MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

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

https://www.lead4pass.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings Users and groups, Cloud apps, and Conditions settings Users and groups, Conditions, and Session settings	V

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy New-ClientAccessRule and Test-ClientAccessRule Get-CASMailbox and Set-CASMailbox	V

Correct Answer:

Answer Area

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings Users and groups, Cloud apps, and Conditions settings Users and groups, Conditions, and Session settings	V

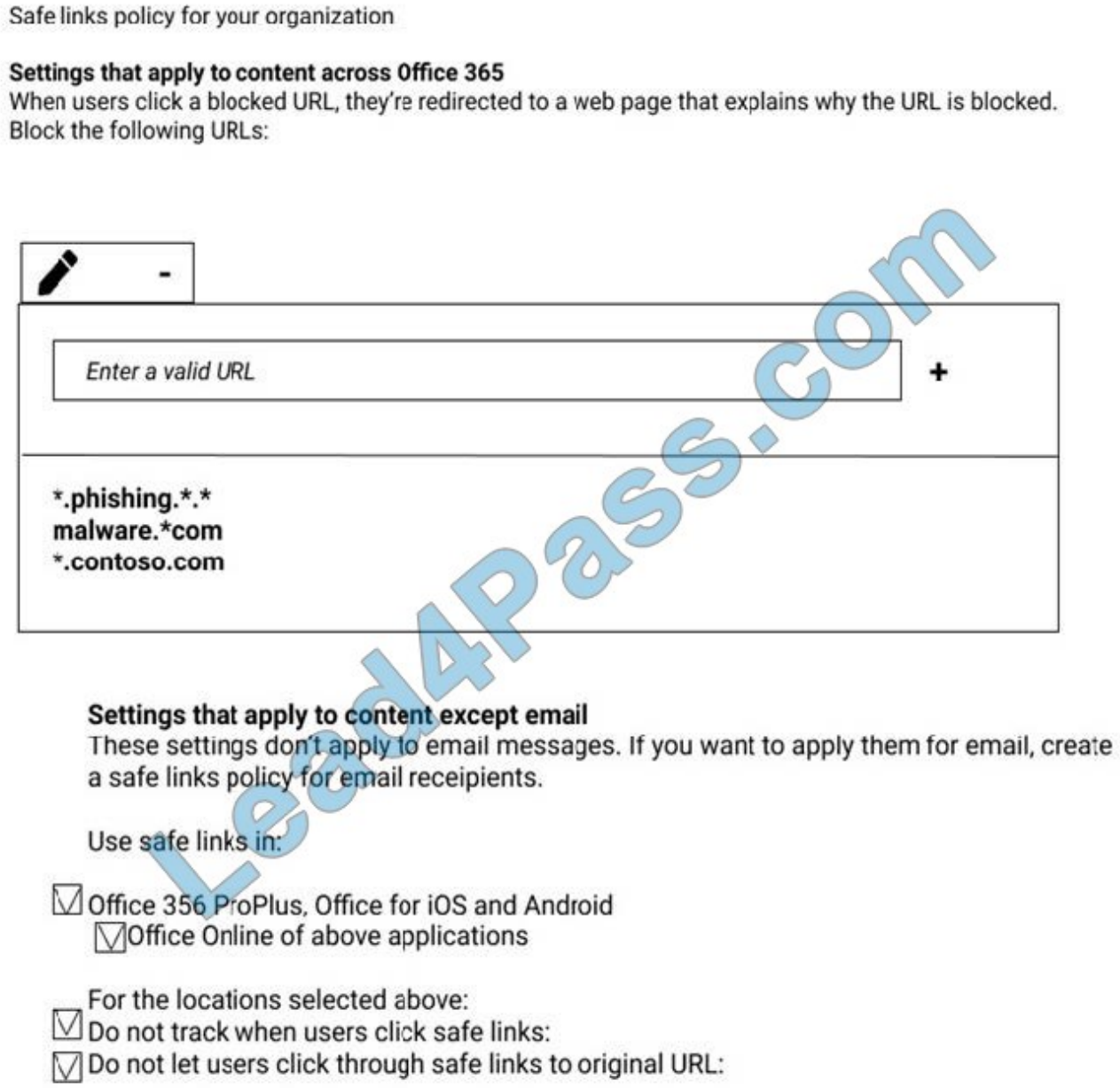
From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy New-ClientAccessRule and Test-ClientAccessRule Get-CASMailbox and Set-CASMailbox	V

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-conditional-access

QUESTION 2

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com. You create a safe links policy, as shown in the following exhibit.



