Etätyöntekijän tietoturvan ja tietosuojan muistilista

Jokainen on velvollinen huolehtimaan tietoturvasta ja tietosuojasta.

Työntekijän oma vastuu tietoturvallisuuden ja tietosuojan hoitamisesta lisääntyy etätyön myötä. Työntekijän tulee kiinnittää toiminnassaan huomiota tietoturvallisiin menettelytapoihin toimiessaan työpaikan toimitilojen ulkopuolella.

Varmuuskopioi.

- **Varmuuskopioiden tarkoituksena on estää tiedon häviäminen.** Varmuuskopioita täytyy muistaa ottaa riittävän usein, aina silloin kun tieto on muuttunut.

Tietokoneen ja älypuhelimen vastuullinen käyttö.

- Tee etätöitä työnantajan tähän tarkoitukseen luovuttamilla laitteilla
- Älä asenna työtehtävien ulkopuoliseen toimintaan liittyviä ohjelmistoja
- Älä anna laitteistoja sivullisten käyttöön
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla, kirjautumalla ulos toimialueelta tai sammuttamalla työasema, kun poistut työpisteeltäsi.
- Älä pidä älypuhelinta luottamuksellisen tiedon varastointipaikkana.
- Huolehdi, että työpuhelimissa käytetään mm. näytön lukitusta ja aikakatkaisua, rajoitetaan lukitusnäytöllä näkyvien ilmoitusten sisältöä sekä huolehditaan puhelinten paikannusasetuksista, salauksesta ja tarvittaessa puhelinten tietojen tyhjennyksestä.
- Puhelinta ei myöskään saa koskaan luovuttaa ulkopuolisille tai jättää ilman valvontaa.

Käyttäjätunnukset, salasanat ja muut tunnisteet

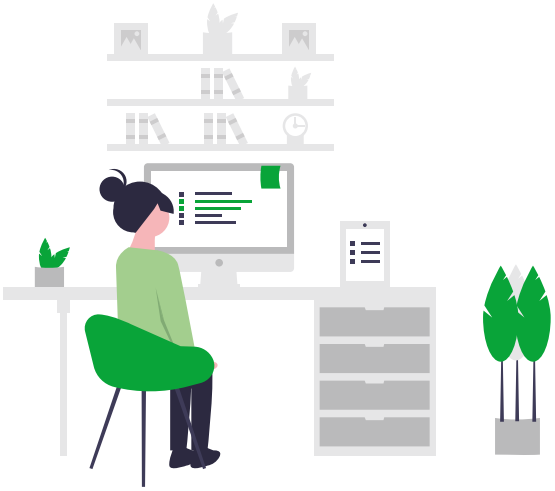
- Omia tunnuksia, salasanoja tai muita tunnisteita (pin-koodit, toimikortit ja muut tunnistusvälineet) ei saa luovuttaa ulkopuolisille tai säilyttää siten, että muut saavat ne tietoonsa.
- Älä luovuta organisaatiolta saamaasi käyttäjätunnusta ja salasanaa kenellekään. Älä myöskään käytä samoja tunnuksia missään Internetin palveluissa.
- Käytä vaikeasti arvattavia ja kyllin pitkiä salasanoja tai lauseita. Tärkeää salasanan luomisessa on se, että teet siitä sellaisen jonka muistat.
- Ota mahdollisuuksien mukaan kaksi- tai monivaiheinen tunnistautuminen käyttöön sähköpostissasi ja sosiaalisen median tileissäsi. Ne antavat merkittävää lisäsuojaa mahdolliselta luvattomalta tunkeutumiselta.

Työskentelytiloissa huomioitavaa

- Työskentelytilojen on vastattava käsiteltävän tietoaineiston turvallisuusvaatimuksia
- Varmista, että sivulliset, kuten perheenjäsenet, eivät käytä työorganisaation töihin tarkoitettuja laitteita ja kotona mukana olevia työpapereita
- Huolehdi ovien ja ikkunoiden lukitsemisesta
- Hoida etätapaamiset kodissasi mahdollisuuksien mukaan siten, että muut kodissa olijat eivät kuule työhösi liittyviä asioita.

Luottamuksellisten tietojen käsittelyssä huomioitavaa

- Vältä mahdollisuuksien mukaan salassa pidettävien ja muuta luottamuksellista informaatiota sisältävien tietojen tulostamista paperille tai tallentamista työpaikan ulkopuolella säilytettäville tietovälineille.
- Älä laita luottamuksellista materiaalia roskakoriin vaan ne on ohjeiden mukaisesti tuhottava (esim. silppuaminen).



- Tarvittaessa aineistojen säilytyspaikka tulee voida lukita.
- Älä pidä luottamuksellisia asiakirjoja turhaan luettavana työpisteellä. Käytä kansioita ja lukittuja kaappeja tai laatikoita.
- Vältä puhumasta luottamuksellisista työasioista ja henkilötiedoista julkisilla paikoilla ja kulkuvälineissä
- Luottamuksellisten asioiden käsittely sosiaalisissa medioissa on kielletty
- Jos työskentelet julkisissa tiloissa, varmistu, etteivät muut henkilöt pysty näkemään käsittelemiäsi tietoja ja asiakirjoja. Älä käytä julkisia päätteitä (esim. nettikahvilat, kirjastot) työasioihin.
- Yksityiset verkkopalvelutilisi, kuten sähköposti tai pilvipalvelut, eivät ole työtäsi koskevien tietojen ja tiedostojen jakamiseen tarkoitettuja.

Tietoliikenneyhteydet

- Tietoliikenneyhteyden ottamisessa ja tietojen välittämisessä työpaikalle tulee käyttää vain sovittuja tapoja ja huolehtia, että sovitut salaus- ja suojausmenettelyt ovat käytössä (esim. palomuuri on päällä ja virustorjunta on ajan tasalla).
- Periaatteena on, ettei kannata käyttää mitään verkkoja, joiden tietoturvaan et voi luottaa. Vieraan verkon sijaan kannattaa käyttää esimerkiksi oman puhelimen verkkoyhteyttä. Jos käytät etätöissä langatonta lähiverkkoa eli WLANia tai WiFiä, katsothan että se on suojattu salasanalla.

Ole tarkkana seuraavissa asioissa:

- Tarkista selaimen osoiteriviltä, että käytössä on salattu yhteys (https://).
- Tarkasta linkin oikeellisuus ennen kuin klikkaat linkkejä (esim. sähköpostiin saapuneiden linkkien osalta)
- Jos saamasi sähköposti aiheuttaa epäilystä, älä avaa sen liitetiedostoja. Hälytyskellojen pitää soida, jos viesti on kirjoitettu huonolla suomella tai se sisältää kirjoitusvirheitä.
- Myös sosiaalisessa mediassa kiertää paljon kalasteluviestejä, joten mieti ennen kuin klikkaat.
- Viranomaiset tai esimerkiksi pankkisi eivät koskaan tiedustele salasanojasi tai muuta arkaluontoista tietoa sähköpostitse.

Ongelmatilanteet

- Työntekijän tulee huolehtia, että hän osaa toimia erilaisissa ongelmatilanteissa, kuten esim. yhteysongelmat, laiteviat ja laitteiden tai tietojen varastaminen.

Muista myös itseäsi

- Älä rasita itseäsi liikaa, muista että aivot tarvitsevat taukoja ja lepoa. Levänneenä muistikin toimii paremmin ja virheitä tulee tehtyä harvemmin.