MS-4017: Manage and extend Microsoft 365 Copilot

Course Outline

1) Prepare your organization for Microsoft 365 Copilot

- Implement Microsoft 365 Copilot
  - Identify the prerequisites for Microsoft 365 Copilot
  - Implement SharePoint Advanced Management to prepare for Microsoft 365 Copilot
  - Prepare your data for Microsoft 365 Copilot searches
  - Assign your Microsoft 365 Copilot licenses
  - Identify Microsoft 365 security features that control oversharing of data in Microsoft 365 Copilot
  - Explain how Copilot agents extend Microsoft 365 Copilot
  - Drive adoption by creating a Copilot Center of Excellence
- Examine data security and compliance in Microsoft 365 Copilot
  - Describe how Microsoft 365 Copilot uses proprietary business data
  - Understand how Microsoft 365 Copilot protects sensitive business data
  - Describe how Microsoft 365 Copilot uses Microsoft 365 isolation and access controls
  - Understand how Microsoft 365 Copilot meets regulatory compliance mandates

2) Manage Microsoft 365 Copilot administration

- Apply principles of Zero Trust to Microsoft Copilots
  - Prepare for Microsoft Copilots using a Zero Trust security framework
  - Apply Zero Trust principles to your Microsoft Copilot and Microsoft 365 Copilot deployments
  - Understand Zero Trust recommendations for your Copilot configuration
  - Deploy and validate your data protection, identity and access, App Protection policies, device management protection, threat protection services, secure collaboration for Microsoft Teams, and minimum user permissions to data
- Manage Microsoft Copilot
  - Identify the differences between Microsoft Copilot and Microsoft 365 Copilot
  - Understand how Microsoft Copilot employs enterprise data protection
  - Manage Microsoft Copilot in Microsoft Edge
  - Manage Microsoft Copilot on mobile devices
- Manage Microsoft 365 Copilot
  - Manage Microsoft 365 Copilot settings
  - Manage web access for Microsoft 365 Copilot
  - Manage Copilot for Microsoft Teams meetings and events
  - Identify Microsoft Purview data protections for AI apps
  - Manage Microsoft Copilot on mobile devices
  - Secure data for AI apps using Microsoft Purview Data Security Posture Management (DSPM) for AI

- Monitor the value of Microsoft 365 Copilot through the Copilot Dashboard
- Track Microsoft 365 Copilot readiness and usage across your organization
- Monitor Microsoft 365 Copilot interactions using a communication compliance policy
- Delete your Microsoft Copilot interaction history

3) Prepare for Microsoft 365 Copilot extensibility

- Microsoft 365 Copilot extensibility fundamentals
  - Explain how Copilot and agents work together to create a personalized, intelligent assistant with the knowledge and skills unique to your business
  - Describe the types of agents and the wide spectrum of capabilities with which they can be customized
  - Explain how to ground your Copilot responses with multiple enterprise data sources for more relevant and reliable responses
- Choose a Microsoft 365 Copilot extensibility development path
  - Decide whether to extend Microsoft 365 Copilot using its existing orchestrator or to build a custom engine agent, based on specific needs and goals
  - Gain insights into the various development tools and methods available, whether they prefer pro-code or low-code/no-code solutions, and how to set up their development environment for building these extensions
  - Understand the different ways to extend Microsoft 365 Copilot, including using declarative agents, custom engine agents, plugins, and connectors
  - Explain data privacy and security considerations for developing each extensibility option
- Manage Microsoft 365 Copilot extensibility
  - Manage Copilot agents in integrated apps
  - Create a connection between a data source and a Microsoft Graph connector
  - Monitor your organization's Microsoft Graph connectors
  - Manage how Microsoft Graph connector content is displayed in Microsoft Copilot