Which URL can a user safely access from Microsoft Word Online?

A. fabrikam.phishing.fabrikam.com

B. malware.fabrikam.com

C. fabrikam.contoso.com

D. www.malware.fabrikam.com

Correct Answer: D

References: https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list-wtih-atp

QUESTION 3

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security and Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

A. From PowerShell, run Set-ManagedContentSettings.

B. From PowerShell, run Set-ComplianceTag.

C. From the Security and Compliance admin center, create a Data Subject Request (DSR).

D. Remove Azure Information Protection from the Site1 files.

Correct Answer: D

References: https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365

QUESTION 4

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

You have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.

Solution: You modify the privacy profile, and then create a Data Subject Request (DSR) case.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 5

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

You have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.

Solution: You start a message trace, and then create a Data Subject Request (DSR) case.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

References: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019

QUESTION 6

Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

1.

Source Anchor: objectGUID

2.

Password Hash Synchronization: Disabled

3.

Password writeback: Disabled

4.

Directory extension attribute sync: Disabled

5.

Azure AD app and attribute filtering: Disabled

6.

Exchange hybrid deployment: Disabled

7.

User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 7

You need to ensure that a user named Allan Deyoung receives incident reports when email messages that contain data covered by the U.K. Data Protection Act are sent outside of your organization.

To complete this task, sign in to the Microsoft 365 admin center.

Correct Answer: See below.

1.

In the Security and Compliance Center > left navigation > Data loss prevention > Policy > + Create a policy.

2.

Choose the U.K. Data Protection Act template > Next.

3.

Name the policy > Next.

4.

Choose All locations in Office 365 > Next.

5.

At the first Policy Settings step just accept the defaults,

6.

After clicking Next, you\\'ll be presented with an additional Policy Settings page

Deselect the Show policy tips to users and send them an email notification option.

Select the Detect when content that\\'s being shared contains option, and configure the number instances to be 10.

Select the Send incident reports in email option.

Select the Choose what to include in the report and who receives it link to add Allan Deyoung as a recipient.

7.

> Next

8.

Select the option to turn on the policy right away > Next.

9.

Click Create to finish creating the policy.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-dlp-policy-templates-include?view=o365-worldwide

---

QUESTION 8

SIMULATION You need to implement a solution to manage when users select links in documents or email messages from Microsoft Office 365 ProPlus applications or Android devices. The solution must meet the following requirements:

1.

Block access to a domain named fabrikam.com

2.

Store information when the users select links to fabrikam.com To complete this task, sign in to the Microsoft 365 portal.

Correct Answer: See below.

You need to configure a Safe Links policy.

1.

Go to the Office 365 Security and Compliance admin center.

2.

Navigate to Threat Management > Policy > Safe Links.

3.

In the Policies that apply to the entire organization section, select Default, and then click the Edit icon.

4.

In the Block the following URLs section, type in *.fabrikam.com. This meets the first requirement in the question.

5.

In the Settings that apply to content except email section, untick the checkbox labelled Do not track when users click safe links. This meets the second requirement in the question.

6.

Click Save to save the changes.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-linkspolicies?view=o365-worldwide

---

QUESTION 9

You have a Microsoft 365 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

A. From the Security and Compliance admin center, modify the Policy Tips of a DLP policy.

B. From the Cloud App Security admin center, apply a filter to the alerts.

C. From the Security and Compliance admin center, modify the User overrides settings of a DLP policy.

D. From the Security and Compliance admin center, modify the matched activities threshold of an alert policy.

Correct Answer: D

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

---

QUESTION 10

You need to ensure that email messages in Exchange Online and documents in SharePoint Online are retained for eight years.

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See below.

NB: For our purposes, the retention period will be 8 years.

For retaining email messages in Exchange Online:

Step 1: Create a retention tag

1.

Navigate to the Exchange Admin Center

2.

Navigate to Compliance management > Retention tags, and then click Add +

3.

Select one of the following options:

Applied automatically to entire mailbox (default): Select this option to create a default policy tag (DPT). You can use DPTs to create a default deletion policy and a default archive policy, which applies to all items in the mailbox.

Applied automatically to a specific folder: Select this option to create a retention policy tag (RPT) for a default folder such as Inbox or Deleted Items.

