

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

Duration – 1 Day

Content:

Module No. 1: Examine the Copilot for Microsoft 365 design

Lessons:

- 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

Labs:

- Obtain your Microsoft 365 credentials
- Set up Adatum's organization profile
- Create a custom theme for Adatum's pilot project team
- Install Microsoft Graph PowerShell
- Turn on Audit Logging to enable Alert policies

Module No. 2: Implement Copilot for Microsoft 365

Lessons:

- 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

Module No. 3: Examine data security and compliance in Copilot for Microsoft 365

Lessons:

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

Module No. 4: Manage secure user access in Microsoft 365

Lessons:

- 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

Labs:

- Create a user account for Adatum's Enterprise Administrator
- Set up Microsoft 365 user account passwords
- Deploy MFA using a Conditional Access policy
- Test MFA for both an included and excluded user
- Deploy Microsoft Entra Smart Lockout

Module No. 4: Manage roles and role groups in Microsoft 365

Lessons:

- 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

Labs:

- Assign an administrator role in the Microsoft 365 admin center
- Assign an administrator role using a role group in the Microsoft 365 admin center
- Assign an administrator role using Windows PowerShell
- Validate role assignments

Module No. 5: Implement data classification of sensitive information

Lessons:

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

Module No. 6: Explore sensitivity labels

Lessons:

- Insider risk management policies

- Insider risk management activities and alerts
- Insider risk management cases

Module No. 6: Implement sensitivity labels

Lessons:

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

Labs:

- Install the Azure Information Protection Unified Labeling client
- Create a sensitivity label
- Assign a pre-existing Sensitivity Label to a document
- Verify the pre-existing Sensitivity Label policy