SC-400$^{Q\&As}$

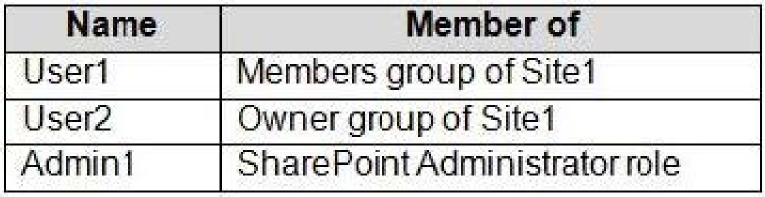
Microsoft Information Protection Administrator

Pass Microsoft SC-400 Exam with 100% Guarantee

QUESTION 1

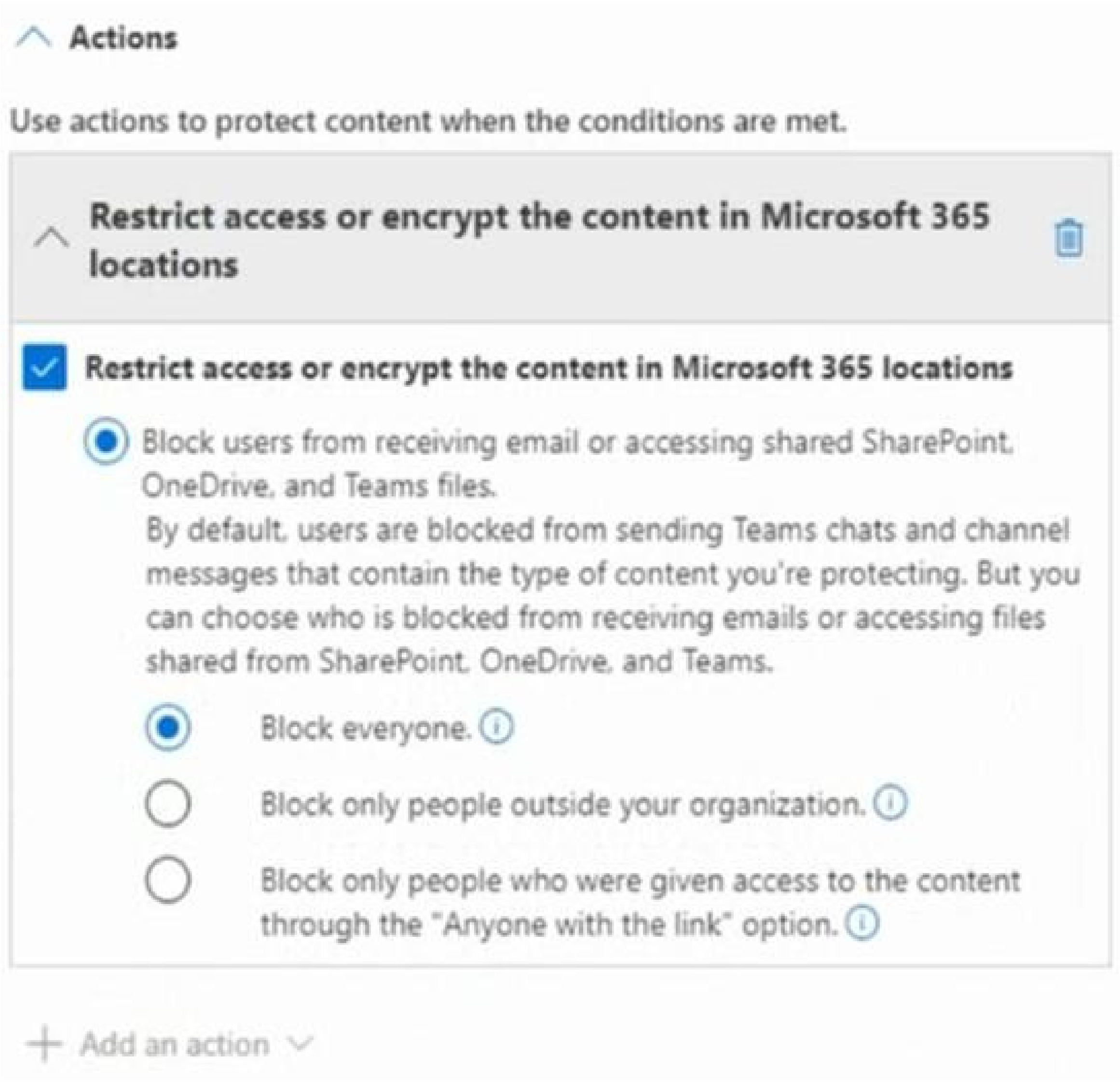
HOTSPOT

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



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

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



Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

☑ Restrict access or encrypt the content in Microsoft 365 locations

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

● Block everyone.

○ Block only people outside your organization.

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

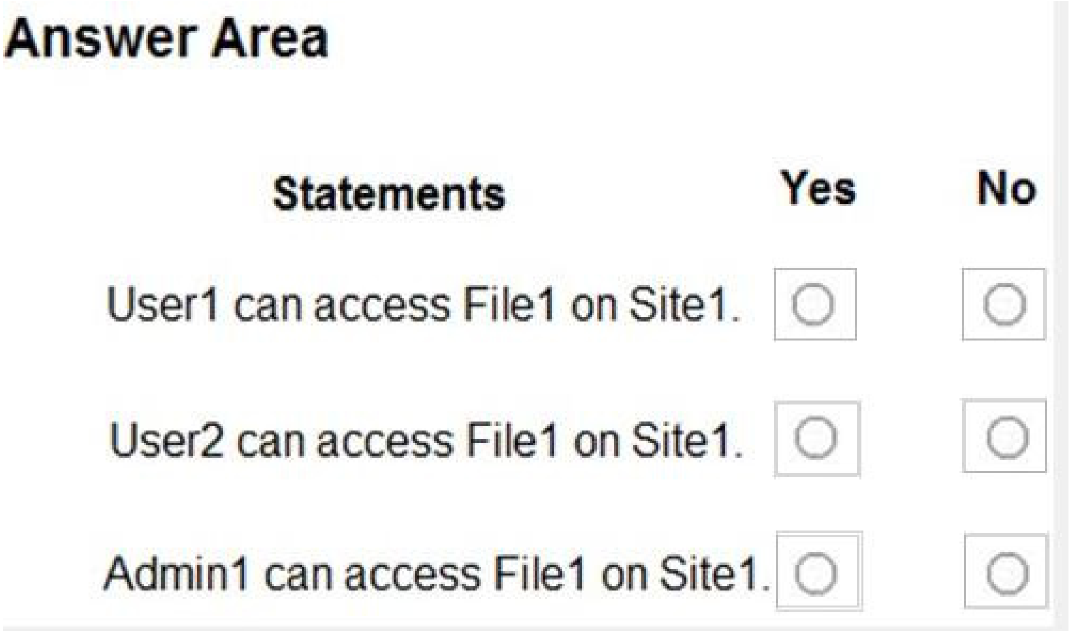
You apply DLP1 to Site1.

User1 uploads a file named File1 to Site1. File1 does NOT match any of the DLP1 rules. User2 updates File1 to contain data that matches the DLP1 rules.

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

NOTE: Each correct selection is worth one point.

