

Microsoft

Exam Questions SC-400

Microsoft Information Protection Administrator



NEW QUESTION 1

- (Topic 1)

You have a Microsoft 365 E5 subscription. You create a role group named Role1.

You need to add a role to Role1 that will enable group members to view the metadata of records that were tagged for deletion automatically at the end of the records' retention period. The solution must use the principle of least privilege.

Which role should you add?

- A. Review
- B. View-Only Retention Management
- C. Retention Management
- D. Disposition Management
- E. Record Management

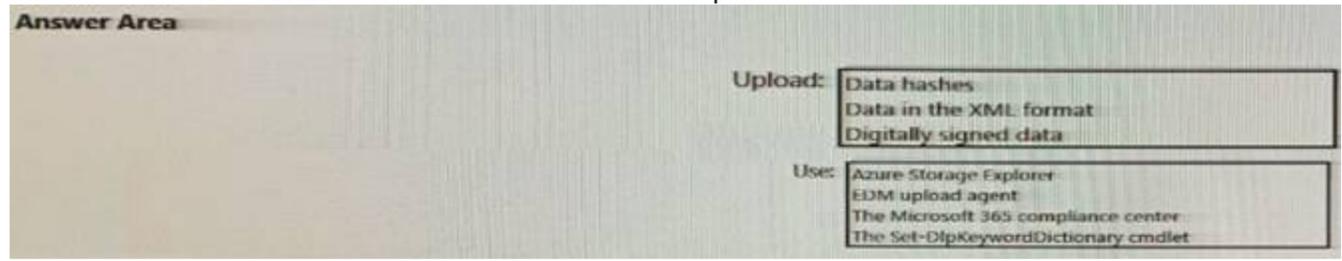
Answer: B

NEW QUESTION 2

HOTSPOT - (Topic 1)

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

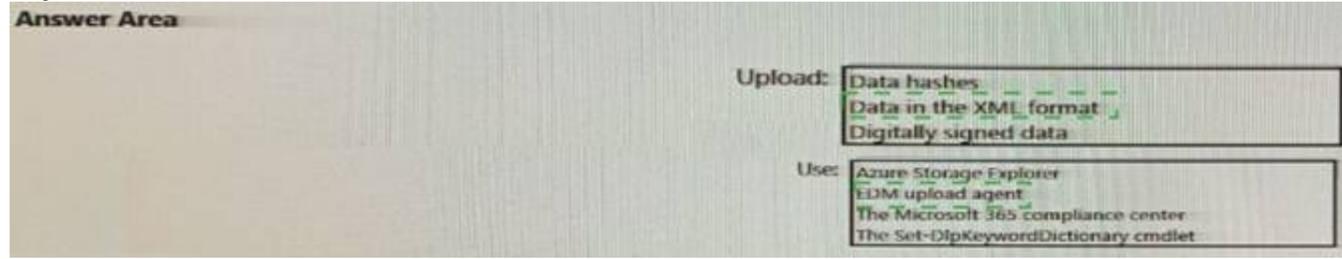
You need to identify what to upload to Microsoft 365, and which tool to use for the upload. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 3

HOTSPOT - (Topic 1)

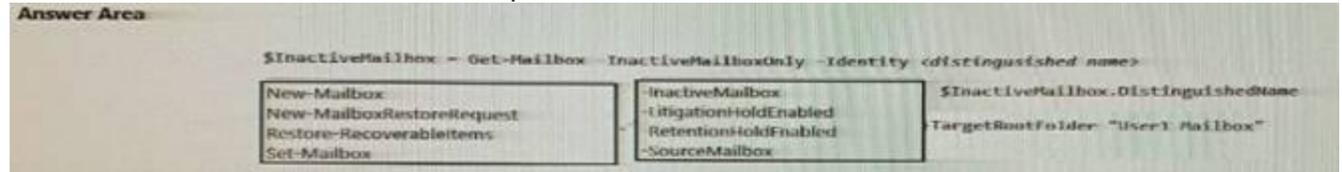
You have a Microsoft 365 tenant that uses a domain named canstoso.com.

A user named User1 leaves your company. The mailbox of User1 is placed on Litigation Hold, and then the account of User1 is deleted from Azure Active Directory (Azure AD).

You need to copy the content of the User1 mailbox to a folder in the existing mailbox of another user named User2.

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

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/restore-an-inactive-mailbox?view=o365-worldwide>

NEW QUESTION 4

HOTSPOT - (Topic 1)

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.

