MS-101^Q&As

Microsoft 365 Mobility and Security

Pass Microsoft MS-101 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ms-101.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

HOTSPOT

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The company stores 2 TB of data in SharePoint Online document libraries.

The tenant has the labels shown in the following table.

Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	○
User2 can access App1 from Device1.	○	○
User2 can access App1 from Device2.	○	○

From the Azure portal, you activate unified labeling.

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 App1 from Device1.	●	○
User2 can access App1 from Device1.	●	○
User2 can access App1 from Device2.	○	●

Correct Answer:

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

QUESTION 2

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

Three files were created on February 1, 2019, as shown in the following table.

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

On March 1, 2019, you create two retention labels named Label1 and Label2. The settings for Lable1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

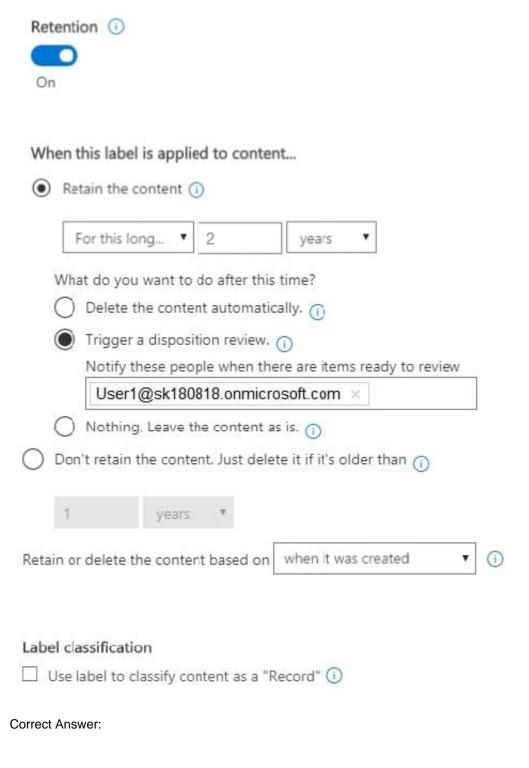The settings for Lable2 are configured as shown in the Label2 exhibit. (Click the Label2 tab.)

Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts. 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:

Label settings

Retention ⓘ

On

When this label is applied to content...

⦿ Retain the content ⓘ

For this long... ▼	2	years ▼

What do you want to do after this time?

○ Delete the content automatically. ⓘ

⦿ Trigger a disposition review. ⓘ

Notify these people when there are items ready to review

User1@sk180818.onmicrosoft.com ×

○ Nothing. Leave the content as is. ⓘ

○ Don't retain the content. Just delete it if it's older than ⓘ

1	years ▼

Retain or delete the content based on | when it was created ▼ | ⓘ

Label classification

☐ Use label to classify content as a "Record" ⓘ

Correct Answer:

Label settings

Retention ⓘ

⬤ On

On

When this label is applied to content...

○ Retain the content ⓘ

| For this long... ▾ | 2 | years ▾ |

⦿ Don't retain the content. Just delete it if it's older than ⓘ

| 1 | years ▾ |

Retain or delete the content based on | when it was created ▾ | ⓘ

Box 1: No

Retention overrides deletion.

Box 2: No

Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that. Thus 100 days in total.

Box 3: No

Items in an Exchange mailbox will be permanently deleted within 14 days of disposition.

References: https://docs.microsoft.com/en-us/office365/securitycompliance/labels

https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews

---

QUESTION 3

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

A. From the Exchange admin center, create a spam filter policy.

B. From the Security and Compliance admin center, create a data governance event.

C. From the Security and Compliance admin center, create an alert policy.

D. From the Exchange admin center, create a mail-flow rule.

Correct Answer: D

You can inspect email attachments in your Exchange Online organization by setting up mail flow rules. Exchange Online offers mail flow rules that provide the ability to examine email attachments as a part of your messaging security and compliance needs. When you inspect attachments, you can then take action on the messages that were inspected based on the content or characteristics of those attachments.

Incorrect answers:

A: A spam filter policy includes selecting the action to take on messages that are identified as spam. Spam filter policy settings are applied to inbound messages.

B: A data governance event commences when an administrator creates it, following which background processes look for content relating to the event and take the retention action defined in the label. The retention action can be to keep or remove items, or to mark them for manual disposition.

References: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-anti-malware-policies https://www.petri.com/office-365-event-based-retention

QUESTION 4

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

A. a custom detection rule

B. an allowed/blocked list rule

C. an alert suppression rule

D. an indicator

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators

QUESTION 5

HOTSPOT

You have three devices enrolled in Microsoft Intune as shown in the following table.

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	○	○
Configuration Manager manages the Windows Update policies for Device1.	○	○
Microsoft Intune manages Endpoint Protection for Device2.	○	○

The device compliance policies in Intune are configured as shown in the following table.

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	○	●
Configuration Manager manages the Windows Update policies for Device1.	○	●
Microsoft Intune manages Endpoint Protection for Device2.	●	○

The device compliance policies have the assignments shown in the following table.

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group2, Group3
Device3	Windows 10	Group2, Group3

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:

Name	Platform	Assigned
Policy1	Windows 10 and later	Yes
Policy2	Android	No
Policy3	Windows 10 and later	Yes

Correct Answer:

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3

Latest MS-101 Dumps   MS-101 Study Guide   MS-101 Braindumps