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

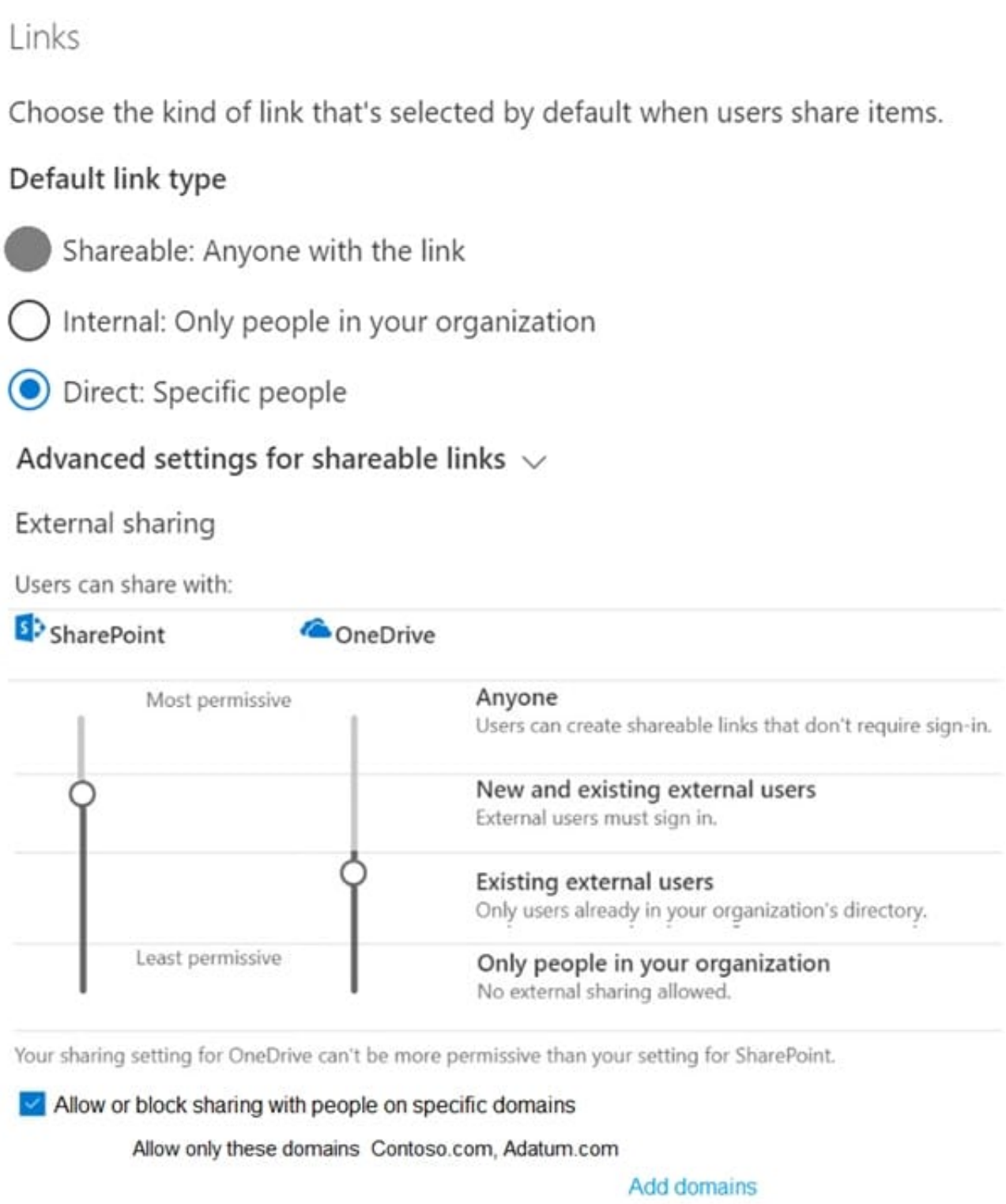
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of litwareinc.com.

You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.