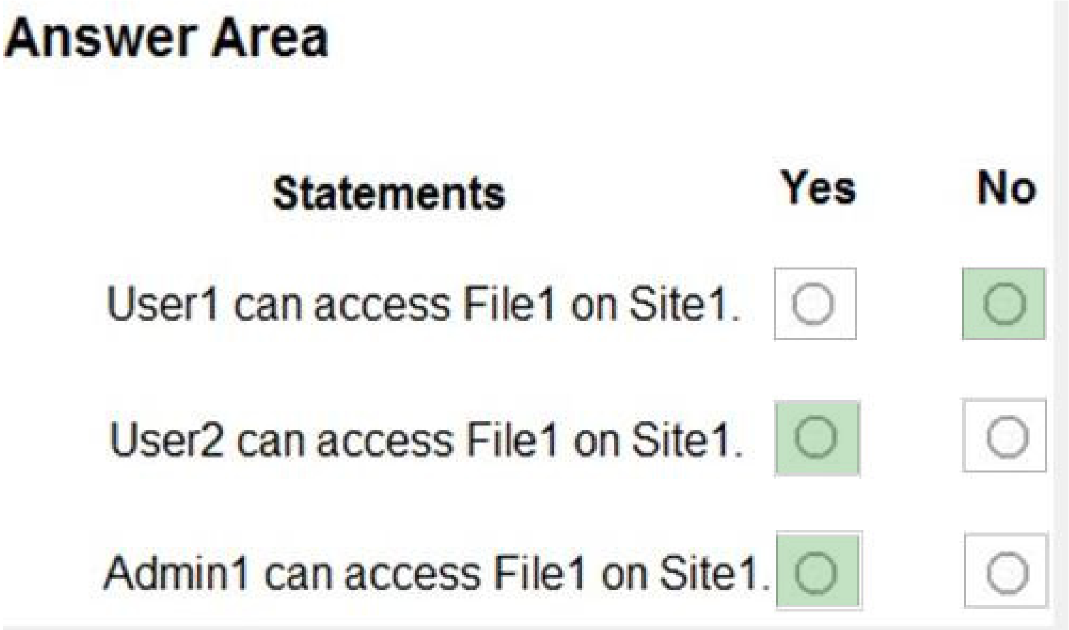
Hot Area:



Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	○
User2 can access File1 on Site1.	○	○
Admin1 can access File1 on Site1.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	[✓ ○]
User2 can access File1 on Site1.	[✓ ○]	○
Admin1 can access File1 on Site1.	[✓ ○]	○

Box 1: No

Note: Actions Any item that makes it through the conditions filter will have any actions that are defined in the rule applied to it. You\\'ll have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action you need to choose from these options:

Block users from accessing shared SharePoint, OneDrive, and Teams content

*

Block everyone. Only the content owner, last modifier, and site admin will continue to have access.

*

etc.

Box 2: Yes

User2 is the last modifier of the file.

Box 3: Yes

Users assigned the SharePoint Administrator role have access to the SharePoint admin center and can create and manage sites (previously called "site collections"), designate site admins, manage sharing settings, and more.

Reference: https://learn.microsoft.com/en-us/sharepoint/sharepoint-admin-role

QUESTION 2

HOTSPOT

You have a Microsoft 365 tenant.

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

1.

An employee ID number that consists of the hire date of the employee followed by a three digit number

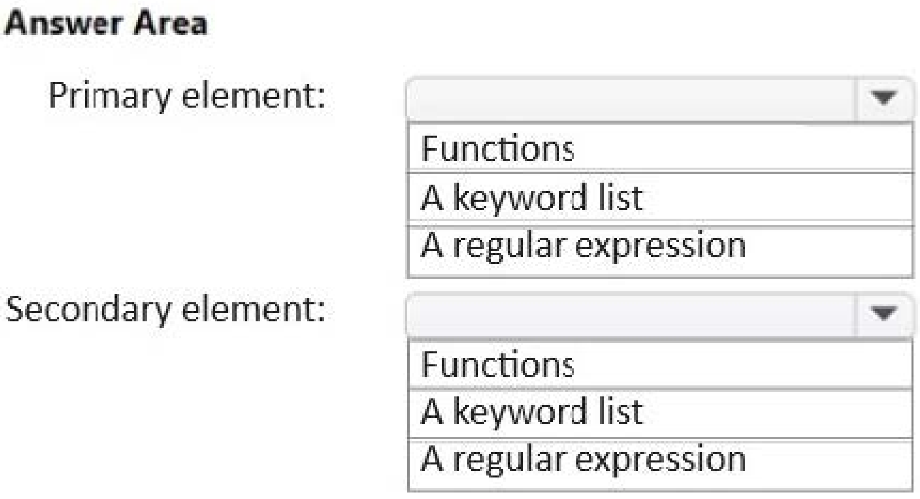
2.

The words “Employee”, “ID”, or “Identification” within 300 characters of the employee ID number

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

NOTE: Each correct selection is worth one point.

Hot Area:

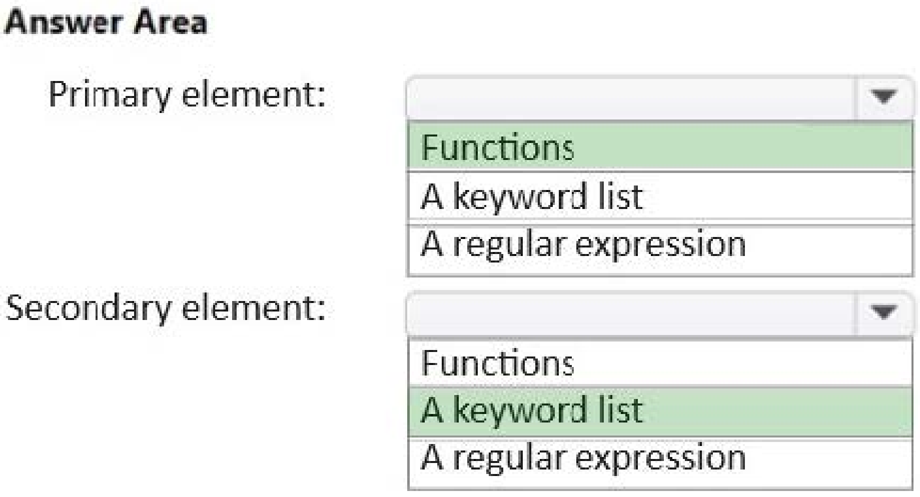


Answer Area

Primary element:
- Functions
- A keyword list
- A regular expression

Secondary element:
- Functions
- A keyword list
- A regular expression

Correct Answer:



Answer Area

Primary element:
- [✓ Functions]
- A keyword list
- A regular expression

Secondary element:
- Functions
- [✓ A keyword list]
- A regular expression

Box 1: Functions

Primary element

Need to include use a date function for the primary element.

Note: Create custom sensitive information types

The primary element can be a Regular expression with an optional validator, a Keyword list, a Keyword dictionary, or one of the pre-configured Functions.

Box 2: A keyword list

Secondary element

Use a keyword list which includes the words “Employee”, “ID”, or “Identification".