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	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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	

NEW QUESTION 5

- (Topic 1)

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

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

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

- A. the priority setting of Rule2 to 0

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

Answer: A

NEW QUESTION 6

HOTSPOT - (Topic 1)

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 7

HOTSPOT - (Topic 1)

You have a Microsoft 365 E5 subscription.

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

Contoso Electronics Microsoft Purview

Sensitive info in email with subject 'Message1'

Details Sensitive info types Metadata

Event details

ID 173fe9ac-3a65-41b0-9914-1db451bba639	Location Exchange
Time of activity Jun 6, 2022 8:22 PM	

Impacted entities

User Megan Bowen	Email recipients victoria@fabrikam.com
Email subject Message1	

Policy details

DLP policy matched Policy1	Rule matched Rule1
Sensitive info types detected Credit Card Number (19, 85%)	Actions taken GenerateAlert
User override policy Yes	Override justification text Manager approved
Sensitive info detected in Document1.docx	

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

Answer Area

The email was [answer choice].

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

The sender's manager [answer choice].

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

The email was [answer choice].

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

The sender's manager [answer choice].

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

NEW QUESTION 8

- (Topic 1)

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

Answer: A

Explanation:

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

NEW QUESTION 9

HOTSPOT - (Topic 1)

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.

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

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

Answer Area

Search Clear **Results**

Activities

Show results for all activities ▼

User administration activities

- Added user
- Deleted user
- Reset user password
- Changed user password
- Updated user
- Set property that forces user to change password
- Set license properties
- Changed user license

Azure AD group administration activities

- Added group
- Updated group
- Added member to group
- Removed member from group
- Deleted group

Application administration activities

- Added service principal
- Removed a service principal from the directory
- Removed credentials from a service principal
- Added delegation entity
- Set delegation entry
- Added credentials to a service principal

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Removed member from group:
 => shows the user that was removed (by modifying dynamic the query)
 Updated group
 => shows what user 'updated' the group.

NEW QUESTION 10

- (Topic 1)

You have a Microsoft 365 tenant that uses the following sensitivity labels:

- Confidential:
- Internal
- External

The labels are published by using a label policy named Policy1.

Users report that Microsoft Office for the web apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.

You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.

What should you do?

- A. Modify the scope of the confidential label.
- B. Modify the publishing settings of Policy1.
- C. Enable sensitivity label support for Office files in Microsoft SharePoint Online and OneDrive.
- D. Run the Execute-AzureAdiabelSync cmdlet.

Answer: A

NEW QUESTION 10

HOTSPOT - (Topic 1)

You have a Microsoft 365 subscription that contains a Microsoft SharePoint site named Site1. For Site1, users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Member

You publish retention labels to Site1 as shown in the following table.

Name	Retention period	During the retention period
Retention1	5 years	Mark items as a record
Retention2	5 years	Mark items as a regulatory record

You publish retention labels to Site1 as shown in the following table. You have the files shown in the following table.

Name	Applied retention label
File1	Retention1
File2	Retention2

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

Answer Area

Statements	Yes	No
User1 can delete File2.	<input type="radio"/>	<input type="radio"/>
User2 can rename File1.	<input type="radio"/>	<input type="radio"/>
User1 can apply Retention2 to File1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 No, Yes, Yes

NEW QUESTION 13

- (Topic 1)

You receive an email that contains a list of words that will be used few a sensitive information type. You need to create a file that can be used as the source of a keyword dictionary. In which format should you save the list?

- A. an XLSX file that contains one word in each cell of the first row
- B. a ISV file that contains words separated by tabs
- C. a JSON file that that an element tor each word
- D. a text file that has one word on each line

Answer: D

Explanation:

Keyword dictionaries can be created either from a text file or from csv file. Note:
 There are several versions of this question in the exam. The question has two possible correct answers:
 ? a CSV file that contains words separated by commas
 ? a text file that has one word on each line
 Other incorrect answer options you may see on the exam include the following:
 ? a TSV file that contains words separated by tabs
 ? a DOCX file that has one word on each line
 ? an XML file that contains a keyword tag for each word
 Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide>

NEW QUESTION 17

- (Topic 1)

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. Rename the files.
- B. Edit the properties of the files.
- C. Change the retention label of the files.

D. Copy the content of the files.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 20

HOTSPOT - (Topic 1)

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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 24

- (Topic 1)

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.

