HOW TO WORK FROM HOME SAFELY

opsec
www.opsec.fi

USERNAME AND PASSWORD

- Never disclose your usernames or passwords to anyone else, or store them in a place that leaves them accessible for anyone else than you. Use different passwords for different services and systems, and make sure that your passwords are strong. If necessary, use employer-approved password management program.

DEVICES, SYSTEMS, SOFTWARE AND CONNECTIONS

- Work devices are meant for completing work tasks, and work-related data may only be saved on the employer's information systems, equipment and data storage.
- Only use employer-approved devices to carry out work. Do not allow anyone else to use the employer's devices, and shut down or lock the devices whenever you leave them unattended.
- Only connect the devices to a secure network specified by the employer. If you are using a VPN connection, make sure that it is enabled.
- Make sure that your device, system and software are all updated and that your equipment has employer-approved antivirus software enabled.
- Don't forget to protect and update other devices on your home network, too.
- Do not store devices in cold, hot or damp conditions. Do not place drinks too close to your device, and make sure that other members of your household do not accidentally damage your devices, disconnect, or disable antivirus software.

E-MAIL, PHONE CALLS, TEX MESSAGES AND SOCIAL MEDIA

- Be generally careful with regard to what you react to, what you open, what you click, and what you share.
- Check the content, significance and context of messages and calls. Be suspicious if a message or call attempts to persuade you to do something such as open a link, visit a site, download an attachment, share content, provide your own or your employer's details, give personal data, any arrangements involving money, etc. Assess whether the content of the message or call is valid; is the caller or sender entitled to the information, are they who they claim to be, would the sender truly send this type of message, etc.?
- Never respond to calls or messages that you suspect to be from a scam company. If necessary, verify the authenticity of the message by contacting the sender or asking a specialist for advice.
- Remember that scam companies may seem very genuine. For example, the address and signature of an e-mail sender may correspond to those of someone you know.

PHYSICAL DATA

- Store hard copies of data, such as print-outs, in locked spaces and make sure that no-one else can access them. Use confidential waste containers to destroy data. Never take data to normal waste containers.

PROBLEMS WORKING FROM HOME?

If you encounter any problems or suspicious situations, always contact the party responsible for data administration, data security and data protection:

opsec

TECHNICAL SUPPORT AND ON-CALL SERVICE

Telephone: +35820 198 66 96
E-mail: tuki@opsec.fi