Module Title : SC-400T00: Microsoft Information Protection Administrator
Duration : 3 days

Overview

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).

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.

Job role: Administrator
Preparation for exam: SC-400
Features: none

Skills gained

- Explain and use sensitivity labels.
- Configure Data Loss Prevention policies.
- Secure messages with Microsoft Purview
- 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.
- Identify and mitigate DLP policy violations.
- Describe the integration of DLP with Microsoft Defender for Cloud Apps.
- Deploy Endpoint DLP
- Describe records management
- Configure event driven retention
- Import a file plan
- Configure retention policies and labels
- Create custom keyword dictionaries
- Implement document fingerprinting

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.

Course Outline

Day 1

9:00am-10:30am

Module 1: Implement Information Protection in Microsoft Purview

Organizations require information protection solutions to protect their data against theft and accidental loss. Learn how to protect your sensitive information. Learn how Microsoft Purview information protection and governance solutions help you protect and govern your data, throughout its lifecycle – wherever it lives, or wherever it travels. Learn about the information available to help you understand your data landscape and know your data. Learn how to use sensitive information types to support your information protection strategy. Learn about how sensitivity labels are used to classify and protect business data while making sure that user productivity and their ability to collaborate are not hindered.

Lessons

- Introduction to information protection in Microsoft Purview
- Classify data for protection and governance

10:30am-10:45pm Morning Break

10:45pm-12:30pm

- Create and manage sensitive information types
- Describe Microsoft 365 encryption
- Deploy message encryption with Microsoft Purview

12:30pm-1:30pm Lunch

1:30pm-3:30pm

- Protect information in Microsoft Purview
- Apply and manage sensitivity labels

3:30pm-3:45pm Afternoon Break

3:45pm-5:00pm

Lab : Implement Information Protection

- Manage Compliance Roles
- Manage Microsoft Purview message encryption
- Manage Sensitive Information Types
- Manage Trainable Classifiers
- Manage Sensitivity Labels

After completing this module, students will be able to:

- Describe Microsoft's approach to information protection and governance.
- List the components of the Data Classification solution.
- Describe how to use sensitive information types and trainable classifiers.
- Implement document fingerprinting
- Create custom keyword dictionaries
- Deploy message encryption in Microsoft Purview

Day 2

9:00am-10:30am

Module 2: Implement Data Loss Prevention

In this module we discuss how to implement data loss prevention techniques to secure your Microsoft 365 data. Learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization. Learn how to configure and implement data loss prevention policies and integrate them with Microsoft Defender for Cloud Apps. Learn how to respond to and mitigate data loss policy violations.

Lessons

- Prevent Data loss with Microsoft Purview
- Implement Endpoint data loss prevention

10:30am-10:45pm Morning Break

10:45pm-12:30pm

- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

12:30pm-1:30pm Lunch

1:30pm-3:30pm

- Manage DLP policies and reports in Microsoft Purview

3:30pm-3:45pm Afternoon Break

3:45pm-5:00pm

Lab : Implement Data Loss Prevention

- Manage DLP policies
- Manage Endpoint DLP
- Manage DLP reports

After completing this module, students will be able to:

- Describe the information protection configuration process.
- Articulate deployment and adoption best practices.
- Describe the integration of DLP with Microsoft Defender for Cloud Apps.
- Configure policies in Microsoft Defender for Cloud Apps.
- Review and analyze DLP reports.
- Identify and mitigate DLP policy violations.
- Mitigate DLP violations in Microsoft Defender for Cloud Apps.

Day 3

9:00am-10:30am

Module 3: Implement Data Lifecycle and Records Management

In this module you will learn how to plan and implement information governance strategies for an organization. Learn how to manage your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. Learn how to manage retention for Microsoft 365, and how retention solutions are implemented in the individual Microsoft 365 services. Learn how to use intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization.

Lessons

- Data Lifecycle Management in Microsoft Purview

10:30am-10:45pm Morning Break

10:45pm-12:30pm

- Manage data retention in Microsoft 365 workloads
- Manage records in Microsoft Purview

12:30pm-1:30pm Lunch

1:30pm-3:30pm

Lab : Implement Data Lifecycle and Records Management

- Configure Retention Labels
- Implement Retention Labels
- Configure Service-based Retention

3:30pm-3:45pm Afternoon Break

3:45pm-5:00pm

- Configure event-based Retention
- Use eDiscovery for Recovery
- Configure Records Management

After completing this module, students will be able to:

- Describe the information governance configuration process.
- Articulate deployment and adoption best practices.
- Describe the retention features in Microsoft 365 workloads.
- Configure retention settings in Microsoft Teams and SharePoint Online.
- Implement retention for Exchange Mailbox items.
- Recover content protected by retention settings.
- Regain protected items from Exchange Mailboxes.
- Describe the records management configuration process.