Tietosuojaohje

Tietosuoja

-Käytettävän tietokoneen ohjelmat on pidettävä päivitettyinä ja hyvässä kunnossa käsiteltäessä yhdistyksen asioita.

-Tietokoneiden käyttöjärjestelmät (esim. Windows, Apple, Linux) ja muut käytössä olevat ohjelmat on päivitettävä aina, kun uusia päivityksiä on saatavilla.

-Myös kaikki muut ohjelmat on suositeltavaa päivittää säännöllisin väliajoin.

-Työasemaa, jossa käsitellään yhdistyksen asioita saa käyttää vain omalla käyttäjätunnuksella ja salasanalla.

-Epäiltäessä työaseman olevan tietokoneviruksen saastuttama, työasemalla työskentely on lopetettava välittömästi ja tästä on ilmoitettava yhdistyksen vastaavalle.

-Turvattomille tai epäilyttäville verkkosivuille meneminen on kiellettyä.

-On suositeltavaa käyttää tehtävää perustuvia sähköpostiosoitteita, kuten esimerkiksi ”hallituksenpj@yhdistys.fi.”

-Virusriskin vuoksi ulkopuolelta tulevan sähköpostin liitetiedostoja ei saa avata, jos viesti tulee epämääräisestä lähteestä.

-Roskapostiviestit on hävitettävä.

-Sähköpostiketjukirjeitä ja muuta niin sanottua roskapostia ei saa lähettää eikä välittää eteenpäin, vaan ne on tuhottava.

-Avoimia julkisia yhteyksiä (VR / hotellit) ei saa työtehtävissä käyttää, vaan tulee käyttää esimerkiksi matkapuhelimen jaettua datayhteyttä.

-Käyttäjätunnus ja salasana mahdollisiin yhdistyksen järjestelmiin on pidettävä salassa. Niitä ei saa antaa muiden tietoon. Käyttäjätunnukset ovat henkilökohtaisia. Tunnuksella on aina vastuullinen haltija (henkilö), jonka nimiin tunnus on myönnetty. Kukin vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä ja tapahtumista. Vapaaehtoistyön päättyessä poistetaan automaattisesti myös käyttöoikeudet.

-Salasana on vaihdettava heti sen saamisen jälkeen ja myöhemmin sovituin aikavälein tai tarvittaessa. Valitse salasanasi huolellisesti. Hyvä salasana on sellainen, jonka muistat itse helposti, mutta jota ulkopuoliset eivät pysty murtamaan. Älä käytä salasanoina jokapäiväisiä tai sinuun liittyviä sanoja.

-Salasana on satunnainen merkkijono.

-Salasanoja ja käyttäjätunnuksia ei saa kirjoittaa lapulle, tallentaa tietokoneelle, ilmoittaa sähköpostitse tai säilyttää asiattomien henkilöiden ulottuvilla.

-Kannettavien tietokoneiden 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/tietoja. Tunnukset on helppo ohittaa, jolloin tietoihin päästään käsiksi. Siksi kiintolevyn salaaminen eli kryptaus on suositeltavaa. Mikäli kone anastetaan, tiedostoja ei voida lukea ilman kryptauksen salasanaa.

-Työasemien (sisältää 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 asiakkaita, sopimuskumppaneita 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 käsittelet luottamuksellisia paperiaineistoja kotona, huolehdi niiden asianmukaisesta säilyttämisestä ja hävittämisestä.

-Yhteytenä kotona käytetään vain esimerkiksi henkilökohtaista salasanalla suojattua kotiverkkoa ja tai kannettavan puhelimen tukiasemaa.

-Yhdistyksen toimitilat on tarkoitettu niiden toimintaa varten, muu toimitilojen käyttö on kiellettyä, ellei tähän ole annettu kirjallista lupaa. Asiattomia ja ulkopuolisia henkilöitä ei saa päästää tiloihin. Vapaaehtoistyöntekijän poistuessa, hänen on varmistuttava, että ovet ja ikkunat menevät kiinni ja lukkoon. Luvatonta henkilöä ei saa päästää tiloihin. Mikäli työntekijä kohtaa

tiloissa henkilön, jonka oleskelun tarkoituksesta tiloissa ei ole varmuutta, on työntekijän velvollisuutena tiedustella asiaa henkilöltä.

-Jos tulostat yhteiskäytössä olevalle kirjoittimelle, nouda tuloste heti tulostamisen jälkeen. Luottamuksellisia asiakirjoja ei koskaan tule heittää tavalliseen roskakoriin vaan erilliseen lukittuun astiaan, josta ne hävitetään turvallisesti.

-Muistitikkujen käyttö ei ole suositeltavaa. Luottamuksellista materiaalia ei tule siirtää muistitikulle. Yhtiön muistitikuilla saa säilyttää pelkästään sellaisia yleisiä materiaaleja, joiden vuotaminen julkisiksi ei aiheuta tietoturvavahinkoa.

-Samoja tallennusvälineitä tai muita tietokoneeseen liitettäviä tietovälineitä ei saa käyttää yhdistyksen tehtävissä ja sen ulkopuolella, jollei ole varmistautunut niiden viruksettomuudesta.

-Rekisteröity saattaa pyytää itseään koskevia tietoja joko luovutettavaksi tai tarkastettavaksi. Ennen luovuttamista tai ilmaisemista on aina varmistuttava tiedustelijan henkilöllisyydestä. Esimerkiksi sähköpostiosoite ei yksilöi henkilöä. Tunnistautumisen täytyy aina tapahtua joko henkilökohtaisesti, luotettavaa tunnistautumistapaa käyttäen kuten henkilökohtainen salasana, jos tällainen järjestelmä on tai esimerkiksi pankkitunnustunnistautumista käyttäen.

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

Jos et ole varma kuinka tulee toimia, ota yhteyttä tietoturvasta ja –suojasta vastaavaan henkilöön:

[Nimi ja yhteystiedot]

Epäselvässä tilanteessa toimen toteuttaminen ohjausta kysymättä on kiellettyä.

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. Yhdistyksen on ilmoitettava 72 tunnin sisällä kirjallisesti henkilötietojen tietoturvaloukkauksesta saatuaan sen tietoonsa viranomaiselle.

Tietokoneviruksista on aina ilmoitettava tietohallintopalveluista vastaavalle.

Kaikista käyttäjätunnusta ja salasanaa koskevista epäselvistä tiedusteluista tulee ilmoittaa välittömästi tulosalueen tietohallintopalveluista vastaavalle.

Allekirjoitus

Olen ymmärtänyt tietosuojaohjeen ja sitoudun noudattamaan ohjetta.

Vapaaehtoistyöntekijän nimi:

Allekirjoitus:_____