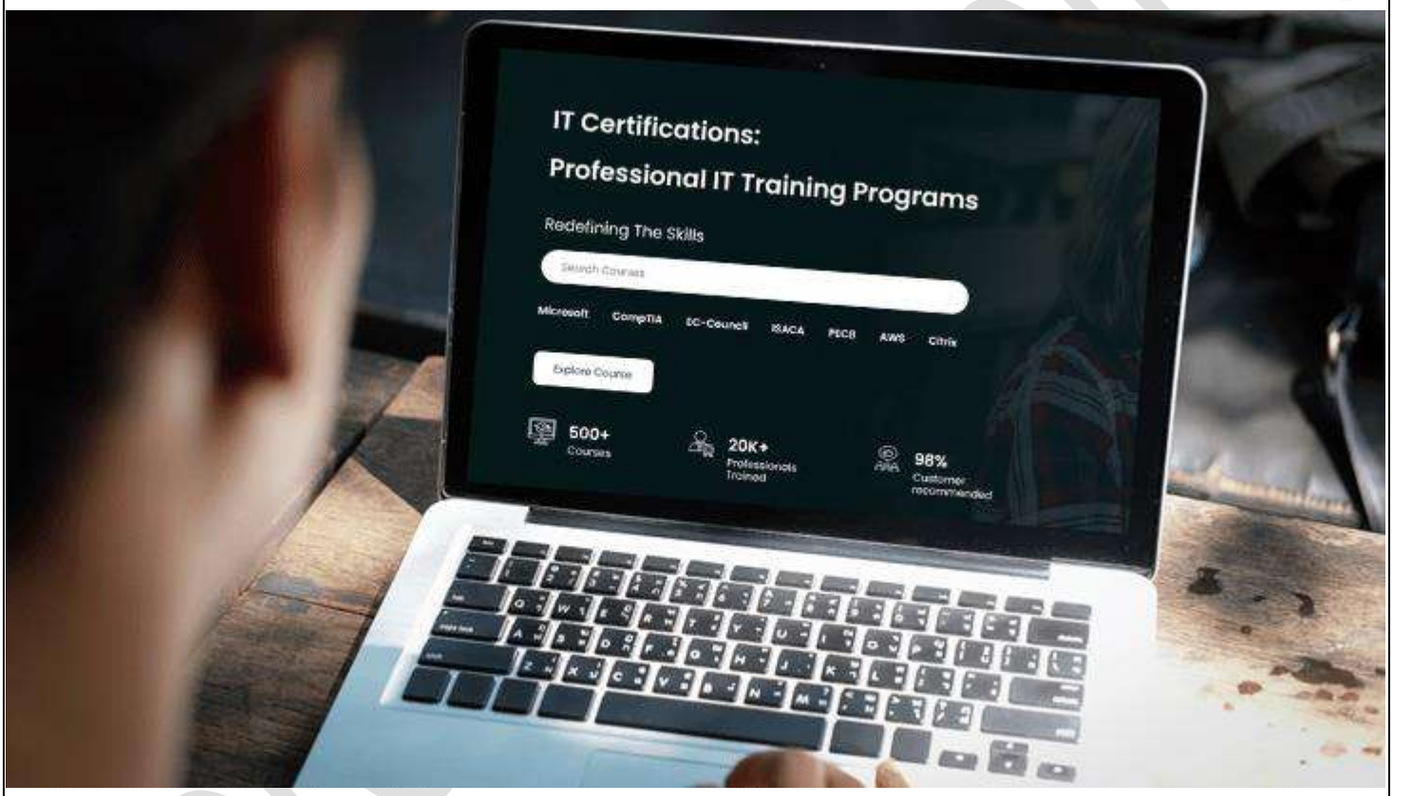
MICROTEK LEARNING | Redefining The Skills



SC-401T00: Protect sensitive information with Microsoft Purview in the AI era Training

DURATION: 4 DAYS

Course Description

The SC-401T00 course prepares you to protect sensitive data and manage information security across Microsoft 365 using Microsoft Purview. Whether you're stepping into this role for the first time or looking to sharpen your existing skills, this course gives you the confidence to implement policies that defend against both internal and external threats. You'll learn how to configure data loss prevention (DLP), apply retention labels, manage insider risks, and respond to security incidents effectively. The course also covers a rapidly growing area in today's compliance landscape—how to classify and protect data used within AI-driven Microsoft services. Built for IT and security administrators who work in collaborative environments, the SC-401 course prepares you to work alongside governance and compliance teams, manage alerts, conduct audits, and apply proven best practices for data protection.

Who should attend this course?

