PassQueen
a.k.a dumpsqueen.com

Administering Information Security in Microsoft 365

Microsoft SC-401

Version Demo

Total Demo Questions: 31

Total Premium Questions: 314

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Implement information protection	134
Topic 2, Implement data loss prevention	115
Topic 3, Implement data lifecycle management	59
Topic 4, Mix Questions	6
Total	314

QUESTION NO: 1

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

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

Which devices support Endpoint DLP?

A. Device1 only

B. Device1 and Device2 only

C. Device1 and Device4 only

D. Device1, Device2, and Device4 only

E. Device1, Device2, Device3, and Device4

ANSWER: D

Explanation:

Device1, Device2, and Device4 only is correct. Microsoft Purview Endpoint data loss prevention supports devices running supported versions of Windows and macOS. Therefore, the Windows 11 device (Device1), Windows 10 device (Device2), and macOS device (Device4) can be included in Endpoint DLP protection. The devices must also meet the applicable operating-system requirements and be onboarded to Microsoft Defender for Endpoint, which is used by Purview to identify and enforce DLP controls on endpoint devices.

After the required onboarding and configuration, Endpoint DLP policies can monitor and restrict sensitive-data activities on supported endpoints, such as copying data to removable media, printing, copying content to the clipboard, uploading data through unsupported browsers, or sharing content with network shares. Support for macOS means that a device running macOS should not be excluded merely because it is not Windows; it can be brought under Endpoint DLP policy coverage when it meets the documented prerequisites. Microsoft documents the supported platforms and setup requirements in Learn about Endpoint DLP and the implementation prerequisites in Endpoint DLP prerequisites.

QUESTION NO: 2

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview insider risk management.

You implement the HR data connector.

You need to prepare the data that will be imported by the data connector. In which format should you prepare the data?

A. JSON

B. CSV

C. TSV

D. XML

E. PRN

ANSWER: B

Explanation:

CSV is the required format for preparing data for the Microsoft Purview Insider Risk Management HR connector. The connector is designed to ingest employee and organizational information from a comma-separated values file, enabling the administrator to map the file's columns to the HR attributes used by Insider Risk Management. These attributes can include

employee identifiers, names, job titles, managers, departments, employment status, and relevant dates such as hire or termination dates.

Using a structured CSV file provides a straightforward tabular representation of HR records: each row represents an employee record and each column represents a defined attribute. During connector configuration, the uploaded file is validated and its columns are mapped to the appropriate Insider Risk Management user and HR fields. Accurate employee identifiers are especially important because the imported HR data must be associated with the corresponding Microsoft Entra ID users for risk policies, indicators, and user context to work correctly.

Microsoft documents the HR connector configuration and its CSV-based upload process in Insider Risk Management settings and the HR connector. For broader deployment prerequisites and configuration context, see Microsoft Purview Insider Risk Management.

QUESTION NO: 3

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

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

What should you do?

A. From Exchange Online PowerShell. run Start-ManagedFolderAssistant.

B. From the Microsoft Purview portal, create a data loss prevention (DLP) policy.

C. From the Microsoft Purview portal, create a label policy.

D. From Exchange Online PowerShell, run start -RetentionAutoTagLearning.

ANSWER: A

Explanation:

Running **Start-ManagedFolderAssistant** from Exchange Online PowerShell is the appropriate way to expedite processing of retention policy tags for a mailbox. In Exchange Online, the Managed Folder Assistant is the mailbox assistant responsible for processing messaging records management retention policies and their retention tags. It evaluates items in the mailbox, applies the appropriate retention-tag metadata, and performs retention actions when the relevant retention age and policy conditions are met.

The assistant normally runs automatically on a background schedule. When tags need to be assigned as soon as possible, an administrator can manually invoke it for the affected mailbox by using **Start-ManagedFolderAssistant -Identity <mailbox>**. This starts mailbox processing without having to wait for the normal scheduled assistant cycle. The command can also be scoped to a particular mailbox, making it suitable when immediate processing is required after a retention policy is assigned or changed.

Microsoft documents that the **Start-ManagedFolderAssistant** cmdlet starts the Managed Folder Assistant for specified mailboxes. For details, see Start-ManagedFolderAssistant cmdlet and Retention tags and retention policies in Exchange Online.

QUESTION NO: 4

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

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

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

Which items can use Trainable 1?

A. Label2 only

B. Label1 and Label2 only

C. Label1 and Policy1 only

D. Label2, Policy1, and DLP1 only

E. Label1, Label2, Policy1, and DLP1

ANSWER: D

Explanation:

Label2, Policy1, and DLP1 only is correct. Microsoft Purview trainable classifiers identify content by evaluating the meaning and context of unstructured data, rather than relying only on exact patterns such as keywords or regular expressions. A trainable classifier can be selected as a condition when configuring automatic retention labeling. Therefore, Label2 can be automatically applied to matching content through the associated auto-apply retention configuration represented by Policy1. This supports retention and records-management scenarios in which content must be classified before the appropriate retention label is applied.

Trainable classifiers are also available as conditions in Microsoft Purview Data Loss Prevention policies. DLP1 can consequently use Trainable1 to identify content matching the classifier and apply the policy's configured protective actions. This enables organizations to detect organization-specific content categories that might not be fully represented by a built-in sensitive information type. The classifier must be in a ready-to-use state and have the required publishing status before it can be selected in these policy configurations. For more details, see Get started with trainable classifiers and Apply retention labels automatically.

QUESTION NO: 5

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

You need to ensure that you receive an alert when a user uploads a document to a third-party cloud storage service.

What should you use?

A. an activity policy

B. a sensitivity label

C. a file policy

D. an insider risk policy

ANSWER: A

Explanation:

An activity policy is the appropriate Microsoft Defender for Cloud Apps policy to generate an alert when a user uploads a document to a third-party cloud storage service. Activity policies evaluate recorded user and administrator actions in cloud apps, using activity filters such as the activity type, the app involved, the user, IP address, device, and other available

metadata. For this requirement, configure an activity policy that filters for upload activities in the relevant third-party cloud storage apps and enable an alert when the policy condition is met. This provides event-based monitoring: each matching upload can create an alert for investigation in the Defender portal and can optionally support further automated response through connected workflows. The organization must first have visibility into the relevant app activities, such as through Defender for Cloud Apps activity logs, connected app connectors, or session controls, depending on how the third-party service is being monitored. Microsoft documents activity policies as the policy type for detecting specific activities and creating alerts based on those activities. See Activity policies in Microsoft Defender for Cloud Apps and Activity filters in Microsoft Defender for Cloud Apps.

QUESTION NO: 6

You have a Microsoft J65 E5 subscription that contains a user named User1.

All users are assigned Microsoft 365 Copilot licenses.

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

You need to ensure that User1 can analyze prompts and responses for AI interaction events. The

solution must follow the principle of least privilege.

