DUMPSBOSS.

Administering Information Security in Microsoft 365

Microsoft SC-401

Version Demo

Total Demo Questions: 10

Total Premium Questions: 178

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1 - (HOTSPOT)

HOTSPOT

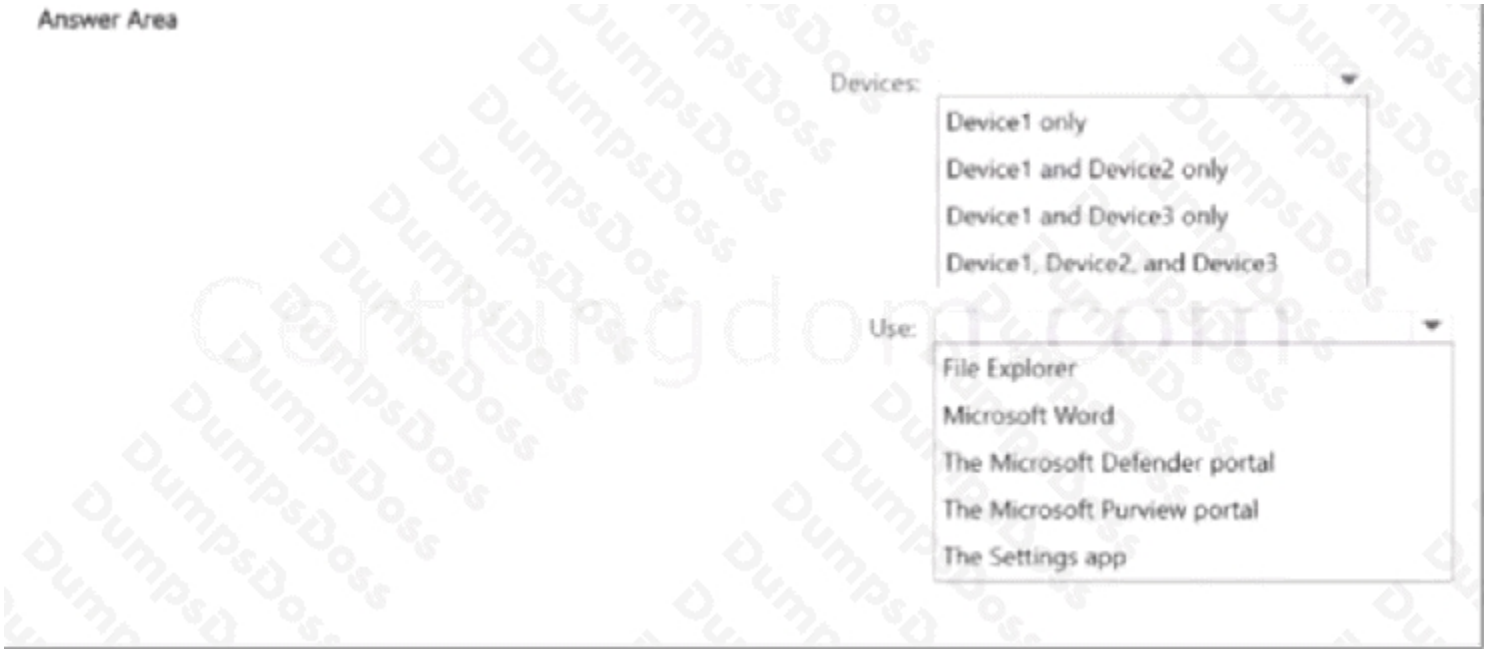
You have a Microsoft 36S ES subscription that contains the devices shown in the following table.

Name	Platform	Chipset
Device1	Windows 11	x64
Device2	Windows 11	ARM64
Device3	Windows 10	x86

You publish Microsoft Purview Information Protection sensitivity labels.

You plan to deploy the information protection client to the devices. The solution must ensure that the labels can be applied to sensitive images and documents

On which devices can you install the information protection client, and what should users use to apply labels? To answer, select the appropriate options in the answer area.



ANSWER:

Explanation:

Looking at the device table, Device1 is Windows 11 x64, Device2 is Windows 11 ARM64, and Device3 is Windows 10 x86. The key detail is the chipset/architecture. The Microsoft “information protection client” used for unified sensitivity labeling on Windows (commonly referred to as the Azure Information Protection (AIP) unified labeling client) is supported on Windows desktop editions running x86 or x64, but it isn’t supported on Windows on ARM (ARM64). That means you can install the client on Device1 (x64) and Device3 (x86), but not on Device2 (ARM64). So the correct device selection is **Device1 and Device3 only**.

