- **Vendor:** Microsoft
- **Exam Code:** MS-500
- **Exam Name:** Microsoft 365 Security Administration
- **New Updated Questions from Braindump2go (Updated in May/2020)**

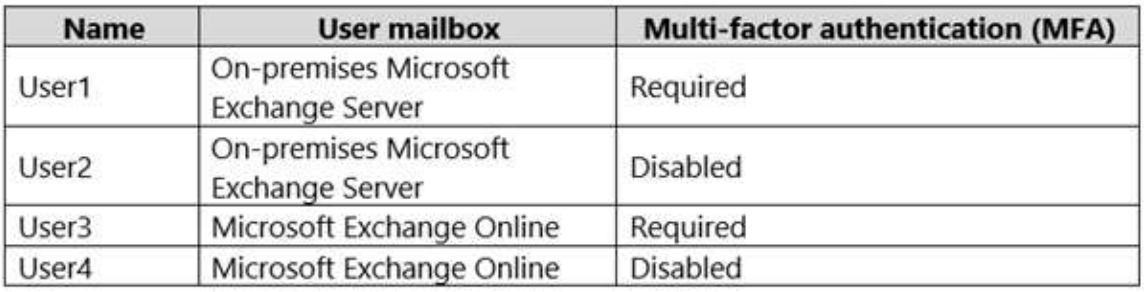
QUESTION 165
SIMULATION
You need to ensure that unmanaged mobile devices are quarantined when the devices attempt to connect to Exchange Online.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure the Exchange ActiveSync Access Settings.
1. Go to the Exchange admin center.
2. Click on Mobile in the left navigation pane.
3. On the Mobile Device Access page, click the Edit button in the Exchange ActiveSync Access Settings area.
4. Select the Quarantine option under When a mobile device that isn't managed by a rule or personal exemption connects to Exchange.
5. Optionally, you can configure notifications to be sent to administrators and a message to be sent to the mobile device user when a device is quarantined.
6. Click Save to save the changes.

QUESTION 166
SIMULATION
You need to ensure that all users must change their password every 100 days.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure the Password Expiration Policy.
1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Settings option.
3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled Set user passwords to expire after a number of days is ticked.
6. Enter 100 in the Days before passwords expire field.
7. Click Save changes to save the changes.

QUESTION 167
SIMULATION
You need to ensure that a user named Grady Archie can monitor the service health of your Microsoft 365 tenant. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to assign the Service Administrator role to Grady Archie.
1. In the Microsoft 365 Admin Center, type Grady Archie into the Search for users, groups, settings or tasks search box.
2. Select the Grady Archie user account from the search results.
3. In the Roles section of the user account properties, click the Edit link.
4. Select the Customized Administrator option. This will display a list of admin roles.
5. Select the Service admin role.
6. Click Save to save the changes.

Explanation:
https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

QUESTION 168
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.



Name	User mailbox	Multi-factor authentication (MFA)
User1	On-premises Microsoft Exchange Server	Required
User2	On-premises Microsoft Exchange Server	Disabled
User3	Microsoft Exchange Online	Required
User4	Microsoft Exchange Online	Disabled

You plan to use Microsoft 365 Attack Simulator.
You need to identify the users against which you can use Attack Simulator.
Which users should you identify?

A. User3 only
B. User1, User2, User3, and User4
C. User3 and User4 only
D. User1 and User3 only

Answer: C
Explanation:
Each targeted recipient must have an Exchange Online mailbox.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide

QUESTION 169
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:

```
- Block access to a domain named fabrikam.com
- Store information when the users select links to fabrikam.com
```

To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure a Safe Links policy.
1. Go to the Office 365 Security & 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.
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide

QUESTION 170
SIMULATION
You need to configure your organization to automatically quarantine all phishing email messages.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to edit the Anti-Phishing policy.
1. Go to the Office 365 Security & Compliance admin center.
2. Navigate to Threat Management > Policy > ATP Anti-Phishing.
3. Click on Default Policy.
4. In the Impersonation section, click Edit.

5. Go to the Actions section.
6. In the If email is sent by an impersonated user: box, select Quarantine the message from the drop-down list.
7. In the If email is sent by an impersonated domain: box, select Quarantine the message from the drop-down list.
8. Click Save to save the changes.
9. Click Close to close the anti-phishing policy window.

QUESTION 171
You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view ATP reports in the Threat management dashboard.
Which role provides User1 with the required role permissions?

A. Security administrators
B. Exchange administrator
C. Compliance administrator
D. Message center reader

Answer: A
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-needed-to-view-the-atp-reports

QUESTION 172
SIMULATION
You discover that Microsoft SharePoint content is shared with users from multiple domains.
You need to allow sharing invitations to be sent only to users in an email domain named contoso.com.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure the Sharing options in the SharePoint admin center.
1. Go to the SharePoint admin Center.
2. Navigate to Policies > Sharing.
3. In the External Sharing section, click on More external sharing settings.
4. Tick the Limit external sharing by domain checkbox.
5. Click the Add domains button.
6. Select the Allow only specific domains option and type in the domain contoso.com.
7. Click Save to save the changes.

QUESTION 173
You have a Microsoft 365 subscription.
Your company uses Jamf Pro to manage macOS devices.
You plan to create device compliance policies for the macOS devices based on the Jamf Pro data.
You need to connect Microsoft Endpoint Manager to Jamf Pro.
What should you do first?

