Information Security Administrator (SC-401)

Description

Develop your information security skills with Microsoft 365

Protecting sensitive data has become a major challenge for all organizations. The “Information Security Administrator (SC-401)” training course prepares you to plan and implement effective protection strategies using Microsoft 365 and Microsoft Purview. This course provides you with the essential skills to secure modern collaboration environments and manage both internal and external risks.

By attending this SC-401 training, you will learn how to prevent data leaks, apply retention policies, master insider risk management, and secure data used by AI services. Through a comprehensive and practical approach, you will know how to protect your most critical information, manage security alerts, and respond to incidents in real-time. You will also be able to configure advanced Data Loss Prevention (DLP) strategies and secure sensitive communications.

Strengthen the protection of your strategic data

The program is built around the most advanced Microsoft 365 tools and services to ensure optimal data protection. You will learn how to classify, label, and encrypt sensitive information while meeting your organization’s compliance requirements. Additionally, you will understand how to integrate security controls into the processes involving the use of artificial intelligence.

Course Content
Module 1: Protect sensitive data in a digital world

- The growing need for data protection
- The challenges of managing sensitive data
- Protecting data in a Zero Trust world
- Understanding data classification and protection
- Preventing data leaks and insider threats
- Managing security alerts and responding to threats
- Protecting data generated and processed by AI

Module 2: Classify data for protection and governance

- Introduction to data classification
- Classify data using sensitive information types
- Classify data with trainable classifiers
- Create a custom trainable classifier

Module 3: Review and analyze data classification and protection

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

Module 4: Create and manage sensitive information types

- Overview of sensitive information types
- Compare built-in and custom sensitive information types
- Create and manage custom sensitive information types
- Create and manage exact data match (EDM) sensitive information types
- Implement document fingerprinting
- Describe named entities
- Create a keyword dictionary

Module 5: Create and configure sensitivity labels with Microsoft Purview

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

Module 6: Apply sensitivity labels for data protection

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

Module 7: Understand encryption in Microsoft 365

- Introduction to encryption in Microsoft 365
- Encrypting data at rest
- Understanding service encryption in Microsoft Purview
- Manage customer keys with Customer Key
- Encrypting data in transit

Module 8: Deploy Microsoft Purview Message Encryption

- Implement Microsoft Purview Message Encryption
- Implement advanced message encryption
- Use encryption templates in mail flow rules

Module 9: Prevent data loss with Microsoft Purview

- Introduction to Data Loss Prevention (DLP)
- Plan and design DLP policies
- Deploy and simulate DLP policies
- Create and manage DLP policies
- Integrate Adaptive Protection with DLP
- Use DLP analytics to identify risks
- Understand DLP alerts and activity tracking

Module 10: Implement endpoint Data Loss Prevention

- Introduction to endpoint DLP
- Understanding the implementation process

- Enroll devices for endpoint DLP
- Configure endpoint DLP settings
- Create and manage endpoint DLP policies
- Deploy the Microsoft Purview browser extension
- Configure Just-in-Time (JIT) protection

Module 11: Configure DLP policies for Defender for Cloud Apps and Power Platform

- Configure DLP policies for Power Platform
- Integrate DLP with Microsoft Defender for Cloud Apps
- Configure policies in Defender for Cloud Apps
- Manage DLP violations in Defender for Cloud Apps

Module 12: Understand insider risk management with Microsoft Purview

- What is insider risk?
- Introduction to insider risk management
- Features of insider risk management
- Case study: Protecting sensitive data

Module 13: Prepare for insider risk management with Microsoft Purview

- Plan insider risk management
- Prepare your organization
- Configure settings
- Integrate data sources and tools

Module 14: Create and manage insider risk management policies

- Understand policy templates
- Compare quick and custom policies
- Create a custom policy
- Manage insider risk policies

Module 15: Manage AI data security challenges with Microsoft Purview

- Apply sensitivity labels with Microsoft 365 Copilot
- Use Endpoint DLP to prevent AI data exposure
- Detect the use of generative AI
- Case study: Protecting AI data with adaptive protection

Module 16: Manage compliance with Microsoft Purview for Microsoft 365 Copilot

- Audit Copilot interactions with Microsoft Purview
- Review and delete interactions with eDiscovery (Premium)
- Manage Copilot retention with Microsoft Purview
- Monitor Copilot communications compliance

Module 17: Identify and mitigate AI data security risks

- Understand AI security risks
- Introduction to Data Security Posture Management (DSPM) for AI
- Configure DSPM for AI

- Analyze AI security reports
- Use data assessments to detect oversharing risks

Module 18: Introduction to information security and compliance in Microsoft Purview

- Foundations of data security and compliance

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.

Participant profiles

- Information Security Administrators
- Compliance and Data Governance Officers
- Cybersecurity Specialists
- Microsoft 365 Administrators
- Data Protection Consultants

Prerequisites

- Understand the basic concepts of Microsoft 365
- Have fundamental knowledge of cybersecurity
- Be familiar with data governance principles

Objectives

- Plan and implement sensitive data protection
- Classify data for protection and governance
- Configure and apply sensitivity labels with Microsoft Purview
- Deploy Data Loss Prevention (DLP) strategies
- Manage data encryption within Microsoft 365
- Identify and mitigate internal and external risks
- Secure data used by AI services
- Ensure data compliance with Microsoft Purview tools

Description
Information Security Administrator (SC-401)
Niveau
Intermédiaire
Classroom Registration Price (CHF)
3200
Virtual Classroom Registration Price (CHF)
3000
Duration (in Days)
4
Reference
SC-401