To which two role groups should you add User1? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

A. Information Protection Analysts

B. Security Reader

C. Content Explorer Content Viewer

D. Insider Risk Management Investigators

E. Content Explorer list Viewer

ANSWER: C E

Explanation:

Microsoft Purview DSPM for AI can surface Microsoft 365 Copilot interaction data for investigation, including the user prompt and the generated response. Access to this sensitive content is intentionally separated into two least-privilege permissions. **Content Explorer list Viewer
** provides the ability to enumerate and locate the relevant classified items and interaction-related records in Content Explorer. This permission supports reviewing the list and associated metadata without granting broader tenant administration capabilities.

Content Explorer Content Viewer provides the additional content-viewing capability required to open the discovered items and inspect their protected content. Assigning both role groups enables User1 to progress from finding relevant AI interaction events to viewing the prompt and response details necessary for analysis. These are narrowly scoped, read-oriented role groups and therefore meet the least-privilege requirement while avoiding permissions to configure policies, alter settings, or administer unrelated security workloads.

Microsoft documents the separate list-view and content-view permissions for Content Explorer, including the requirement for appropriate role-group membership to view item contents. See Content Explorer in Microsoft Purview and Content Explorer permissions.

QUESTION NO: 7

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

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

You recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted. Solution: You configure a mail flow rule that matches the text patterns. Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Configuring a mail flow rule to match text patterns only establishes a detection condition; by itself, it does not apply encryption to a message. To meet the stated goal, the configuration must include an enforcement action that encrypts messages when the relevant content is detected. For example, an Exchange mail flow rule can use a regular-expression condition to identify the expected key format and then apply Microsoft Purview Message Encryption as the rule action.

For a more maintainable data-protection design, an organization can also use a Microsoft Purview Data Loss Prevention policy with a custom sensitive information type designed to identify Azure Storage account keys. The DLP policy can then apply encryption when a match occurs, including for mail sent to external recipients. This separates sensitive-data classification from enforcement and supports policy-based protection as requirements evolve. Microsoft documents mail-flow rule actions for applying encryption at Apply Microsoft Purview Message Encryption with mail flow rules and describes creating tailored detection patterns at Create a custom sensitive information type.

QUESTION NO: 8

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

You place a preservation lock on RP1.

You need to modify RP1.

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

NOTE : Each correct selection is worth one point.

A. Add locations to the policy.

B. Delete the policy.

C. Remove locations from the policy.

D. Decrease the retention period of the policy.

E. Disable the policy.

F. Increase the retention period of the policy.

ANSWER: A F

Explanation:

Add locations to the policy. and **Increase the retention period of the policy.** are permitted changes after a preservation lock is applied to a Microsoft Purview retention policy. A preservation lock is intended for regulatory scenarios in which an organization must make retention requirements immutable, preventing changes that would reduce the scope or duration of preservation. However, Microsoft allows changes that strengthen the policy's retention posture. Adding locations extends policy coverage to additional workloads or containers, such as more Exchange mailboxes, SharePoint sites, OneDrive accounts, or Microsoft 365 groups. Increasing the retention period similarly extends the duration for which covered content is retained. These changes maintain or increase the policy's compliance protection rather than weakening it. This behavior enables an organization to expand its compliance obligations over time while preserving the locked policy's original minimum

retention commitment. Microsoft documents that locked retention policies can be made more restrictive by adding locations or increasing the retention period. For details, see Lock a retention policy and Retention settings.

QUESTION NO: 9 - (SIMULATION)

You have a Microsoft 365 tenant that uses Microsoft Teams.

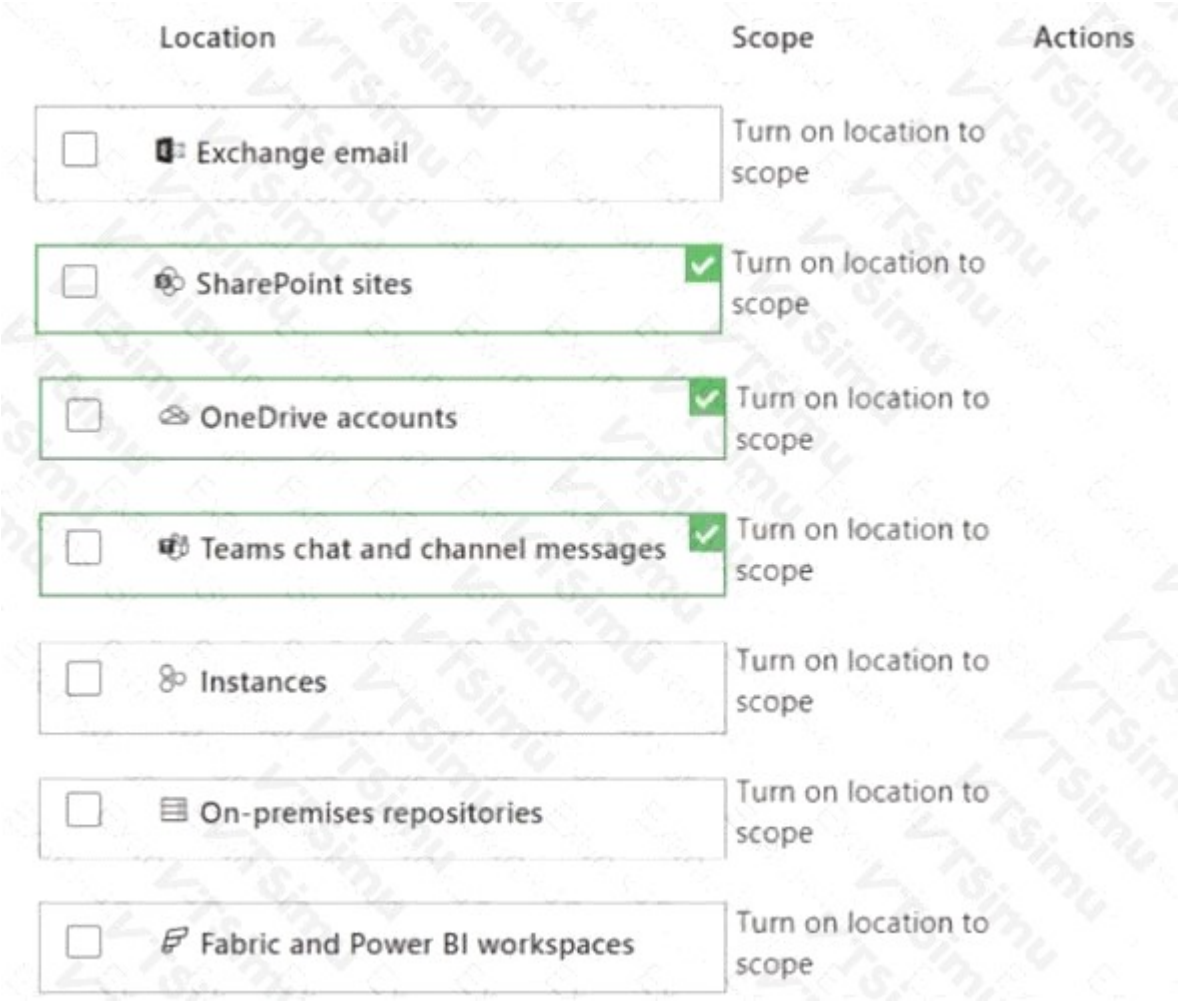
You create a data loss prevention (DLP) policy to prevent Microsoft Teams users from sharing sensitive information. You need to identify which locations must be selected to meet the following requirements:

• Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams.