The second part of the question is about how users should apply labels to **sensitive images and documents**. If you pick an Office app like Microsoft Word, you’ll only cover Office file types and won’t meet the “images” requirement broadly. The AIP client adds integration into **File Explorer**, allowing users to right-click files (including many non-Office file types such as images) and apply sensitivity labels via the Explorer context menu. That’s why the correct “Use” choice is **File Explorer**.

In other words, the combination of (1) installing the client only on supported CPU architectures (x86/x64) and (2) using File Explorer for labeling is what satisfies the requirement to label both images and documents on those endpoints. For more details, see Microsoft’s documentation on the AIP unified labeling client and its platform support and Explorer integration: AIP unified labeling client and Sensitivity labels in Microsoft Purview.

QUESTION NO: 2

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: B G

Explanation:

When you deploy DSPM for AI, it can create and rely on Purview controls that already exist in the platform. The “default policies” you’ll typically want to tweak are the ones that protect sensitive data and control how it can be shared or used.

To edit sensitivity labels, label policies, and related protection settings, you go to **Information Protection**. That’s where the labeling and encryption/marking rules live, so it’s the right place to adjust how data is classified and protected. See https://learn.microsoft.com/en-us/purview/sensitivity-labels

To edit the actual policy rules that detect and block risky sharing (including scenarios DSPM for AI flags), you use **Data Loss Prevention (DLP)**. DLP is where you change conditions, locations, and actions for preventing sensitive info from being exposed. See https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

The other options (like Compliance Manager or Information Barriers) don’t generally host the editable “default policies” that DSPM for AI sets up for protecting AI-related data flows.

QUESTION NO: 3

You have a Microsoft 365 E5 subscription that contains a user named User1. You deploy Microsoft Purview Data Security Posture Management for AD (DSPM for AD). You need to ensure that User1 can verify the auditing status of the subscription. The solution must follow the principle of least privilege. To which role group should you add User1?

A. Insider Risk Management Analysts

B. Security Reader

C. Insider Risk Management Investigators

D. View-Only Organization Management for Microsoft Exchange Online

ANSWER: B

Explanation:

To verify whether auditing is enabled and working, User1 needs read-only visibility into security-related settings and status, not the ability to change anything. The **Security Reader** role is designed for exactly that: it lets someone view security settings, security reports, and relevant status information across Microsoft 365 without granting admin rights.

The other options don’t really fit. Insider Risk roles are scoped to Insider Risk Management investigations and analysis, not tenant-wide auditing status. And the Exchange “View-Only Organization Management” role is limited to Exchange Online configuration, so it won’t reliably cover auditing status for the whole Microsoft 365 subscription.

So, to stick with least privilege and still let User1 check auditing status, add them to **Security Reader**.

References: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#security-reader, https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-security-roles

QUESTION NO: 4

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

Explanation:

In Microsoft Purview DLP, rule order matters. When content matches multiple rules in the same policy, the rule with the highest priority (the lowest priority number) is evaluated first, and its user notification (the policy tip) is what users will typically see.

So if you want users to see **Tip 2** when a document matches everything, you need **Rule2** to win the “who gets evaluated first” race. The simplest way is to move Rule2 to the top by setting its priority to **0**. That makes Rule2 the first rule processed, so Tip 2 is shown.

The “stop processing” setting isn’t needed here—within a single policy you normally solve this by rule priority. Changing other rules to priority 0 would just create conflicts, and setting Rule2 to 2 would push it lower, making it even less likely to show Tip 2.

Reference: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp#dlp-policies-and-rules

QUESTION NO: 5

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

A. Compliance Administrator

B. Security Reader

C. Security Operator

D. Compliance Data Administrator

ANSWER: D

Explanation:

To let someone *view* DLP alerts in the Microsoft Purview portal without giving them extra power, you should use a role that's scoped to DLP and is read-focused. The **Compliance Administrator** role is much broader than needed—it can manage a lot of compliance features, not just view alerts—so it doesn't really follow least privilege.

Compliance Data Administrator is the better fit here because it's designed for working with compliance data and investigations, including viewing things like DLP-related alert information, without granting full admin control over the whole compliance setup.

The "Security Reader" and "Security Operator" roles are mainly for Microsoft Defender/security experiences, and they don't specifically cover Purview DLP alert visibility the way compliance roles do.