Applied by users to items and folders (Personal): Select this option to create personal tags. These tags allow Outlook and Outlook on the web (formerly known as Outlook Web App) users to apply archive or deletion settings to a message

or folders that are different from the settings applied to the parent folder or the entire mailbox.

4.

The New retention tag page title and options will vary depending on the type of tag you selected. Complete the following fields:

Name: Enter a name for the retention tag. The tag name is for display purposes and doesn\\'t have any impact on the folder or item a tag is applied to. Consider that the personal tags you provision for users are available in Outlook and Outlook

on the web.

Apply this tag to the following default folder: This option is available only if you selected Applied automatically to a specific folder.

Retention action: Select one of the following actions to be taken after the item reaches its retention period:

Delete and Allow Recovery: Select this action to delete items but allow users to recover them using the Recover Deleted Items option in Outlook or Outlook on the web. Items are retained until the deleted item retention period configured for

the mailbox database or the mailbox user is reached.

Permanently Delete: Select this option to permanently delete the item from the mailbox database.

Move to Archive: This action is available only if you\\'re creating a DPT or a personal tag. Select this action to move items to the user\\'s In-Place Archive.

Retention period: Select one of the following options:

Never: Select this option to specify that items should never be deleted or moved to the archive.

When the item reaches the following age (in days): Select this option and specify the number of days to retain items before they\\'re moved or deleted. The retention age for all supported items except Calendar and Tasks is calculated from

the date an item is received or created. Retention age for Calendar and Tasks items is calculated from the end date.

Comment: User this optional field to enter any administrative notes or comments. The field isn\\'t displayed to users.

Step 2: Create a retention policy

1.

Navigate to Compliance management > Retention policies, and then click Add +

2.

In New Retention Policy, complete the following fields:

Name: Enter a name for the retention policy.

Retention tags: Click Add + to select the tags you want to add to this retention policy.

A retention policy can contain the following tags:

One DPT with the Move to Archive action.

One DPT with the Delete and Allow Recovery or Permanently Delete actions.

One DPT for voice mail messages with the Delete and Allow Recovery or Permanently Delete actions.

One RPT per default folder such as Inbox to delete items.

Any number of personal tags.

Step 3: Apply a retention policy to mailbox users

After you create a retention policy, you must apply it to mailbox users. You can apply different retention policies to different set of users.

1.

Navigate to Recipients > Mailboxes.

2.

In the list view, use the Shift or Ctrl keys to select multiple mailboxes.

3.

In the details pane, click More options.

4.

Under Retention Policy, click Update.

5.

In Bulk Assign Retention Policy, select the retention policy you want to apply to the mailboxes, and then click Save.

For retaining documents in SharePoint Online

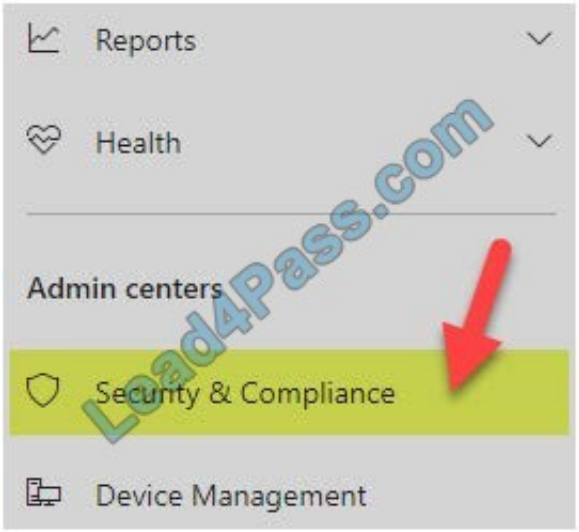
Access Security and Compliance Admin Center

1.