• If a user attempts to share sensitive information during a Microsoft Teams chat session, the message must be deleted immediately.

Which three locations should you select? To answer, select the appropriate locations in the answer area

NOTE: Each correct selection is worth one point.



ANSWER: See the explanation for the answer

Explanation:

Select these three locations:

SharePoint sites
OneDrive accounts
Teams chat and channel messages

Reasoning: Files shared in Teams channels are stored in the team's SharePoint site, while files shared in Teams chats are stored in the sender's OneDrive. Therefore, both **SharePoint sites** and **OneDrive accounts** must be included to protect documents shared through Teams. Selecting **Teams chat and channel messages** applies DLP to the actual chat/channel message content and can block and immediately delete messages containing sensitive information.

QUESTION NO: 10

You have a Microsoft 365 E5 subscription that contains Microsoft SharePoint Online sites and Exchange Online mailboxes.

You need to automatically apply a sensitivity label to existing documents and email messages that contain a specific sensitive information type.

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

NOTE: Each correct selection is worth one point.

A. Create a sensitivity label.

B. Create an auto-labeling policy.

C. Create a retention label policy.

D. Create an audit retention policy.

E. Create an eDiscovery hold.

ANSWER: A B

Explanation:

You must **create a sensitivity label**. The sensitivity label defines the classification and protection settings that will be applied to matching documents and email messages. For example, the label can apply content markings or encryption according to the organization's requirements.

You must also **create an auto-labeling policy**. An auto-labeling policy evaluates content in supported Exchange Online, SharePoint Online, and OneDrive locations. The policy can use the specified sensitive information type as a condition and apply the selected sensitivity label when content matches the configured criteria.

A sensitivity label policy publishes labels for manual selection by users, but it does not automatically apply a label based on content inspection. For more information, see Apply a sensitivity label automatically to content.

QUESTION NO: 11

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

You need to delegate the following tasks to separate users:

* Create and manage communication compliance policies.

* Review policy matches and remediate detected communications.

Which two role groups should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Communication Compliance

B. Communication Compliance Analysts

C. Content Explorer Content Viewer

D. Insider Risk Management Investigators

E. Records Management

ANSWER: A B

Explanation:

The **Communication Compliance** role group provides permissions to configure and manage Communication Compliance policies. Members can create policies, define users in scope, configure detection conditions, and manage policy settings.

The **Communication Compliance Analysts** role group provides the permissions needed to review policy matches and take remediation actions in Communication Compliance. This role group supports the review workflow without granting the user unnecessary permissions to configure policies.

Separating policy administration from review duties supports least privilege and helps maintain an appropriate separation of duties. For more information, see Microsoft Purview Communication Compliance.

QUESTION NO: 12

You have a Microsoft 365 E5 subscriptions.

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

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

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

NOTE: Each correct selection is worth one point.

A. Insider Risk Management

B. Information Protection

C. Compliance Manager

D. DSPMforAI

E. Information Barriers

F. Data Lifecycle Management

G. Data Loss Prevention

ANSWER: A G

Explanation:

Microsoft Purview DSPM for AI uses integrated Purview controls to help an organization discover and reduce data risks associated with AI applications and Microsoft 365 Copilot. Its deployment includes policy capabilities that are managed in the relevant underlying Purview solutions rather than solely from the DSPM for AI experience.

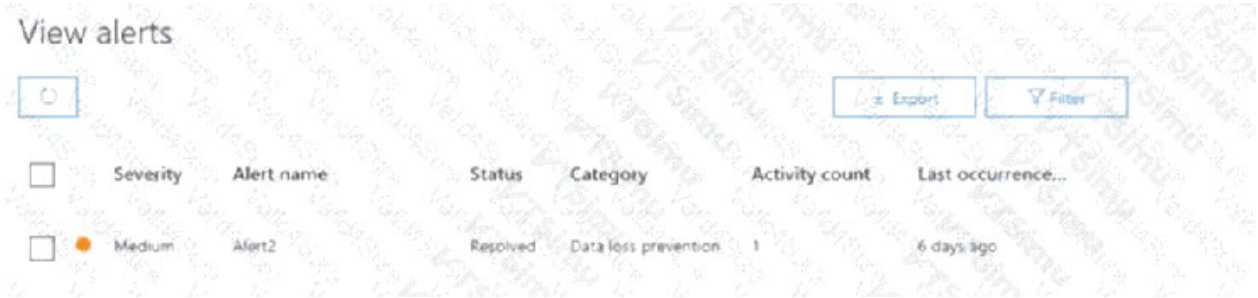
Insider Risk Management is used to manage the policy that identifies risky user activity involving AI. This includes signals and activities that can indicate potentially risky handling of sensitive data when users interact with generative AI. Administrators can edit the policy configuration, such as its indicators, users and groups in scope, and alert settings, from the Insider Risk Management area of the Microsoft Purview portal.

Data Loss Prevention is used to manage the policy controls that detect sensitive information and apply protective actions in supported locations and AI-related scenarios. From Data Loss Prevention, administrators can adjust policy rules, conditions, sensitive information types, included users, locations, and enforcement actions to match organizational requirements.

These two solutions provide the operational policy-management surfaces for the default AI risk controls deployed with DSPM for AI. For implementation details, see Microsoft Purview Insider Risk Management and Learn about Microsoft Purview Data Loss Prevention.

QUESTION NO: 13

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



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

A. The status cannot be changed.

B. Dismissed only

C. Investigating only

D. Active or Investigating only

E. Investigating. Active, or Dismissed

ANSWER: E

Explanation:

Alert2 is currently in the Resolved state, but resolution does not permanently close the alert's lifecycle. Microsoft 365 alert management supports updating an alert's status as triage information changes. A previously resolved alert can be reopened as Active when it requires renewed attention, moved to Investigating when an administrator is actively reviewing related activity, or classified as Dismissed when the alert is determined not to require further action. Therefore, the available status changes from Resolved are Investigating, Active, or Dismissed.

This flexibility is important for operational investigations because conclusions can change when new evidence, correlated alerts, or remediation results become available. Updating the status provides a clear record of the alert's current handling stage for security and compliance administrators. Microsoft's alert-policy documentation describes managing alerts and their investigation workflow in the Microsoft Purview portal. See Alert policies in Microsoft Purview and Investigate alerts in Microsoft Defender XDR.

QUESTION NO: 14

You have a Microsoft 365 E5 subscription.

You need to enable support for sensitivity labels in Microsoft SharePoint Online. What should you use?