Links
Choose the kind of link that's selected by default when users share items.
Default link type
Shareable: Anyone with the link
Internal: Only people in your organization
Direct: Specific people
Advanced settings for shareable links
External sharing
Users can share with:
SharePoint
OneDrive
Most permissive
Least permissive
Anyone
Users can create shareable links that don't require sign-in.
New and existing external users
External users must sign in.
Existing external users
Only users already in your organization's directory.
Only people in your organization
No external sharing allowed.
Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.
Allow or block sharing with people on specific domains
Allow only these domains Contoso.com, Adatum.com
Add domains

Hot Area:

Answer Area

A user who has an email address of user1@fabrikam.com

- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

If a new guest user is created for user2@contoso.com,

- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

Correct Answer:

Answer Area

A user who has an email address of user1@fabrikam.com

- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

If a new guest user is created for user2@contoso.com,

- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

Reference: https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

QUESTION 2

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online.

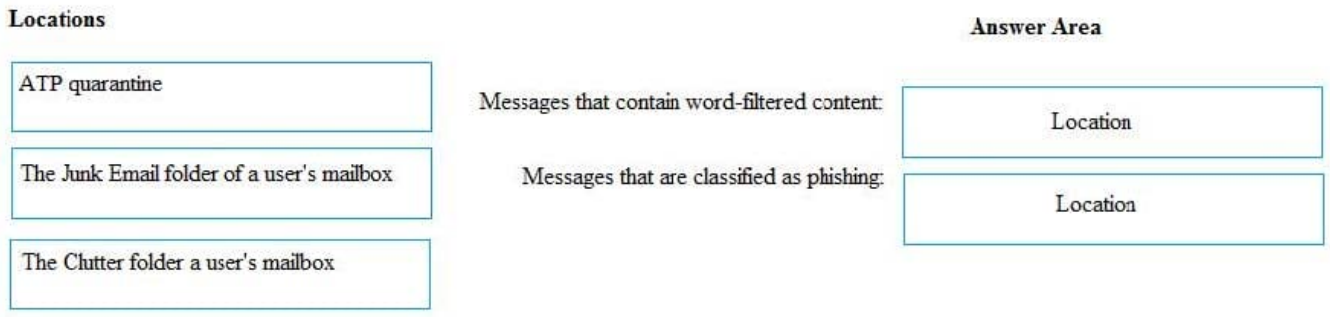
Microsoft 365 is configured to use the default policy settings without any custom rules.

You manage message hygiene.

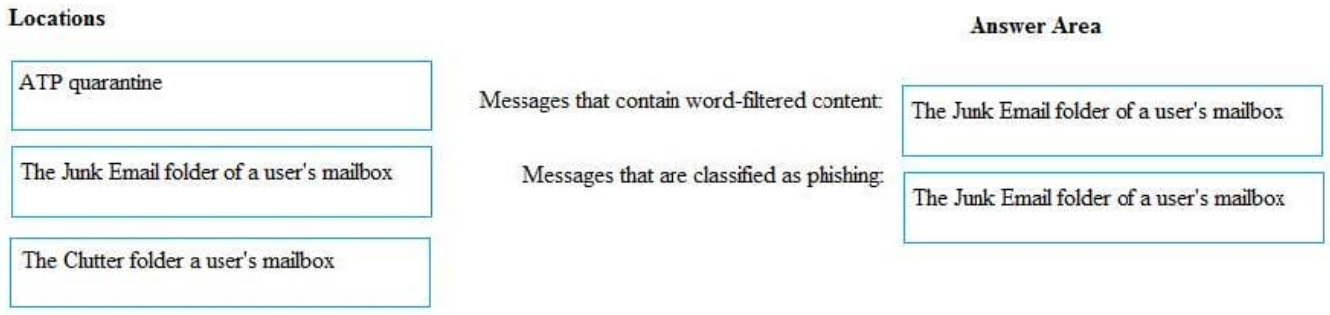
Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location may be used once, more than once, or not at all. You may need to drag the split bar between

panes or scroll to view content.

Select and Place:



Correct Answer:



QUESTION 3

DRAG DROP

You have a Microsoft 365 tenant.