- Security Administrator
- Security Governance and Risk Manager

What you will learn

- Implement Microsoft Purview to classify, protect, and govern sensitive data.
- Configure data loss prevention (DLP) policies to prevent unauthorized data sharing.
- Manage insider risk using Microsoft Purview Insider Risk Management tools.
- Apply sensitivity labels and encryption to enhance data security in Microsoft 365.
- Secure AI environments by mitigating risks with Microsoft Purview solutions.
- Implement retention policies and labels to ensure compliance with data regulations.
- Investigate and respond to security incidents using Microsoft Purview Audit.
- Monitor and manage data security risks across Microsoft 365 collaboration tools.

Prerequisites

Required

- Familarity with all Microsoft 365 services, PowerShell, Microsoft Entra, the Microsoft Defender portal, and Microsoft Defender for Cloud Apps.

Recommended

- SC-900T00: Introduction to Microsoft Security, Compliance, and Identity

Curriculum

Module 1: Implement Microsoft Purview Information Protection

Protect sensitive data in a digital world

- Introduction
- The growing need for data protection
- The challenges of managing sensitive data
- Protect data in a Zero Trust world
- Understand data classification and protection
- Prevent data leaks and insider threats
- Manage security alerts and respond to threats
- Protect AI-generated and AI-processed data

Classify data for protection and governance

- Introduction
- Data classification overview
- Classify data using sensitive information types
- Classify data using trainable classifiers
- Create a custom trainable classifier

Review and analyze data classification and protection

- Introduction
- Review classification and protection insights
- Analyze classified data with data and content explorer
- Monitor and review actions on labeled data

Create and manage sensitive information types

- Introduction
- Sensitive information type overview
- Compare built-in versus custom sensitive information types
- Create and manage custom sensitive information types
- Create and manage exact data match sensitive info types
- Implement document fingerprinting
- Describe named entities
- Create a keyword dictionary

Create and configure sensitivity labels with Microsoft Purview

- Introduction
- Sensitivity label overview
- Create and configure sensitivity labels and label policies
- Configure encryption with sensitivity labels
- Implement auto-labeling policies
- Track and evaluate sensitivity label usage in Microsoft Purview

Apply sensitivity labels for data protection

- Introduction
- Foundations of sensitivity label integration in Microsoft 365
- Manage sensitivity labels in Office apps
- Apply sensitivity labels with Microsoft 365 Copilot for secure collaboration
- Protect meetings with sensitivity labels
- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites

Classify and protect on-premises data with Microsoft Purview

- Introduction
- Protect on-premises files with Microsoft Purview
- Prepare your environment for the Microsoft Purview Information Protection scanner
- Configure and install the Microsoft Purview Information Protection scanner
- Run and manage the scanner
- Enforce data loss prevention policies on on-premises files

Understand Microsoft 365 encryption

- Introduction to Microsoft 365 encryption
- Learn how Microsoft 365 data is encrypted at rest
- Understand service encryption in Microsoft Purview

- Explore customer key management using Customer Key
- Learn how data is encrypted in-transit

Protect email with Microsoft Purview Message Encryption

- Introduction
- Understand message encryption
- Plan for Microsoft Purview Message Encryption
- Configure Microsoft Purview Message Encryption
- Customize encrypted email branding with Microsoft Purview
- Control encrypted email access with Advanced Message Encryption
- Use Microsoft Purview Message Encryption templates in mail flow rules

Module 2: Implement and manage Microsoft Purview Data Loss Prevention

Prevent data loss with Microsoft Purview

- Introduction
- Data loss prevention overview
- Plan and design DLP policies
- Understand DLP policy deployment and simulation mode
- Create and manage DLP policies
- Integrate Adaptive Protection with DLP
- Use DLP analytics (preview) to identify data risks
- Understand DLP alerts and activity tracking

Implement endpoint data loss prevention (DLP) with Microsoft Purview

- Introduction
- Endpoint data loss prevention (DLP) overview
- Understand the endpoint DLP implementation workflow
- Onboard devices for endpoint DLP
- Configure settings for endpoint DLP
- Create and manage endpoint DLP policies
- Deploy the Microsoft Purview browser extension
- Configure just-in-time (JIT) protection

Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

- Introduction
- Configure data loss prevention policies for Power Platform
- Integrate data loss prevention in Microsoft Defender for Cloud Apps
- Configure policies in Microsoft Defender for Cloud Apps
- Manage data loss prevention violations in Microsoft Defender for Cloud Apps

Investigate and respond to Microsoft Purview Data Loss Prevention alerts

- Introduction
- Understand data loss prevention (DLP) alerts
- Understand the DLP alert lifecycle
- Configure DLP policies to generate alerts
- Investigate DLP alerts in Microsoft Purview
- Investigate DLP alerts in Microsoft Defender XDR
- Investigate DLP alerts with Security Copilot and AI agents
- Respond to DLP alerts
- Exercise – Investigate a DLP alert and related incident

