

Training: Microsoft

## SC-400 Administering Information Protection and Compliance in Microsoft 365



### TRAINING GOALS:

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 Office 365 message encryption among other related topics. The course helps learners prepare for the Microsoft Information Protection Administrator exam (SC-400).

#### 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.
- 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

#### 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.

## CONSPECT:

- Implement Information Protection in Microsoft 365
  - Introduction to information protection and governance in Microsoft 365
  - Classify data for protection and governance
  - Create and manage sensitive information types
  - Describe Microsoft 365 encryption
  - Deploy message encryption in Office 365
  - Configure sensitivity labels
  - Apply and manage sensitivity labels
- Implement Data Loss Prevention in Microsoft 365
  - Prevent Data loss in Microsoft 365
  - Implement Endpoint data loss prevention
  - Configure DLP policies for Microsoft Cloud App Security and Power Platform
  - Manage DLP policies and reports in Microsoft 365
- Implement Data Lifecycle and Records Management
  - Data Lifecycle Management in Microsoft Purview
  - Manage data retention in Microsoft 365 workloads
  - Manage records in Microsoft Purview

## REQUIREMENTS:

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.

## Difficulty level



## CERTIFICATE:

Certificate of completing an authorized Microsoft training.

## TRAINER:

Microsoft Certified Trainer.