A. the Microsoft Purview portal

B. the Microsoft Entra admin center

C. the SharePoint admin center

D. the Microsoft 365 admin center

E. the Microsoft SharePoint Online Management Shell

ANSWER: E

Explanation:

The Microsoft SharePoint Online Management Shell is required to enable sensitivity-label support for SharePoint Online containers. Specifically, an administrator connects to SharePoint Online PowerShell and runs `Set-SPOTenant -EnableAIPIntegration $true`. This tenant-level setting enables SharePoint Online to recognize and apply sensitivity labels to SharePoint sites and Microsoft 365 groups. The setting is commonly described as enabling Azure Information Protection integration, reflecting the original name of the information-protection capability.

After the integration is enabled, sensitivity labels that are configured in Microsoft Purview and scoped to groups and sites can be published for users to apply when they create or manage supported containers. The labels can then enforce configured privacy, external-sharing, and unmanaged-device access controls for labeled SharePoint sites. The account running the command needs the appropriate SharePoint administrative permissions, and the SharePoint Online Management Shell module must be installed and connected to the tenant before executing it.

Microsoft documents the required `EnableAIPIntegration` SharePoint Online PowerShell setting in its guidance for using sensitivity labels with Microsoft Teams, Microsoft 365 Groups, and SharePoint sites. The command syntax and parameters are also documented in the Set-SPOTenant reference.

QUESTION NO: 15

You are configuring a data loss prevention (DLP) policy to report when credit card data is found on a Microsoft Entra joined Windows device.

You plan to use information from the policy to restrict the ability to copy the sensitive data to the clipboard.

What should you configure in the policy advanced DLP rule?

A. an action

B. the incident report

C. user notifications

D. user overrides

ANSWER: A

Explanation:

an action is correct because an advanced DLP rule uses conditions to identify content that meets the rule criteria, such as content containing a credit card sensitive information type, and uses an action to determine the enforcement behavior on an onboarded Windows device. For Endpoint DLP, the relevant action is *Audit or restrict activities on devices*. Within that action, the administrator can select device activities to monitor or block, including copying protected content to the clipboard. The action can be configured to audit the activity first, producing evidence in DLP reporting and activity exploration, and it can then be changed to block the clipboard activity when enforcement is required. This supports a staged deployment: validate detections and their impact before preventing users from placing matching sensitive data on the clipboard. Endpoint DLP applies these controls to supported Windows devices that are onboarded and meet the applicable management and licensing prerequisites. Microsoft documents device activity controls, including clipboard restrictions, in its Endpoint DLP guidance and describes how advanced rules pair conditions with enforcement actions. See Learn about Endpoint DLP and Create and deploy DLP policies.

QUESTION NO: 16

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

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

Which two conditions can you use in Rule1? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Document property is

B. Attachment's file extension is

C. Document size equals or is greater than

D. Content is shared from Microsoft 365

E. Content contains

ANSWER: D E

Explanation:

Content contains is a supported advanced DLP rule condition. It enables Rule1 to inspect the content of items for data that an organization wants to protect, including sensitive information types, keywords or keyword dictionaries, sensitivity labels, and trainable classifiers where applicable. This condition provides the core content-inspection capability used to identify regulated, confidential, or otherwise sensitive information in the workloads covered by the policy.

Content is shared from Microsoft 365 is also a supported advanced DLP rule condition for the relevant Microsoft 365 content locations. It allows the rule to evaluate the sharing state of protected content, such as whether an item has been shared externally or shared with people outside the organization. Combining sharing context with content inspection lets an

organization apply DLP actions only when sensitive content is exposed through a particular sharing scenario, reducing unnecessary matches while protecting data at the point of sharing.

Microsoft documents the available DLP rule conditions and their supported workloads in the Microsoft Purview DLP policy reference. For more detail on creating and configuring DLP policies across Microsoft 365 locations, see Learn about data loss prevention.

QUESTION NO: 17

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

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

You need to identify and categorize the resumes. The solution must minimize administrative effort. What should you include in the solution?

A. a trainable classifier

B. a keyword dictionary

C. a function

D. an exact data match (EDM) classifier

ANSWER: A

Explanation:

A trainable classifier is appropriate because Microsoft Purview uses trainable classifiers to identify document categories based on the content and context of a document, rather than requiring one fixed phrase or structured identifier. The built-in Resume classifier is designed to recognize English-language resumes and considers characteristic resume content, including education, work experience, and accomplishments. This directly matches the required classification criteria.

Because this is a prebuilt classifier, it minimizes administrative effort: the organization can use the existing Resume classifier rather than collecting representative files, labeling them for training, and maintaining custom detection logic. After the classifier is available in the tenant, it can be selected as a condition in an auto-labeling policy for sensitivity labels. The policy can be scoped to SharePoint Online locations, allowing documents in the Site1 library that are identified as resumes to receive the selected sensitivity label automatically.

Microsoft documents the available built-in trainable classifiers, including the Resume classifier, and explains how classifiers can be used in Microsoft Purview solutions. For implementation guidance, see Learn about trainable classifiers and Apply a sensitivity label automatically.

QUESTION NO: 18

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

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

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

NOTE: Each correct selection is worth one point.

A. Document property is

B. Attachment's file extension is

C. Document size equals or is greater than

D. Content is shared from Microsoft 365

E. Content contains

ANSWER: D E

Explanation:

Content is shared from Microsoft 365 and **Content contains** are valid conditions for an advanced Microsoft Purview Data Loss Prevention rule. The content-sharing condition enables a rule to evaluate the sharing state of content in supported Microsoft 365 storage locations. This allows a DLP policy to apply protections based on how content is shared, such as when the content is shared externally. It is useful when the risk depends not only on the presence of sensitive data, but also on whether that data is available beyond the organization.

The **Content contains** condition is the core DLP detection condition. It can evaluate content for configured sensitive information types, trainable classifiers, exact data match classifications, keywords, and other supported content-based classifiers. For example, an organization can use it to detect financial account numbers, government-issued identifiers, or custom sensitive information types before applying the rule's actions and user notifications.

These conditions can be combined in an advanced rule so that protection is targeted at content matching the organization's data-protection criteria and sharing-risk requirements. Microsoft documents DLP policy conditions and supported actions in DLP conditions and actions and provides an overview of policy-based protections in Learn about data loss prevention.

