

**Copilot for Microsoft 365 for Administrators (MS-4006)**

**Course Number:** MOC-MS-4006
**Duration:** 1 day

**Overview**

This Copilot for Microsoft 365 for Administrators (MS-4006) course begins by examining the Microsoft Copilot for Microsoft 365 design and then focuses on the security and compliance features. Administrators learn how to configure their Microsoft 365 tenant to protect their company's organizational data before implementing Copilot for Microsoft 365.

**Prerequisites**

This Copilot for Microsoft 365 course is designed for administrators, Microsoft 365 administrators, or persons aspiring to the Microsoft 365 Administrator role who have completed at least one of the Microsoft 365 role-based administrator certification paths.

**Materials**

All Microsoft 365 training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computer for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will be fine.

**Objectives**

* Understand the Microsoft Copilot for Microsoft 365 design and how it works
* Grasp the key tasks administrators must complete when implementing Microsoft Copilot for Microsoft 365
* Understand how Microsoft Copilot for Microsoft 365 adheres to existing privacy and compliance obligations
* Implement the various features provided in the Microsoft 365 ecosystem for securing user access
* Use roles and role groups in the Microsoft 365 permission model
* Use sensitivity labels from the Microsoft Information Protection solution to classify and protect data
* Implement sensitivity labels and apply for proper administrative permissions

**Outline**

* Examine the Copilot for Microsoft 365 design
	+ Examine the Copilot for Microsoft 365 logical architecture
	+ Examine the key components of Copilot for Microsoft 365
	+ Explore the Copilot for Microsoft 365 service and tenant architecture
	+ Extend Copilot for Microsoft 365 with plugins and Microsoft Graph connectors
* Implement Copilot for Microsoft 365
	+ Get ready for Copilot for Microsoft 365
	+ Prepare your data for searches in Copilot for Microsoft 365
	+ Protect your Copilot for Microsoft 365 data with Microsoft 365 security tools
	+ Assign your Copilot for Microsoft 365 licenses
	+ Drive Copilot for Microsoft 365 adoption with a Copilot Center of Excellence
* Examine data security and compliance in Copilot for Microsoft 365
	+ Examine how Copilot for Microsoft 365 uses your proprietary business data
	+ Examine how Copilot for Microsoft 365 protects sensitive business data
	+ Examine how Copilot for Microsoft 365 uses Microsoft 365 isolation and access controls
	+ Examine how Copilot for Microsoft 365 meets regulatory compliance mandates
* Manage secure user access in Microsoft 365
	+ Examine the identity and access tools used in Microsoft 365
	+ Manage user passwords
	+ Implement Conditional Access policies
	+ Enable pass-through authentication
	+ Implement multifactor authentication
	+ Enable passwordless sign-in with Microsoft Authenticator
	+ Explore self-service password management
	+ Explore Windows Hello for Business
	+ Implement Microsoft Entra Smart Lockout
	+ Explore Security Defaults in Microsoft Entra ID
	+ Investigate authentication issues using sign-in logs
* Manage permissions, roles, and role groups in Microsoft 365
	+ 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
* Implement data classification of sensitive information
	+ 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
* Explore sensitivity labels
	+ 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
* Implement sensitivity labels
	+ Plan your deployment strategy for sensitivity labels
	+ Examine the requirements to create a sensitivity label
	+ Create sensitivity labels
	+ Publish sensitivity labels
	+ Remove and delete sensitivity labels