References: https://learn.microsoft.com/en-us/purview/permissions and https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

QUESTION NO: 6

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

Setting	
Location	• Exchange email (All reci • SharePoint sites (All site
Retain items for a specific period	5 years (When items were cr
At the end of the retention period	Delete items automatically

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:

Once you put a preservation lock on a retention policy, Microsoft treats it like a “can’t loosen this later” compliance setting. The whole point is to stop anyone (even admins) from weakening the policy after the fact, so you can’t delete it, disable it, remove locations, or shorten the retention time.

What you *can* still do is make the policy stricter or broader. That means you’re allowed to add new locations (for example, include more Exchange mailboxes or SharePoint sites) because that expands coverage instead of reducing it. You’re also allowed to increase the retention period, since keeping content longer is a stricter requirement and doesn’t break the compliance promise made when the lock was applied.

Microsoft documents this behavior under retention settings and preservation lock behavior in Purview. See https://learn.microsoft.com/en-us/purview/retention-settings and https://learn.microsoft.com/en-us/purview/retention-policies for the details.

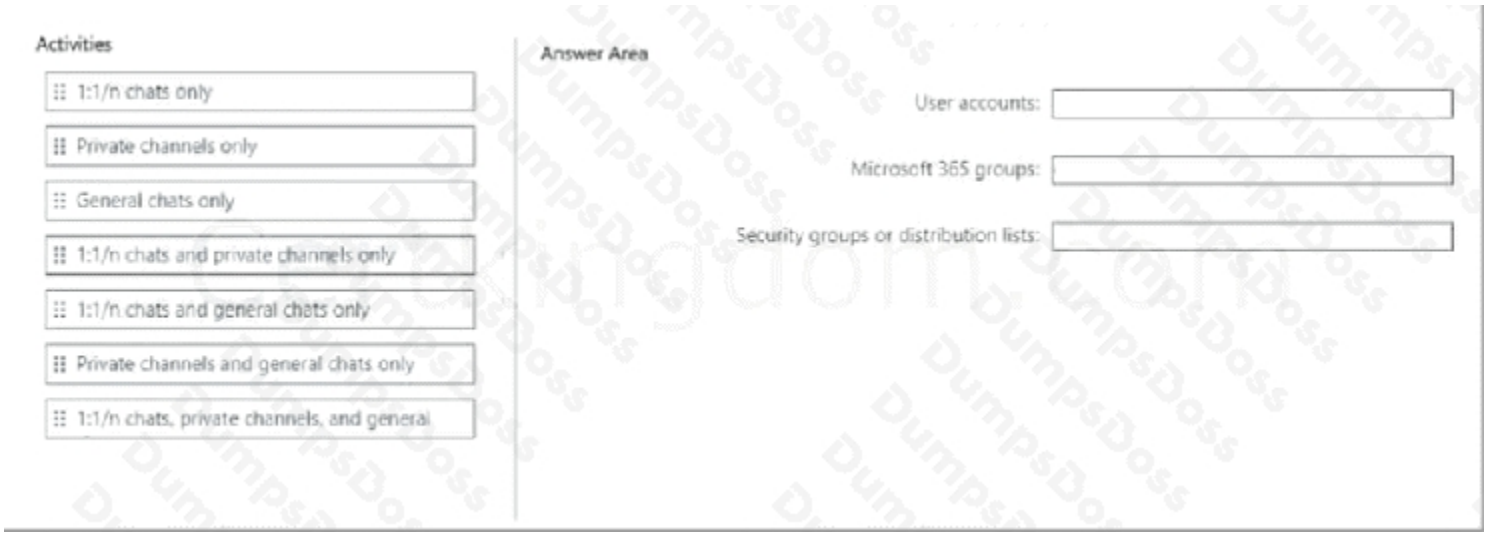
QUESTION NO: 7 - (DRAG DROP)