Module 3: Implement and manage Microsoft Purview Insider Risk Management

Understand Microsoft Purview Insider Risk Management

- Introduction
- What is an insider risk?
- Microsoft Purview Insider Risk Management overview
- Microsoft Purview Insider Risk Management features
- Case study – Protect sensitive data with Insider Risk Management

Prepare for Microsoft Purview Insider Risk Management

- Introduction
- Plan for Insider Risk Management
- Prepare your organization for Insider Risk Management
- Configure settings for Insider Risk Management
- Integrate Insider Risk Management with data sources and tools

Create and manage Insider Risk Management policies

- Introduction
- Understand Insider Risk Management policy templates
- Compare quick and custom insider risk policies
- Create a custom Insider Risk Management policy
- Manage policies in Insider Risk Management

Investigate insider risk alerts and related activity

- Introduction
- Understand insider risk alerts and investigations
- Manage alert volume in Insider Risk Management
- Investigate and triage insider risk alerts in Microsoft Purview
- Investigate insider risk alerts with Security Copilot and AI agents
- Analyze alert context with the All risk factors tab
- Investigate activity details with the Activity explorer tab
- Review patterns over time with the User activity tab
- Investigate insider risk alerts in Microsoft Defender XDR
- Manage and take action on insider risk cases
- Exercise – Investigate potential data theft using Insider Risk Management

Implement Adaptive Protection in Insider Risk Management

- Introduction
- Adaptive Protection overview
- Understand and configure risk levels in Adaptive Protection
- Configure Adaptive Protection
- Manage Adaptive Protection

Module 4: Secure AI interactions and environments with Microsoft Purview

Understand How to Secure AI Data with Microsoft Purview

- Introduction
- Understand AI data security risks
- Understand how Microsoft Purview secures AI data
- Evaluate compliance risks for AI usage
- Identify AI-related data exposure risks
- Understand how Microsoft Purview controls AI data access

- Detect and respond to risky AI activity
- Retain and search Copilot prompts and responses

Secure Microsoft 365 Copilot interactions with Microsoft Purview

- Introduction
- Understand how Microsoft 365 Copilot changes data protection needs
- Assess Copilot regulatory compliance with Compliance Manager
- Audit Copilot interactions with Microsoft Purview
- Analyze Copilot interactions with Communication Compliance
- Classify and protect Copilot content with sensitivity labels
- Apply DLP policies to Microsoft 365 Copilot
- Apply retention policies to Copilot prompts and responses
- Investigate and delete Copilot activity with eDiscovery

Secure enterprise and browser-based AI apps with Microsoft Purview

- Introduction
- Understand risks from enterprise and non-Microsoft AI tools
- Assess AI usage for security and compliance
- Identify policy violations with Communication Compliance
- Detect risky AI usage with Insider Risk Management
- Protect sensitive data in AI apps with Microsoft Purview DLP
- Case study – Use Adaptive Protection to respond to AI-related risk
- Apply retention policies to AI app prompts and responses

Secure developer AI environments with Microsoft Purview

- Introduction
- Understand risks and responsibilities in AI development environments
- Discover and assess AI apps with DSPM for AI
- Classify, restrict, and retain AI prompt data
- Enforce protections in Azure AI services and Azure AI Foundry
- Apply controls for Microsoft Entra-registered custom AI apps
- Secure AI agents built in Copilot Studio
- Manage data risks in Copilot in Fabric
- Investigate and respond to risky AI activity

Module 5: Implement and manage Microsoft 365 retention and recovery

Understand retention in Microsoft Purview

- Introduction
- Overview of retention and the data lifecycle
- Understand retention labels and retention policies
- Decide when to apply retention

Implement and manage Microsoft 365 retention and recovery

- Introduction
- Plan for retention and disposition with retention labels
- Create and publish retention labels
- Create and manage auto-apply retention labels
- Create and configure adaptive scopes
- Create and configure retention policies
- Understand policy and label precedence in Microsoft Purview

- Recover content in Microsoft 365 workloads

Module 6: Audit and search activity in Microsoft Purview

Search and investigate with Microsoft Purview Audit

- Introduction
- Microsoft Purview Audit overview
- Configure and manage Microsoft Purview Audit
- Conduct searches with Audit (Standard)
- Audit Microsoft Copilot for Microsoft 365 interactions
- Investigate activities with Audit (Premium)
- Export audit log data
- Configure audit retention with Audit (Premium)

Search for content with Microsoft Purview eDiscovery

- Introduction
- Understand eDiscovery and content search capabilities
- Prerequisites for using eDiscovery in Microsoft Purview
- Create an eDiscovery search
- Conduct an eDiscovery search
- Export eDiscovery search results

For any query Contact Us – Microtek Learning