



# 10 soovitus TURVALISEKS KAUGTÖÖKS

Juuli 2025

Kaugtöö on tänapäeval äärmiselt levinud töötegemise vorm, mida oleme harjunud tegema kodus, kohvikus, rongis, lennukis jm. Asutuse infoturbe tagamiseks on kaugtööd tehes oluline järgida üldisi turvalise kaugtöö soovitusi ja pidada kinni enda asutuse arvutitöökoha kasutamise juhenditest.

## 1. Hoida töö- ja eraelu lahus

**Kasuta tööks vaid tööarvutit ja -telefoni ning kasuta neid vaid ise!**

Kasuta töö tegemiseks vaid tööandja antud seadmeid, vältides isiklikes seadmetes tööandja andmete töötlemist.

Tööseadmetes tee ainult tööasju ning isiklikud tegevused, näiteks e-poes ostlemine, jäta isiklikesse seadmetesse.

Tööseadmeid ei tohi anda kasutada mitte kellelegi teisele, ka oma lastele mitte. Esmapilgul võib lapse Zoomi koolitund või veebimäng tunduda ohutu, kuid ka nii võib seadmesse jõuda pahavara või lekkida andmeid.

## 2. Tea ja järgi tööandja reegleid ning ole teadlik küberohtudest

Tutvu tööandja arvutikasutuse, kaugtöö jm valdkonda reguleerivate reeglite ja põhimõtetega ning järgi neid. Et olla teadlik küberohtudest, läbi alati tööandja poolt pakutavad küberhügieeni kursused ja testid ning tutvu jagatud infoturbematerjalide ning portaalis itvaatlik.ee olevate juhistega.

## 3. Väärtusta privaatsust

**Kaugtööd tehes on oluline olla teadlik keskkonnast, kus tööd tehakse, et tagada seadmete füüsiline turvalisus ja hoida tööandja andmed kaitstuna.** Leia töö tegemiseks võimalikult privaatne ja rahulik asukoht, kus saad keskenduda ja tagada tööandmete konfidentsiaalsuse:

- Taga seadmete füüsiline turvalisus, et keegi ei saaks neid ära varastada, sinna midagi ühendada või neid kuidagi kahjustada.
- Jälgi, et monitor või telefoni ekraan on paigutatud nii, et keegi üle õla või kõrvalt ei näeks parooli sisestamist või ekraanil kuvatavat tööinfot. Jälgi ka, et sa ei ole ühegi võõra kaamera vaateväljas.
- Kui kasutad sülearvutit avalikus ruumis, näiteks ühistranspordis või kohvikus, tasub ekraanile paigaldada privaatsusfilter. Privaatsusfilter ei anna 100% kindlust, et ekraanil toimuv jääb kõrvaliste inimeste eest varju, kuid vähendab oluliselt selle tõenäosust.
- Asutusesiseste ja tundlike teemade arutamisel jälgi alati, et kõrvalised inimesed vestlust ei kuuleks.
- Videokoosolekuid tehes jälgi, et kõnes ei oleks kõrvalisi isikuid, sinu taustal ei oleks konfidentsiaalset teavet ja et sa ei paljastaks seda ka ekraani jagades.
- **Avalikus ruumis ei tohi jätta arvutit järelevalveta. Privaatses ruumis arvuti juurest lahkudes lukusta alati ekraan ja eemalda ID kaart.**

## 4. Kasuta turvalist võrguühendust

Kasuta internetti ühendumiseks mobiili hotspoti või turvalist kodust võrku ja tööandja VPNi, mis loob sinu arvuti ja tööandja serveri vahele turvatud ühenduse. Välti avalike WiFi võrkude kasutamist.

Koduse võrgu turvalisuse tagamiseks seadista kodune WiFi ruuter ja tulemüür:

- Veendu, et sinu kodune ruuter on tootja poolt toetatud ja sellele antakse välja turvauuendusi ning et viimased turvauuendused on paigaldatud. Kui ruuter ei ole enam tootja poolt toetatud, tuleb see välja vahetada ja sellise seadme kaudu kaugtööd teha ei tohi.

- Veendu, et ruuterile on seatud tugev ja unikaalne parool.
- Kasuta WPA3-krüpteerimist (*encryption*), kui see on ruuteril valikus. Kui mitte, siis kasuta WPA2 pika ja tugeva parooliga.
- Vajadusel muuda ära koduse WiFi võrgu nimetus, et see ei oleks sinuga seostatav.
- Oma ülevaadet kõigist oma kodusse võrku ühendatud seadmetest ja turva need (tugevad unikaalsed paroolid, tarkvara regulaarne uuendamine).
- Kui kasutad paljusid värvõrguseadmeid (IoT) ja jagad oma WiFi-t külalistega, planeeri oma võrk segmenteerituna ehk tükeldatuna virtuaalseteks kohtvõrkudeks (näiteks põhivõrk, IoT seadmete võrk, külaliste võrk), millele saab kodus ruuteris määrata erinevad õigused.

