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.passapply.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 contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create and enforce an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy that has the following settings:

1.

Assignments: Include Group1, Exclude Group2

2.

Conditions: User risk level of Medium and above

3.

Access: Allow access, Require password change

The users attempt to sign in. The risk level for each user is shown in the following table.

User	User risk level
User1	High
User2	Medium
User3	High

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
User1 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

Correct Answer:

Statements	Yes	No
User1 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

Box 1: Yes.

User1 is in Group1 which the policy applies to.

Box 2: No

User2 is in Group2 which is excluded from the policy.

Box 3: No

User3 is in Group1 which is included in the policy and Group2 which is excluded from the policy. In this case, the exclusion wins so the policy does not apply to User3.

QUESTION 2

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You have a Data Subject Request (DSR) case named Case1.

You need to allow User1 to export the results of Case1. The solution must use the principle of least privilege.

Which role should you assign to User1 for Case1?

A. eDiscovery Manager

B. Security Operator

C. eDiscovery Administrator

D. Global Reader

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide#step-1-assign-ediscovery-permissions-to-potential-case-members

QUESTION 3

You have a Microsoft 365 subscription named contoso.com.

You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:

1.

Enable file sharing for users that have a Microsoft account.

2.

Block file sharing for anonymous users. What should you do?

A. From Advanced settings for external sharing, select Allow or block sharing with people on specific domains and add contoso.com.

B. From the External sharing settings for OneDrive, select Only people in your organization.

C. From the External sharing settings for OneDrive, select Existing external users.

D. From the External sharing settings for OneDrive, select New and existing external users.

Correct Answer: D

Reference: https://www.sharepointdiary.com/2020/09/enable-external-sharing-in-onedrive-for-business.html

QUESTION 4

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1 and the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a communication compliance policy named Policy1.

You need to identify whose communications can be monitored by Policy1, and who can be assigned the Reviewer role for Policy1.

Who should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Policy1 can monitor the communications of:
- User1 only
- User1, Group1, and Group2 only
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

The Reviewer role for Policy1 can be assigned to:
- User1 only
- User1 and Group4 only
- User1, Group3, and Group4 only
- User1, Group1, Group3, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Correct Answer:

Policy1 can monitor the communications of:
- User1 only
- **User1, Group1, and Group2 only**
- User1, Group2, and Group3 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

The Reviewer role for Policy1 can be assigned to:
- **User1 only**
- User1 and Group4 only
- User1, Group3, and Group4 only
- User1, Group1, Group3, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance-configure?view=o365-worldwide

QUESTION 5

HOTSPOT

You have a Microsoft 365 E5 subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains three groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create a new access package as shown in the following exhibit.

New access package ...

* Basics Resource roles * Requests Requestor information
* Lifecycle Review + Create

Summary of access package configuration

Basics

Name	Package1
Description	Package1 description
Catalog name	General

Resource roles

Resource	Type	Sub Type	Role
Group1	Group and Team	Security Group	Member
Group3	Group and Team	Security Group	Member
Site1	SharePoint Site	SharePoint Online Site	Site1 Members

Requests

Users who can request access	For users in your directory(Group2)
Require approval	No
Enabled	Yes

Requestor information

Questions

Question	Answer format	Required

Lifecycle

Access package assignments expire	After 10 days
Require access reviews	No

You assign Package1 on June 1, 2021, by using die following configurations:

1.

Select users: User1, User2, User3

2.

Select policy: Initial policy

3.

