

# SC-400T00: Microsoft Information Protection Administrator

---

## Course Description

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).

## Course Duration

4 days

## 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

- Introduction to information protection and data lifecycle management in Microsoft Purview
- Prevent data loss
- Classify data for protection and governance
- Create and manage sensitive information types
- Understand Microsoft 365 encryption
- Deploy Microsoft Purview Message Encryption
- Protect information in Microsoft Purview
- Apply and manage sensitivity labels
- Prevent data loss in Microsoft Purview
- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform
- Manage data loss prevention policies and reports in Microsoft 365
- Manage the data lifecycle in Microsoft Purview
- Manage data retention in Microsoft 365 workloads
- Manage records in Microsoft Purview

## Who Should Attend

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.