Answer: D

NEW QUESTION 27

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

Does that meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 30

- (Topic 1)

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: years months days
 Custom

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.

Answer: A

Explanation:

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

NEW QUESTION 32

- (Topic 1)

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-OrganizationSegaent
- B. Get-InformationBarrierPoliciesApplicationStatus
- C. Get-InformationBarrierPolicy
- D. Get-InformationBarrierRecipientStatus

Answer: D

NEW QUESTION 37

- (Topic 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 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

Answer: A

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>

NEW QUESTION 38

- (Topic 1)

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.

New alert policy

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

Review your settings

Review your settings

Name	AlertPolicy1
Description	Add a description
Severity	● Medium
Category	Others
Filter	Activity is Uploaded file and File extension is Like any of
Aggregation	Trigger an alert when any activity ma
Scope	All users
Recipients	User1@sk220416.onmicrosoft.com Edit
Daily notification limit	Do not send email notifications

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

Answer: C

NEW QUESTION 41

HOTSPOT - (Topic 1)

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
Group1 (2)							
Assessment1	Incomplete	64%	0 of 227 completed	355 of 355 completed	Group1	Microsoft 365	CSA CCM
Assessment2	Incomplete	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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 46

- (Topic 1)

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 48

HOTSPOT - (Topic 1)

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text Description automatically generated

NEW QUESTION 52

HOTSPOT - (Topic 1)

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

Name	Platform	Microsoft Intune
Device1	Windows 11	Not enrolled
Device2	macOS	Enrolled

You need to onboard the devices to Microsoft Purview. The solution must ensure that you can apply Endpoint data loss prevention (Endpoint DLP) policies to the devices. What can you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1: ▼

- The Company Portal app only
- Microsoft Endpoint Manager only
- A local script and Group Policy only
- The Company Portal app and Microsoft Endpoint Manager only
- A local script, Group Policy, and Microsoft Endpoint Manager

Device2: ▼

- The Company Portal app only
- A local script only
- Microsoft Endpoint Manager only
- A local script and Microsoft Endpoint Manager only
- The Company Portal app and Microsoft Endpoint Manager only
- The Company Portal app, a local script, and Microsoft Endpoint Manager

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 55

- (Topic 1)

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



You need to manage the status of Alert2. To which status can you change Alert2?

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

Answer: E

NEW QUESTION 59

- (Topic 1)

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

Answer: AB

NEW QUESTION 64

- (Topic 1)

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

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

All documents that use this naming format must be labeled as Project Documents: You need to create an auto-apply retention label policy.

What should you use to identify the files?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 68

HOTSPOT - (Topic 1)

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.

(\s)(

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

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

(\s)(

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

 \

▼
d{000-999}
d{123}
d{3}

) (\s)

NEW QUESTION 70

HOTSPOT - (Topic 1)

You have a Microsoft 365 E5 tenant.

You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.

What should you do first? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Action to perform:

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

To perform the action, assign the role of:

▼
Compliance Administrator
Compliance Administrator
Global Administrator
Security Administrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 71

HOTSPOT - (Topic 1)

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.

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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"/>

NEW QUESTION 73

- (Topic 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 tenant and 500 computers that run Windows 10. The computers are onboarded to the Microsoft 365 compliance center.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

Use the unallowed apps list instead.

Reference:

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

NEW QUESTION 78

- (Topic 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 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 the text patterns.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2019>

NEW QUESTION 82

HOTSPOT - (Topic 1)

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



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

Supporting elements



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



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

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"/>

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 83

- (Topic 1)

You are creating a data loss prevention (DLP) policy that will apply to all available locations. You configure an advanced DLP rule in the policy. Which type of condition can you use in the rule?

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

Answer: A

NEW QUESTION 86

- (Topic 1)

You have a Microsoft 365 tenant.

You discover that email does NOT use Microsoft Office 365 Message Encryption (OME). You need to ensure that OME can be applied to email.

What should you do first?

- A. Enable Microsoft Defender for Office 365.
- B. Activate Azure Information Protection.
- C. Activate Azure Rights Management (Azure RMS).
- D. Create an Azure key vault.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide>

NEW QUESTION 89

- (Topic 1)

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 GoogleChrome 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 anallowed service domain.