QUESTION NO: 19 - (HOTSPOT)

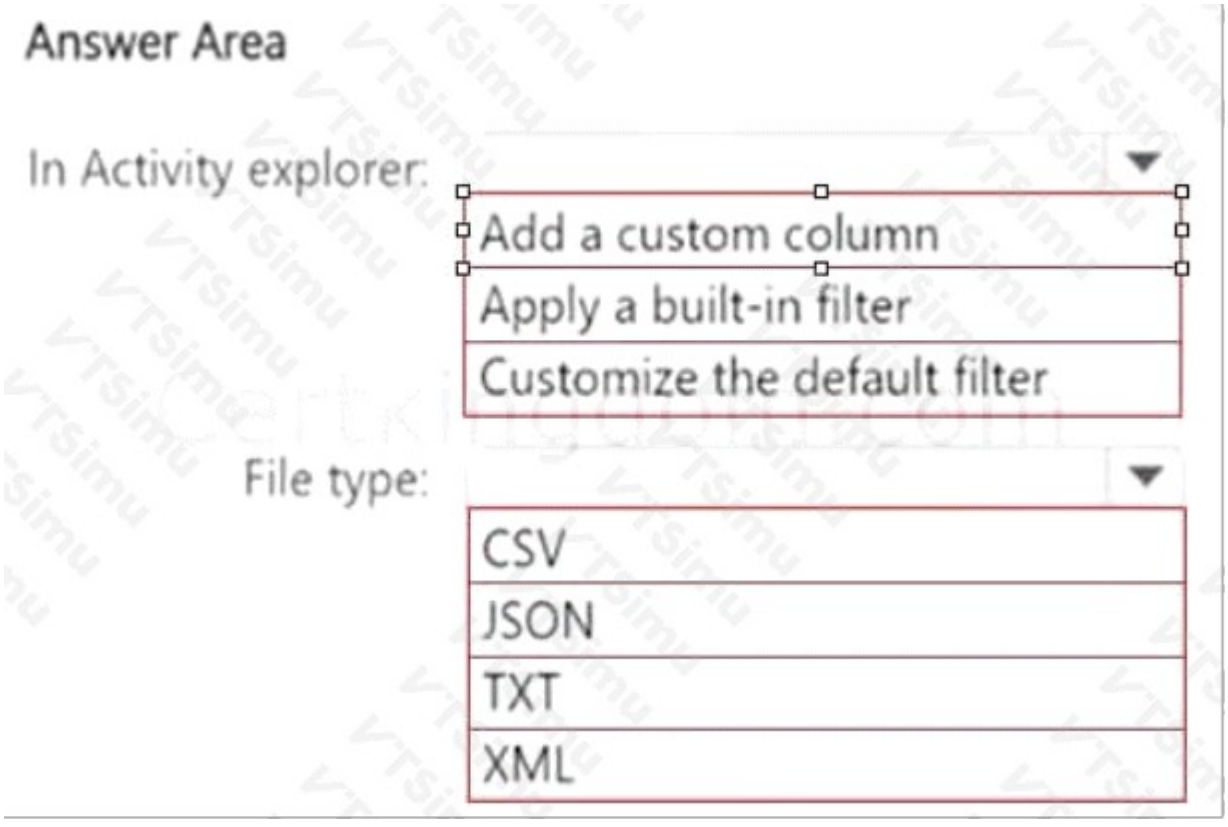
HOTSPOT

You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

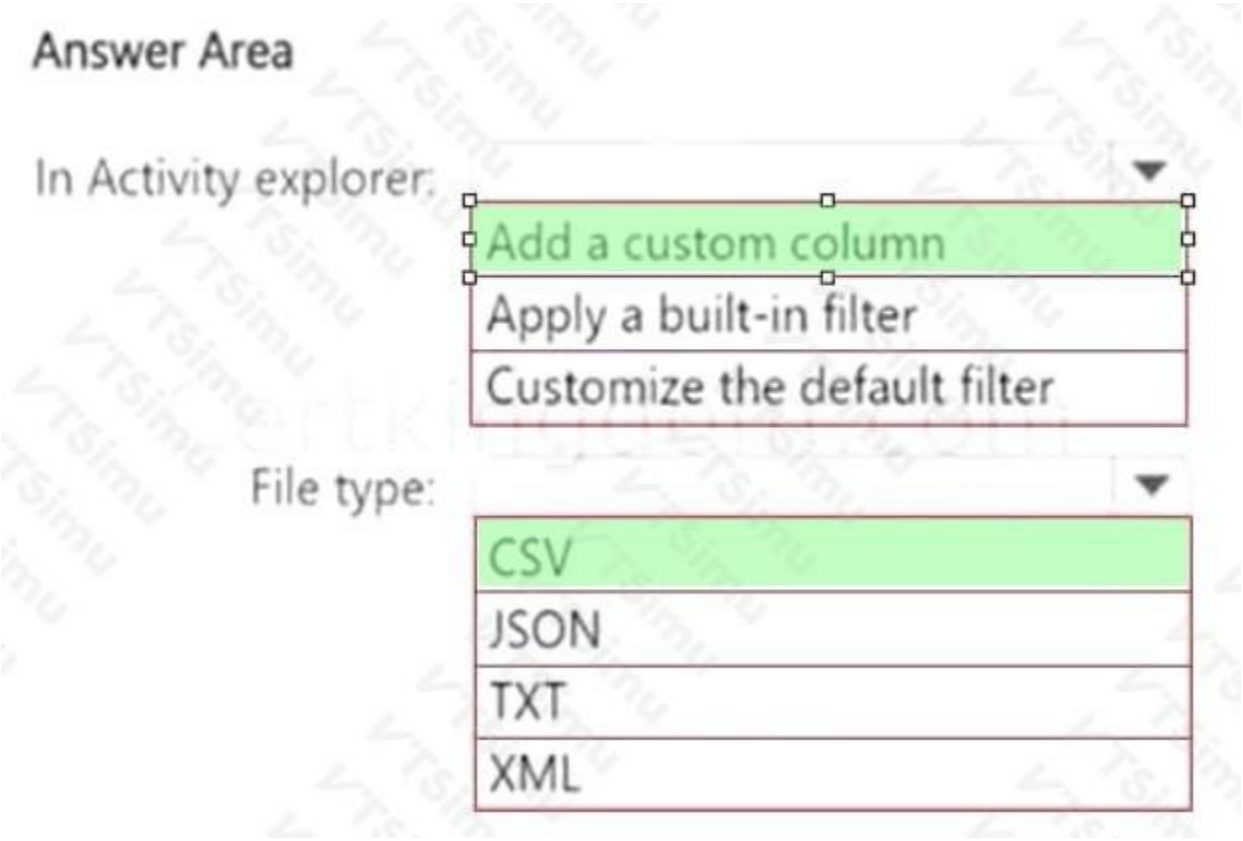
You plan to export DLP activity by using Activity explorer.

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

What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:

In Activity explorer, select **Add a custom column** before exporting. Activity explorer lets an administrator tailor the results grid to show the investigation details needed for the current review. To satisfy the requirement, add the column that contains the detected sensitive information type. This makes the sensitive info type visible alongside the DLP activity and rule-match data, so the exported result includes the sensitive-information classification associated with each matching event. This is useful when reviewing DLP detections because a single policy can contain several rules or can detect several kinds of sensitive information; including the sensitive info type provides the required context for each match.

The export file format is **CSV**. After the Activity explorer results are configured with the desired columns, export the filtered and displayed investigation data as a comma-separated values file. CSV is supported broadly by Excel, Power BI, and scripts, making it suitable for further analysis, retention, or sharing with authorized compliance personnel. Microsoft documents Activity explorer as the place to review data related to DLP activities and to customize the information used in an investigation. See Activity explorer in Microsoft Purview for Activity explorer capabilities and Learn about data loss prevention for how DLP detects and acts on sensitive information. Thus, adding the appropriate custom column first and exporting the results as CSV produces an export that displays the detected sensitive info type for each DLP rule match.

QUESTION NO: 20

You have a Microsoft 365 E5 subscription that contains a device named Device1.