DRAG DROP

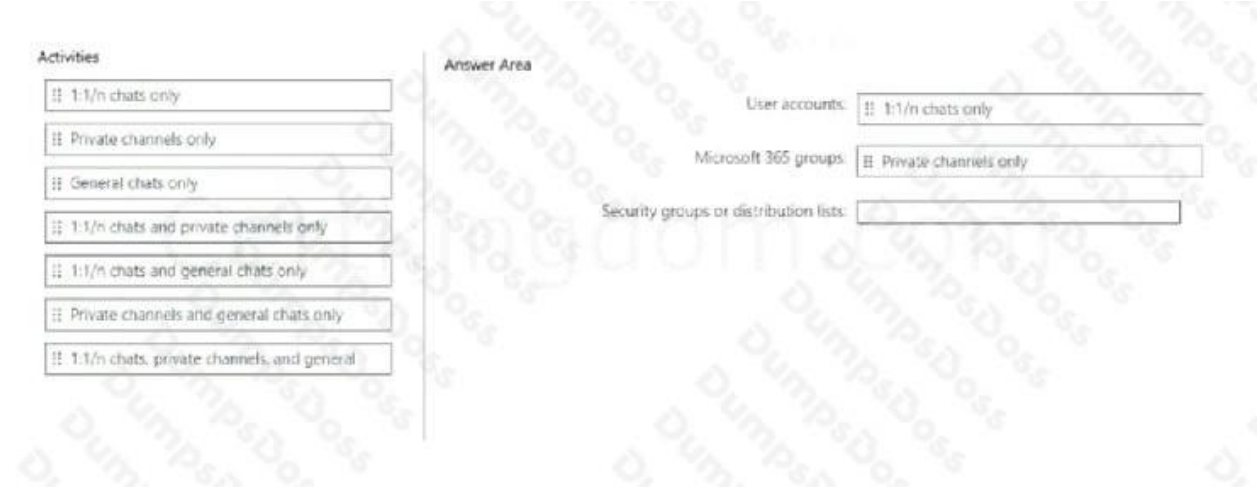
You have a Microsoft 365 Â£5 subscription.

You need to prevent the sharing of sensitive information in Microsoft Teams.

Which entities can you protect by applying a data loss prevention (DLP) policy to each resource? To answer, drag the appropriate activities to the correct entity. Each activity 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:

For Microsoft Purview DLP in Microsoft Teams, it helps to think in terms of what each "entity" actually represents in the service. **User accounts** are the natural scope for chat-based communications because 1:1 chats and group chats are tied to the participants (users), not to a Microsoft 365 group container. So if you want to prevent users from sharing sensitive info in chats, you scope the policy to **user accounts** and include chat messages (1:1 and group chats). In the drag options, that corresponds to "**1:1/n chats only**."

Microsoft 365 groups are what back a Team in Microsoft Teams. When you scope DLP to a Microsoft 365 group, you're scoping to the Team's content—most importantly, **channel messages** in that Team. In the choices provided, the closest match for that Team/channel scope is "**Private channels and general chats only**" or "**Private channels only**" depending on what the exam expects; however, "**General chats only**" is not a good fit because "general chats" are not group-scoped objects. In most exam-style mappings, Microsoft 365 groups align to **channels** (standard/private), not chats.

Finally, **security groups or distribution lists** are commonly used to assign policies in Microsoft 365, but for Teams DLP location scoping, they are not the container that represents Teams messages the way Microsoft 365 groups (Teams) do. If the question forces a mapping for this row, the best practice answer is that you scope DLP by **users** and **Microsoft 365 groups (Teams)**, not by distribution lists for Teams message locations.

References: Microsoft Purview DLP in Teams and supported locations/scoping are described in Microsoft documentation such as Data loss prevention in Microsoft Teams and general DLP location/scoping guidance at Learn about data loss prevention.

QUESTION NO: 8

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.

A user named User 1 sends link based, branded emails that are encrypted by using Microsoft Purview Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients Can User1 revoke the emails?

A. Recipient1 only

B. Recipient4 only

C. Reciptent1 and Recipient^ only

D. Reclpient3 and Recipients only

E. Reciptent1, Recipient2. Recipient3, and Recipient4

ANSWER: D

Explanation:

With Microsoft Purview Advanced Message Encryption (the link-based, branded experience), the sender can revoke access only for recipients who authenticate to open the protected message. In practice, that means recipients signing in with a Microsoft work/school account (Entra ID) or a Microsoft account, where access is tied to an identity and can be turned off later.

Recipients who use the “one-time passcode” flow (common for external users with non-Microsoft mailboxes) don’t have the same durable identity binding, so revocation isn’t supported in the same way for them. That’s why User1 can revoke only for the recipients in the table who open the message by signing in (not OTP).

So, based on the recipients shown, the ones that support sign-in access are Recipient3 and Recipient5, and those are the only ones User1 can revoke.