Answer: CD

Explanation:

Reference:

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

NEW QUESTION 92

HOTSPOT - (Topic 1)

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

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

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User 1, Group 1, and Group 2 27/27
 SSPR (Self-Service Password Reset) does not require an E5 license. SSPR is included in Microsoft 365 and Office 365 subscriptions, including lower-tiered plans such as Microsoft 365 Business Standard and Office 365 E3.
 Microsoft 365 Groups can be configured to use SSPR (Self-Service Password Reset). In fact, Microsoft 365 Groups inherit the SSPR settings from the underlying Azure Active Directory (Azure AD) tenant.
 SSPR (Self-Service Password Reset) can also be configured for security groups in Microsoft 365.
 Like Microsoft 365 Groups, security groups in Microsoft 365 inherit the SSPR settings from the underlying Azure Active Directory (Azure AD) tenant. To enable SSPR for security groups, you need to ensure that SSPR is enabled in your Azure AD tenant and that the appropriate user accounts are registered for SSPR.

NEW QUESTION 96

- (Topic 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 sensitivity label.

Does this meet the goal?

- A. Yes

B. NO

Answer: A

NEW QUESTION 98

HOTSPOT - (Topic 1)

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.

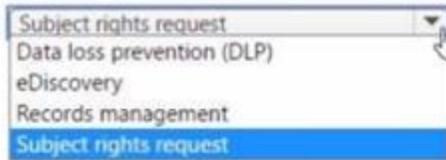
Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

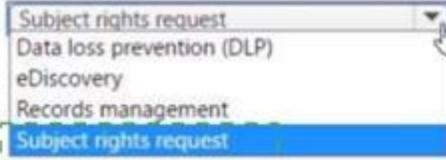
Answer Area

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

NEW QUESTION 99

HOTSPOT - (Topic 1)

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

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.

Answer Area

Can update the Assessment1 title:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Can update the Assessment1 title:

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

NEW QUESTION 101

HOTSPOT - (Topic 1)

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 105

- (Topic 1)

You have a Microsoft 365 ES tenant that uses Microsoft Teams and contains two users named User1 and User2. You create a data loss prevention (DLP) policy that is applied to the Teams chat and channel messages location for user1 and user2. Which Teams entities will have DLP protection? Purview compliance portal?

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

Answer: BD

NEW QUESTION 107

- (Topic 1)

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.

Answer: C

Explanation:

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

NEW QUESTION 111

- (Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 115

- (Topic 1)
You have a Microsoft 365 tenant that uses the following sensitivity labels:

- * Confidential
- * Internal
- * External

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

- A. Yes
- B. No

Answer: A

NEW QUESTION 120

- (Topic 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 compliancedepartment.
- 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.

Answer: A

Explanation:

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

NEW QUESTION 124

- (Topic 1)
You create a retention label that has a retention period of seven years. You need to ensure that documents containing a credit card number are retained for seven years. Other documents must not be retained. What should you create?

- A. a retention label policy of type publish
- B. a retention policy that retains files automatically
- C. a retention policy that deletes files automatically
- D. a retention label policy of type auto-apply

Answer: D

Explanation:

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

NEW QUESTION 128

- (Topic 1)
You have a Microsoft 365 subscription that uses Microsoft Exchange Online. You need to receive an alert if a user emails sensitive documents to specific external domains. What should you create?

- A. a data loss prevention (DLP) policy that uses the Privacy category

- B. a Microsoft Cloud App Security activity policy
- C. a Microsoft Cloud App Security file policy
- D. a data loss prevention (DLP) alert filter

Answer: A

Explanation:

Reference:

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

NEW QUESTION 129

HOTSPOT - (Topic 1)

You have a Microsoft 365 tenant.

A retention hold is applied to all the mailboxes in Microsoft Exchange Online.

A user named User1 leaves your company, and the account of User1 is deleted from Azure Active Directory (Azure AD).

You need to create a new user named User2 and provide User2 with access to the mailbox of User1.

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

NOTE: Each correct selection is worth one point.

