



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.geekcert.com/ms-500.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

You have a Microsoft 365 E5 subscription and 5,000 users.

You create several alert policies that are triggered every time activities match rules.

You need to create an alert policy that is triggered when the volume of matched activities becomes unusual.

What should you do first?

- A. Enable Microsoft Office 365 auditing.
- B. Enable Microsoft Office 365 analytics.
- C. Enable Microsoft Office 365 Cloud App Security.
- D. Deploy a Microsoft Office 365 add-in to all the users.

Correct Answer: B

QUESTION 2

You have a Microsoft 365 E5 subscription that contains a user named User1.

User1 needs to be able to create Data Subject Requests (DSRs) in the Microsoft 365 compliance center.

To which role or role group should you add User1?

- A. the Compliance Data Administrator role
- B. the Data Investigator role
- C. the eDiscovery Manager role
- D. the Records Management role group

Correct Answer: C

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-manage-gdpr-data-subject-requests-with-the-dsr-case-tool>

QUESTION 3

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains a user named User1.

You configure information barriers.

You need to identify which information barrier policies apply to User1.



Which cmdlet should you use?

- A. Get-InformationBarrierRecipientStatus
- B. Get-InformationBarrierPoliciesApplicationStatus
- C. Get-InformationBarrierPolicy
- D. Get-OrganizationSegment

Correct Answer: A

Get-InformationBarrierRecipientStatus -Identity

Use the Get-InformationBarrierRecipientStatus cmdlet with the Identity parameter.

You can use any identity value that uniquely identifies each recipient, such as Name, Alias, Distinguished name (DN), Canonical DN, Email address, or GUID.

<https://learn.microsoft.com/en-us/microsoft-365/troubleshoot/information-barriers/information-barriers-troubleshooting>

Reference:

<https://docs.microsoft.com/en-us/office365/troubleshoot/information-barriers/information-barriers-troubleshooting>

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

HOTSPOT



You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:

Rule1:

7.

Conditions: Label1, Detect content that's shared with people outside my organization

8.

Actions: Restrict access to the content for external users

9.

User notifications: Notify the user who last modified the content 10. User overrides: On 11. Priority: 0

Rule2:

12. Conditions: Label1 or Label2

13. Actions: Restrict access to the content

14. Priority: 1

Rule3:

15. Conditions: Label2, Detect content that's shared with people outside my organization

16. Actions: Restrict access to the content for external users 17. User notifications: Notify the user who last modified the content 18. User overrides: On 19. Priority: 2

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:



Statements	Yes	No
External users can access File1	<input type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2	<input type="radio"/>	<input type="radio"/>
External users can access File3	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
External users can access File1	<input type="radio"/>	<input checked="" type="radio"/>
The users in contoso.com can access File2	<input type="radio"/>	<input checked="" type="radio"/>
External users can access File3	<input type="radio"/>	<input checked="" type="radio"/>

All of them will match Rule2 because it is the most restrictive.

When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced. For example, if content matches all of the

following rules, Rule 3 is enforced because it's the highest priority, most restrictive rule:

Rule 1: only notifies users

Rule 2: notifies users, restricts access, and allows user overrides

Rule 3: notifies users, restricts access, and does not allow user overrides

Rule 4: only notifies users



Rule 5: restricts access

Rule 6: notifies users, restricts access, and does not allow user overrides

Source: <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=0365-worldwide>

[Latest MS-500 Dumps](#)

[MS-500 PDF Dumps](#)

[MS-500 Practice Test](#)