



Kestus: 40 akadeemilist tundi

Äripäev, Vana-Lõuna 39/1, Tallinn

[Vaata kõiki toimumiskuupäevi](#)

The main purpose of this course is to teach how to secure user access to your organization's resources. The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to setup and use Azure AD Connect, and introduces you to conditional access in Microsoft 365.



During this five-days course students will learn about threat protection technologies that help protect Microsoft 365 environment. Specifically, they will learn about threat vectors and Microsoft's security solutions to mitigate threats. Students will gain knowledge about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. In the course they will learn about information protection technologies that help secure your Microsoft 365 environment. The course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, students will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. 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.

Target audience:

The Microsoft 365 Security administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and to ensure 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 hybrid environments. This role has strong skills and experience with identity protection, information protection, threat protection, security management and data governance.

Job role: Administrator

Preparation for exam: **MS-500**

Features: none

After completing this course, students will be able to:

- Administer user and group access in Microsoft 365.
- Explain and manage Azure Identity Protection.
- Plan and implement Azure AD Connect.
- Manage synchronized user identities.
- Explain and use conditional access.
- Describe cyber-attack threat vectors.
- Explain security solutions for Microsoft 365.
- Use Microsoft Secure Score to evaluate and improve your security posture.
- Configure various advanced threat protection services for Microsoft 365.
- Plan for and deploy secure mobile devices.
- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Windows information protection for devices.
- Plan and deploy a data archiving and retention system.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.
- Explain and use sensitivity labels.

Prerequisites to the course (recommended):

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.

Training Principles:

The training is held in Estonian!

Each learning module is supported by practical exercises with hands-on laboratories.

The prerequisite for issuing the certificate is full participation in training.

Length: 40 academic hours

Access to the individual exercise environment Microsoft Labs Online (MLO) for an additional fee.

Choose the Microsoft exam that suits you and buy it through IT Training 10% cheaper (register your purchase in our exam center until December 31, 2021).

Koolituse läbiviimise põhimõtted:

Koolitus toimub eesti keeles!

Koolituse osad on toetatud praktiliste harjutustega õpilaborites.

Tunnistuse väljastamise eelduseks on koolitusel osalemine terves mahus.

Maht: 40 akadeemilist tundi

Lisatasu eest ligipääs iseseisvale harjutuskeskkonnale Microsoft Labs Online (MLO).

Vali endale sobiv Microsofti eksam ja osta see läbi IT Koolituse 10% soodsamalt (registreeri ost meie eksamikeskuses kuni 31.12. 2021).

Continuing Education Curriculum Group: 0688 Information and Communication Technology Interdisciplinary curriculum group

The training topics and description:

Module 1: User and Group Management

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to the Zero Trust concept as well as authentication. The module sets the foundation for the remainder of the course.

Module 2: Identity Synchronization and Protection

This module explains concepts related to synchronizing identities for Microsoft 365. 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: Identity and Access Management

This module explains 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. We discuss identity governance as a concept and its components.

Module 4: Security in Microsoft 365

This module explains the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions used to mitigate 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 5: Threat Protection

This module explains the various threat protection technologies and services available for Microsoft 365. The module covers message protection through Exchange Online Protection, Microsoft Defender for Identity and Microsoft Defender for Endpoint.

Module 6: Threat Management

This module explains Microsoft Threat Management which provides you with the tools to evaluate and address cyber threats and formulate responses. You will learn how to use the Security dashboard and Azure Sentinel for Microsoft 365.

Module 7: Microsoft Cloud Application Security

This module focuses on cloud application security in Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts. You will learn how these features work to secure your cloud applications.

Module 8: Mobility

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

Module 9: Information Protection and Governance

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

Module 10: Rights Management and Encryption

This module explains information rights management in Exchange and SharePoint. The module also describes encryption technologies used to secure messages.

Module 11: Data Loss Prevention

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

notifications to protect your data.

Module 12: Compliance Management

This module explains the Compliance center in Microsoft 365. It discusses the components of compliance score.

Module 13: Insider Risk Management

This module focuses on insider risk related functionality within Microsoft 365. It covers not only Insider Risk Management in the compliance center but also information barriers and privileged access management as well.

Module 14: Discover and Respond

This module focuses on content search and investigations. The module covers how to use eDiscovery to conduct advanced investigations of Microsoft 365 data. It also covers audit logs and discusses GDPR data subject requests.

More detailed information about the training/ TÄPSEMAT INFOT KOOLITUSE KOHTA SAAD:

<https://docs.microsoft.com/en-us/learn/certifications/courses/ms-500t00>

The training price also includes:

- study materials;
- a trainer's consultation on the topics learned, by e-mail after the training;
- certificate.

As an added value, we offer:

- free parking;
- lunch;
- hot drinks with cookies;
- fresh fruits.

You can participate in the training also with the Unemployment Insurance Fund training card.

See you at the training!

AJAKAVA

09:15 - 09:30 ○ Gathering

The training takes place at Vana-Lõuna 39/1, Tallinn, IT Training premises. You can park in the Europark car park at Veerenni 36, EP63. Parking is free by registering at the IT Training on the first floor.

09:30 - 11:00 ○ I module

11:00 - 11:15 ○ **Coffee break**

11:15 - 12:45 ○ II module

12:45 - 13:30 ○ **Lunch**

13:30 - 15:00 ○ III module

15:00 - 15:15 ○ **Coffee break**

15:15 - 16:45 ○ IV module

LISAINFO

Osalemise tingimused

Registreerudes e-poe, e-kirja või telefoni teel, saadame Teile arve ja täpsema info osalemise kohta. Üksteist päeva enne koolitust saadame Teile e-kirjaga meenutuse osalemise infoga.

Koolitusel osalemine on nimeline, kuid saate osalejat tasuta muuta kuni koolituse alguseni.

Koolituse eest tasumine toimub arvel viidatud arveldusarvele. Arve saadetakse maksja aadressile e-postiga. Arve tuleb tasuda enne koolituse algust arvel märgitud maksetähtajaks.

Kui Te ei saa mingil põhjusel osaleda, palun andke sellest kindlasti teada e-posti aadressil info@koolitus.ee või telefonil 618 1727. Kui teatate koolitusel mitteosalemisest kuni 10 tööpäeva enne algust, pakume mõnd muud samaväärset koolitust või tagastame 100% tasutud koolituse maksumusest. Mitteosalemisest vähemalt 5 tööpäeva varem teatades, tagastame 50%. Muul juhul kuulub arve tasumisele. Raha tagastame ette antud summas juhul, kui pole tehtud koolituse korraldamisega seotud kulutusi (ostetud õppematerjale jms). Koolitusele mitteilmumisel, sellest mitteteatamisel või koolituse poolelühendamisel õppetasu ei tagastata.

IT Koolitusel on õigus koolitusgrupi mitte täitumisel koolituse toimumine edasi lükata või koolitus ära jätta. Koolitusele registreerunud teavitatakse kursuse edasi lükkumisest või ära jätmisest telefoni või e-posti teel. Koolituse ära jäämisel korraldajatest tulenevatel põhjustel makstakse õppetasu tagasi. .

IT Koolitus on Eesti Töötukassa koolituskaardi koostööpartner. Tutvuge koolituskaardi infoga [SIIN](#). Täpsema info saamiseks võtke meiega ühendust telefonil 618 1727 või info@koolitus.ee.