KillTest

High Quality. Better Service

Practice Questions

https://www.killtest.com

Free updates for one year

Exam : **AB-650**

Title : Administering Microsoft 365 and AI Services (beta)

Version : DEMO

1.Topic: Manage and secure AI services in Microsoft 365
You have a Microsoft 365 tenant. You are preparing to deploy Microsoft 365 Copilot for your organization.
You need to prevent Microsoft 365 Copilot from generating responses based on documents stored in a specific SharePoint Online site named "Project_Alpha". The documents within this site do not currently have any sensitivity labels applied, but they contain highly confidential merger discussions.
What should you do?
A. From the Microsoft Purview compliance portal, create a Data Loss Prevention (DLP) policy that blocks access to the Project_Alpha site.
B. From the Microsoft Entra admin center, create a Conditional Access policy that targets Microsoft 365 Copilot and blocks access for all users.
C. From the SharePoint admin center, configure the site settings of Project_Alpha to exclude the site from Microsoft Search.
D. From the Microsoft 365 admin center, disable the Copilot for Microsoft 365 license for all users who are members of the Project_Alpha site.
Answer: C
Explanation:
Microsoft 365 Copilot relies on Microsoft Search to discover and ground its responses in tenant data. If a SharePoint site is excluded from Microsoft Search, Copilot will not be able to access or utilize the content within that site for its responses. This is the official and most direct method to prevent data exposure for unlabelled, highly sensitive sites. DLP (A) is for preventing data exfiltration, not Copilot grounding. Conditional Access (B) controls user sign-ins. Disabling licenses (D) stops the *users* from using Copilot, but does not protect the site's data from *other* users who have Copilot licenses.

2.Topic: Govern and secure Microsoft 365 tenants and workloads
Your organization uses Microsoft Defender for Office 365.
You are investigating a recent increase in sophisticated credential harvesting attempts targeting your finance department. You need to configure a policy that proactively protects these users from malicious URLs in emails, Microsoft Teams messages, and supported Office apps, while also identifying which users are most susceptible to these attacks to mandate further education.
Which two actions should you perform? Each correct answer presents part of the solution.
A. Configure a Safe Attachments policy with the "Dynamic Delivery" option enabled for the finance department.
B. Create a Safe Links policy in Microsoft Defender for Office 365 and apply it to the finance department.
C. Run a credential harvest training campaign using Attack simulation training in Microsoft Defender for Office 365.
D. Enable Microsoft Entra ID Protection user risk policies to require a password change for high-risk users.
E. Deploy a Microsoft Purview Data Security Posture Management (DSPM) policy targeting the finance department's SharePoint sites.
Answer: B, C
Explanation:
To proactively protect users from malicious URLs across Exchange, Teams, and Office apps, you must configure a Safe Links policy (B). To identify which users are susceptible to credential harvesting (as

mentioned in the scenario) and mandate education, you must use Attack simulation training (C). Safe Attachments (A) protects against malicious files, not URLs. Entra ID Protection (D) responds to compromised accounts but doesn't prevent the URL click or simulate attacks for training. Purview DSPM (E) is for data security posture, not email threat protection.

3.Topic: Manage and secure AI services in Microsoft 365
You are the Microsoft 365 and AI services administrator for your company.
An internal development team has built a custom conversational agent to assist HR with onboarding. You need to make this agent available *only* to the HR department via the agent registry, ensuring proper lifecycle and security governance.
Which four actions should you perform in sequence?
[Actions List]
1. The development team submits the custom agent to the organization's agent registry.
2. Publish the agent and restrict access to the HR Department's Microsoft 365 group.
3. Review the custom agent's data privacy, permissions, and compliance details in the agent registry.
4. Approve the custom agent request in the agent registry.
5. Create a Conditional Access policy in Microsoft Entra ID to block third-party AI providers.
Answer:
1 -> 3 -> 4 -> 2
Explanation:
The correct lifecycle workflow for custom agents in Agent 365 is: First, the agent is submitted to the registry by the developer (1). Next, the administrator must review the agent's details and compliance scope (3). Upon successful review, the admin approves the request (4). Finally, the admin publishes the agent and configures access controls, limiting it to the specific HR group (2). Action 5 is a distractor and not part of the agent registry approval lifecycle.

4.Topic: Configure and manage Microsoft 365 tenants and workloads
You have a Microsoft 365 tenant. You are preparing to assign Microsoft 365 Copilot licenses to 500 users.
Before assigning the licenses, you must ensure that every user has a valid usage location configured, as required by Microsoft's licensing model. You have a CSV file containing the users and their locations.
You decide to use Microsoft Graph PowerShell to perform a bulk update.
How should you complete the Microsoft Graph PowerShell command?
Select the correct parameters from the dropdown options.
`[Dropdown 1] -UserId $user.Id [Dropdown 2] $user.LocationCode`
[Dropdown 1 Options]
- `Set-MgUser`
- `Update-MgUser`
- `Set-MgUserProfile`

[Dropdown 2 Options]
- `-Country`
- `-UsageLocation`
- `-Location`

Answer:

`Update-MgUser` AND `-UsageLocation`

Explanation:

In Microsoft Graph PowerShell, the correct cmdlet to modify properties of an existing user is `Update-MgUser`. The specific parameter required by Microsoft 365 licensing to define the country for billing and service availability is `-UsageLocation`.

5.Topic: Govern and secure Microsoft 365 tenants and workloads

You are utilizing Microsoft Purview to protect data in your Microsoft 365 tenant.

You need to ensure that Microsoft 365 Copilot cannot summarize or process specific documents containing credit card numbers and passport information, regardless of where these documents reside in SharePoint or OneDrive.

What is the most administratively efficient method to achieve this requirement?

A. Create a Data Loss Prevention (DLP) policy that detects credit card and passport Sensitive Information Types (SITs) and configure the action to block Copilot access.

B. Create a retention label policy that applies to documents containing credit card and passport information, and set the retention period to 0 days.

C. Configure SharePoint Advanced Management to run a data access governance report on all sites containing credit card numbers.

D. Publish an auto-labeling policy that applies a sensitivity label configured with "EXTRACT_ALLOWED=FALSE" (usage rights) to documents containing the specific Sensitive Information Types.

Answer: D

Explanation:

To prevent Copilot from processing specific sensitive data globally, the best practice is to use Microsoft Purview Information Protection. By automatically applying a sensitivity label that removes the "View Rights" for the Copilot application (technically enforced via rights management/encryption where extraction is not allowed), Copilot is cryptographically blocked from reading the file contents. DLP policies (A) are currently used to prevent the *output* of Copilot from being shared inappropriately or to block users from pasting sensitive data *into* prompts, but sensitivity labels are the primary mechanism for locking down the underlying files from Copilot's indexing and summarization.