You need to enable Endpoint data loss prevention (Endpoint DLP) for Device1. What should you do first in the Microsoft Purview portal?

A. Turn on device onboarding.

B. Enable Microsoft Priva Privacy Risk Management.

C. Create a Microsoft Purview Information Barriers (IBs) segment.

D. Add a Microsoft Purview Information Protection scanner cluster.

E. Onboard Device1 to Microsoft Purview.

ANSWER: A

Explanation:

Turn on device onboarding. is the required first action because Endpoint DLP can enforce protections only on devices that are connected to the Microsoft Purview service through the endpoint onboarding process. In the Microsoft Purview portal, an administrator first enables device onboarding for the tenant. This prepares the tenant for endpoint integration and makes the relevant onboarding workflow and deployment packages available. The onboarding package is then deployed to Device1 by using a supported management method, such as Microsoft Intune, Microsoft Configuration Manager, Group Policy, or a local script, depending on the operating system and deployment model.

After the device is successfully onboarded and reports its status, Endpoint DLP policies can identify sensitive information and monitor or restrict supported actions involving that information on the device, such as copying to removable media, printing, or uploading through supported browsers. A Microsoft 365 E5 subscription provides the licensing needed for these Endpoint DLP capabilities, but enabling device onboarding is still necessary before a specific endpoint can participate in policy enforcement. For the official onboarding sequence and supported deployment methods, see Get started with Endpoint DLP and Device onboarding for Microsoft Purview.

QUESTION NO: 21

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

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

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

NOTE: Each correct selection is worth one point.

A. Document property is

B. Attachment ' s file extension is

C. Document size equals or is greater than

D. Content is shared from Microsoft 365

E. Content contains

ANSWER: D E

Explanation:

Content is shared from Microsoft 365 and **Content contains** are supported conditions for an advanced Microsoft Purview Data Loss Prevention rule. The **Content contains** condition is the core content-inspection condition used to detect protected data in scope. It can evaluate content against sensitive information types, trainable classifiers, sensitivity labels, and other supported content-based criteria. This enables Rule1 to identify information that requires protection before the rule applies its configured user notifications, access restrictions, incident reports, or other DLP actions.

Content is shared from Microsoft 365 evaluates sharing activity for content stored in Microsoft 365 workloads that support the condition, such as SharePoint and OneDrive. It enables a DLP rule to apply controls according to the sharing context of a file, including whether content is shared externally. This is useful when an organization needs different protection behavior for information that remains internal versus information made available through sharing.

Microsoft Purview evaluates DLP rules only in the workloads selected for the policy and supported by the relevant condition. Together, these conditions allow Rule1 to identify sensitive content and apply protection based on its Microsoft 365 sharing state. See Learn about Microsoft Purview DLP and DLP policy reference.

QUESTION NO: 22

You have a Microsoft 365 E5 subscription that contains 500 Windows devices.

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

You need to ensure that you can monitor user activities on third-party generative AI websites.

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

NOTE: Each correct selection is worth one point.

A. Install the Microsoft Purview extension on the devices.

B. Create a data leaks policy.

C. Onboard the devices to Microsoft Purview.

D. Create a communication compliance policy.

E. Create an Endpoint data loss prevention (Endpoint DLP) policy.

F. Enroll the devices in Microsoft Intune.

ANSWER: A C

Explanation:

To monitor user interactions with supported third-party generative AI websites, Microsoft Purview DSPM for AI requires endpoint-level visibility. **Onboard the devices to Microsoft Purview.** This prepares Windows endpoints for Purview endpoint capabilities and enables the service to receive the relevant device and activity signals. Endpoint onboarding is the foundational requirement for applying Purview controls and monitoring to activity that occurs outside Microsoft 365 services.

Install the Microsoft Purview extension on the devices. The Purview browser extension captures supported browser interactions with generative AI sites, allowing DSPM for AI to identify activities such as prompts that might contain sensitive information. The extension is deployed to managed devices and works with the supported browsers and endpoint configuration. Together, Purview onboarding and browser-extension deployment provide the telemetry required for DSPM for AI to discover and monitor AI usage on endpoints. After those prerequisites are in place, an organization can configure the applicable policies and controls based on its data-protection requirements.

For implementation details, see Microsoft Purview DSPM for AI documentation and Get started with Endpoint DLP.

QUESTION NO: 23

You have a Microsoft 365 E5 subscription.

You have an on-premises database that contains employee identification numbers.

You need to use the database values to identify employee identification numbers in Microsoft 365 content. The solution must minimize false positives.

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

NOTE: Each correct selection is worth one point.

A. An exact data match (EDM) schema

B. An exact data match (EDM) data source

C. A document fingerprint

D. A trainable classifier

E. A retention event

ANSWER: A B

Explanation:

An exact data match (EDM) schema is required to define the fields that Microsoft Purview uses to identify records from the source database. The schema specifies the primary element and any supporting elements used for matching.

An exact data match (EDM) data source is also required. The data source contains hashed values derived from the organization's database records. Microsoft Purview compares detected content against the hashed source values without storing the original sensitive values in the service. This provides more precise detection than pattern-based matching alone and helps minimize false positives.

For more information, see Learn about Exact Data Match sensitive information types and Get started with Exact Data Match.

QUESTION NO: 24

You have a Microsoft 365 E5 subscription that contains Microsoft SharePoint Online sites.

You need to automatically apply retention settings to SharePoint documents that contain a specific sensitive information type.

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

NOTE: Each correct selection is worth one point.

A. Create a retention label.

B. Create an auto-apply retention label policy.

C. Create a sensitivity label policy.

D. Create a Content Search.

E. Configure a SharePoint site retention policy.

ANSWER: A B

Explanation:

Create a retention label is required because the retention label defines the retention period and action for the documents. For example, the label can retain content for a specified number of years and then trigger disposition review or delete the content.

Create an auto-apply retention label policy is also required. An auto-apply policy evaluates content in supported locations, including SharePoint Online, and can apply a retention label when a document contains the selected sensitive information type. The policy automates retention labeling without requiring users to manually select a label.

