

Tietoturvallinen etätyö

Etätyössä käytettävistä tietoteknisistä välineistä ensisijaisesti käytetään Metropolian kannettavaa tietokonetta ja matkapuhelinta. Tietoturvallisuutta koskevat samat ohjeet ja määräykset kuin varsinaisella työpaikalla. Tietoja ei saa paljastua ulkopuolisille, eikä työnantajan tietokoneita saa luovuttaa ulkopuolisten käyttöön. Ulkopuolisilla tarkoitetaan myös perheenjäseniä.

VPN:ää suositellaan käytettäväksi aina Metropolian verkon ulkopuolella tietoturvasyistä, mutta esim. kotitoimistolla VPN jatkuva käyttö ei ole tarpeellista.

1. Käytä työtietokonetta vain työnteekoon

Älä käytä etätöissä muuta tietokonetta työn tekemiseen, kun yritykseltä saatua tietokonetta. Siten takaat, että työasiat eivät sekoitu henkilökohtaisiin palveluihin tai salassa pidettäviä materiaaleja ei tallenneta omalle henkilökohtaiselle tietokoneelle.

2. Käytä luotettavaa verkkoyhteyttä

Julkiset avoimet verkkoyhteyden eivät ole luotettavia kampuksen ulkopuolella. Esimerkiksi lentokenttien tai kauppakeskusten langattomat yhteyden eivät ole turvallisia käyttää. **Jos käytät julkisia verkkoyhteyksiä kuten edellä mainituissa paikoissa on VPN-yhteyttä käytettävä aina.**

Jos työnteke tehdään muualla kuin kotona pystyy matkapuhelimesta jakamaan verkkoyhteyden, joka on turvallisempi kuin julkinen verkkoyhteys. Verkkoyhteyden jakaminen puhelimesta on helppoa ks. ohje [Elisan verkkosivuilta](#).

3. VPN-etäyhteys

Pitkään jatkunut etätyö vaikuttaa tietokoneelle tuleviin tietoturva- ja ohjelmistopäivityksiin silloin kun tietokone ei ole ollut yhteydessä yrityksen verkkoon VPN-yhteyden avulla. Sen vuoksi on pidettävä VPN-yhteyttä päällä noin kaksi tuntia kerrallaan 1-2 kertaa viikossa, jotta mahdolliset päivitykset latautuvat tietokoneelle. Muuten VPN-yhteyttä ei pidä turhaa käyttää, jos työnkuva ei sitä vaadi. Tietohallinnon sivuilta löytyy tarkempi ohje [VPN-etäyhteyden käytöstä](#).

Ulkomaanmatkalla on muistettava, että työskennellessä kaikkia verkkoyhteyksiä on käytettävä aina VPN-yhteyden kanssa, mukaan lukien lankaverkot ja salasanaa suojatut verkkoyhteydet. VPN-yhteys suojaa datan kryptauksella, jolloin ulkopuolinen ei pysty lukemaan verkkoliikenteessä liikkuvaa dataa. Ulkomaanmatkoihin koskevasta työnteosta on laadittu [IT-ohjeistus](#).

4. Etätyöpisteen sijainti

Liikkuva ihminen voi joutua tekemään etätyötä missä, milloinkin. Tärkeätä on huolehtia etätyöpisteen turvallisesta sijainnista siten, että ulkopuolinen henkilö ei pysty näkemään tai kuulemaan luottamuksellisia asioita. Mieti siis missä voit työskennellä ilman, että muut voivat kuulla keskustelujasi tai nähdä tietokoneesi ruutua.

5. Varo huijauksia

Tällä hetkellä liikkeellä on muun muassa teknisen tuen nimissä soitettuja huijauspuheluja ja sähköposteja. Koronavirusta hyödynnetään häikäilemättömästi erilaisissa huijausyrityksissä. Ole siis tarkkana, mitä klikkaat ja mihin tietojasi annat.

Jos olet klikannut linkkiä huijausviestissä toimi näin:

1. Vaihda salasanasasi VÄLITTÖMÄSTI osoitteessa <https://salasana.metropolia.fi>
2. Ilmoita asiasta Helpdeskille soittamalla Helpdeskin puhelinpalveluun, 09 7424 6777 (avoinna arkisin klo 8–16). Jos puhelinpalvelu ei ole avoinna, ilmoita asiasta tekemällä palvelupyyntö osoitteessa <https://hd.metropolia.fi> tai sähköpostitse helpdesk@metropolia.fi

[Secure remote work](#)