

MS-4002: Prepare security and compliance to support Microsoft 365 Copilot

Course Outline

1) Manage secure user access in Microsoft 365

- Manage user passwords
- Create Conditional Access policies
- Enable security defaults
- Describe pass-through authentication
- Enable multifactor authentication
- Describe self-service password management
- Implement Microsoft Entra Smart Lockout

2) Implement app protection by using Microsoft Defender for Cloud Apps

- Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications
- Explain how to deploy Microsoft Defender for Cloud Apps
- Control your cloud apps with file policies
- Manage and respond to alerts generated by those policies
- Configure and troubleshoot Cloud Discovery

3) Implement endpoint protection by using Microsoft Defender for Endpoint

- Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Onboard supported devices to Microsoft Defender for Endpoint
- Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses
- Configure device discovery to help find unmanaged devices connected to your corporate network
- Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations

4) Implement threat protection by using Microsoft Defender for Office 365

- Describe the protection stack provided by Microsoft Defender for Office 365
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant
- Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization

5) Explore retention in Microsoft 365

- Explain how retention policies and retention labels work
- Identify the capabilities of both retention policies and retention labels

- Select the appropriate scope for a policy depending on business requirements
- Explain the principles of retention
- Identify the differences between retention settings and eDiscovery holds
- Restrict retention changes by using preservation lock

6) Implement Microsoft Purview Information Barriers

- Describe how information barriers can restrict or allow communication and collaboration among specific groups of users
- Describe the components of an information barrier and how to enable information barriers
- Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site
- Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint

7) Implement Microsoft Purview Data Loss Prevention

- Create a data loss prevention implementation plan
- Implement Microsoft 365's default DLP policy
- Create a custom DLP policy from a DLP template and from scratch
- Create email notifications and policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

8) Implement sensitivity labels

- Create a deployment strategy for implementing sensitivity labels that satisfies your organization's requirements
- Enable sensitivity labels in SharePoint Online and OneDrive so they can use encrypted files
- Create and configure sensitivity labels
- Publish sensitivity labels by creating a label policy
- Identify the differences between removing and deleting sensitivity labels