## 5. Tee tööd ainult lubatud kanalites

Hoia kogu tööalane suhtlus ja failivahetus vaid tööandja lubatud kanalites ja tööandja antud kontrol (tööandja e-mail, Teams, RocketChat, Zoom, Slack, Signal, iMessage, FaceTime, MS OneDrive/SharePoint vmt). Väldi isiklike kanalite (Messenger, isiklik DropBox, Gmail vmt) kasutamist tööalaseks suhtluseks, kuna see suurendab andmelekke riski.

## 6. Taga tööandja seadmete ja rakenduste turve

Taga kõigi tööandja antud (aga ka isiklike seadmete) turvalisus. Selleks jälgi, et seadmel oleks:

- Aktiveeritud ekraanilukk (PIN kood või parool);
- Operatsioonisüsteem ja rakendused uuendatud;
- Rakendused laetud ainult ametlikest rakendusepoodidest ning kasutuse rakendused eemaldatud;
- Rakendustele antud vaid õigused, mida rakendus vajab oma funktsiooni täitmiseks;
- Paigaldatud viirusetõrjetarkvara;
- Jälgi, et kõik kontod on kaitstud tugeva unikaalse parooli ja 2-astmelise autentimisega.

## 7. Arvesta välisriigis kaugtöö tegemise eripäradega

**Kaugtöö välisriigis kooskõlasta alati vahetu juhi ja infoturbejuhiga.**

Välisriiki reisimisel jälgi alati, et tööandja seadmed oleksid sinu kontrolli all:

- Transpordi seadmeid vaid käsipagasis;
- Taga seadmete turvalisus hotellis ja ka mujal viibides;
- Kasuta vaid oma mobiili hotspoti ja väldi avalike WiFi võrkude kasutamist;
- Ära jaga teavet välisriigis viibimise kohta sotsiaalmeedias;
- Kasuta seadme laadimiseks vaid vooluvõrgu pistikut ja oma laadijaid. Ära lae seadet avalikus laadimispunktis, kuna sealsete laadimiskaablite kaudu saab seadmest andmeid varastada või seadmesse pahavara paigaldada;
- Arvesta, et mõne riigi piirikontrollitöötajatel on õigus nõuda ligipääsu reisija seadmetesse (arvutid, telefonid jms).

## 8. Väldi riskiriike ja konfliktipiirkondasid<sup>1</sup>

**Kaugtöö tegemine riskiriikides ja konfliktipiirkonnas on üldjuhul mittesoovitav ja sellistesse riikidesse on tööandja seadmete kaasa võtmine üldjuhul keelatud.**

Riskiriiki või konfliktipiirkonda reisimisel küsi täpsemaid juhiseid enda asutuse infoturbejuhilt.

## 9. Seadme rikke või kaotuse korral teavita kohe tööandjat

**Kui seade kaob või varastatakse, võta koheselt ühendust asutuse IT abiga.** Kui seade läheb katki või vajab tehnilist abi, võta ühendust oma asutuse IT abiga ja too seade kontorisse (kulleriga saatmine või ise remontija valimine ei ole lubatud). Kui oled kasutanud kahtlast WiFi võrku või märkad arvuti juures midagi ebatavalist, võta ühendust IT abiga, kust saad juhised edasi tegutsemiseks.

## 10. Ole valvas õngitsuskirjade ja sotsiaalse manipulatsiooni suhtes

Küberrünnak algab sageli õngitsuskirjast või sotsiaalsest manipulatsioonist. Kontrolli kirja saamisest ja kirjutamisest alati saatja ja saaja usaldusväärsust. Samuti ära ava kirja saamisest tundmatuid manuseid ega linke. Ole tähelepanelik ja ära jaga infot, kui keegi tunneb huvi sinu töö või tööseadmete vastu.

<sup>1</sup> Riskiriikideks loetakse järgmisi riike: Venemaa Föderatsioon, Valgevene Vabariik, Armeenia Vabariik, Aserbaidžaan Vabariik, Hiina Rahva-vabariik (sh Hongkongi ja Macau erihalduspiirkond), Iraani Islamivabariik, Kasahstani Vabariik, Kirgiisi Vabariik, Korea Rahvademokraatlik Vabariik (Põhja-Korea), Tadžikistani Vabariik, Türkmenistan, Usbekistani Vabariik