Course Outline

ProTech Professional Technical Services, Inc.

SC-400T00: Microsoft Information Protection Administrator

Course Summary

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

Objectives

At the end of this course, students will be able to:

- 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 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
- Implement document fingerprinting

Topics

- Introduction to information protection and data lifecycle management in Microsoft Purview
- 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
- Explore compliance in Microsoft 365
- Search for content in the Microsoft Purview compliance portal
- Manage Microsoft Purview eDiscovery (Standard)
- Manage Microsoft Purview eDiscovery (Premium)
- Manage Microsoft Purview Audit (Standard)
- Prepare Microsoft Purview Communication Compliance
- Manage insider Risk in Microsoft Purview
- Implement Microsoft Purview Information Barriers
- Manage Regulatory and privacy requirements with Microsoft Priva
- Implement privileged access management
- Manage Customer Lockbox

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Course Summary (cont'd)

Audience

The information protection administrator translates an organization's risk and compliance requirements into technical implementation. They are responsible for implementing and managing solutions for content classification, data loss prevention (DLP), information protection, data lifecycle management, records management, privacy, risk, and compliance. They also work with other roles that are responsible for governance, data, and security to evaluate and develop policies to address an organization's risk reduction and compliance goals. This role assists workload administrators, business application owners, human resources departments, and legal stakeholders to implement technology solutions that support the necessary policies and controls.

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.

Duration

Four days

Course Outline

I. Introduction to information protection and data lifecycle management in Microsoft Purview

A. Discuss information protection and data lifecycle management and why it's important.
B. Describe Microsoft's approach to information protection and data lifecycle management.
C. Define key terms associated with Microsoft's information protection and data lifecycle management solutions.
D. Identify the solutions that comprise information and data lifecycle management in Microsoft Purview

II. Classify data for protection and governance

A. List the components of the Data Classification solution.
B. Identify the cards available on the Data Classification overview tab.
C. Explain the Content explorer and Activity explorer.
D. Describe how to use sensitive information types and trainable classifiers

III. Create and manage sensitive information types

A. Recognize the difference between built-in and custom sensitivity labels
B. Configure sensitive information types with exact data match-based classification
C. Implement document fingerprinting
D. Create custom keyword dictionaries

IV. Understand Microsoft 365 encryption

A. Explain how encryption mitigates the risk of unauthorized data disclosure.
B. Describe Microsoft data-at-rest and data-in-transit encryption solutions.
C. Explain how Microsoft 365 implements service encryption to protect customer data at the application layer.
D. Understand the differences between Microsoft managed keys and customer managed keys for use with service encryption.

V. Deploy Microsoft Purview Message Encryption

A. Configure Microsoft Purview Message Encryption for end users
B. Implement Microsoft Purview Advanced Message Encryption

VI. Protect information in Microsoft Purview

A. Discuss the information protection solution and its benefits.
B. List the customer scenarios the information protection solution addresses.
C. Describe the information protection configuration process.
D. Explain what users will experience when the solution is implemented.
E. Articulate deployment and adoption best practices.

VII. Apply and manage sensitivity labels

A. Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.
B. Monitor label usage using label analytics.
C. Configure on-premises labeling.
D. Manage protection settings and marking for applied sensitivity labels.
E. Apply protections and restrictions to email.
F. Apply protections and restrictions to files.

Course Outline

VIII. Prevent data loss in Microsoft Purview

A. Discuss the data loss prevention solution and its benefits.
B. Describe the data loss prevention configuration process.
C. Explain what users experience when the solution is implemented.

IX. Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

A. Discuss the data loss prevention solution and its benefits.
B. Describe the data loss prevention configuration process.
C. Explain what users experience when the solution is implemented.

X. Manage data loss prevention policies and reports in Microsoft 365

A. Review and analyze DLP reports.
B. Manage permissions for DLP reports.
C. Identify and mitigate DLP policy violations.
D. Mitigate DLP violations in Microsoft Defender for Cloud Apps.

