Information Security

Metropolia's activities are guided by existing legislation of public authorities, which instruct on the proper accessibility, availability and integrity of documents and information systems and the data they contain. These policies are continuously developed, monitored and, where necessary, improved. These developments are carried out in cooperation with all Metropolia departments.

(i) **Mandatory information security training for Metropolia's personnel**

How can I find the mandatory information security training course of the personnel?

Dear the staff of the Metropolia university, remember to complete the compulsory information security training by the end of the year. By click the above heading you can read more about completing the course.

Information security in short

Information security is one of the means of achieving data protection. Information security refers to the appropriate protection of various data, systems, services and data transmission using administrative and technical measures. Administrative measures consist of a company's practices, such as its password policy. Technical measures are protection mechanisms functioning in the background, including firewalls and identity management.

Data can be secured through a variety of technical measures, but as a user you are the most responsible for the security of your data.

It's highly recommended to complete the information security training in Moodle.

General guidelines

- Choose a strong password with both upper and lower case letters, numbers and special characters. If someone asks for your password, they are invariably on the wrong side of the tracks. IT services will never ask for your password.
- Always use different passwords for Metropolia services than for other services.
- If you forget your password or accidentally click on a scam message, change your password immediately with strong authentication at salasana. metropolia.fi.
- Do not open suspicious emails. If the suspicious message appears to be from someone you know, contact them by some other means, such as calling them. That way you can verify the authenticity of the message.
- Phishing messages are not limited to email – you may come across them in social media, text messages or instant messaging services (e.g. WhatsApp or Teams). In some cases, scammers call victims by phone. Never give out any of your personal details to unknown people.

Table of contents

Important information security guidelines and rules:

Useful Information management tools

Sensitive data server (Metroarch)

- Metropolia has its own server, which is intended especially for storing and processing sensitive data from RDI-projects. Access rights can be granted to the material on the server for project employees both inside and outside of Metropolia.

Funet FileSender, secure way to share large files

- Funet FileSender is a web based application that allows authenticated users to securely and easily send arbitrarily large files to other users. FileSender is developed to the requirements of the higher education and research community. The service is not intended for permanent storage of files, as the files will be deleted after certain time.

Secure e-mail

- Secure e-mail is a tool that allows sensitive or confidential information to be sent securely to e-mail addresses.

Adobe Creative Cloud

- Adobe Creative Cloud is a set of applications and services that gives access to a collection of software used for graphic design.

E-lomake

- With E-form software, you make inquiries involving the processing of personal data, manage registrations and organize electronic recruitment flexibly, securely and easily.

Problems with computing or IT?

Submit a request of service at
https://hd.metropolia.fi

Phone service +358 9 7424 6777
Week days 8 - 16

Service points and opening hours

Note. Some instructions are only visible to logged in users. You can log in from the Login button in the upper right corner of the screen by using Metropolia, Haka or Visitor login.

Tietoturva ohjeistukset ja säännöt