Reference:

https://learn.microsoft.com/en-us/purview/sit-learn-about-exact-data-match-based-sits

QUESTION 3

HOTSPOT

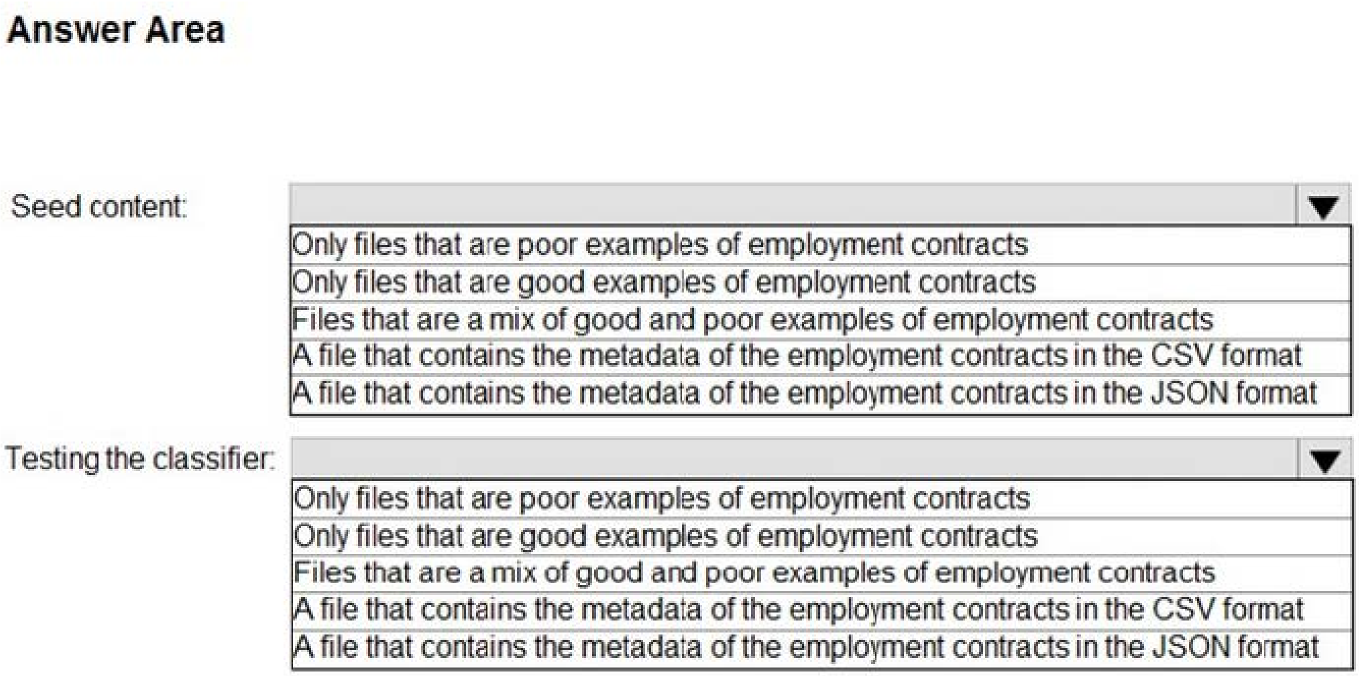
You plan to implement a sensitive information type based on a trainable classifier. The sensitive information type will identify employment contracts.

You need to copy the required files to Microsoft SharePoint Online folders to train the classifier.

What should you use to seed content and test the classifier? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

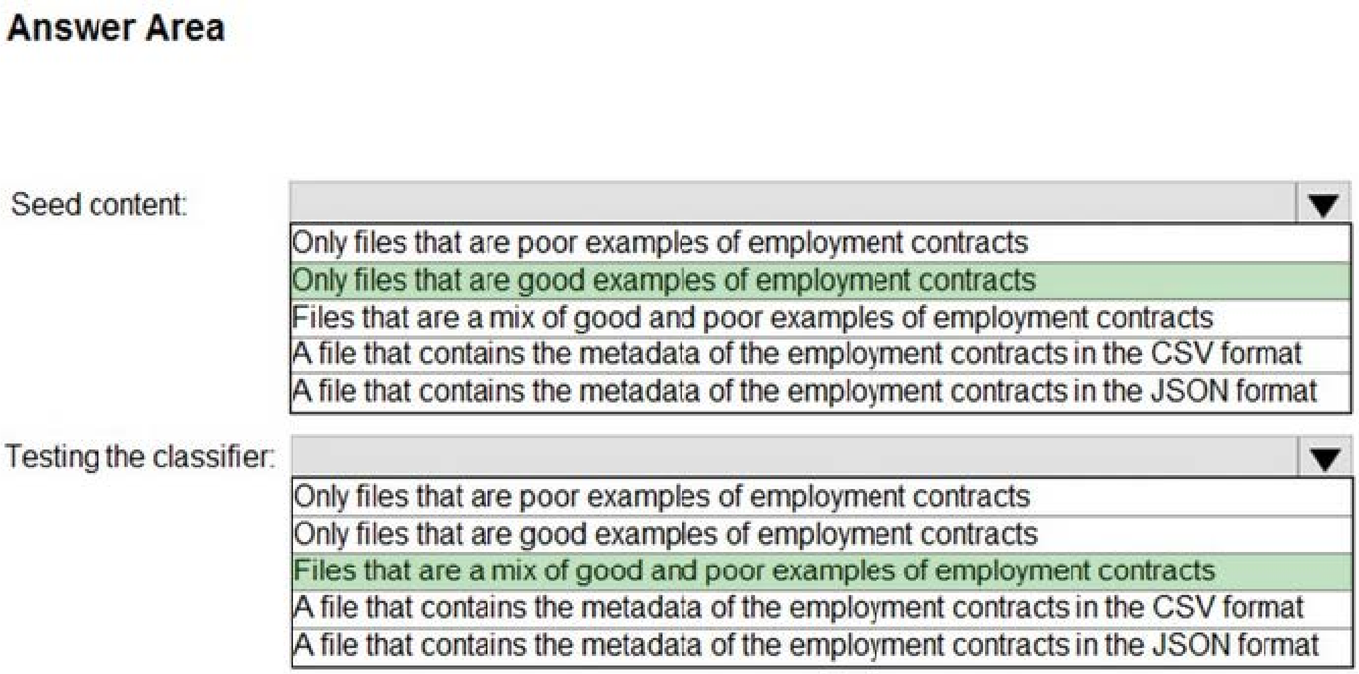
Seed content:

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

Testing the classifier:

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

Correct Answer:



Answer Area

Seed content:

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

Testing the classifier:

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

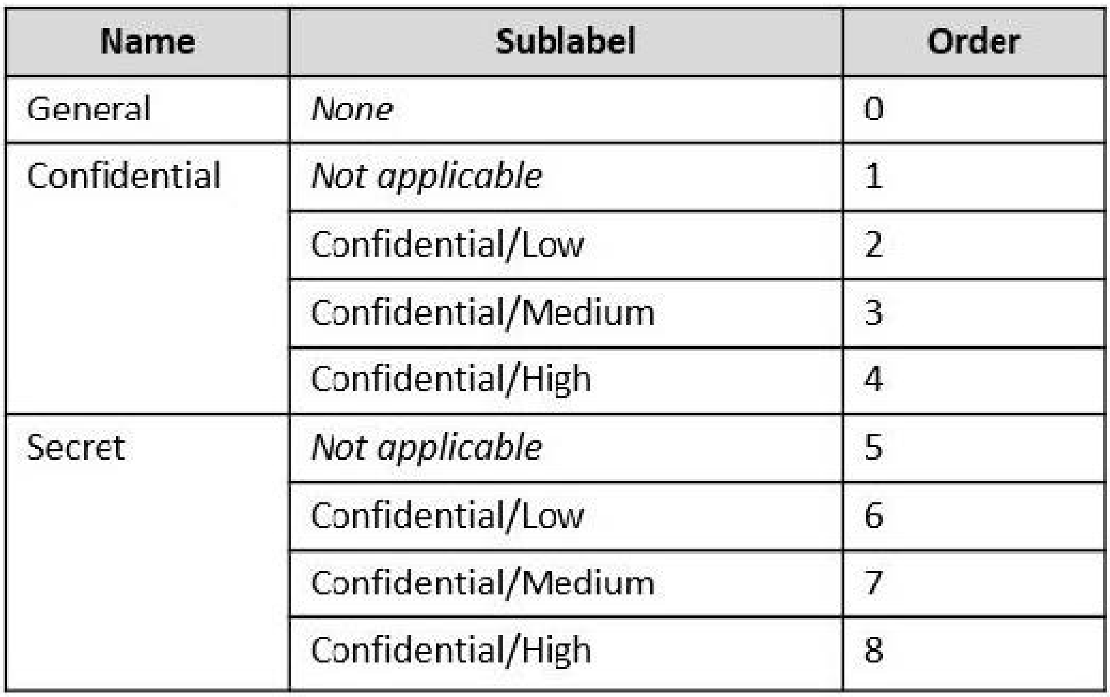
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

QUESTION 4

HOTSPOT

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2 and a group named Group1. User1 is a member of Group1.

