Administering Information Protection and Compliance in Microsoft 365 (SC-400)

Description

Protect your critical information with Microsoft 365

In a digital world where data has become the new battlefield, protecting it has become a top priority. The Administration of Information Protection and Compliance in Microsoft 365 (SC-400) training provides you with all the essential skills to securely manage, classify, and govern your sensitive information.

Through this comprehensive course, you will learn how to implement advanced data protection and compliance strategies within your organization. You will master powerful tools such as Microsoft Purview, data loss prevention (DLP) strategies, sensitivity labels, and advanced eDiscovery features. Through structured modules, you will discover how to safeguard your data at every stage of its lifecycle.

Learn to master information compliance and governance

This training also prepares you for the official Microsoft Information Protection Administrator (SC-400) certification exam, a strong recognition of your skills by employers. Each module has been carefully designed to guide you step-by-step, including practical exercises to reinforce your knowledge effectively.

Course Content
Module 1 : Foundations of data security and compliance with Microsoft Purview

- Discover the tools and concepts in Microsoft Purview for managing and protecting sensitive data
- Understand how to keep data secure and compliant throughout its lifecycle across different environments
- Know your data
- Protect your data
- Prevent data loss
- Govern your data

Module 2 : Classify data for protection and governance

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

Module 3 : Create and manage sensitive information types

- 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

Module 4 : 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

Module 5 : Deploy Microsoft Purview Message Encryption

- Implement Microsoft Purview Message Encryption
- Implement Microsoft Purview Advanced Message Encryption
- Use Microsoft Purview Message Encryption templates in mail flow rules

Module 6 : Create and configure sensitivity labels with Microsoft Purview

- Sensitivity label overview
- Create and configure sensitivity labels and label policies
- Configure encryption with sensitivity labels
- Implement auto-labeling policies
- Use the data classification dashboard to monitor sensitivity labels

Module 7 : Apply sensitivity labels for data protection

- 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

Module 8 : Prevent data loss in Microsoft Purview

- 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

Module 9 : Implement endpoint data loss prevention (DLP) with Microsoft Purview

- 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

Module 10 : Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

- 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

Module 11 : Manage data loss prevention policies and reports in Microsoft 365

- Configure data loss prevention for policy precedence
- Implement data loss prevention policies in test mode
- Explain data loss prevention reporting capabilities
- Manage permissions for data loss prevention reports
- Manage and respond to data loss prevention policy violations

Module 12 : Manage the data lifecycle in Microsoft Purview

- Data Lifecycle Management overview
- Configure retention policies
- Configure retention labels
- Configure manual retention label policies
- Configure auto-apply retention label policies
- Import data for Data Lifecycle Management
- Manage, monitor, and remediate Data Lifecycle Management

Module 13 : Manage data retention and deletion in Microsoft 365 workloads

- Explain retention in SharePoint Online and OneDrive
- Explain retention in Microsoft Teams
- Explain retention in Copilot for Microsoft 365
- Explain retention in Viva Engage
- Explain retention in Exchange Online
- Apply mailbox holds in Microsoft Exchange
- Recover content in Microsoft Exchange
- Recover content in Microsoft 365 workloads

Module 14 : Manage records in Microsoft Purview

- Records management overview
- Import a file plan
- Configure retention labels
- Configure event driven retention
- Manage, monitor, and remediate records

Module 15 : Explore compliance in Microsoft 365

- Plan for security and compliance in Microsoft 365

- Plan your beginning compliance tasks in Microsoft Purview
- Manage your compliance requirements with Compliance Manager
- Examine the Compliance Manager dashboard
- Analyze the Microsoft Compliance score

Module 16 : Search for content in the Microsoft Purview compliance portal

- Explore Microsoft Purview eDiscovery solutions
- Create a content search
- View the search results and statistics
- Export the search results and search report
- Configure search permissions filtering
- Search for and delete email messages

Module 17 : Manage Microsoft Purview eDiscovery (Standard)

- Explore Microsoft Purview eDiscovery solutions
- Implement Microsoft Purview eDiscovery (Standard)
- Create eDiscovery holds
- Search for content in a case
- Export content from a case
- Close, reopen, and delete a case

Module 18 : Manage Microsoft Purview eDiscovery (Premium)

- Explore Microsoft Purview eDiscovery (Premium)
- Implement Microsoft Purview eDiscovery (Premium)
- Create and manage an eDiscovery (Premium) case
- Manage custodians and non-custodial data sources
- Collect content for a case
- Review and manage case content
- Analyze case content

Module 19 : Search and investigate with Microsoft Purview Audit

- 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)

Module 20 : Prepare Microsoft Purview Communication Compliance

- Introduction to communication compliance
- Plan for communication compliance
- Identify and resolve communication compliance workflow
- Introduction to communication compliance policies
- Communication compliance with Copilot for Microsoft 365
- Case study - Configure an offensive language policy
- Investigate and remediate communication compliance alerts

Module 21 : Manage insider risk in Microsoft Purview

- Insider risk management overview
- Introduction to managing insider risk policies
- Create and manage insider risk policies
- Investigate insider risk alerts
- Take action on insider risk alerts through cases
- Manage insider risk management forensic evidence
- Create insider risk management notice templates

Module 22 : Implement Adaptive Protection in Insider Risk Management

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

Module 23 : Implement Microsoft Purview Information Barriers

- Explore Microsoft Purview Information Barriers
- Configure information barriers in Microsoft Purview
- Examine information barriers in Microsoft Teams
- Examine information barriers in OneDrive
- Examine information barriers in SharePoint

Module 24 : Manage regulatory and privacy requirements with Microsoft Priva

- Create and manage risk management policies
- Investigate and remediate risk management alerts
- Create rights requests
- Manage data estimate and retrieval for rights requests
- Review data from rights requests
- Get reports from rights requests

Module 25 : Implement privileged access management

- Understand privileged access management
- Configure privileged access management
- Manage privileged access management
- Case study - Implement privileged access management

Module 26 : Manage Customer Lockbox

- Understand Customer Lockbox
- Configure Customer Lockbox
- Manage Customer Lockbox requests

Lab / Exercises

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and

educational content to deepen your knowledge and develop your technical skills.

Exam

- This course prepares you to the SC-400: Microsoft Information Protection Administrator exam

Participant profiles

- Compliance administrators
- Data security consultants
- IT and data governance managers
- Cybersecurity auditors
- Information protection officers

Prerequisites

- Understand the basics of Microsoft security and compliance
- Understand the fundamental concepts of cloud computing and Microsoft 365
- Have basic knowledge of Microsoft Purview compliance features

Objectives

- Implement information protection strategies with Microsoft Purview
- Classify and label sensitive data for effective governance
- Create and manage standard and custom sensitive information types
- Configure and deploy encryption solutions in Microsoft 365
- Implement and optimize data loss prevention (DLP)
- Manage data lifecycle and apply retention policies
- Configure advanced compliance policies and manage records
- Use eDiscovery and Audit to search, review, and protect data

Description
Administering Information Protection and Compliance in Microsoft 365 (SC-400)
Niveau
Intermédiaire
Classroom Registration Price (CHF)
3200
Virtual Classroom Registration Price (CHF)
3000
Duration (in Days)
4
Reference
SC-400T00