Navigate to the Office 365 Admin Centers

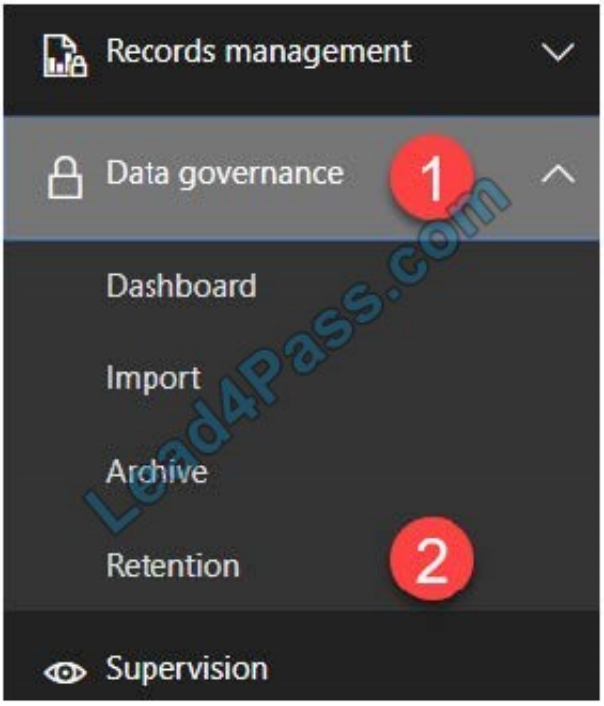
2.

From the list of available Admin Centers, click on Security and Compliance



How to create and publish a Retention Policy on a SharePoint site

Now that we are in the Security and Compliance Admin Center, we are ready to create and publish a Retention Policy on a SharePoint site. Under Data Governance, click Retention



QUESTION 11

You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See below.

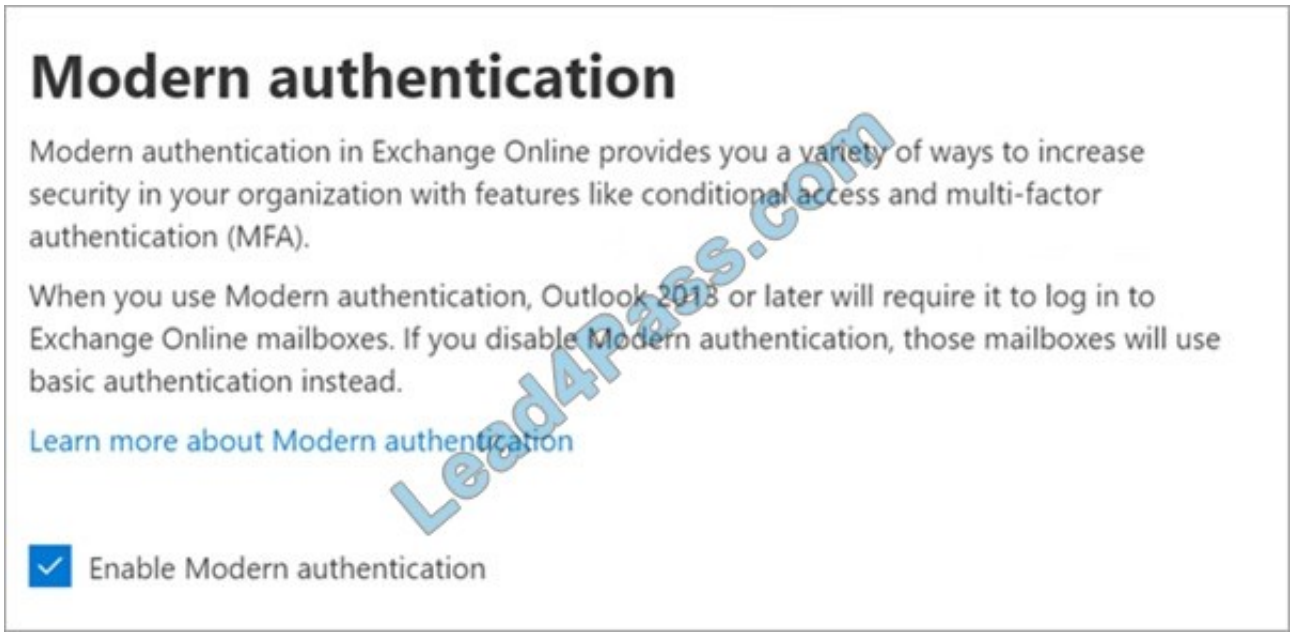
Enable Modern authentication for your organization

1.

To enable modern authentication, from the admin center, select Settings > Settings and then in the Services tab, choose Modern authentication from the list.

2.

Check the Enable modern authentication box in the Modern authentication panel.



Enable multi-factor authentication for your organization

1.

In the admin center, select Users and Active Users.

2.

In the Active Users section, Click on multi-factor authentication.

3.

On the Multi-factor authentication page, select user if you are enabling this for one user or select Bulk Update to enable multiple users.

4.

Click on Enable under Quick Steps.