References: https://learn.microsoft.com/en-us/purview/ome and https://learn.microsoft.com/en-us/purview/email-encryption

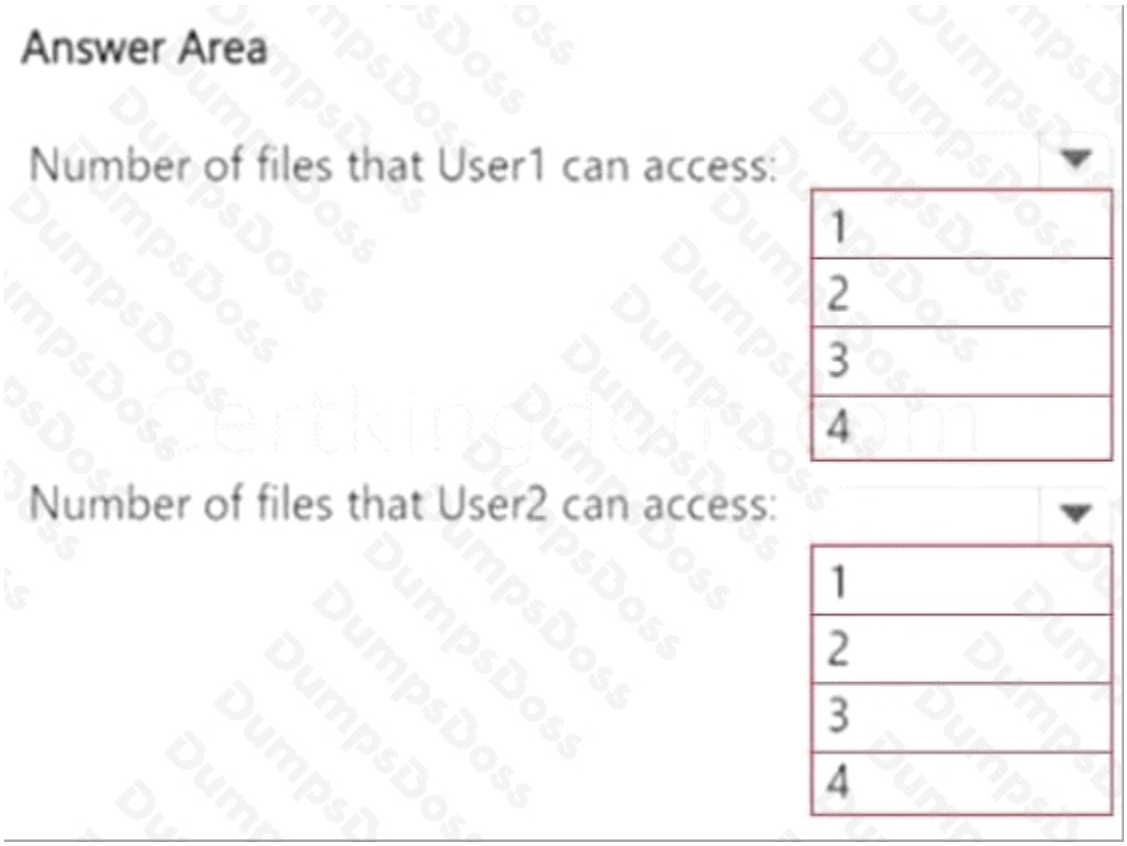
QUESTION NO: 9 - (HOTSPOT)

