MS-MS4002: PREPARE SECURITY AND COMPLIANCE TO SUPPORT MICROSOFT 365 COPILOT

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Microsoft 365	Instructor-led	NA

INTRODUCTION

This learning path examines the key Microsoft 365 security and compliance features that administrators must prepare in order to successfully implement Microsoft 365 Copilot.

AUDIENCE PROFILE

This course is designed for professionals who want to build and manage intelligent search solutions using Azure AI. The primary audience includes:

- AI Engineers
- Solution Architects

PREREQUISITES

Before attending this course, delegates must have:

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

COURSE OBJECTIVES

After completing this course, students will be able to:

- Manage secure user access using multifactor authentication and Conditional Access policies.
- Implement app protection with Microsoft Defender for Cloud Apps and manage cloud security policies.
- Utilize Microsoft Defender for Endpoint to detect and respond to advanced threats on devices.
- Deploy Microsoft Defender for Office 365 to safeguard against email and collaboration threats.
- Apply retention policies and labels to ensure compliance and protect sensitive data.
- Implement Microsoft Purview Information Barriers and Microsoft Purview Data Loss Prevention to enhance data protection.

COURSE CONTENT

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.

Lessons

- Introduction
- Get ready for Microsoft 365 Copilot
- Implement SharePoint Advanced Management tools to prepare for Microsoft 365 Copilot
- Prepare your data for searches in Microsoft 365 Copilot
- Protect your Microsoft 365 Copilot data with Microsoft 365 security tools
- Assign your Microsoft 365 Copilot licenses
- Extend Microsoft 365 Copilot
- Drive Microsoft 365 Copilot adoption throughout your organization
- Knowledge check
- Summary

By the end of this module, you'll 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.

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.

Lessons

- Introduction
- Examine the identity and access tools used in Microsoft 365
- Manage user passwords

- Implement Conditional Access policies
- Enable pass-through authentication
- Implement multifactor authentication
- Explore passwordless authentication options
- Explore self-service password management
- Implement Microsoft Entra Smart Lockout
- Explore Security Defaults in Microsoft Entra ID
- Investigate authentication issues using sign-in logs
- Knowledge check
- Summary

By the end of this module, you'll 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.

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.

Lessons

- Introduction
- Examine the use of roles in the Microsoft 365 permission model
- Manage roles across the Microsoft 365 ecosystem
- Explore administrator roles in Microsoft 365
- Examine best practices when configuring administrative roles
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Implement role groups in Microsoft 365
- Manage permissions using administrative units in Microsoft Entra ID
- Manage SharePoint permissions to prevent oversharing of data
- Elevate privileges using Microsoft Entra Privileged Identity Management
- Knowledge check
- Summary

By the end of this module, you'll 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.

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.

Lessons

- Introduction
- Explore Microsoft 365 Apps for enterprise functionality
- Complete a self-service installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Configuration Manager
- Deploy Microsoft 365 Apps for enterprise from the cloud
- Deploy Microsoft 365 Apps for enterprise from a local source
- Manage updates to Microsoft 365 Apps for enterprise
- Explore the update channels for Microsoft 365 Apps for enterprise
- Manage your cloud apps using the Microsoft 365 Apps admin center
- Add Microsoft 365 Apps for enterprise to Microsoft Intune
- Deploy Microsoft 365 Apps for enterprise security baseline
- Knowledge check
- Summary

In this module you'll learn how 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.

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.

Lessons

- Introduction
- Plan to implement Microsoft Purview Data Loss Protection
- Implement Microsoft Purview's default DLP policies
- Design a custom DLP policy
- Create a custom DLP policy from a template
- Configure email notifications for DLP policies
- Configure policy tips for DLP policies
- Knowledge check
- Summary

In this module you'll learn how 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

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.

Lessons
- Introduction
- Plan your deployment strategy for sensitivity labels
- Enable sensitivity labels for files in SharePoint and OneDrive
- Examine the requirements to create a sensitivity label
- Create sensitivity labels
- Publish sensitivity labels
- Remove and delete sensitivity labels
- Knowledge check
- Summary

In this module you'll learn how 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.

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.

Lessons
- Introduction
- Manage Copilot agents in integrated apps
- Create a connection between a data source and a Microsoft Graph connector
- Monitor your Microsoft Graph connectors
- Manage how Microsoft Graph connector content is displayed in Microsoft 365 Copilot
- Knowledge check
- Summary

In this module you'll learn how 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.

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or Exam for this course, however, there is an assessment to achieve your Applied Skills credential. (Assessment Link)