Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

SC-401 Information Security Administrator

CODE:	LENGTH:	PRICE:
MCS_SC-401T00	32 Hours (4 days)	€2,295.00

Description

The Information Security Administrator course equips you with the skills needed to plan and implement information security for sensitive data using Microsoft Purview and related services. The course covers essential topics such as information protection, data loss prevention (DLP), retention, and insider risk management. You learn how to protect data within Microsoft 365 collaboration environments from internal and external threats. Additionally, you learn how to manage security alerts and respond to incidents by investigating activities, responding to DLP alerts, and managing insider risk cases. You also learn how to protect data used by AI services within Microsoft environments and implement controls to safeguard content in these environments.

Audience

As an Information Security Administrator, you plan and implement information security for sensitive data using Microsoft Purview and related services. You're responsible for mitigating risks by protecting data within Microsoft 365 collaboration environments from internal and external threats, as well as safeguarding data used by AI services. Your role involves implementing information protection, data loss prevention (DLP), retention, and insider risk management. You also manage security alerts and respond to incidents by investigating activities, responding to DLP alerts, and managing insider risk cases. In this role, you collaborate with other roles responsible for governance, data, and security to develop policies that address your organization's information security and risk reduction goals. You work with workload administrators, business application owners, and governance stakeholders to implement technology solutions that support these policies and controls.

Prerequisites

- Familiarity with Microsoft Purview compliance solutions
- Basic understanding of data protection and security concepts

- Foundational knowledge of Microsoft security and compliance technologies
- Basic knowledge of Microsoft 365 data governance capabilities
- Foundational knowledge of Microsoft security and compliance technologies
- Basic understanding of audit logs and content discovery

Programme

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
- Module assessment
- Summary

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
- Module assessment
- Summary

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
- Module assessment
- Summary

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
- Module assessment
- Summary and resources

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
- Module assessment
- Summary

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
- Apply sensitivity labels in Power BI
- Module assessment
- Summary and resources

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
- Module assessment
- Summary

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
- Summary and knowledge check

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 assessment
- Summary and resources

Understand and plan data loss prevention

- Introduction
- Understand the role of data loss prevention (DLP)
- Understand how DLP applies protection
- Plan and design DLP policies
- Understand DLP deployment and simulation mode
- Evaluate advanced DLP controls for your environment
- Module assessment
- Summary

Create and manage data loss prevention policies

- Introduction
- Understand how DLP policy decisions fit together
- Choose a template or create a custom policy
- Define what the policy detects
- Align policy scope to risk
- Define how the policy responds
- Validate policy behavior using simulation mode
- Manage DLP policies
- Adjust enforcement dynamically based on risk
- Guided walkthrough: Create a DLP policy
- Module assessment
- Summary

Implement endpoint data loss prevention (DLP) with Microsoft Purview

- Introduction
- Understand endpoint data loss prevention
- 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 assessment
- Summary and resources

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
- Module assessment
- Summary and resources

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 assessment
- Summary

Understand retention in Microsoft Purview

- Introduction

- Overview of retention and the data lifecycle
- Understand retention labels and retention policies
- Decide when to apply retention
- Module assessment
- Summary

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 assessment
- Summary

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
- Module assessment
- Summary

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
- Module assessment
- Summary

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
- Module assessment
- Summary

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
- Module assessment
- Summary

Implement Adaptive Protection in Microsoft Purview

- Introduction
- Understand Adaptive Protection and insider risk levels
- Evaluate and configure insider risk levels
- Set up Adaptive Protection

- Configure Adaptive Protection with Data Loss Prevention
- Configure Adaptive Protection with Conditional Access
- Evaluate Adaptive Protection with Data Lifecycle Management
- Module assessment
- Summary

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)
- Module assessment
- Summary

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
- Module assessment
- Summary and resources

Test and Certification

Microsoft Certified: Information Security Administrator Associate

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
15 Mar 2027	Virtual Classroom (CET / UTC+1)	CET	English	Instructor Led Online		€2,295.00
07 Jun 2027	Virtual Classroom (CET / UTC+1)	CEDT	English	Instructor Led Online		€2,295.00

Additional Information

This training is also available as onsite training. Please contact us to find out more.