

## KOENIG SOLUTIONS · COURSE OUTLINE

# MS-4006-A: Copilot for Microsoft 365 for Administrators

Learn to deploy, secure and administer Copilot for Microsoft 365, from architecture and data protection to access and sensitivity labels.

**1 Day**

8 HOURS

**8**

MODULES

**36**

TOPICS

**18**

HANDS-ON LABS

## COURSE OVERVIEW

The MS-4006-A: Copilot for Microsoft 365 for Administrators certification is designed to validate the skills required to manage and optimize Microsoft 365 services effectively. It focuses on deploying, configuring, and securing Microsoft 365 applications for any organizational environment. The certification ensures that administrators are proficient in handling the suite's tools to enhance productivity, collaboration, and communication. Industries leverage this certification to ensure their IT staff can fully utilize Microsoft 365 capabilities, align IT infrastructure with business goals, improve operational efficiencies, and maintain a secure and compliant digital workspace, thus facilitating seamless technological integration and better management of cloud services.

## WHO THIS COURSE IS FOR

**IT professionals and administrators responsible for managing Microsoft 365 environments**

**Individuals seeking to enhance their skills in deploying, configuring, and maintaining Microsoft 365 services**

**Persons interested in understanding and utilizing the full capabilities of Copilot for Microsoft 365**

## LEARNING OBJECTIVES

- Explain the Copilot for Microsoft 365 logical architecture and components
- Identify prerequisites for implementing Copilot for Microsoft 365
- Describe how Copilot data is protected using Microsoft 365 security tools
- Assess how Copilot uses proprietary business data securely
- Configure secure user access with MFA and Conditional Access
- Implement roles and role groups for Microsoft 365 administration
- Apply data classification using trainable classifiers and fingerprinting
- Create and publish sensitivity labels for sensitive information

## 8 Modules, 36 Topics

01

5 Labs

### Examine the Copilot for Microsoft 365 Design

#### TOPICS

- The Copilot for Microsoft 365 logical architecture
- The key components of Copilot for Microsoft 365
- The Copilot for Microsoft 365 service and tenant architecture
- Extending Copilot for Microsoft 365 with Microsoft Graph connectors

02

### Implement Copilot for Microsoft 365

#### TOPICS

- Complete the prerequisites 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 Centre of Excellence

03

### Examine Data Security and Compliance in Copilot for Microsoft 365

#### TOPICS

- Uses an organization's proprietary business data
- Protects sensitive business data
- Uses Microsoft 365 isolation and access controls
- Meets regulatory compliance mandates

**04****5 Labs**

## Manage Secure User Access in Microsoft 365

### TOPICS

- Password policies and authentication
- Microsoft Entra Pass-Through Authentication (PTA) and Multifactor authentication (MFA)
- Passwordless sign-in with Microsoft Authenticator
- Self-service Password Management and Windows Hello for Business
- Microsoft Entra Smart Lockout and Conditional access policies
- Microsoft Entra Security Defaults

**04****4 Labs**

## Manage Roles and Role Groups in Microsoft 365

### TOPICS

- Microsoft 365 permission model
- Microsoft 365 admin roles and best practices
- Implement roles and role groups in Microsoft 365
- Delegate admin roles to partners
- Manage permissions using administrative units in Microsoft Entra ID
- Elevate privileges

**05**

## Implement Data Classification of Sensitive Information

### TOPICS

Data classification in Microsoft 365 · Trainable classifiers · Viewing sensitive data · Document fingerprinting

**06**

## Explore Sensitivity Labels

### TOPICS

Insider risk management policies · Insider risk management activities and alerts · Insider risk management cases

**06****4 Labs**

## Implement Sensitivity Labels

### TOPICS

Sensitivity label requirements · Developing a data classification framework · How to create and publish sensitivity labels · How to remove and delete sensitivity labels

# Practise What You Learn

| #  | MODULE                                               | ACTIVITY                                                                                                                                                                                                                                                                                                                                  |
|----|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01 | <b>Examine the Copilot for Microsoft 365 Design</b>  | <ul style="list-style-type: none"> <li>■ Obtain your Microsoft 365 credentials</li> <li>■ Set up Datum's organization profile</li> <li>■ Create a custom theme for Adatum's pilot project team</li> <li>■ Install Microsoft Graph PowerShell</li> <li>■ Turn on Audit Logging to enable Alert policies</li> </ul>                         |
| 04 | <b>Manage Secure User Access in Microsoft 365</b>    | <ul style="list-style-type: none"> <li>■ Create a user account for Adatum's Enterprise Administrator</li> <li>■ Set up Microsoft 365 user account passwords</li> <li>■ Deploy MFA using a Conditional Access policy</li> <li>■ Test MFA for both an included and excluded user</li> <li>■ Deploy Microsoft Entra Smart Lockout</li> </ul> |
| 04 | <b>Manage Roles and Role Groups in Microsoft 365</b> | <ul style="list-style-type: none"> <li>■ Assign an administrator role in the Microsoft 365 admin centre</li> <li>■ Assign an administrator role using a role group in the Microsoft 365 admin centre</li> <li>■ Assign an administrator role using Windows PowerShell</li> <li>■ Validate role assignments</li> </ul>                     |
| 06 | <b>Implement Sensitivity Labels</b>                  | <ul style="list-style-type: none"> <li>■ Install the Azure Information Protection Unified Labeling client</li> <li>■ Create a sensitivity label</li> <li>■ Assign a pre-existing Sensitivity Label to a document</li> <li>■ Verify the pre-existing Sensitivity Label policy</li> </ul>                                                   |

#### WHAT IS INCLUDED

## Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

#### ABOUT KOENIG

## Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

#### FLEXIBLE DELIVERY

## Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

## Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit [koenig-solutions.com](https://koenig-solutions.com)

✉ [info@koenig-solutions.com](mailto:info@koenig-solutions.com)