XI. Manage the data lifecycle in Microsoft Purview

A. Discuss the Data Lifecycle Management solution and its benefits.
B. List the customer scenarios the Data Lifecycle Management solution addresses.
C. Describe the Data Lifecycle Management configuration process.
D. Explain what users will experience when the solution is implemented.
E. Articulate deployment and adoption best practices.

XII. Manage data retention in Microsoft 365 workloads

A. Describe the retention features in Microsoft 365 workloads.
B. Configure retention settings in Microsoft Teams, Yammer, and SharePoint Online.
C. Recover content protected by retention settings.
D. Regain protected items from Exchange Mailboxes.

XIII. Manage records in Microsoft Purview

A. Discuss the Microsoft Purview Records Management solution and its benefits.
B. List the customer scenarios the Microsoft Purview Records Management solution addresses.
C. Describe the Microsoft Purview Records Management configuration process.
D. Explain what users will experience when the solution is implemented.
E. Articulate deployment and adoption best practices.

XIV. Explore compliance in Microsoft 365

A. Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
B. Plan your beginning compliance tasks in Microsoft Purview.
C. Manage your compliance requirements with Compliance Manager.
D. Manage compliance posture and improvement actions using the Compliance Manager dashboard.
E. Explain how an organization's compliance score is determined.

Course Outline

XV. Search for content in the Microsoft Purview compliance portal

A. Describe how to use content search in the Microsoft Purview compliance portal.
B. Design and create a content search.
C. Preview the search results.
D. View the search statistics.
E. Export the search results and search report.
F. Configure search permission filtering.

XVI. Manage Microsoft Purview eDiscovery (Standard)

A. Describe how Microsoft Purview eDiscovery (Standard) builds on the basic search and export functionality of Content search.
B. Describe the basic workflow of eDiscovery (Standard).
C. Create an eDiscovery case.
D. Create an eDiscovery hold for an eDiscovery case.
E. Search for content in a case and then export that content.
F. Close, reopen, and delete a case.

XVII. Manage Microsoft Purview eDiscovery (Premium)

A. Describe how Microsoft Purview eDiscovery (Premium) builds on eDiscovery (Standard).
B. Describe the basic workflow of eDiscovery (Premium).
C. Create and manage cases in eDiscovery (Premium).
D. Manage custodians and non-custodial data sources.
E. Analyze case content and use analytical tools to reduce the size of search result sets.

XVIII. Manage Microsoft Purview Audit (Standard)

A. Describe the differences between Audit (Standard) and Audit (Premium).
B. Identify the core features of the Audit (Standard) solution.
C. Set up and implement audit log searching using the Audit (Standard) solution.
D. Export, configure, and view audit log records.
E. Use audit log searching to troubleshoot common support issues

XIX. Prepare Microsoft Purview Communication Compliance

A. List the enhancements in communication compliance over Office 365 Supervision policies, which it will replace.
B. Explain how to identify and remediate code-of-conduct policy violations.
C. List the prerequisites that need to be met before creating communication compliance policies.
D. Describe the types of built-in, pre-defined policy templates.

XX. Manage insider risk in Microsoft Purview

A. Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
B. Describe the types of built-in, pre-defined policy templates.
C. List the prerequisites that need to be met before creating insider risk policies.
D. Explain the types of actions you can take on an insider risk management case.

Course Outline

XXI. Implement Microsoft Purview Information Barriers

A. Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
B. Describe the components of an information barrier and how to enable information barriers.
C. Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site.
D. Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.

XXII. Manage Regulatory and privacy requirements with Microsoft Priva

A. Create and manage risk management policies for data overexposure, data transfer, and data minimization
B. Investigate and remediate risk alerts
C. Send user notifications
D. Create and manage Subject Rights Requests
E. Estimate and retrieve subject data
F. Review subject data
G. Create subject rights reports

XXIII. Implement privileged access management

A. Explain the difference between privileged access management and privileged identity management.
B. Describe the privileged access management process flow.
C. Describe how to configure and enable privileged access management.

XXIV. Manage Customer Lockbox

A. Describe the Customer Lockbox workflow.
B. Explain how to approve or deny a Customer Lockbox request.
C. Explain how you can audit actions performed by Microsoft engineers when access requests are approved.