5.

In the Pop-up window, Click on Enable Multi-Factor Authentication.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.

Reference: https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-

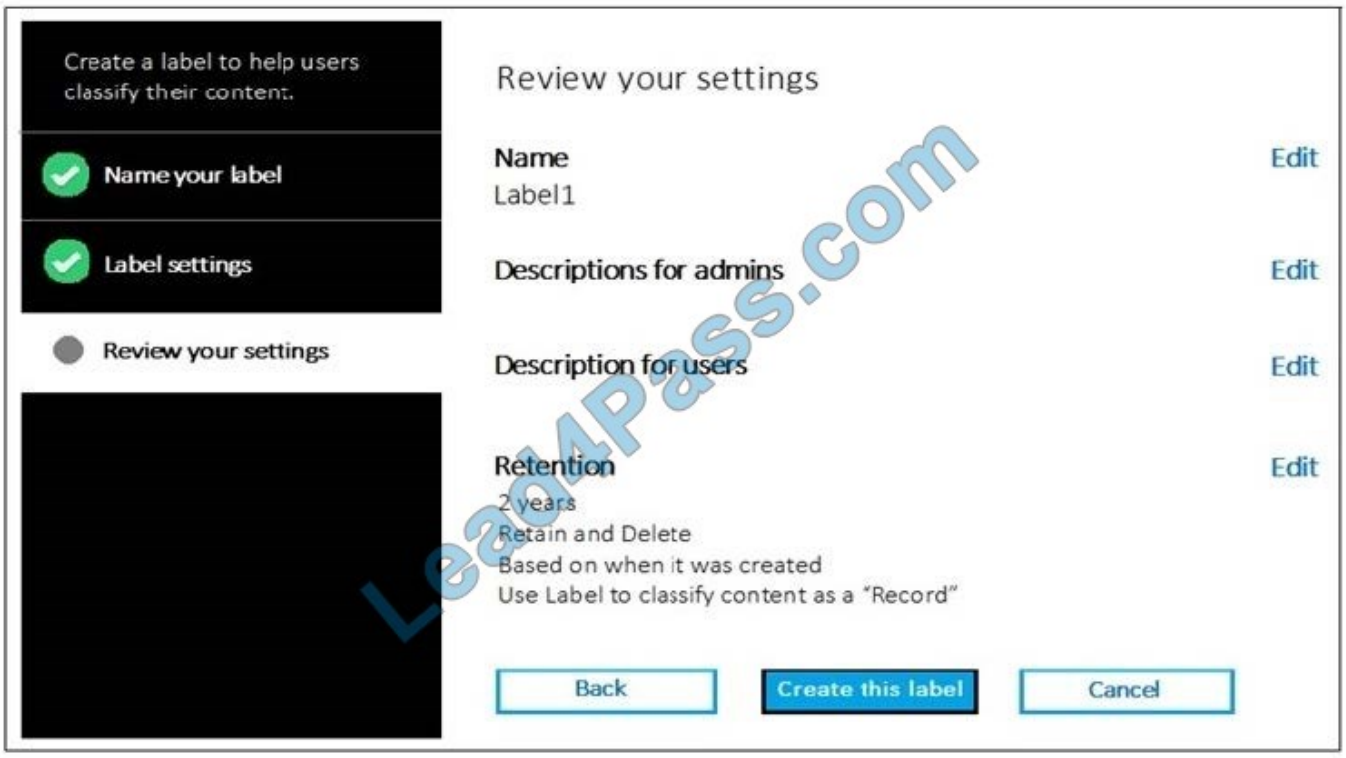
authentication?view=o365-worldwide

QUESTION 12

HOTSPOT

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.



You publish Label1 to SharePoint sites.

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:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

- never delete the file.
- delete the file before January 1, 2021.
- delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

- always remain in the library.
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

Correct Answer:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

- never delete the file.
- delete the file before January 1, 2021.
- delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

- always remain in the library.
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

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

QUESTION 13

You have a Microsoft 365 subscription.

A user reports that changes were made to several files in Microsoft OneDrive.

You need to identify which files were modified by which users in the user\\'s OneDrive.

What should you do?

A. From the Azure Active Directory admin center, open the audit log

B. From the OneDrive admin center, select Device access

C. From Security and Compliance, perform an eDiscovery search

D. From Microsoft Cloud App Security, open the activity log

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/cloud-app-security/activity-filters