

MS-4006: Microsoft 365 Copilot for Administrators

Duration: 1 Day

Course Description:

This course focuses on the design, deployment, security, compliance, and administration of Microsoft 365 Copilot. Learners will understand how to prepare their Microsoft 365 environment, secure organizational data, manage permissions, and implement governance controls before enabling Copilot for users.

Course Outlines:

Module 1: Examine the Microsoft 365 Copilot Design

- Introduction
- Examine the Microsoft 365 Copilot Logical Architecture
- Examine the Key Components of Microsoft 365 Copilot
- Explore the Microsoft 365 Copilot Service and Tenant Architecture
- Extend Microsoft 365 Copilot with Plugins and Microsoft Graph Connectors

Module 2: Implement Microsoft 365 Copilot

- Introduction
- Get Ready 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
- Drive Microsoft 365 Copilot Adoption with a Copilot Centre of Excellence

Module 3: Examine Data Security and Compliance in Microsoft 365 Copilot

- Introduction
- Examine How Microsoft 365 Copilot Uses Your Proprietary Business Data
- Examine How Microsoft 365 Copilot Protects Sensitive Business Data
- Examine How Microsoft 365 Copilot Uses Microsoft 365 Isolation and Access Controls
- Examine How Microsoft 365 Copilot Meets Regulatory Compliance Mandates

Module 4: Manage Secure User Access in Microsoft 365

- 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

Module 5: Manage Permissions, Roles, and Role Groups in Microsoft 365

- 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

Module 6: Implement Data Classification of Sensitive Information

- Introduction
- Explore Data Classification
- Implement Data Classification in Microsoft 365
- Explore Trainable Classifiers
- Create and Retrain a Trainable Classifier
- View Sensitive Data Using Content Explorer and Activity Explorer
- Detect Sensitive Information Documents Using Document Fingerprinting

Module 7: Explore Sensitivity Labels

- Introduction
- Manage Data Protection Using Sensitivity Labels
- Explore What Sensitivity Labels Can Do
- Determine a Sensitivity Label's Scope
- Apply Sensitivity Labels Automatically
- Explore Sensitivity Label Policies

Module 8: Implement Sensitivity Labels

- 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

REGISTER NOW!

training@trends.com.ph
(+632) 8863-2123
www.trendssacademy.com.ph