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

	\$InactiveMailbox.DistinguishedName
New-Mailbox	-InactiveMailbox
New-MailboxRestoreRequest	-LitigationHoldEnabled
Restore-RecoverableItems	-RetentionHoldEnabled
Set-Mailbox	-SourceMailbox

```
-Name User2 -DisplayName User2 -MicrosoftOnlineServicesID user2@contoso.com
-Password (ConvertTo-SecureString -String 'RdFGFfhjjhgff$^7' -AsPlainText -Force)
-ResetPasswordOnNextLogon $true
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

	\$InactiveMailbox.DistinguishedName
New-Mailbox	-InactiveMailbox
New-MailboxRestoreRequest	-LitigationHoldEnabled
Restore-RecoverableItems	-RetentionHoldEnabled
Set-Mailbox	-SourceMailbox

```
-Name User2 -DisplayName User2 -MicrosoftOnlineServicesID user2@contoso.com
-Password (ConvertTo-SecureString -String 'RdFGFfhjjhgff$^7' -AsPlainText -Force)
-ResetPasswordOnNextLogon $true
```

NEW QUESTION 134

- (Topic 2)

You need to meet the technical requirements for the Site3 documents. What should you create?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 136

- (Topic 2)

You need to meet the technical requirements for the creation of the sensitivity labels. Which administrative users are currently missing the Sensitivity label administrator role?

- A. Admin1 only
- B. Admm1, Admin2, Admin4, and Admin5 only
- C. Admin 1, Admin2, and Admin3 only
- D. Admin 1 and Admin5 only
- E. Admin 1 and Admin4 only

Answer: C

NEW QUESTION 140

- (Topic 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

Answer: D

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>

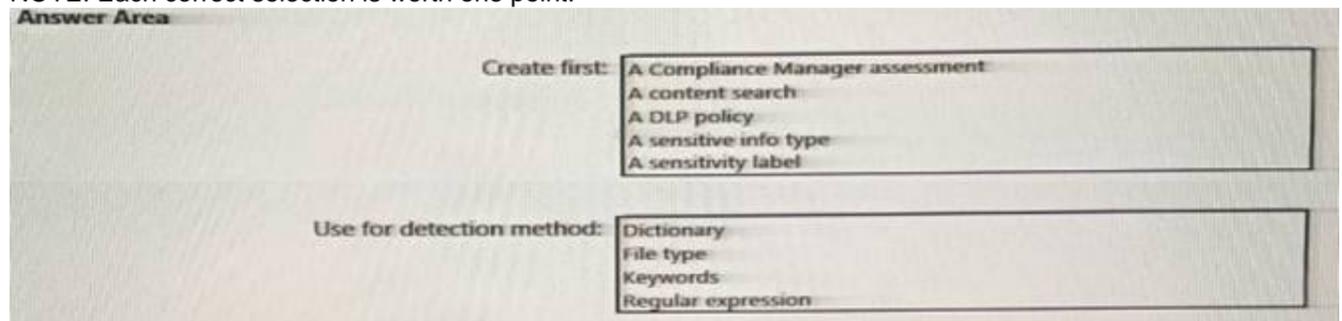
NEW QUESTION 145

HOTSPOT - (Topic 2)

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.

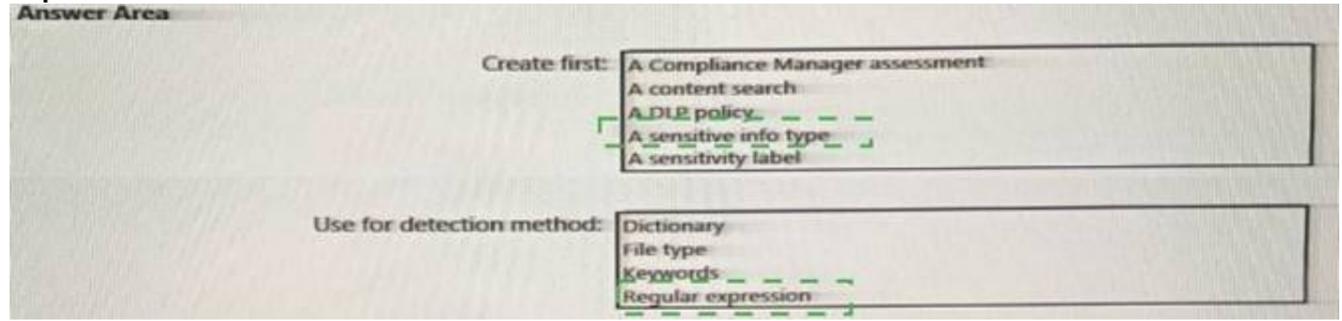
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 146

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SC-400 Practice Exam Features:

- * SC-400 Questions and Answers Updated Frequently
- * SC-400 Practice Questions Verified by Expert Senior Certified Staff
- * SC-400 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SC-400 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SC-400 Practice Test Here](#)