The subscription contains the sensitivity labels shown in the following table.



Name	Sublabel	Order
General	*None*	0
Confidential	*Not applicable*	1
	Confidential/Low	2
	Confidential/Medium	3
	Confidential/High	4
Secret	*Not applicable*	5
	Confidential/Low	6
	Confidential/Medium	7
	Confidential/High	8

You have a sensitivity label policy named Policy1 that is published to User1 and User2. The policy includes the following labels:

1.

General

2.

Confidential

3.

Confidential/Low

4.

Confidential/High

5.

Confidential/Medium

For Policy1, the default label for documents is Confidential/Low.

You have a sensitivity label policy named Policy2 that is published to Group1. The policy includes the following labels:

1.

Secret

2.

General

3.

Secret/Low

4.

Secret/High

5.

Secret/Medium

For Policy2, the default label for documents is Secret/Low.

You have a sensitivity label policy named Policy3 that is published to User1 and User2. The policy includes the following labels:

1.

Secret

2.

General

3.

Secret/Low

4.

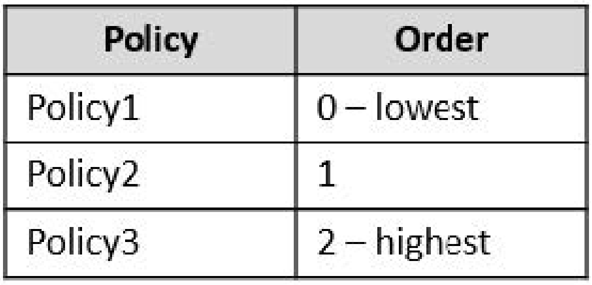
Secret/High

5.

Secret/Medium

For Policy3, the default label for documents is Secret/Medium.

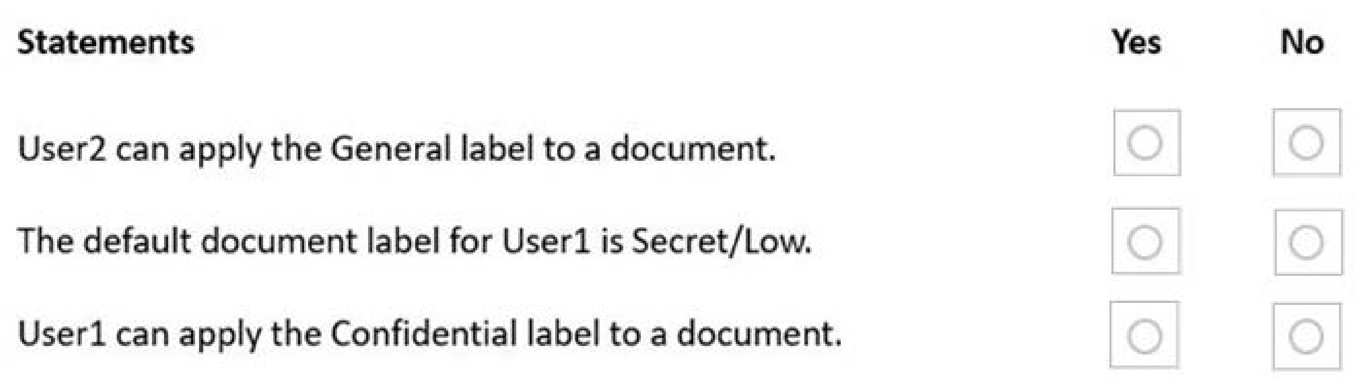
The order of the policies is shown in the following table.



Policy	Order
Policy1	0 – lowest
Policy2	1
Policy3	2 – highest

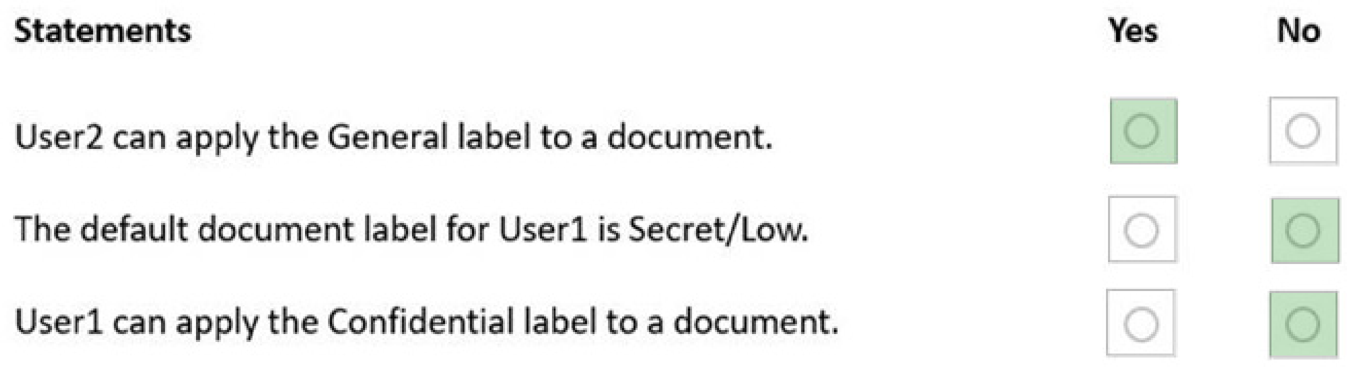
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User2 can apply the General label to a document.	○	○
The default document label for User1 is Secret/Low.	○	○
User1 can apply the Confidential label to a document.	○	○

Correct Answer:



Statements	Yes	No
User2 can apply the General label to a document.	[✓ ○]	○
The default document label for User1 is Secret/Low.	○	[✓ ○]
User1 can apply the Confidential label to a document.	○	[✓ ○]

QUESTION 5

HOTSPOT

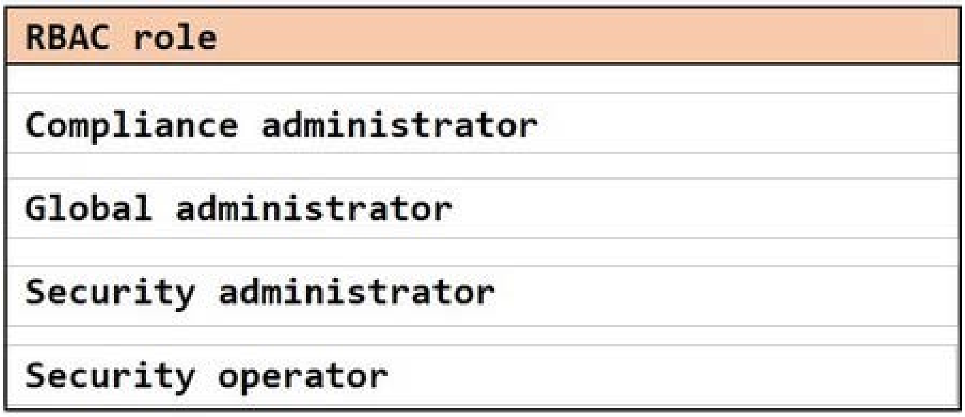
You plan to create a custom trainable classifier based on an organizational form template.

