
Microsoft 365 Security Administrator

Duration: 4 Days **Course Code: M-MS500** **Version: A**

Overview:

This course is comprised of the following Microsoft Official Curriculum modules: MS-500T01 Managing Microsoft 365 Identity and Access, MS-500T02 Implementing Microsoft 365 Threat Protection, MS-500T03 Implementing Microsoft 365 Information Protection and MS-500T04 Administering Microsoft 365 Built-in Compliance.

MS-500T01 Managing Microsoft 365 Identity and Access

Help protect against credential compromise with identity and access management. In this course you will learn how to secure user access to your organization's resources. Specifically, this course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to configure Active Directory federation services, how to setup and use Azure AD Connect, and introduces you to Conditional Access. You will also learn about solutions for managing external access to your Microsoft 365 system.

MS500T02 Implementing Microsoft 365 Threat Protection

Threat protection helps stop damaging attacks with integrated and automated security. In this course you will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft's security solutions for them. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and how to use Microsoft 365 Threat Intelligence. It also discusses securing mobile devices and applications. The goal of this course is to help you configure your Microsoft 365 deployment to achieve your desired security posture.

MS500T03 Implementing Microsoft 365 Information Protection

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.

MS500T04 Administering Microsoft 365 Built-in Compliance

Internal policies and external requirements for data retention and investigation may be necessary for your organization. In this course you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. Specifically, this course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations. The course also helps your organization prepare for Global Data Protection Regulation (GDPR).

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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.

Prerequisites:

Delegates wishing to attend the M-MS500 course should 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.

Content:

Module 1: User and Group Security

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to Privileged Identity Management in Azure AD as well as Identity Protection. The module sets the foundation for the remainder of the course.

Module 2: Identity Synchronization

This module explains concepts related to synchronizing identities. Specifically, it focuses on Azure AD Connect and managing directory synchronization to ensure the right people are connecting to your Microsoft 365 system.

Module 3: Federated Identities

This module is all about Active Directory Federation Services (AD FS). Specifically, you will learn how to plan and manage AD FS to achieve the level of access you want to provide users from other directories.

Module 4: Access Management

This module describes Conditional Access for Microsoft 365 and how it can be used to control access to resources in your organization. The module also explains Role Based Access Control (RBAC) and solutions for external access.

Module 5: Security in Microsoft 365

This module starts by explaining the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions to thwart those threats. The module finishes with an explanation of Microsoft Secure Score and how it can be used to evaluate and report your organizations security posture.

Module 6: Advanced Threat Protection

This module explains the various threat protection technologies and services available in Microsoft 365. Specifically, the module covers message protection through Exchange Online Protection, Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection.

Module 7: Threat Intelligence

This module explains Microsoft Threat Intelligence which provides you with the tools to evaluate and address cyber threats. You will learn how to use the Security Dashboard in the Microsoft 365 Security and Compliance Center. It also explains and configures Microsoft Advanced Threat Analytics.

Module 8: Mobility

This module is all about securing mobile devices and applications. You will learn about Mobile Device Management and how it works with Intune. You will also learn about how Intune and Azure AD can be used to secure mobile applications.

Module 9: 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.

Module 10: 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.

Module 11: 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.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK