Secure remote work

The devices used in the remote work are primarily laptops and mobile phones provided by Metropolia. Keep in mind that same information security instructions and regulations apply to the office as while working remotely. Any work-related information should not be disclosed to third parties and the employer's computer should never be given to any third-party members. Third-party members are also family members.

It is recommended to always use VPN outside Metropolia's network for security reasons, but continuous use of VPN in a home office, for example, is not necessary.

1. Use the work computer only for work

Do not use another computer for work other than the computer provided by the company. This ensures that work matters are not confused with personal services or that confidential materials are not stored on your personal computer.

2. Use a reliable network connection

Publicly open network connections are not reliable off-campus. For example, wireless connections in airports or shopping malls are not safe to use. **If you use any public networks for work you should always use VPN-connection.**

If the work is done away from home, it is possible to share an internet connection from a mobile phone, which is more secure than a public network connection. Sharing a network connection from your phone is easy, see instructions (Finnish) on Elisa website.

3. VPN-connection

Prolonged remote work can affect security and software updates to your computer if the computer has not been connected to your corporate network through a VPN connection. Therefore, it necessary to connect to VPN connection on for about two hours at a time, 1-2 times a week. This way any updates can be downloaded to your computer. Note. A VPN connection should not be used unnecessarily if the job description does not require it. More detailed instructions on using a VPN connection can be found here.

When traveling abroad all network connections must always be used with a VPN-connection while working, including wired networks and password-protected network connections. A VPN-connection protects data with encryption, which prevents an outsider from reading the data traffic. There is guide for traveling abroad, that must be followed while abroad.

4. Remote workstation

A mobile person may have to work remotely anywhere, anytime. It is important to keep the remote workstation in a safe location so that no outside person can see or hear confidential matters. So keep in mind where you can work without others being able to hear your conversation or see your computer screen.

5. Watch out for scams

There are currently scams and emails made in the name of technical support, among other things. The coronavirus is ruthlessly exploited in various scam attempts. So be careful what you click and where you provide your information.

If you have click a link in a phishing email act as instructed:

1. Change your password IMMIDEADTLY at https://salasana.metropolia.fi
2. Contact Helpdesk by calling the phone service, 09 7424 6777 (open weekdays 8-16). If the phone services are not available, open a service ticket at https://hd.metropolia.fi or by email helpdesk@metropolia.fi

Tietoturvallinen etätyö