You need to identity which role based access control (RBAC) role is required to create the trainable classifier and where to classifier. The solution must use the principle of least privilege.

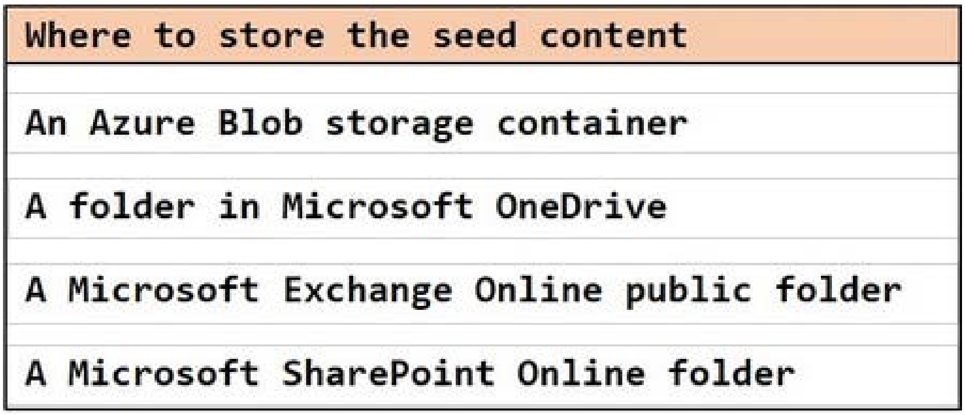
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

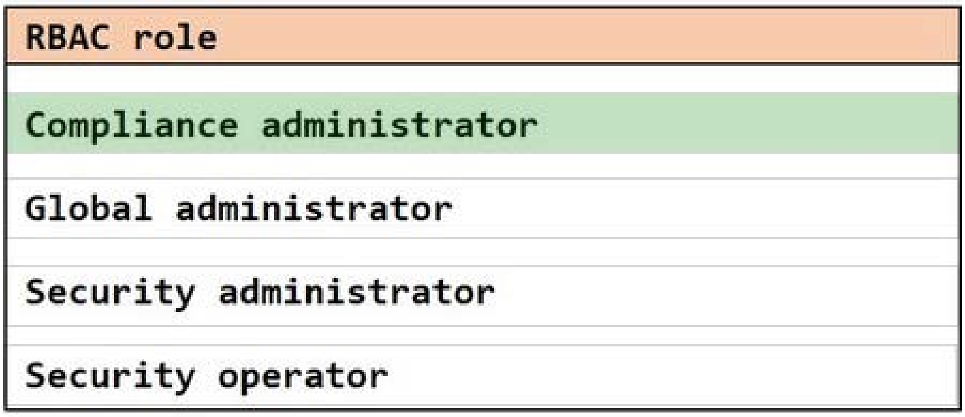


RBAC role
Compliance administrator
Global administrator
Security administrator
Security operator

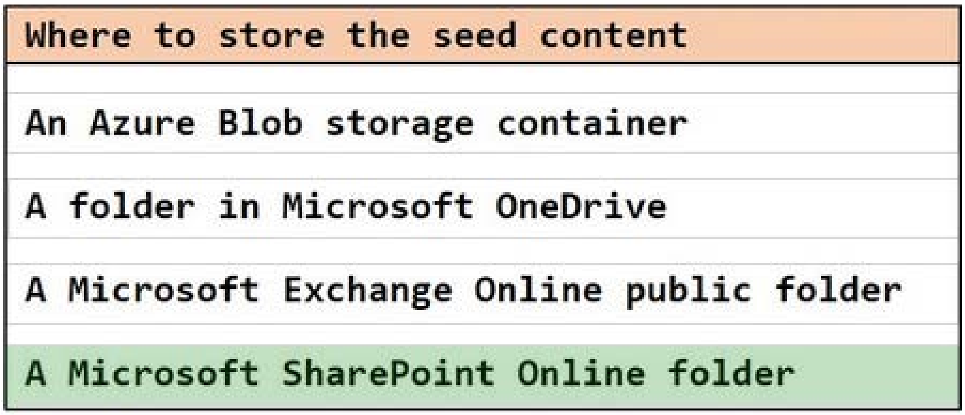


Where to store the seed content
An Azure Blob storage container
A folder in Microsoft OneDrive
A Microsoft Exchange Online public folder
A Microsoft SharePoint Online folder

Correct Answer:



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



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

QUESTION 6

HOTSPOT

You have a Microsoft 365 E5 subscription.

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

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

1.

Provide data loss prevention (DLP) policy recommendations.

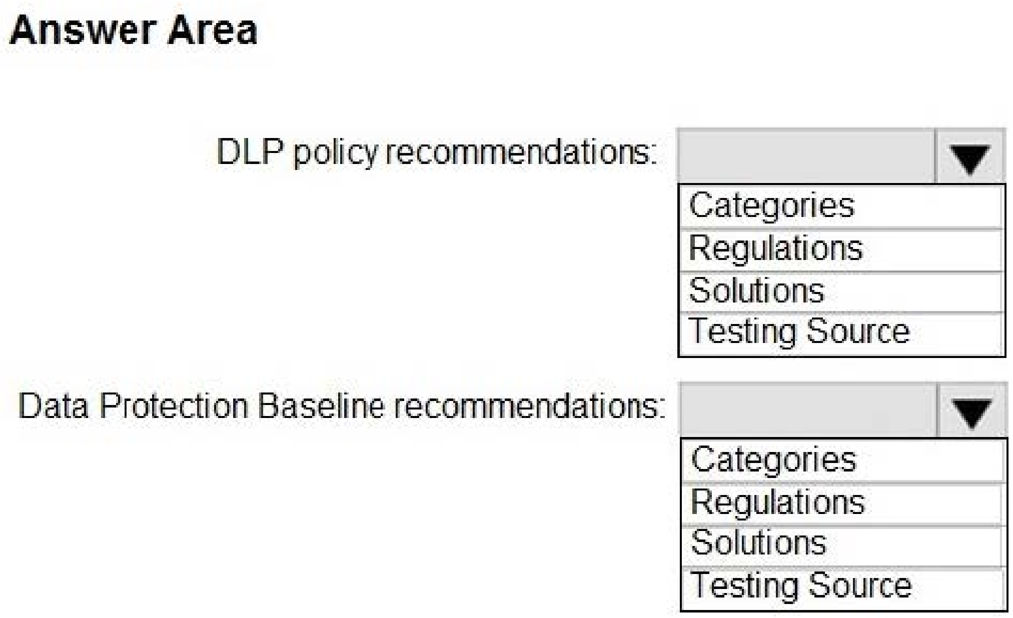
2.

Provide Data Protection Baseline recommendations.

