div>
Email:	<div>▼</div> <div> <div>Preservation Hold</div> <div>Recoverable Items</div> <div>SubstrateHolds</div> <div>The first-stage Recycle Bin</div> </div>

Correct Answer:

Answer Area

File.docx:

Email:

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 6 You have a Microsoft 365 tenant that uses records management.

You use a retention label to mark legal files stored in a Microsoft SharePoint Online document library as regulatory records.

What can you do to the legal files?

- A. Remove the retention label of the files.
- B. Edit the properties of the files.
- C. Move the files to a different folder within the document library.
- D. Delete the content from the files.

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide#records>

QUESTION 7

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

Name	Role
User1	Global administrator
User2	Security administrator
User3	Compliance administrator
User4	Search administrator

You configure a retention label to trigger a disposition review at the end of the retention period.

Which users can access the Disposition tab in the Microsoft 365 compliance center to review the content?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User3E. User3 and User4

Correct Answer: C

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide>

QUESTION 8

HOTSPOT

While creating a retention label, you discover that the following options are missing:

- Mark items as a record
- Mark items as a regulatory record


You need to ensure that the options are available when you create retention labels in the Microsoft 365 compliance center.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



```
$UserCredential = Get-Credential
Import-Module
```

AzureRM
ExchangeOnlineManagement
Microsoft.Online.SharePoint.PowerShell
MicrosoftTeams

```
-Credential $UserCredential
```

Connect-AadrmService
Connect-AzureAD
Connect-AzureRMAccount
Connect-IPPSSession

```
-Enabled $true
```

Enable-ComplianceTagStorage
New-ComplianceTag
Set-RegulatoryComplianceUI
Set-RetentionCompliancePolicy

Correct Answer:

Answer Area

```
$UserCredential = Get-Credential
```

Import-Module
▼

AzureRM

ExchangeOnlineManagement

Microsoft.Online.SharePoint.PowerShell

MicrosoftTeams

▼

Connect-AadrmService

Connect-AzureAD

Connect-AzureRMAccount

Connect-IPPSSession

 -Credential \$UserCredential

▼

Enable-ComplianceTagStorage

New-ComplianceTag

Set-RegulatoryComplianceUI

Set-RetentionCompliancePolicy

 -Enabled \$true



Section: [none]

Explanation

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>
<https://docs.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps>

QUESTION 9

You need to ensure that documents in a Microsoft SharePoint Online site that contain a reference to Project Alpha are retained for two years, and then deleted.

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

NOTE: Each correct selection is worth one point.

- A. a retention policy
- B. an auto-apply label policy
- C. a sensitive info type
- D. a retention label
- E. a sensitivity label
- F. a publishing label policy

Correct Answer: BD

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide>

QUESTION 10

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



Define retention settings

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

☒ **Retain items for a specific period**
 Labeled items will be retained for the period you choose. During the retention period, Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. [Learn more](#)

Retention period of years months days

Start the retention period based on

+ Create new event type

At the end of the retention period

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

☐ Trigger a disposition review

☐ Do nothing
 Items will be left in place. You'll have to manually delete them if you want them gone.

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

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



You need to ensure that documents that have Label1 applied are deleted three years after the end of your company's fiscal year.

What should you do?

- A. Create a new event type.
- B. Select Only delete items when they reach a certain age.
- C. Modify the Retention period setting.
- D. Set At the ends of the retention period to Trigger a disposition review.

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention?view=o365-worldwide>

QUESTION 11

HOTSPOT

You enable archive mailboxes for all the users at your company.

The Default MRM Policy is shown in the MRM exhibit.

Default MRM Policy

This policy contains the following retention tags

1 Month Delete

1 Week Delete

1 Year Delete

5 Year Delete

6 Month Delete

Default 2 year move to archive

Junk Email

Never Delete

Personal 1 year move to archive

Personal 5 year move to archive

Personal never move to archive

Recoverable items 14 days move to archive

A Microsoft 365 retention label policy is shown in the Label Policy exhibit.

Exchange Label Policy

Status

Enabled (Pending)

Policy name

Exchange Label Policy

Description

Label policy for Exchange

Applies to content in these locations

Exchange email

Settings

Publish labels for your users

- 10 Year – Do not Delete
- 2 Year Delete

Preservation lock

No



You need to identify the following:

- How many years until an email is archived?
- What should you modify to change the retention period for archiving?

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

By default, email is:

Deleted after two years
Deleted after one month
Retained in the mailbox for 10 years
Moved to the archive mailbox after two years

To change the retention period for archiving, modify:

The Default MRM Policy
The Exchange Label Policy
The properties of the archive mailbox

Correct Answer:

Answer Area

By default, email is:

Deleted after two years
Deleted after one month
Retained in the mailbox for 10 years
Moved to the archive mailbox after two years

To change the retention period for archiving, modify:

The Default MRM Policy
The Exchange Label Policy
The properties of the archive mailbox

Section: [none]
Explanation

Explanation/Reference:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence>

QUESTION 12 You have a Microsoft 365 tenant.

You have a Microsoft SharePoint Online site that contains employment contracts in a folder named EmploymentContracts. All the files in EmploymentContracts are marked as records.

You need to recommend a process to ensure that when a record is updated, the previous version of the record is kept as a version of the updated record.

What should you recommend?

- A. Upload an updated file plan that contains the record definition.
- B. Unlock the record, modify the record, and then lock the record.
- C. Create a copy of the record and enter a version in the file metadata.
- D. Create a new label policy associated to an event that will apply to the record.

Correct Answer: B

Section: [none]

Explanation

Explanation/Reference:

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



Testlet 2

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	<i>None</i>
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

HOTSPOT

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
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	<input type="radio"/>	<input type="radio"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

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

Section: [none]

Explanation

Explanation/Reference:

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

QUESTION 2 You need to meet the retention requirement for the users' Microsoft 365 data.

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

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

Correct Answer: A

Section: [none]

Explanation

Explanation/Reference:

Reference:

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