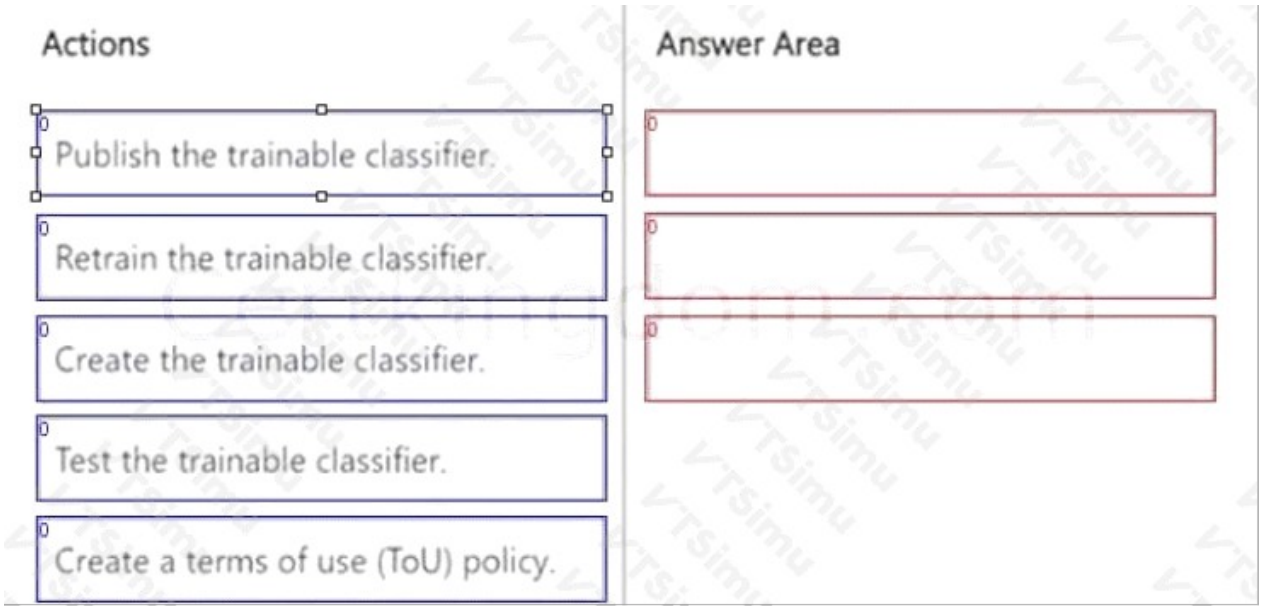
For more information, see Apply retention labels automatically and Create retention labels.

QUESTION NO: 25 - (DRAG DROP)

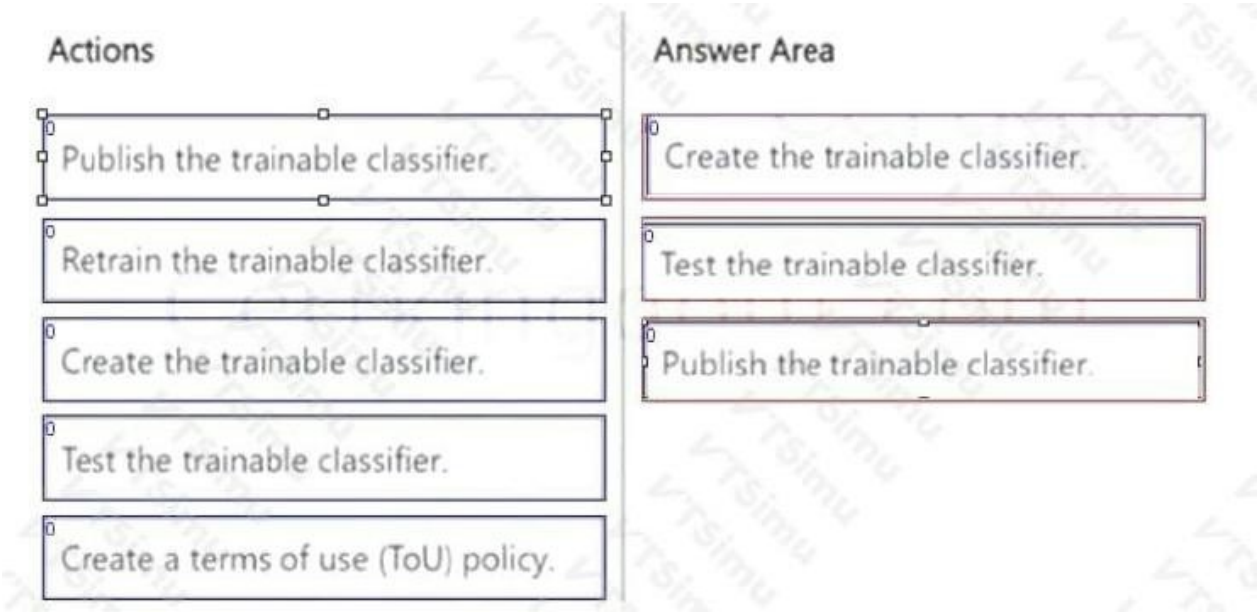
DRAG DROP

You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.

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



ANSWER:



Explanation:

A custom trainable classifier must follow the standard Microsoft Purview workflow before it can be used to identify content for an auto-apply retention label policy. First, create the trainable classifier. This establishes the classifier and its intended content category, allowing the initial positive and negative training examples to be supplied. Those examples teach the classifier what content belongs to the category and what similar content should not be identified.

Next, test the trainable classifier. Testing evaluates the classifier against content and displays its predicted matches, so the administrator can assess whether the classifier is recognizing the intended type of document or message accurately. This validation step confirms that the classifier has learned enough from its training data to be suitable for policy use. Where necessary, testing can be repeated during refinement, but the essential workflow proceeds once the classifier's results are acceptable.

Finally, publish the trainable classifier. Publishing makes the completed classifier available for use throughout applicable Microsoft Purview experiences, including as a condition for automatically applying retention labels. An auto-apply retention label policy can then use the published classifier to locate matching items and apply the selected retention label according to the organization's retention requirements. Microsoft documents the create, test, and publish lifecycle for custom classifiers in its Trainable classifiers documentation. For the policy configuration that uses classified content to apply retention labels, see Automatically apply a retention label to content.

QUESTION NO: 26

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

aei_AA989.docx

bd_WS098.docx cei_DF112.docx ebc_QQ454.docx ecc_BB565.docx

All documents that use this naming format must be labeled as Project Documents: You need to create an auto-apply retention label policy. What should you use to identify the files?

A. A retention label

B. A trainable classifier

C. A sensitive info type

ANSWER: C

Explanation:

A sensitive info type is the appropriate identifier because it can be customized to recognize a consistent, structured pattern by using a regular expression. The filenames shown share a predictable convention: a lowercase prefix, an underscore, two uppercase characters, and a numeric suffix. A custom sensitive information type can define a pattern that represents this naming convention and can then be selected as the condition for an auto-apply retention label policy.

Microsoft Purview supports automatically applying retention labels to SharePoint Online and OneDrive content when matching conditions are detected. Sensitive information types are one of the supported conditions for this auto-labeling scenario. Creating a custom type is appropriate when the organization needs to identify an internal identifier or other organization-specific pattern rather than one of the built-in sensitive-information definitions. Configure the custom pattern with sufficient precision for the project-document convention, publish the retention label, and use the sensitive information type as the policy's detection condition. This enables Project Documents to be labeled automatically as matching files are indexed and evaluated.

See Apply retention labels automatically and Create custom sensitive information types.