HOTSPOT

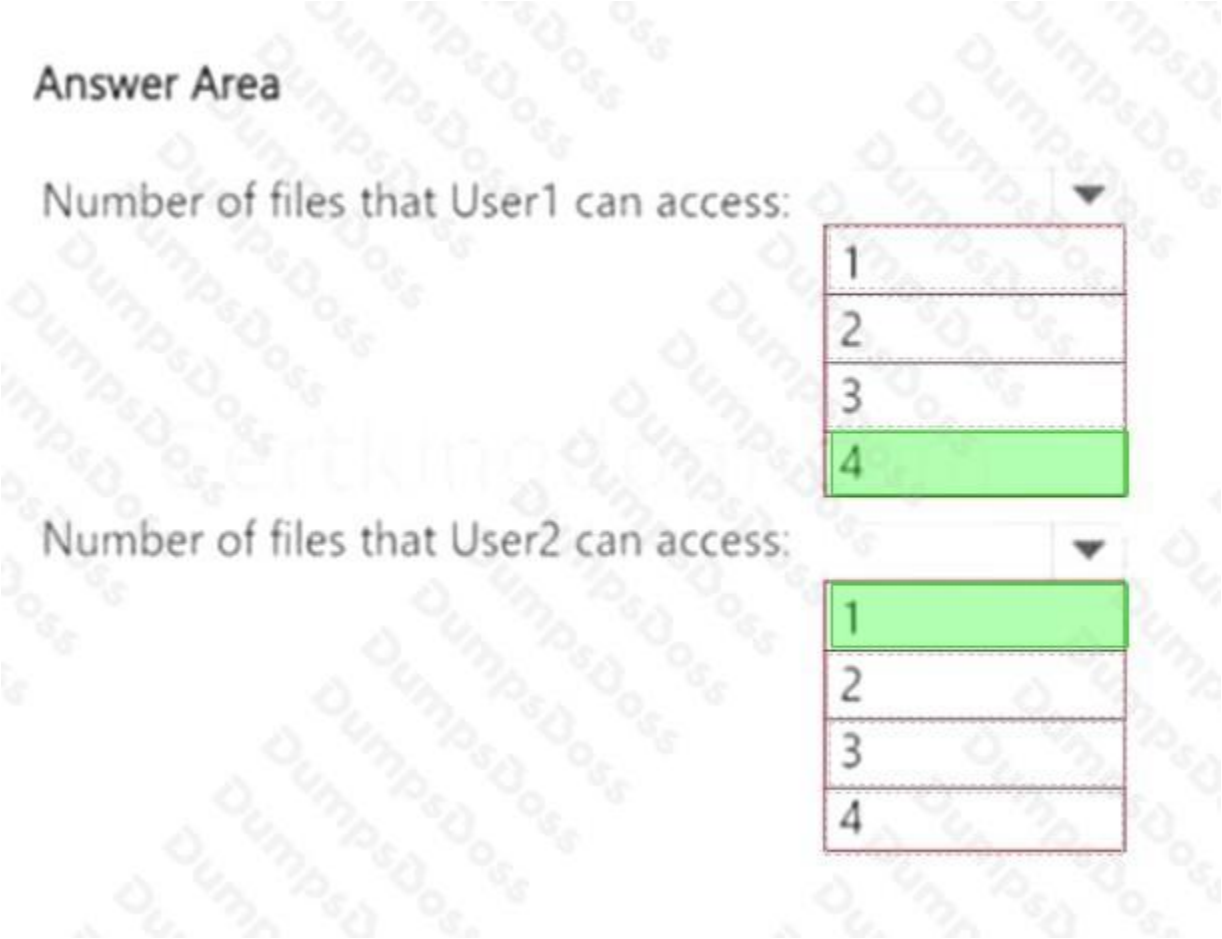
How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select

the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


Answer Area
Number of files that User1 can access:
1
2
3
4
Number of files that User2 can access:
1
2
3
4

ANSWER:



Explanation:

Looking at the exhibits, Site2 contains four files. The table shows the SWIFT code instance counts: File1.docx has 1, while File2.bmp has 4, File3.txt has 3, and File4.xlsx has 7. The DLP rule condition is triggered when the content contains SWIFT codes with an instance count of 2 or more. That means the DLP restriction applies to File2.bmp, File3.txt, and File4.xlsx, but it does *not* apply to File1.docx because it's below the threshold.

The key point is how Microsoft Purview DLP "restrict access" works for SharePoint/OneDrive. When you configure a DLP policy action to restrict access in Microsoft 365 locations, the restricted file remains accessible to specific "allowed" people, including the site owner (and typically the file owner/last modifier), while everyone else is blocked. So a Site Owner like User1 can still open the restricted files, but a Visitor like User2 (read-only) will be blocked from the restricted files and will only be able to access the file that wasn't restricted.

Therefore, after turning on DLPpolicy1, User1 can access all 4 files in Site2 (the 3 restricted files plus the 1 unrestricted file), while User2 can access only 1 file (File1.docx). For more detail on how DLP restricts access in SharePoint/OneDrive and who can still access restricted content, see Microsoft's documentation: Learn about data loss prevention and Learn about DLP for SharePoint and OneDrive.

QUESTION NO: 10

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 what users are doing on third-party generative AI sites (like copying/pasting prompts, sending sensitive data, etc.), DSPM for AI relies on endpoint visibility. That means your Windows devices have to be onboarded for Microsoft Purview features, and you also need the Microsoft Purview browser extension so the activity in supported browsers can actually be captured and evaluated.

Just creating policies (like DLP, data leaks, or communication compliance) isn't the "prerequisite" piece here—those come after you've got the devices and browser telemetry wired up. Intune enrollment can help with deployment, but it's not strictly required as a DSPM for AI prerequisite by itself.

References: https://learn.microsoft.com/en-us/purview/dspm-for-ai-overview and https://learn.microsoft.com/en-us/purview/endpoint-dlp-getting-started