User attributes are synced from your company\\'s human resources (HR) system to Azure Active Directory (Azure AD).

The company has four departments that each has its own Microsoft SharePoint Online site. Each site must be accessed only by the users from its respective department.

You are designing an access management solution that has the following requirements:

1.

Users must be added automatically to the security group of their department.

2.

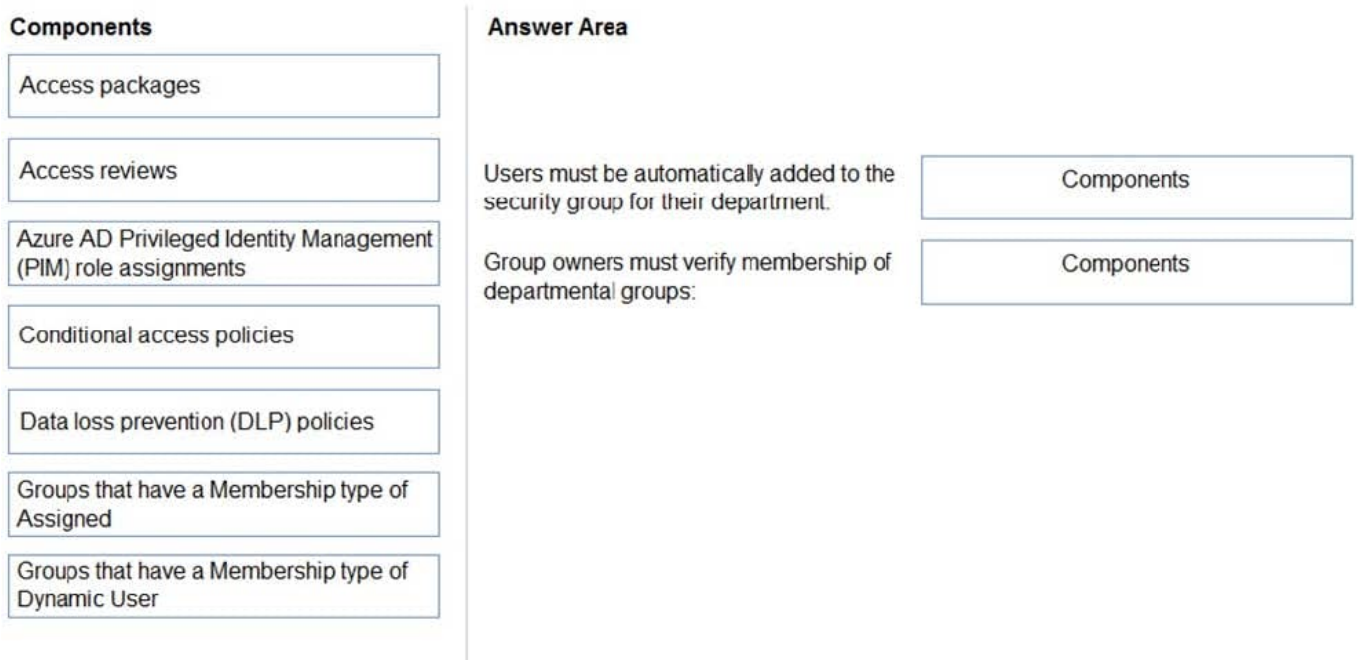
All security group owners must verify once quarterly that only the users in their department belong to their group.

Which components should you recommend to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may only be used once, more than once, or not at all. You may need to drag

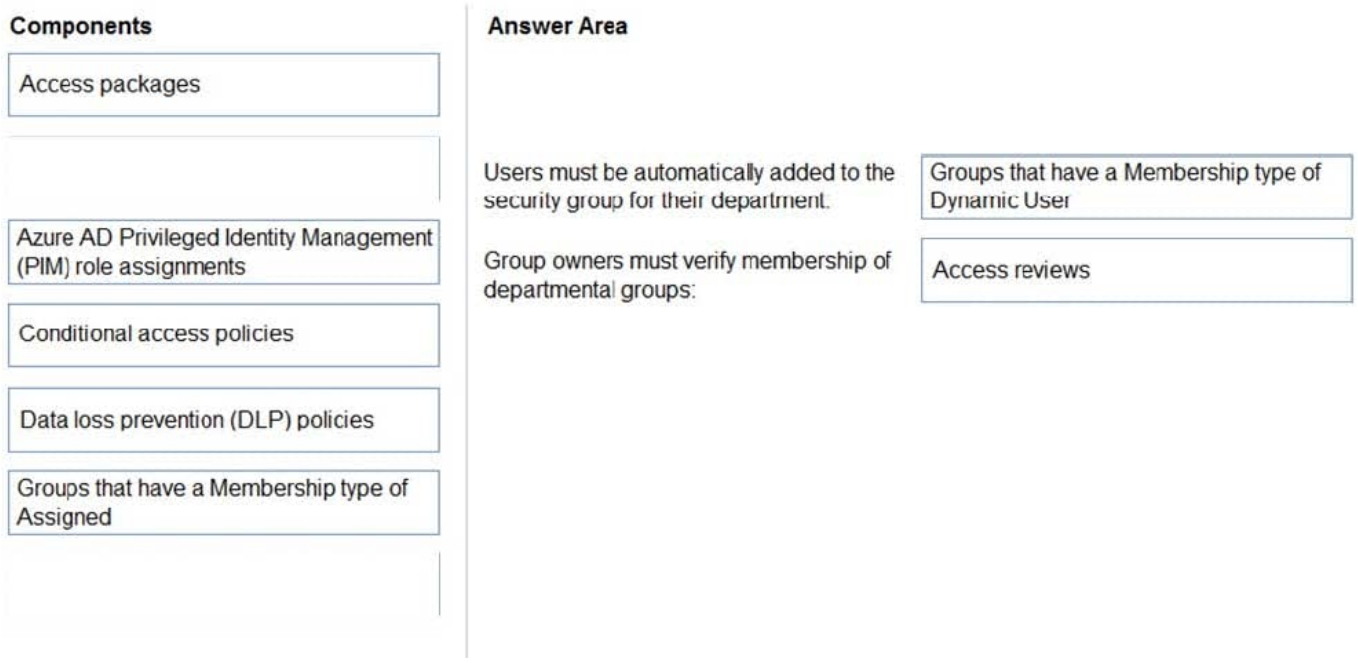
the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference: https://cloudbuild.co.uk/tag/create-a-dynamic-security-group-in-azure-ad/

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

QUESTION 4

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 questions 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 the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Compliance Manager uses a role-based access control (RBAC) permission model. Only users who are assigned a role may access Compliance Manager, and the actions allowed by each user are restricted by role type. https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

QUESTION 5

HOTSPOT

You have a Microsoft Defender for Endpoint deployment that has custom network indicators turned on. Microsoft Defender for Endpoint protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender foe Endpoint has the device groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	*None*

From Microsoft Defender Security Center, you create the URLs/Domains indicators shown in the following table.

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

Hot Area:

Answer Area

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	○	○
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	○	○
From a web browser on Computer2, you can open http://www.litwareinc.com.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	○	●
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	●	○
From a web browser on Computer2, you can open http://www.litwareinc.com.	●	○

Computer1 www.contoso.com > No

1.

No, as Computer1 is Member of Group1 and group1 prohibits access.

Computer1 www.litwareinc.com/public > Yes

2.

Yes, as there is no block for this URL at all.

Computer2 www.litwareinc.com > Yes

3.

Yes, as Computer2 is a member of Group1 and Group1 does not have a block for this URL.

Computers can only be part of one group

based on the ranking if conditions are met for multiple groups.

Group1 membership is higher than Group2, so Computer2 is in Group1.

Computer can be member on just 1 atp group, and priority is used

Both computers are on group1 because contains 1 and group 1 have the highest priority.

"Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags, and OS platform.

If a device is also matched to other groups, it\\'s added only to the highest ranked device group"

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/machine-groups