A. From the Azure Active Directory admin center, add a Mobility (MDM and MAM) application.
B. From the Endpoint Management admin center, add the Mobile Threat Defense connector.
C. From the Endpoint Management admin center, configure Partner device management.
D. From the Azure Active Directory admin center, register an application.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf

QUESTION 174
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 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

Answer: B

QUESTION 175
SIMULATION
You need to ensure that administrators can publish a label that adds a footer to email messages and documents.
To complete this task, sign in to the Microsoft Office 365 portal.
Answer:
You need to configure a Sensitivity label.
1. Go to the Security & Compliance Admin Center.
2. Navigate to Classification > Sensitivity labels.
3. Click on + Create a label to create a new label.
4. Give the label a name and description then click Next.
5. Leave the Encryption option as None and click Next.
6. On the Content Marking page, tick the checkbox Add a footer.
7. Click the Customize Text link and add the footer text and click Save (for the question, it doesn't matter what text you add).
8. Click Next.
9. Leave the Auto-labeling for Office apps off and click Next.
10.Click the Submit button to save your changes.
11.The label is now ready to be published. Click the Done button to exit the page and create the label.

QUESTION 176
SIMULATION
You plan to publish a label that will retain documents in Microsoft OneDrive for two years, and then automatically delete the documents.
You need to create the label.
To complete this task, sign in to the Microsoft Office 365 portal.
Answer:
You need to create a retention label.
1. Go to the Security & Compliance Admin Center.
2. Navigate to Classification > Retention labels.
3. Click on + Create a label to create a new label.
4. Give the label a name and click Next.
5. On the File plan descriptors, leave all options empty. The options in this page are used for auto-applying the retention label. Click Next.
6. Turn the Retention switch to On.
7. Under Retain the content, set the period to 2 years.
8. Under What do you want to do after this time?, select the Delete the content automatically option.
9. Click Next.
10.Click the Create this label button to create the label. The label is now ready to be published to Microsoft OneDrive.

QUESTION 177
SIMULATION
You plan to add a file named ConfidentialHR.docx to a Microsoft SharePoint library.
You need to ensure that a user named Megan Bowen is notified when another user accesses ConfidentialHR.xlsx.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure an alert policy.

1. Go to the Security & Compliance Admin Center.
2. Navigate to Alerts > Alert Policies.
3. Click on + New alert policy to create a new policy.
4. Give the policy a name and select a severity level. For example: Medium.
5. In the Category section, select Information Governance and click Next.
6. In the Select an activity section, select Any file or folder activity.
7. Click Add a condition and select File name.
8. Type in the filename ConfidentialHR.xlsx and click Next.
9. In the email recipients section, add Megan Bowen and click Next.
10.Click Finish to create the alert policy.

QUESTION 178
SIMULATION
You need to create a policy that identifies content in Microsoft OneDrive that contains credit card numbers.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure auto-labeling in `simulation' mode. In the policy, you can select the `Credit Card' sensitive info type.
1. In the Microsoft 365 compliance center, navigate to sensitivity labels:
Solutions > Information protection
2. Select the Auto-labeling (preview) tab.
3. Select + Create policy.
4. For the page Choose info you want this label applied to: Select one of the templates, such as Financial or Privacy. You can refine your search by using the Show options for dropdown. Or, select Custom policy if the templates don't meet your requirements. Select Next.
5. For the page Name your auto-labeling policy: Provide a unique name, and optionally a description to help identify the automatically applied label, locations, and conditions that identify the content to label.
6. For the page Choose locations where you want to apply the label: Select OneDrive. Then select Next.
7. For the Define policy settings page: Keep the default of Find content that contains to define rules that identify content to label across all your selected locations. The rules use conditions that include sensitive information types and sharing options. For sensitive information types, you can select both built-in and custom sensitive information types.
8. Then select Next.
9. For the Set up rules to define what content is labeled page: Select + Create rule and then select Next.
10.On the Create rule page, name and define your rule, using sensitive information types and then select Save.
11.Click Next.
12.For the Choose a label to auto-apply page: Select + Choose a label, select a label from the Choose a sensitivity label pane, and then select Next.
13.For the Decide if you want to run policy simulation now or later page: Select Run policy in simulation mode if you're ready to run the auto-labeling policy now, in simulation mode. Otherwise, select Leave policy turned off. Select Next.
14.For the Summary page: Review the configuration of your auto-labeling policy and make any changes that needed, and complete the wizard.
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

QUESTION 179
SIMULATION
Your company plans to merge with another company.
A user named Debra Berger is an executive at your company.
You need to provide Debra Berger with all the email content of a user named Alex Wilber that contains the word merger.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to run a content search then export the results of the search.
1. Go to the Microsoft 365 Compliance admin center.
2. Navigate to Content Search under the Solutions section in the left navigation pane.
3. Click on + New Search to create a new search.
4. In the Keywords box, type in `merger'.
5. In the Locations section, select Specific locations then click the Modify link.
6. Click on the Choose users, groups or teams link.

7. Type Alex Wilber in the search field the select his account from the search results.
8. Click the Choose button to add the user then click Done.
9. Click Save to close the locations pane.
10.Click Save & run to run the search.
11.The next step is to export the results. Select the search then under Export results to a computer, click Start export.
12.On the Export the search results page, under Output options, select All items. 13.Under Export Exchange content as, select One PST file for each mailbox. 14.Click on Start export. When the export has finished, there will be an option to download the exported PST file.

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide