Rekisterinpitäjä: Nupumies Oy

Henkilötietojen käsittelijä: Palvelun tarjoaja

Rekisterinpitäjän ohje henkilötietojen käsittelystä

Alla ohjeita henkilötietojemme käsittelyyn:

- Käytettävien tietokoneiden ohjelmat on pidettävä päivitettyinä ja hyvässä kunnossa yrityksemme asioita käsiteltäessä.
- Tietokoneiden käyttöjärjestelmät (esim. Windows, Apple, Linux) ja muut käytössä olevat ohjelmat on päivitettävä aina, kun uusia päivityksiä on saatavilla.
- Palomuurit ja virustorjunta on oltava asianmukaisia ja päivitettynä.
- Työasemat, jossa yrityksemme asioita käsitellään, saa käyttää vain käyttäjän omalla käyttäjätunnuksella ja salasanalla.
- Epäiltäessä työaseman olevan haittaohjelman saastuttama, työasemalla työskentely on lopetettava välittömästi ja tästä on ilmoitettava yrityksen vastaavalle.
- Yritykseemme liittyvien tietojen sähköpostitse siirtämisessä on käytettävä Suomen valtakunnan verkossa olevaa palveluntarjoajaa. Ilmaissähköpostiosoitteita, kuten gmail, hotmail, yahoo ei ole sallittua käyttää.
- Luottamuksellista materiaalia saa siirtää ainoastaan suojatusti, kuten esim. SafeMail, Deltagon tms. turvallista tiedonsiirtopalvelua käyttäen.
- Avoimia julkisia yhteyksiä (VR / hotellit / tms) ei yritykseemme liittyvässä tietojen siirrossa saa käyttää.
- Käyttäjätunnus ja salasana mahdollisiin yrityksemme järjestelmiin on pidettävä turvassa ja niitä ei saa antaa muiden tietoon. Tunnuksella on aina vastuullinen haltija, joka vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä ja tapahtumista. Käyttöoikeudet on myös poistettava toimeksiannon tai sopimuksen päättyessä.
- Salasana on vaihdettava heti sen saamisen jälkeen. Hyvä salasana on sellainen, jonka muistat itse helposti, mutta jota ulkopuoliset eivät pysty murtamaan. Älä käytä salasanoina jokapäiväisiä tai sinuun ja perheeseesi liittyviä sanoja, ihmisten / lemmikkien nimiä.
- Yrityksemme järjestelmiin liittyvien salasanojen on oltava vähintään 10 – merkin mittaisia.
- Salasanoja ja käyttäjätunnuksia ei saa kirjoittaa lapulle, tallentaa tietokoneelle, ilmoittaa sähköpostitse tai säilyttää asiattomien henkilöiden ulottuvilla.
- Mobiilien päätelaitteiden osalta riski joutua anastusrikoksen uhriksi on suurempi kuin pöytätietokoneiden, joten salaus tulisi ottaa erityisesti niiden käytössä huomioon.

- Pelkkä käyttäjätunnus ja salasana suojaavat tietokoneeseen kirjautumista, mutta eivät tietokoneessa, ulkoisella kovalevyllä, puhelimessa, muistissa tai kiintolevyllä olevaa sisältöä. Siksi kiintolevyn salaaminen eli kryptaus on suositeltavaa.

- Työasemien (sisältää myös tietoverkkoon langallisesti/langattomasti liitetyt atk-laitteet), tietoliikenneverkon ja atk-järjestelmien käyttöoikeudet annetaan vain niille, jotka ovat allekirjoittaneet salassapitosopimuksen.

- Palvelussuhteen/muun työtehtävän aikana tai sen päätyttyä ei työssä saatuja asiakkaitamme, sopimuskumppaneitamme tai muita yhteistyötahoja koskevia luottamuksellisia tai salassa pidettäviä tietoja saa ilmaista ulkopuoliselle tai sivulliselle.

- Rekisterien katselu- tai käyttöoikeutta ei ole muihin kuin tehtävien edellyttämiin tietoihin.

- Mikäli luottamuksellisia paperiaineistoja käsitellään muualla kuin henkilötietojen käsittelijän toimitiloissa, on huolehdittava niiden asianmukaisesta säilyttämisestä sekä tietoturvallisesta hävittämisestä.

- Yhteytenä kotona käytetään vain esimerkiksi henkilökohtaista salasanalla suojattua verkkoa ja tai älypuhelimen tukiasemaa.

- Toimitilojen fyysisestä turvallisuudesta on huolehdittava. Kokonaisuuden kannalta tarkoituksenmukaisinta olisi tehdä tietoturvaselvitys, joka uusitaan säännöllisin väliajoin.

- Luottamuksellinen aineisto tulee aina hävittää tietoturvallisesti, ei koskaan tavallisen jätteen mukana.

- Muistitikkujen käyttö ei ole suositeltavaa ja luottamuksellista materiaalia sinne ei saa tallentaa ollenkaan.
- Rekisteröity saattaa pyytää itseään koskevia tietoja joko luovutettavaksi tai tarkastettavaksi. Ennen luovuttamista tai ilmaisemista on aina varmistuttava tiedustelijan henkilöllisyydestä.

- Tiedon siirrolle kolmannelle taholle tulee aina olla asetuksen mukainen peruste (esim. laki, sopimus, oikeutettu etu tai suostumus). Älä siirrä tietoa, ennen kuin ole varmistunut siirron asetuksen mukaisuudesta.

Jos olt epävärma siitä, miten pitää toimia, ota yhteyttä tietoturvasta ja –suojasta vastaavaan henkilöömme

Rikkomuksista tiedotetaan aina esimiehelle. Jos kyseessä on tahallinen tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli tahallisesta rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, on aiheuttaja myös vahingonkorvausvelvollinen.
Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

Havaitsemistasi tietosuojarikkomuksista tai sellaisen yrityksistä tulee aina ilmoittaa välittömästi tietohallintopalveluista vastaavalle. Yrityksen on ilmoitettava 72 tunnin sisällä kirjallisesti henkilötietojen tietoturvaloukkauksesta saatuaan sen tietoonsa viranomaiselle.
Tietokoneviruksista on aina ilmoitettava tietohallintopalveluista vastaavalle.