Prepare security and compliance to support Microsoft 365 Copilot (MS-40020)

Duration: 1 Day **Course Code: M-MS4002** **Delivery Method: Virtual Learning**

Overview:

This learning path examines the key Microsoft 365 security and compliance features that administrators must prepare in order to successfully implement Microsoft 365 Copilot.
This course has been created by Microsoft as a "Bring Your Own Environment" course, allowing individuals to use their personal devices and settings. If a student wants to complete the hands-on activities, the individual must bring their own CoPilot environment. Otherwise, demonstrations and lectures will be conducted by the instructor

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Prerequisites:

- Students should have basic functional experience with Microsoft 365 services.
- Students must have a proficient understanding of general IT practices.

Content:

1- Implement Microsoft 365 Copilot

- Identify the prerequisites for Microsoft 365 Copilot.
- Implement SharePoint Advanced Management to prepare for Microsoft 365 Copilot.
- Prepare your data for Microsoft 365 Copilot searches.
- Assign your Microsoft 365 Copilot licenses.
- Identify Microsoft 365 security features that control oversharing of data in Microsoft 365 Copilot.
- Explain how Copilot agents extend Microsoft 365 Copilot.
- Drive adoption by creating a Copilot Center of Excellence.

2- Manage secure user access in Microsoft 365

- Manage user passwords.
- Create Conditional Access policies.
- Enable security defaults.
- Describe pass-through authentication.
- Enable multifactor authentication.
- Describe self-service password management.
- Implement Microsoft Entra Smart Lockout.

3- Manage permissions, roles, and role groups in Microsoft 365

- Understand how roles are used in the Microsoft 365 ecosystem.
- Describe the Azure role-based access control permission model used in Microsoft 365.
- Identify the key tasks assigned to the common Microsoft 365 admin roles.
- Identify best practices when configuring admin roles.
- Delegate admin roles to partners.
- Implement role groups in Microsoft 365.
- Manage permissions using administrative units in Microsoft Entra ID.
- Manage permissions in SharePoint to prevent oversharing of data.
- Elevate privileges to access admin centers by using Microsoft Entra ID Privileged Identity Management.

4- Deploy Microsoft 365 Apps for enterprise

- Describe the Microsoft 365 Apps for enterprise functionality.
- Plan a deployment strategy for Microsoft 365 Apps for enterprise.
- Complete a user-driven installation of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager.
- Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
- Describe how to manage Microsoft 365 Apps for enterprise updates.
- Determine which update channel and application method applies for your organization.
- Add Microsoft 365 Apps for enterprise to Microsoft Intune.
- Deploy Microsoft 365 Apps for enterprise security baseline.

5- Implement Microsoft Purview Data Loss Prevention

- Create a data loss prevention implementation plan. Implement Microsoft 365's default DLP policy.
- Create a custom DLP policy from a DLP template and from scratch.
- Create email notifications and policy tips for users when a DLP rule applies.
- Create policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

6- Implement sensitivity labels

- Create a deployment strategy for implementing sensitivity labels that satisfies your organization's requirements.
- Enable sensitivity labels in SharePoint Online and OneDrive so they can use encrypted files.
- Create and configure sensitivity labels.
- Publish sensitivity labels by creating a label policy.
- Identify the differences between removing and deleting sensitivity labels.

7- Manage Microsoft 365 Copilot extensibility

- Manage Copilot agents in integrated apps.
- Create a connection between a data source and a Microsoft Graph connector.
- Monitor your organization's Microsoft Graph connectors.
- Manage how Microsoft Graph connector content is displayed in Microsoft Copilot.

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE