email : techcenter@trainocate.com.my
contact : +603-2281-1111

MS-4002: Prepare security and compliance to support Microsoft 365 Copilot

Course Code: MS-4002
Duration: 1 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

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.

SKILLS COVERED

- Implement Microsoft 365 Copilot
- Manage secure user access in Microsoft 365
- Manage permissions, roles, and role groups in Microsoft 365
- Deploy Microsoft 365 Apps for enterprise
- Implement Microsoft Purview Data Loss Prevention
- Implement sensitivity labels
- Manage Microsoft 365 Copilot extensibility

WHO SHOULD ATTEND?

- Administrator
- Functional Consultant
- Solution Architect
- Technology Manager

PREREQUISITES

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

MODULES

Module 1: Implement Microsoft 365 Copilot

This module examines the key tasks that administrators must complete when implementing Microsoft 365 Copilot, such as completing prerequisites, preparing data for searches, assigning Copilot licenses, and extending Copilot.

Learning objectives

By the end of this module, you should be able to:

- 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.

Prerequisites

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

Module 2: Manage secure user access in Microsoft 365

This module examines the various features provided in the Microsoft 365 ecosystem for securing user access, such as Conditional Access policies, multifactor authentication, self-service password management, Smart Lockout policies, and security defaults.

Learning objectives

By the end of this module, you should be able to:

- 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.

Prerequisites

None

Module 3: Manage permissions, roles, and role groups in Microsoft 365

This module examines the use of roles and role groups in the Microsoft 365 permission model, including role management, best practices when configuring admin roles, delegating roles, and elevating privileges.

Learning objectives

By the end of this module, you should be able to:

- 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.

Prerequisites

None

Module 4: Deploy Microsoft 365 Apps for enterprise

This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.

Learning objectives

By the end of this module, you should be able to:

- 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.

Prerequisites

- None

Module 5: Implement Microsoft Purview Data Loss Prevention

This module examines how organizations can use Microsoft Purview Data Loss Prevention to help protect sensitive data and define the protective actions that organizations can take when a DLP rule is violated.

Learning objectives

By the end of this module, you should be able to:

- 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

Prerequisites

None

Module 6: Implement sensitivity labels

This module examines the process for implementing sensitivity labels, including applying proper administrative permissions, determining a deployment strategy, creating, configuring, and publishing labels, and removing and deleting labels.

Learning objectives

By the end of this module, you should be able to:

- 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.

Prerequisites

None

Module 7: Manage Microsoft 365 Copilot extensibility

This module examines the tasks that administrators must perform to manage Microsoft 365 Copilot extensibility, such as managing Copilot agents and creating and monitoring connectors.

Learning objectives

By the end of this module, you should be able to:

- 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.

Prerequisites

- None

OF PAGE