Which filter should you use 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

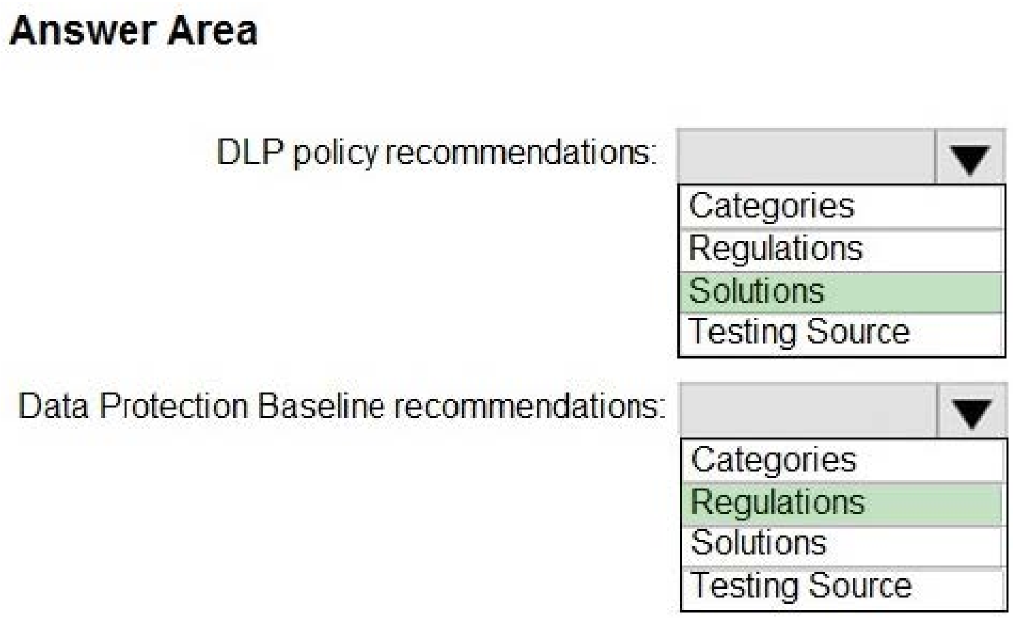
DLP policy recommendations:

- Categories
- Regulations
- Solutions
- Testing Source

Data Protection Baseline recommendations:

- Categories
- Regulations
- Solutions
- Testing Source

Correct Answer:



Answer Area

DLP policy recommendations:

- Categories
- Regulations
- [✓ Solutions]
- Testing Source

Data Protection Baseline recommendations:

- Categories
- [✓ Regulations]
- Solutions
- Testing Source

Box 1: Solutions

Provide data loss prevention (DLP) policy recommendations.

Incorrect:

*

Regulations

*

Categories

*

Testing Source

Box 2: Regulations

Provide Data Protection Baseline recommendations.

Compliance Manager assessments help your organization evaluate its compliance with industry and regional regulations. Setting up the most relevant assessments for your organization can help you implement policies and operational

procedures to limit your compliance risk. Ready-to-use regulatory templates for over 360 regulations contain the necessary controls and improvement actions for completing the assessment.

Data Protection Baseline default assessment

To get you started, Microsoft provides a default assessment for the Microsoft 365 data protection baseline. This baseline assessment has a set of controls for key regulations and standards for data protection and general data governance.

This baseline draws elements primarily from NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) and ISO (International Organization for Standardization), as well as from FedRAMP (Federal Risk and

Authorization Management Program) and GDPR (General Data Protection Regulation of the European Union).

This assessment is used to calculate your initial compliance score the first time you come to Compliance Manager, before you configure any other assessments. Compliance Manager collects initial signals from your Microsoft 365 solutions.

You\\'ll see at a glance how your organization is performing relative to key data protection standards and regulations, and see suggested improvement actions to take. Compliance Manager becomes more helpful as you build and manage your

own assessments to meet your organization\\'s particular needs.

Reference:

https://learn.microsoft.com/en-us/purview/compliance-manager-assessments

QUESTION 7

You have a Microsoft 365 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.

You plan to configure a retention label named Label1 and apply Label1 to all the files in Site1.

You need to ensure that two years after a file is created in Site1, the file moves automatically to Site2.

How should you configure the Choose what happens after the retention period setting for Label1?

A. Run a Power Automate flow

B. Change the label

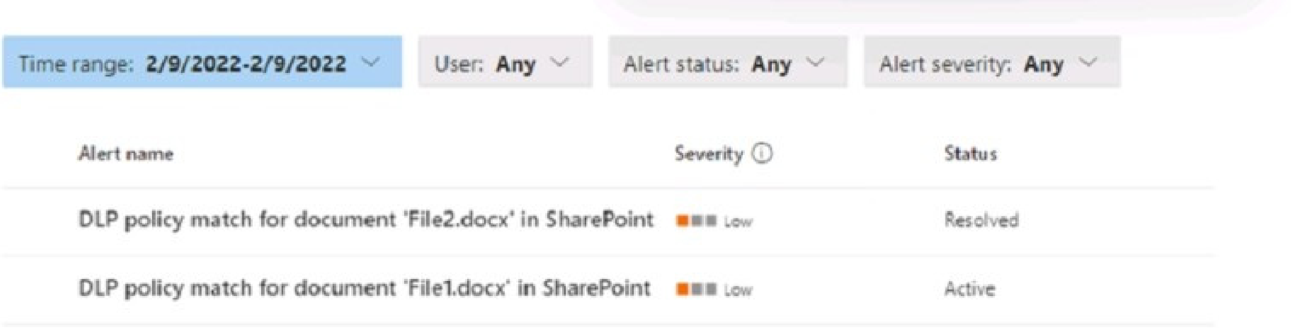
C. Deactivate retention settings

D. Start a disposition review

Correct Answer: A

QUESTION 8

HOTSPOT

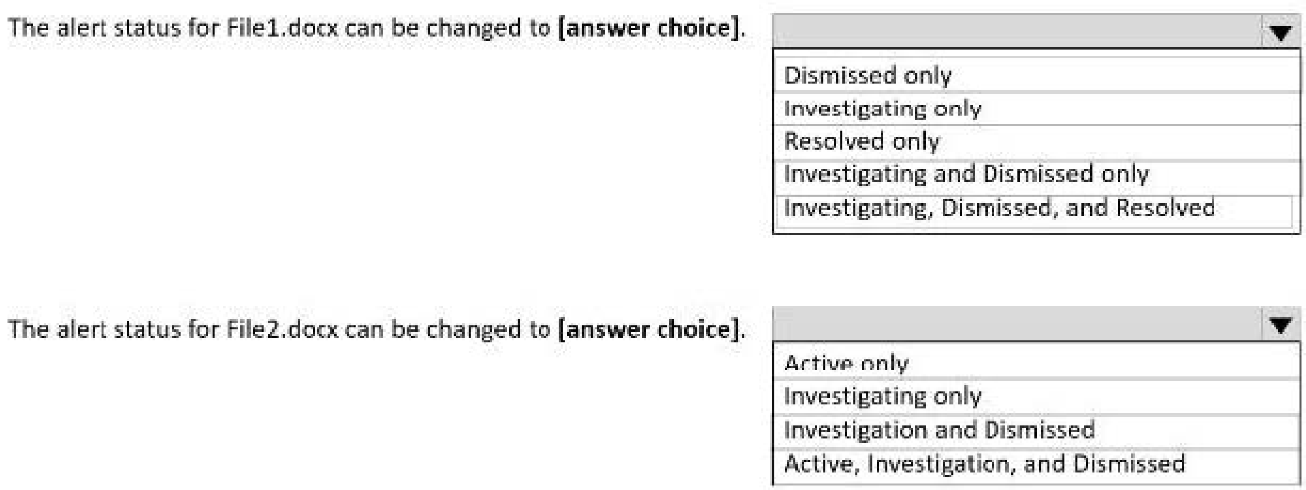


Time range: **2/9/2022-2/9/2022** | User: **Any** | Alert status: **Any** | Alert severity: **Any**

Alert name	Severity	Status
DLP policy match for document 'File2.docx' in SharePoint	■■■ Low	Resolved
DLP policy match for document 'File1.docx' in SharePoint	■■■ Low	Active

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

Hot Area:



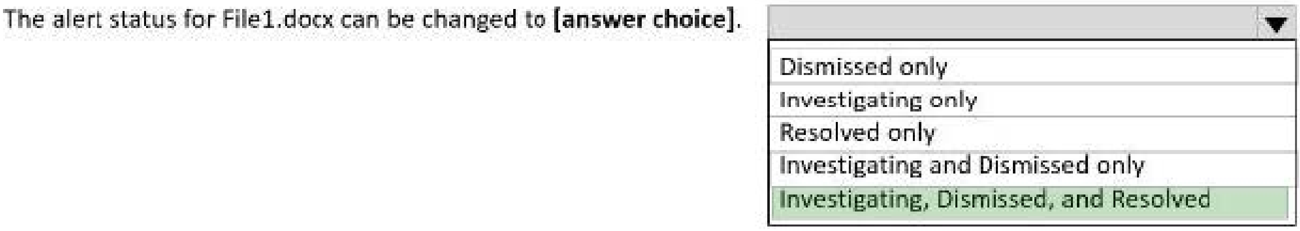
The alert status for File1.docx can be changed to **[answer choice]**.

- Dismissed only
- Investigating only
- Resolved only
- Investigating and Dismissed only
- Investigating, Dismissed, and Resolved

The alert status for File2.docx can be changed to **[answer choice]**.

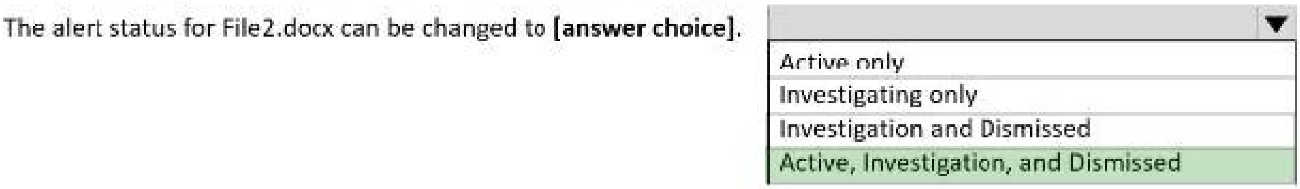
- Active only
- Investigating only
- Investigation and Dismissed
- Active, Investigation, and Dismissed

Correct Answer:



The alert status for File1.docx can be changed to **[answer choice]**.

- Dismissed only
- Investigating only
- Resolved only
- Investigating and Dismissed only
- [✓ Investigating, Dismissed, and Resolved]



The alert status for File2.docx can be changed to **[answer choice]**.

- Active only
- Investigating only
- Investigation and Dismissed
- [✓ Active, Investigation, and Dismissed]

QUESTION 9

You have a Microsoft 365 E5 subscription that uses Yammer.

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

What should you do first?

A. Configure Hybrid Mode for Yammer.

B. Configure Native Mode for Yammer.

C. Configure the Yammer network admin settings.

D. Assign each user a Yammer license.

Correct Answer: B

QUESTION 10

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

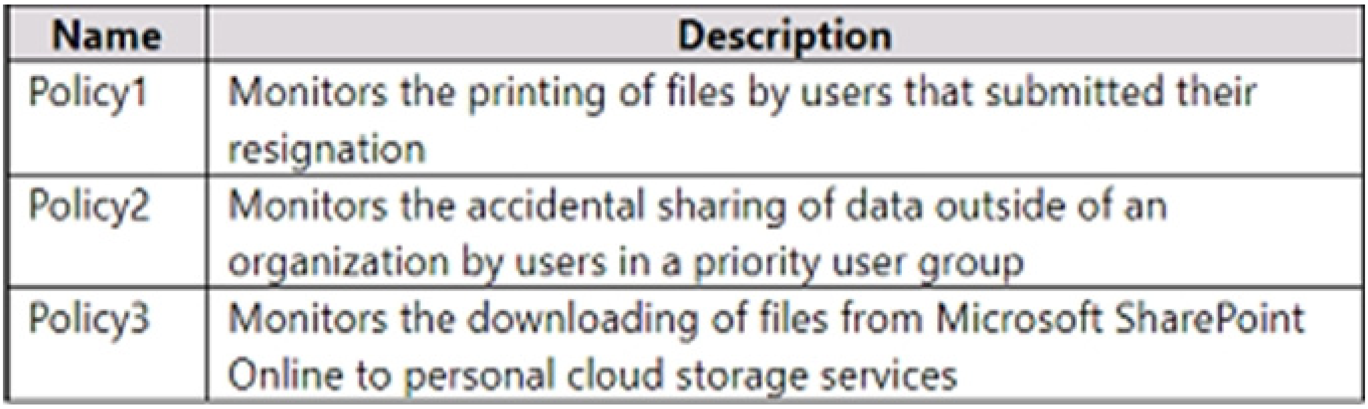
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/record-versioning?view=o365-worldwide

QUESTION 11

DRAG DROP

You have a Microsoft 365 E5 subscription.

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



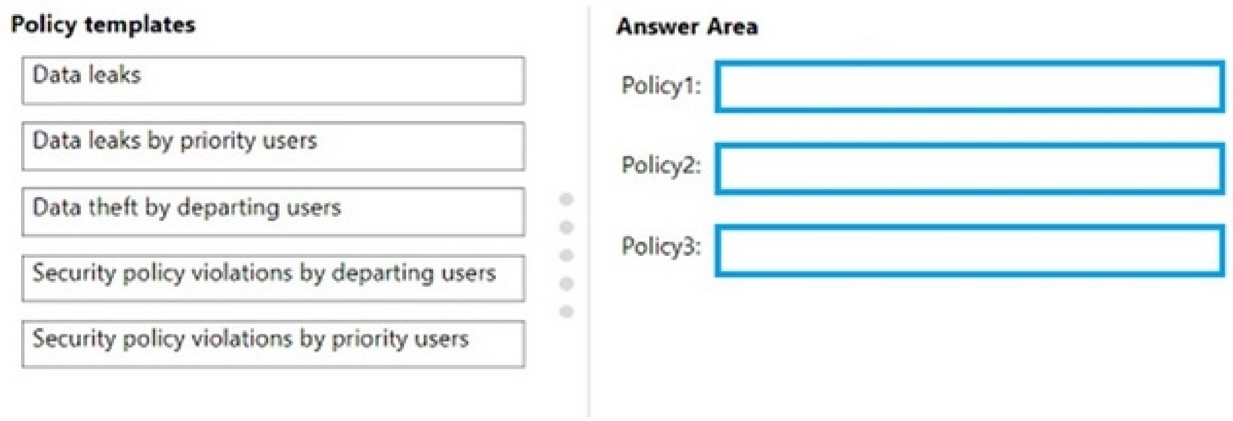
Name	Description
Policy1	Monitors the printing of files by users that submitted their resignation
Policy2	Monitors the accidental sharing of data outside of an organization by users in a priority user group
Policy3	Monitors the downloading of files from Microsoft SharePoint Online to personal cloud storage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

Which policy template should you use for each policy? To answer, drag the appropriate policy templates to the correct policies. Each template may be used once, more than once, or not at all. You may need to drag the split bar between

panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Policy templates

- Data leaks
- Data leaks by priority users
- Data theft by departing users
- Security policy violations by departing users
- Security policy violations by priority users