QUESTION NO: 27 - (DRAG DROP)

DRAG DROP

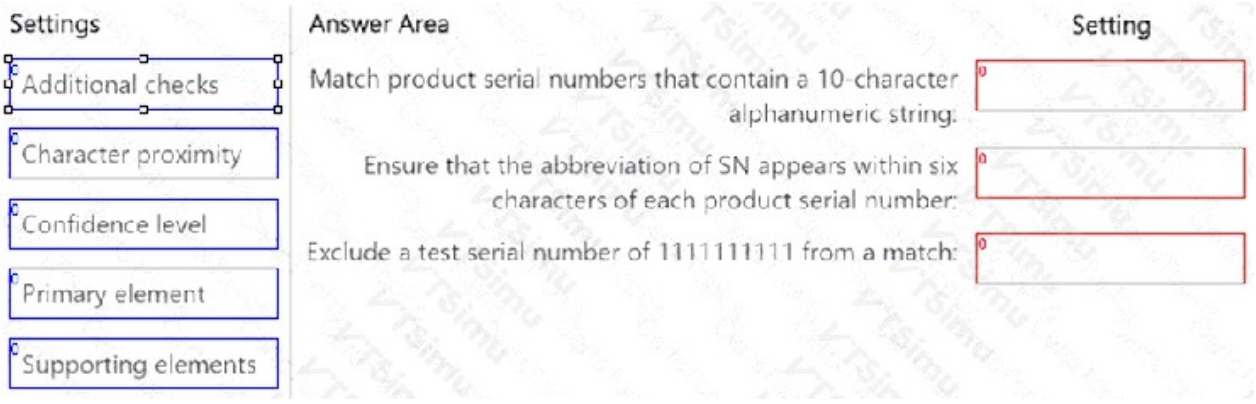
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You need to create a custom sensitive info type. The solution must meet the following requirements:

- Match product serial numbers that contain a 10-character alphanumeric string.
- Ensure that the abbreviation of SN appears within six characters of each product serial number.
- Exclude a test serial number of 1111111111 from a match.

Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

A custom sensitive information type is built around a pattern that identifies the actual sensitive value first. In this case, the product serial number is the value that DLP must recognize, and its required format is exactly 10 alphanumeric characters. That format is configured as the **Primary element**, typically by using a regular expression that represents the allowed serial-number structure.

The presence of **SN** is contextual evidence that helps confirm the nearby 10-character value is a product serial number. The requirement is specifically about the maximum distance between that abbreviation and the detected serial number, so **Character proximity** is the correct setting. It limits the supporting contextual match to within six characters of the primary element, ensuring that the contextual indicator is sufficiently close to the serial-number value.

The value **1111111111** is a known test serial number and must not trigger a match. This is configured by using **Additional checks** to apply an exclusion condition for that exact value. The primary pattern can still detect valid serial numbers in the same required format, while the exclusion prevents the designated test value from being treated as sensitive content.

This follows the custom sensitive information type pattern model in Microsoft Purview, where primary elements define the sensitive data format, proximity adds contextual constraints, and additional checks refine matching behavior. For more information, see Create custom sensitive information types in Microsoft Purview and Learn about sensitive information types.

QUESTION NO: 28 - (SIMULATION)

You have a Microsoft 36S ES subscription.

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

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

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

ANSWER: See the explanation for the answer

Explanation:

Use the following Microsoft Purview Insider Risk Management policy templates:

Policy1 (monitor printing of files by users who submitted a resignation) → **Data theft by departing users**
Policy2 (monitor accidental external sharing by users in a priority user group) → **Data leaks by priority users**
Policy3 (monitor files downloaded from SharePoint Online to personal cloud storage services) → **Data leaks**

The departing-users template is specifically intended to detect potentially risky exfiltration actions, including printing, by users identified as leaving. The priority-users template targets data leakage activity by members of a configured priority user group. The general **Data leaks** template covers data exfiltration activities such as transfer to personal cloud storage.

QUESTION NO: 29

You have a Microsoft 365 E5 subscription.

You plan to create an adaptive scope for a retention policy. The scope must include only users in the Finance department who are located in Canada.

Which two user attributes can you use in the adaptive scope query? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Department

B. Country or region

C. Sensitivity label

D. Device operating system

E. Mailbox size

ANSWER: A B

Explanation:

Department and **Country or region** are supported Microsoft Entra ID user attributes that can be used in an adaptive scope query. You can create a user-based adaptive scope that evaluates these attributes and dynamically includes users whose department is Finance and whose country or region is Canada.

Adaptive scopes reduce administrative effort because scope membership is evaluated from user, site, or Microsoft 365 group attributes. When an employee's department or country value changes in Microsoft Entra ID, the applicable retention policy scope can be updated automatically without manually changing the policy's included users.

For more information, see Learn about adaptive scopes.

QUESTION NO: 30 - (HOTSPOT)

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

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

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

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

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

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

NOTE; Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	○
Action2 will be retained for three years.	○	○
Action3 will be retained for six months.	○	○

ANSWER:

Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	●
Action2 will be retained for three years.	●	○
Action3 will be retained for six months.	●	○

Explanation:

Microsoft Purview Audit retention policies can be scoped to users, record types, and individual activities. All of the listed policies apply to User1's SharePoint audit records, but a policy that specifies an activity applies only when that exact activity is recorded. The policy whose Activities value is *None* acts as the applicable policy for SharePoint audit activities that are not otherwise listed as a particular activity in the policy table. Its configured retention duration is three years.

When User1 archives a site, that operation is not the listed *Created site collection* activity and is not the listed *Renamed site* activity. The applicable SharePoint policy is therefore the policy with no activity restriction, and its three-year duration applies. The first statement must consequently be marked No.

Creating a site collection is covered by the policies that include that activity, and the applicable retention outcome is three years. The second statement must be marked Yes.

Renaming a site is specifically covered by the policy for the *Renamed site* activity. That policy has priority 10. In Purview Audit retention policies, a lower priority number indicates a higher priority, so this policy takes precedence over the all-activities policy with priority 20. Its configured six-month retention period is applied to the rename audit record. The third statement must be marked Yes.

This behavior allows administrators to use broad baseline retention policies while applying more specific retention durations to selected, high-value audit activities. See Manage audit log retention policies and Microsoft Purview Audit (Premium) for policy scope, priority, and retention details.

QUESTION NO: 31

You have a sensitive information type based on a trainable classifier.

You are unsatisfied with the result of the trainable classifier.

You need to retrain the classifier.

What should you use in the Microsoft Purview portal?

A. Content explorer from Data classification

B. Labels from Information protection

C. Labels from Information governance

D. Content search

ANSWER: A

Explanation:

Content explorer from Data classification is the appropriate place to provide the feedback needed to improve a trainable classifier. Trainable classifiers use machine learning to identify content that belongs to a category based on examples and ongoing feedback. After the classifier has evaluated content, Content explorer lets an administrator inspect the items that were matched by the classifier and assess whether those matches are relevant to the intended category. This review process supplies the classifier with useful positive and negative feedback, which can then be used when retraining to improve future classification accuracy.

Content explorer is part of the Microsoft Purview data-classification experience and is designed to provide visibility into classified items across supported Microsoft 365 locations. Its integration with trainable classifiers makes it the relevant operational interface when classification outcomes need validation and refinement. Microsoft documents the workflow for reviewing classifier results and retraining classifiers in its trainable-classifier guidance. For further details, see Get started with trainable classifiers and Content explorer in Microsoft Purview.