SC-401: Information Security Administrator

Level: Intermediate
Length: 4 Days

Course Overview

About this course

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.

Course Details

Learning Path 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.

- Protect sensitive data in a digital world
- Classify data for protection and governance
- Review and analyze data classification and protection
- Create and manage sensitive information types
- Create and configure sensitivity labels with Microsoft Purview
- Apply sensitivity labels for data protection
- Classify and protect on-premises data with Microsoft Purview
- Understand Microsoft 365 encryption
- Protect email with Microsoft Purview Message Encryption

Learning Path 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.

- Prevent data loss in Microsoft Purview
- Implement endpoint data loss prevention (DLP) with Microsoft Purview
- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform
- Investigate and respond to Microsoft Purview Data Loss Prevention alerts

Learning Path 3: 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.

- Understand Microsoft Purview Insider Risk Management
- Prepare for Microsoft Purview Insider Risk Management
- Create and manage Insider Risk Management policies
- Investigate insider risk alerts and related activity
- Implement Adaptive Protection in Insider Risk Management

Learning Path 4: Protect data in AI environments with Microsoft Purview

AI tools like Microsoft Copilot are changing the way people work, but they also increase the risk of oversharing and accidental data exposure. Microsoft Purview helps organizations apply the right controls to keep sensitive data protected across AI-enabled environments.

- Discover AI interactions with Microsoft Purview
- Protect sensitive data from AI-related risks
- Govern AI usage with Microsoft Purview
- Assess and mitigate AI risks with Microsoft Purview

Learning Path 5: 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.

- Understand retention in Microsoft Purview
- Implement and manage Microsoft 365 retention and recovery

Learning Path 6: 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.

- Search and investigate with Microsoft Purview Audit
- Search for content with Microsoft Purview eDiscovery