Module Title : MS-500T03-A: Implementing Microsoft 365 Information Protection
Duration : 1 day

About this course

Information protection is the concept of locating and classifying data anywhere it lives. In this course you will learn about information protection technologies that help secure your Microsoft 365 environment. Specifically, this course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, the course explains the deployment of Microsoft Cloud App Security.

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance.

The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, learners should be able to:

- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Azure information protection for Microsoft 365.
- Implement Windows information protection for devices.

Course Outline

Module 1: Information Protection

This module explains information rights management in Exchange and SharePoint. It also describes encryption technologies used to secure messages. The module introduces how to implement Azure Information Protection and Windows Information Protection.

Lessons

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

Lab : Data Loss Prevention

- Create and license users in your organization
- Configure MDM auto-enrollment
- Configure AIP and WIP

After completing this module, students will be able to:

- Describe the different Microsoft 365 Encryption Options.
- Describe the use of S/MIME.
- Describe how Office 365 Message Encryption works.
- Configure labels and policies for Azure Information Protection.
- Configure the advance AIP service settings for Rights Management Services (RMS) templates.
- Plan a deployment of Windows Information Protection policies.

Module 2: Data Loss Prevention

This module is all about data loss prevention in Microsoft 365. You will learn about how to create policies, edit rules, and customize user notifications.

Lessons

- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips

Lab : Data Loss Prevention

- Create and license users in your organization
- Create a DLP policy
- Testing DLP Policies

After completing this module, learners should be able to:

- Describe Data Loss Prevention (DLP).
- Recognize how actions and conditions work together for DLP.
- Use policy templates to implement DLP policies for commonly used information.
- Describe the different built-in templates for a DLP policies.
- Configure the correct rules for protecting content.
- Describe how to modify existing rules of DLP policies.
- Configure the user override option to a DLP rule.
- Describe how to work with managed properties for DLP policies.
- Explain how SharePoint Online creates crawled properties from documents.
- Describe the user experience when a user creates an email that contains sensitive information.

Module 3: Cloud Application Security

This module is all about cloud app security for Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts.

Lessons

- Cloud Application Security Explained
- Using Cloud Application Security Information
- Office 365 Cloud App Security

After completing this module, students will be able to:

- Describe Cloud App Security.
- Explain how to deploy Cloud App Security.
- Control your Cloud Apps with Policies.
- Troubleshoot Cloud App Security.
- Use the Cloud App Catalog.
- Use the Cloud Discovery Dashboard.
- Prepare for Office 365 Cloud App Security.
- Manage cloud app permissions.

Prerequisites

Learners should start this course already having the following skills:

- Basic conceptual understanding of Microsoft Azure
- Experience with Windows 10 devices
- Experience with Office 365
- Basic understanding of authorization and authentication
- Basic understanding of computer networks
- Working knowledge of managing mobile devices