

MS-4006: Microsoft 365 Copilot for Administrators

Course Duration: 8 Hours

Course code: MS-4006

1. Course Overview

MS-4006 is a **one-day, instructor-led course** that introduces administrators to the design and architecture of Microsoft 365 Copilot, with a strong emphasis on security and compliance measures that must be in place before deploying Copilot in a Microsoft 365 tenant.

2. What You'll Learn

- Explore the **architecture and design** of Copilot for Microsoft 365
 - Prepare and **implement Copilot** in your tenant environment
 - Understand and apply **security and compliance controls** relevant to Copilot deployments
 - Manage **secure user access**, authentication, roles, and permissions
 - Apply **data classification** methodologies and implement **sensitivity labels** to protect sensitive information
-

3. Target Audience

This course is intended for:

- Microsoft 365 Administrators
- IT professionals aspiring to a Microsoft 365 Administrator role
- Security or Compliance Officers involved in Copilot rollout

These individuals typically should have completed at least one Microsoft 365 role-based administrator certification path.

4. Pre-Requisites

Participants are expected to have:

- Completed at least one Microsoft 365 role-based administrator training (e.g., Messaging, Security & Compliance, Teamwork)
- Basic functional experience with Microsoft 365 services and an understanding of general IT practices; familiarity with PowerShell is recommended
- A general awareness of how Copilot functions

5. Course Content (Modules)

Module 1: Examine the Copilot for Microsoft 365 Design

- Copilot logical architecture, components, service/tenant design, plugins, Graph connectors

Module 2: Implement Copilot for Microsoft 365

- Readiness, data preparation, licensing, security tooling, adoption strategies such as Copilot Center of Excellence

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

- Data usage, protection, access controls, compliance alignment

Module 4: Manage Secure Access in Microsoft 365

- Identity tools, password management, Conditional Access, MFA, passwordless options, sign-in log investigations

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

- Admin roles, delegation to partners, role groups, administrative units, PIM, SharePoint permissions

Module 6: Implement Data Classification of Sensitive Information

- Classification strategies, trainable classifiers, content/activity explorer, document fingerprinting

Module 7: Explore Sensitivity Labels

- Label capabilities, scope, auto-application, policies

Module 8: Implement Sensitivity Labels

- Deployment planning, enabling for SharePoint/OneDrive, label creation, publishing, removal/deletion

