Microsoft Information Protection Administrator

Course: SC 400T00

Length: 3 Days

About this Course

Learn how to protect information in your Microsoft 365 deployment. This course focuses on data governance and information protection within your organization. The course covers implementation of data loss prevention policies, sensitive information types, sensitivity labels, data retention policies and Microsoft Purview message encryption among other related topics. The course helps learners prepare for the Microsoft Information Protection Administrator exam (SC-400)

Prerequisites

Before attending this course, students should have:

- Foundational knowledge of Microsoft security and compliance technologies.
- Basic knowledge of information protection concepts.
- Understanding of cloud computing concepts.
- Understanding of Microsoft 365 products and services.

Audience profile

The Information Protection Administrator plans and implements controls that meet organizational compliance needs. This person is responsible for translating requirements and compliance controls into technical implementation. They assist organizational control owners to become and stay compliant. They work with information technology (IT) personnel, business application owners, human resources, and legal stakeholders to implement technology that supports policies and controls necessary to sufficiently address regulatory requirements for their organization. They also work with the compliance and security leadership such as a Chief Compliance Officer and Security Officer to evaluate the full breadth of associated enterprise risk and partner to develop those policies. This person defines applicable requirements and tests IT processes and operations against those policies and controls. They are responsible for creating policies and rules for content classification, data loss prevention, governance, and protection.

Skills gained

- Explain and use sensitivity labels.
- Configure Data Loss Prevention policies.
- Secure messages in Office 365.
- Describe the information governance configuration process.
- Define key terms associated with Microsoft's information protection and governance solutions.
- Explain the Content explorer and Activity explorer.
- Describe how to use sensitive information types and trainable classifiers.
- Review and analyze DLP reports. o
- Identify and mitigate DLP policy violations.
- Describe the integration of DLP with Microsoft Cloud App Security (MCAS).
- Deploy Endpoint DLP
- Describe records management
- Configure event driven retention
- Import a file plan
- Configure retention policies and labels
- Create custom keyword dictionaries

Microsoft Information Protection Administrator

Course: SC 400T00

Length: 3 Days

Course Outline

Module 1: Implement Information Protection in Microsoft 365

Lessons

- Introduction to information protection in Microsoft Purview
- Classify data for protection and governance
- Create and manage sensitive information types
- Describe Microsoft 365 encryption
- Deploy message encryption in Microsoft Purview
- Protect information in Microsoft Purview
- Apply and manage sensitivity labels

Lab Exercises

- Exercise 1: Manage Compliance Roles
- Exercise 2: Manage Microsoft Purview message encryption
- Exercise 3: Manage sensitive information types
- Exercise 4: Manage trainable classifiers
- Exercise 5: Manage sensitivity labels

Module 2: Implement Data Loss Prevention

Lessons

- Prevent data loss with Microsoft Purview
- Implement Endpoint data loss prevention
- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform
- Manage DLP policies and reports in Microsoft Purview

Lab Exercises

- Exercise 1: Manage DLP policies
- Exercise 2: Manage Endpoint DLP
- Exercise 3: Manage DLP reports

Module 3: Implement Data Lifecycle and Records Management

Lessons

- Data Lifecycle Management in Microsoft Purview
- Manage data retention in Microsoft 365
- Implement records management in Microsoft 365

Lab Exercises

- Exercise 1: Configure Retention Policies
- Exercise 2: Implement Retention Labels
- Exercise 3: Configure Service-based Retention
- Exercise 4: Configure event-based Retention
- Exercise 5: Use eDiscovery for Recover