MS-101^{Q&As}

Microsoft 365 Mobility and Security

Pass Microsoft MS-101 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ms-101.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 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune.

You plan to purchase volume-purchased apps and deploy the apps to the devices.

You need to track used licenses and manage the apps by using Intune.

What should you use to purchase the apps?

A. Microsoft Store for Business

B. Apple Business Manager

C. Apple iTunes Store

D. Apple Configurator

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

QUESTION 2

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

A. Device 1, Device2, and Device3 only

B. Device3onry

C. Device2 and Device3 only

D. Device1, Device2, Devices and Device4

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

QUESTION 3

DRAG DROP

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

1.

Use a file plan to manage retention labels.

2.

Identify, monitor, and automatically protect sensitive information.

3.

Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or

scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Solutions

Data loss prevention
Information governance
Insider risk management
Records management

Identify, monitor, and automatically protect sensitive information:	Solution
Capture employee communications for examination by designated reviewers:	Solution
Use a file plan to manage retention labels:	Solution

Correct Answer:

Solutions

	Records management
Identify, monitor, and automatically protect sensitive information:	Data loss prevention
Capture employee communications for examination by designated reviewers:	Insider risk management
Use a file plan to manage retention labels:	Information governance

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide

QUESTION 4

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

A. Enable Microsoft 365 usage analytics.

B. Create a communication compliance policy.

C. Enable auditing.

D. Create an Insider risk management policy.

Correct Answer: C

Explanation:

Manage auditing and alert policies, Alert policies in Microsoft 365.

Default alert policy includes:

Elevation of Exchange admin privilege - Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in

Exchange Online. This policy has a Low severity setting.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

QUESTION 5

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

A. only the settings of Policy!

B. only the settings of Policy2

C. only the settings of Policy3

D. no settings

Correct Answer: C

MS-101 PDF Dumps   MS-101 Practice Test   MS-101 Study Guide