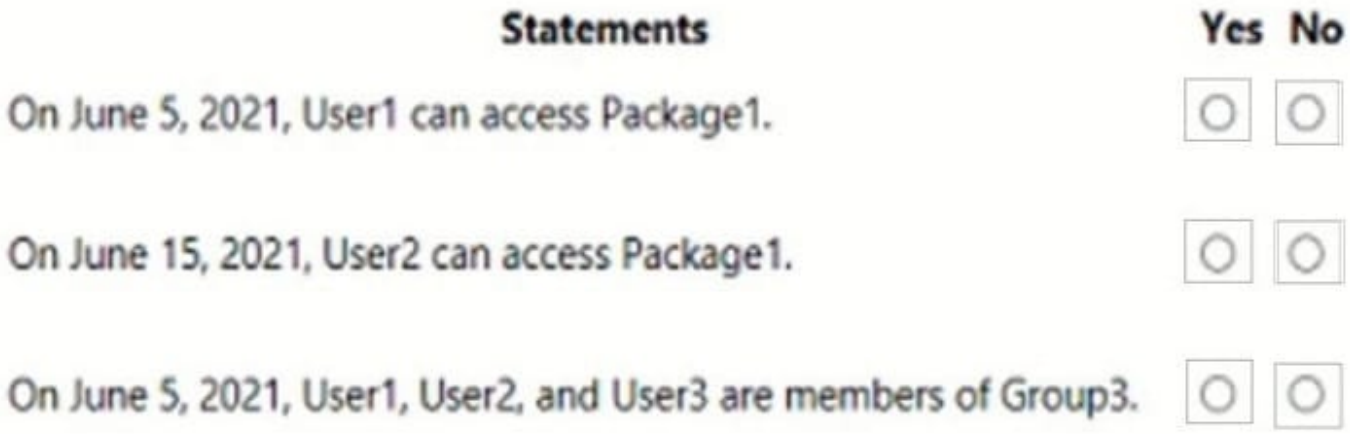
Assignment starts: June 1, 2021

4.

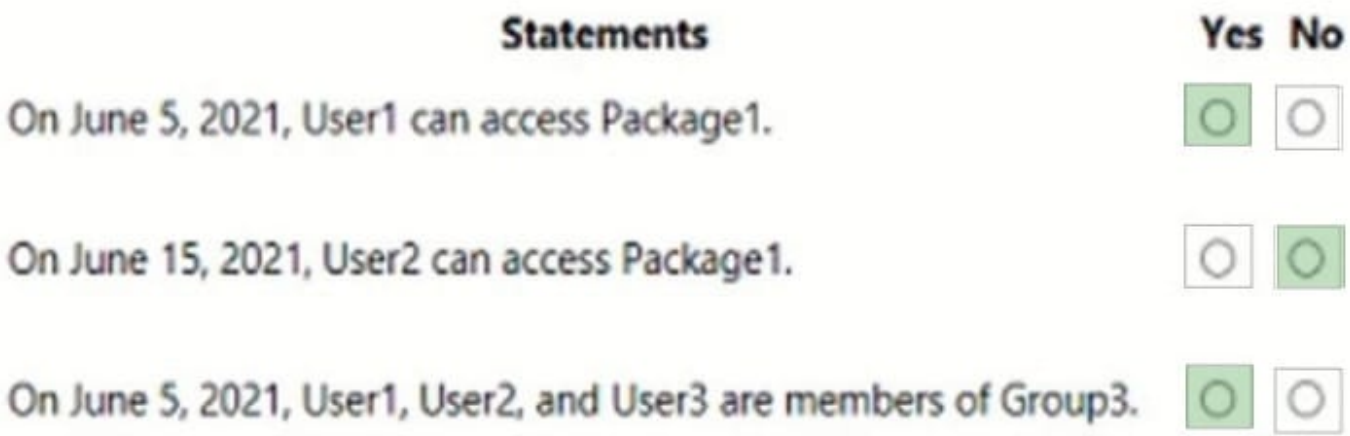
Assignment ends: July 1, 2021

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:



Correct Answer:



Box 1: Yes

Box 2: No Lifecycle, Access package assignments expires: After 10 days

Box 3: Yes The access package resource roles includes: Group3 Member Note: Entitlement management introduces to Azure AD the concept of an access package. An access package is a bundle of all the resources with the access a user needs to work on a project or perform their task. Access packages are used to govern access for your internal employees, and also users outside your organization. Here are the types of resources you can manage user\\'s access to, with entitlement management:

1.

Membership of Azure AD security groups

2.

Membership of Microsoft 365 Groups and Teams

3.

Assignment to Azure AD enterprise applications, including SaaS applications and custom-integrated applications that support federation/single sign-on and/or provisioning

4.

Membership of SharePoint Online sites

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview