Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

MS-SC401T00: PROTECT SENSITIVE INFORMATION WITH MICROSOFT PURVIEW IN THE AI ERA

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	CERTIFICATION
4 Days	Intermediate	Security	Instructor-led	SC-401 Exam

INTRODUCTION

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 PROFILE

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

Before attending this course, delegates must have:

- Experience working with Microsoft 365 services, especially in security, compliance, or governance roles.
- Knowledge of Microsoft Purview solutions, including information protection, data loss prevention, insider risk management, and compliance tooling.
- Familiarity with data classification, sensitivity labels, and retention concepts within Microsoft 365.
- Experience managing security or data protection policies in cloud collaboration environments.
- General understanding of risk management and responding to security alerts, especially related to insider risks and DLP.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Implement information protection policies using Microsoft Purview, including data classification, sensitivity labels, and content marking.
- Configure and manage Data Loss Prevention (DLP) across Microsoft 365 to prevent unauthorized data sharing and leakage.
- Implement and manage retention policies to support compliance, data lifecycle management, and secure information governance.
- Investigate and respond to insider risk alerts and DLP incidents, mitigating risks from internal threats.
- Protect AI-generated and AI-processed data using adaptive security controls to reduce emerging AI-related risks.
- Manage information security alerts and activities across Microsoft 365 security tools.
- Collaborate with governance, compliance, and security teams to design policies aligning with organizational risk-reduction goals.

COURSE CONTENT

Module 1: Implement Microsoft Purview Information Protection

Organizations need effective information protection to prevent data exposure, ensure compliance, and maintain security across cloud and on-premises environments. Microsoft Purview enables classification, labeling, and encryption to safeguard sensitive data across Microsoft 365 services, Exchange, and on-premises storage.

Module 1.1: Protect sensitive data in a digital world

Discover how Microsoft Purview helps organizations classify, protect, and monitor sensitive data across cloud, endpoint, and AI environments. This module explores strategies for securing data

Module 1.2: Classify data for protection and governance

Learn about the information available to help you understand your data landscape and know your data.

through classification, labeling, encryption, and proactive risk management.

Module 1.3: Review and analyze data classification and protection

Discover how Microsoft Purview helps organizations monitor and analyze data classification and protection. This module explores how security teams can track classification trends, investigate labeled content, and assess policy effectiveness using Information Protection Reports, Data explorer, Content explorer, and Activity explorer.

Module 1.4: Create and manage sensitive information types

Learn how to use sensitive information types to support your information protection strategy.

Module 1.5: Create and configure sensitivity labels with Microsoft Purview

Microsoft Purview sensitivity labels enable you to classify and protect sensitive data throughout your organization, including in the cloud and on devices. This module covers how to classify and protect sensitive information to ensure its security and compliance.

Module 1.6: Apply sensitivity labels for data protection

Learn about how sensitivity labels are used to classify and protect business data while making sure that user productivity and their ability to collaborate aren't hindered.

Module 1.7: Classify and protect on-premises data with Microsoft Purview

Learn how to classify and protect sensitive data stored on-premises using Microsoft Purview. This module guides you through deploying the Information Protection scanner, applying sensitivity labels, and enforcing DLP policies to reduce data exposure risks.

Module 1.8: Understand Microsoft 365 encryption

Learn how Microsoft 365 encrypts data-at-rest and in-transit, securely manages encryption keys, and provides key management options to customers to meet their business needs and compliance obligations.

Module 1.9: Protect email with Microsoft Purview Message Encryption

Learn how to configure Microsoft Purview Message Encryption to protect sensitive email, apply encryption with mail flow rules, and customize the recipient experience with branded templates.

Module 2: Implement and manage Microsoft Purview Data Loss Prevention

Organizations must prevent data loss and protect sensitive information across cloud and endpoint environments. Microsoft Purview provides data loss prevention (DLP) policies to detect, restrict, and respond to risky activities involving sensitive data. Learn how to plan and configure DLP policies, track policy effectiveness, and analyze data security risks to improve your organization's protection strategy.

Module 2.1: Understand and plan data loss prevention

Effective data loss prevention (DLP) starts with understanding how risk is evaluated and how protection decisions are applied. This module focuses on the concepts and planning considerations that help organizations design DLP policies that protect sensitive data without disrupting everyday work.

Module 2.2: Create and manage data loss prevention policies

Effective data loss prevention (DLP) policies are shaped by a series of deliberate decisions rather than individual settings. Clear intent, well-defined detection, appropriate scope, and measured actions determine how policies behave in real workflows. Validation and ongoing adjustment help ensure protection remains effective as risk and usage change.

Module 2.3: Implement endpoint data loss prevention (DLP) with Microsoft Purview

Endpoint DLP in Microsoft Purview helps organizations protect sensitive data on endpoint devices by monitoring, restricting, or allowing actions such as file transfers, copying, and sharing. Learn how to onboard devices, configure settings, and create custom policies to ensure data security across your organization.

Module 2.4: Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

Learn how to configure and implement data loss prevention policies and integrate them with Microsoft Defender for Cloud Apps.

Module 2.5: Investigate and respond to Microsoft Purview Data Loss Prevention alerts

Microsoft Purview and Microsoft Defender XDR help organizations detect potential data loss risks and respond quickly to protect sensitive information. Investigation and response activities include reviewing DLP alerts, applying appropriate remediation actions, and documenting findings in a structured and consistent way.

Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

Module 3: Implement and manage Microsoft 365 retention and recovery

Learn how to manage the data lifecycle in Microsoft 365 using retention policies and labels. Understand how to configure and apply retention settings that meet organizational requirements for preserving or deleting content across Microsoft 365 services.

Module 3.1: Understand retention in Microsoft Purview

Microsoft Purview retention helps organizations manage how long data is kept and when it can be deleted. Learn how to apply retention strategically to meet compliance requirements, reduce risk, and protect important information throughout its lifecycle.

Module 3.2: Implement and manage Microsoft 365 retention and recovery

Microsoft Purview provides tools to manage how long content is retained and when it's deleted across Microsoft 365 services. These retention settings apply lifecycle rules using labels, policies, and adaptive scopes. When content is deleted, recovery options are managed within the individual services, such as SharePoint and Exchange. Together, these tools support compliance and information security by reducing the risk of retaining unnecessary or outdated data.

Module 4: Implement and manage Microsoft Purview Insider Risk Management

Implement Microsoft Purview Insider Risk Management to detect, investigate, and respond to internal risks while protecting data, ensuring compliance, and maintaining employee trust.

Module 4.1: Understand Microsoft Purview Insider Risk Management

Understand insider risks and discover how Microsoft Purview Insider Risk Management identifies risky activities, analyzes context, and helps organizations protect data while respecting privacy.

Module 4.2: Prepare for Microsoft Purview Insider Risk Management

Discover strategies for planning and configuring Microsoft Purview Insider Risk Management to meet organizational needs and protect privacy.

Module 4.3: Create and manage Insider Risk Management policies

Create and manage Microsoft Purview Insider Risk Management policies to detect and address potential insider risks while supporting organizational security and privacy.

Module 4.4: Investigate insider risk alerts and related activity

Investigate insider risk alerts and manage related cases in Microsoft Purview to assess user behavior, take appropriate action, and coordinate deeper reviews across teams.

Module 4.5: Implement Adaptive Protection in Insider Risk Management

Understand how Adaptive Protection applies machine learning to assess user risk and automatically enforce the right level of security controls. By dynamically assigning Data loss prevention, Data lifecycle management, and Conditional Access policies, it strengthens data security while reducing unnecessary alerts and manual intervention.

Module 5: Audit and search activity in Microsoft Purview

Understand how to use Microsoft Purview to log activity and search for content across Microsoft 365 services. Learn how audit logging supports investigations and compliance requirements, and how content search can help locate specific emails, documents, and other items when needed.

Module 5.1: Search and investigate with Microsoft Purview Audit

Enhance data security and compliance with Microsoft Purview Audit by configuring detailed audits, managing logs, and analyzing access patterns.

Module 5.2: Search for content with Microsoft Purview eDiscovery

Use Microsoft Purview eDiscovery to search for content across Microsoft 365. This module covers how to configure cases, define search criteria, and locate messages, files, and other organizational data.

Module 6: Secure AI interactions and environments with Microsoft Purview

AI tools such as Microsoft Copilot and custom AI apps can access and generate sensitive content across your organization.

Module 6.1: Understand How to Secure AI Data with Microsoft Purview

Microsoft Purview helps organizations assess how Microsoft 365 Copilot and other AI tools interact with sensitive data. Using Data Security Posture Management (DSPM) for AI, organizations can evaluate exposure risks, understand which AI tools are in use, and identify how sensitive data is accessed during AI interactions. Audit provides visibility into specific Copilot prompts and responses for compliance and investigation scenarios.

Module 6.2: Secure Microsoft 365 Copilot interactions with Microsoft Purview

AI tools like Microsoft 365 Copilot create new ways to interact with sensitive data, but they also introduce new risks. Learn how Microsoft Purview helps you apply security and compliance controls that protect data, manage AI activity, and support responsible use at scale.

Data4Every1

Powered by EDUQE EXPERTS IN IT TRAINING

Module 6.3: Secure enterprise and browser-based AI apps with Microsoft Purview

AI tools across enterprise and public environments create new opportunities but also introduce data security and compliance risks. Microsoft Purview helps reduce these risks by discovering AI usage, assessing compliance needs, and applying integrated controls for protection, retention, and responsible use.

Module 6.4: Secure developer AI environments with Microsoft Purview

Microsoft Purview provides tools to secure developer AI environments by discovering apps, assessing data access, and applying appropriate protections. This includes detecting generative AI usage, assigning user risk levels, and applying dynamic enforcement based on user behavior and data sensitivity.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the SC-401 Microsoft Certified: Information Security Administrator Associate Exam.