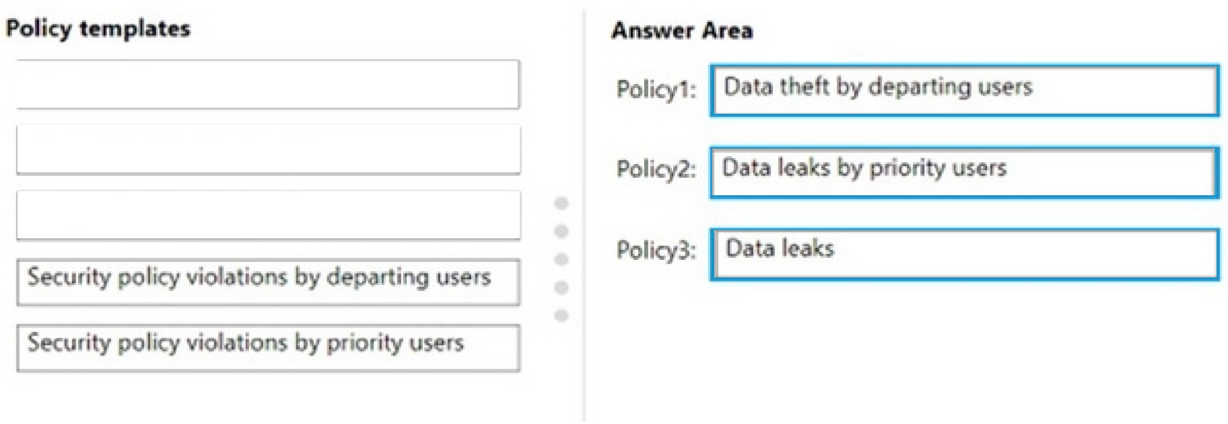
Answer Area

Policy1:

Policy2:

Policy3:

Correct Answer:



Policy templates

Security policy violations by departing users

Security policy violations by priority users

Answer Area

Policy1: Data theft by departing users

Policy2: Data leaks by priority users

Policy3: Data leaks

Box 1: Data theft by departing users

Policy1: Monitors the printing of files by users that submitted their resignation.

Data theft by departing users

When users leave your organization, there are specific risk indicators typically associated with potential data theft by departing users. This policy template uses exfiltration indicators for risk scoring and focuses on detection and alerts in this

risk area. Data theft for departing users might include downloading files from SharePoint Online, *printing files*, and copying data to personal cloud messaging and storage services near their employment resignation and end dates.

Note: Insider risk management analysts and investigators may use cumulative exfiltration detection insights to help identify exfiltration activities that may not typically generate alerts but are above what is typical for their organization. Some

examples may be departing users slowly exfiltrate data across a range of days, or when users repeatedly share data across multiple channels more than usual for data sharing for your organization, or compared to their peer groups.

Incorrect:

* Security policy violations by departing users

Box 2: Data leaks by priority users

Policy2: Monitors the accidental sharing of data outside of an organization by users in a priority user group.

Data leaks by priority users (preview)

Protecting data and preventing data leaks for users in your organization might depend on their position, level of access to sensitive information, or risk history. Data leaks can include accidental *oversharing* of highly sensitive information

outside your organization or data theft with malicious intent. With an assigned data loss prevention (DLP) policy as a triggering event option, this template starts scoring real-time detections of suspicious activity and result in an increased

likelihood of insider risk alerts and alerts with higher severity levels. Priority users are defined in priority user groups configured in the insider risk management settings area.

Box 3: Data Leaks

Policy3: Monitors the downloading of files from Microsoft SharePoint Online to personal cloud storage services

Data leaks

Protecting data and preventing data leaks is a constant challenge for most organizations, particularly with the rapid growth of new data created by users, devices, and services. Users are empowered to create, store, and share information

across services and devices that make managing data leaks increasingly more complex and difficult. Data leaks can include accidental oversharing of information outside your organization or data theft with malicious intent. With an assigned

Microsoft Purview Data Loss Prevention (DLP) policy, built-in, or customizable triggering events, this template starts scoring real-time detections of suspicious *SharePoint Online data downloads*, file and folder sharing, printing files, and

copying data to personal cloud messaging and storage services.

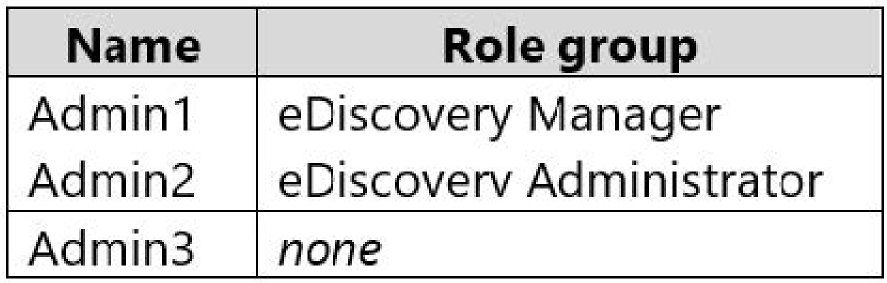
Reference:

https://learn.microsoft.com/en-us/purview/insider-risk-management-policy-templates

https://learn.microsoft.com/en-us/purview/insider-risk-management-policies

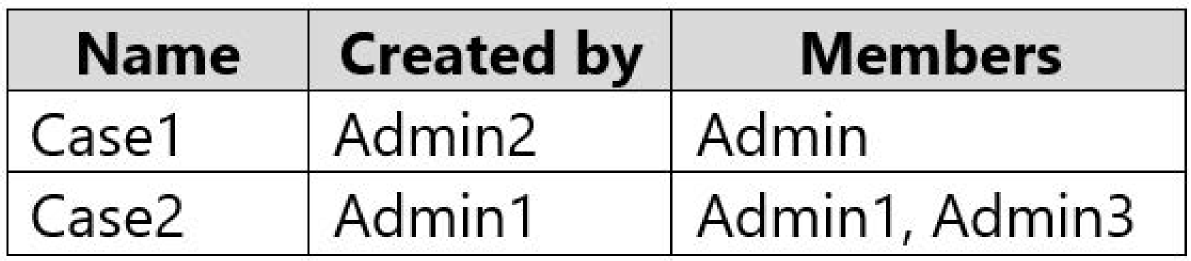
QUESTION 12

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



Name	Role group
Admin1	eDiscovery Manager
Admin2	eDiscoverv Administrator
Admin3	*none*

You have the core eDiscovery cases shown in the following table.



Name	Created by	Members
Case1	Admin2	Admin
Case2	Admin1	Admin1, Admin3

You need to ensure that Admin3 can create holds in Case1 and Case2. The solution must use the principle of least privilege. To what should you add Admin3?

A. the Global Administrator role

B. the eDiscovery Manager role group

C. the Compliance Manager Contributors role group

D. the eDiscovery Administrator role group

Correct Answer: D

QUESTION 13

You have a Microsoft 365 E5 tenant.

You need to add a new keyword dictionary.

What should you create?

A. a trainable classifier

B. a sensitivity label E3

C. a sensitive info type

D. a retention policy

Correct Answer: C

QUESTION 14

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

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

QUESTION 15

You have a Microsoft 365 tenant that has a retention label policy. You need to configure the policy to meet the following requirements:

1.

Prevent the disabling or deletion of the policy.

2.

Ensure that new labels can be added.

3.

Prevent the removal of labels. What should you do?

A. Import a file plan.

B. Enable insider risk management.

C. Enable the regulatory record option.

D. Create a preservation lock.

Correct Answer: D