HENKILÖSTÖN TIETOTURVAOHJEET

25.1.2016

Tietosuojatyöryhmä:

Anne-Mari Kivilahti (tietosuojavastaava)
Elina Ketonen
Riitta Laine
Sanna Laitamäki

SISÄLLYSLUETTELO Sivu

1. JOHDANTO

1.1. Yhteinen vastuu tietoturvallisuudesta

Tietoturvallisuus perustuu lainsäädäntöön. Kauhajoen Vanhaintuki ry:n tietoturvan toteuttamisen perustana on johtoryhmän hyväksymä tietoturvaohje ja tietosuojaselosteet, jotka annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle.

Vastuu tietoturvallisuudesta, siihen liittyvästä osaamisesta ja annettujen ohjeiden ja määräysten noudattamisesta kuuluu omalta osaltaan jokaiselle, myös sinulle.

Esimies vastaa tietoturvan ja tietosuojan toteutumisesta, ohjeiden noudattamisesta, ideoittamisesta ja valvonnasta omassa yksikössään. Esimies huolehtii, että jokainen työntekijä on tutustunut Kauhajoen Vanhaintuki ry:n tietoturvaohjeisiin ja -selosteisiin ja on tehnyt vaitiolo- ja salassapitositoumuksen ennen tietojärjestelmän käyttöluvan saamista. Heidän apunaan toimii tietosuojatyöryhmä.

Tietoturvaohjeet ja -selosteet sekä tietoturvan huoneentaulu ovat saatavissa Kauhajoen Vanhaintuki ry:n Y-asemalta Y:\Henkilökunta\Tietosuoja sekä kotisivuilta www.kauhajoenvanhaintuki.fi, lisäksi paperiversiona jokaisesta yksiköstä.

1.2. Vaitiolovelvollisuus ja salassapito

Kaikkia Kauhajoen Vanhaintuki ry:n työntekijöitä koskee vaitiolovelvollisuus ja asiakirjojen salassapitovelvollisuus, joka perustuu lainsäädäntöön.

Vaitiolovelvollisuus koskee kaikkea salassa pidettävää tietoa riippumatta siitä, miten tai mihin ne on tallennettu tai millä tavalla tieto on saatu (kirjallisesti, suullisesti tai havainnoimalla). Salassa pidettäviä tietoja ovat mm. asiakastiedot, henkilötiedot sekä liike- ja ammattisalaisuudet.

Luottamuksellisia tietoja voivat käsitellä vain henkilöt, jotka tarvitsevat niitä työssään. Salassa pidettävien tietojen selville ottaminen muita, kuin työtehtäviä varten, on ehdottomasti kielletty ja jo sellaisenaan rangaistavaa. Luottamuksellisista tiedoista ei keskustella sivullisen kuullen. Sivullisia ovat esim. kaikki asukkaan hoitoon osallistumattomat henkilöt. Salassa pidettäviä tietoja käsitellessä on noudatettava erityistä huolellisuutta ja tietoja saa luovuttaa ainoastaan asiakkaan kirjallisella suostumuksella tai erityislainsäädännön nojalla.

Uudet vakinaiset työntekijät, sijaiset, harjoittelijat ja opiskelijat sekä luottamushenkilöt ja vapaaehtoistyöntekijät allekirjoittavat vaitiolo- ja salassapitositoumuksen, liite. Vaitiolo- ja salassapitovelvollisuus jatkuvat palvelussuhteen tai tehtävän hoitamisen päätyttyäkin.

1.3. Henkilötietorekisteriä koskevat asiakkaan oikeudet
Jokaisella on oikeus saada tieto itseään koskevista asiakirjoista. Siten asiakkaalla on oikeus saada myös itseään koskevia salassa pidettäviä tietoja. Lisäksi henkilöllä on asianosaisasemaan perustuva tiedonsaantioikeus tietoon, joka on voinut vaikuttaa hänen asiansa käsittelyyn. Asianosainen on hakija, valittaja tai joku muu, jonka oikeutta, etua tai velvollisuutta asia koskee. Tällöin hän voi asianosaisena saada tietoja myös toista henkilöä koskevista salassa pidettävistä asiakirjoista. Mikäli päämies ei tilansa vuoksi kykene ymmärtämään asian merkitystä, hän tarvitsee edunvalvontaa myös henkilöä koskevassa asiassa.

Jokaisella on oikeus myös tarkastaa, mitä häntä koskevia tietoja on talletettu. Tietojen tarkastaminen on maksutonta kerran vuodessa. Tarkastusoikeus voidaan evätä, jos tietojen antamisesta saattaisi aiheutua vakavaa vaaraa rekisteröidyn terveydelle tai hoidolle tai jonkun muun oikeuksille.

Henkilörekisterin pitäjän on ilman aiheetonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Mikäli pyyntöä henkilötietorekisterin tarkastusoikeudesta tai vaatimusta tiedon korjaamisesta ei hyväksytä, vaatimuksen esittäjä voi saattaa asian tietosuojavaltuutetun ratkaistavaksi.

Kauhajoen Vanhaintuki ry:n jokaisesta henkilörekisteristä on laadittu rekisteriseloste, jotka ovat saatavilla yksiköistä, kotisivuilta www.kauhajoenvanhaintuki.fi sekä Y-asemalta Y:\Henkilökunta\Tietosuoja.

Selosteesta ilmenee, kuka on henkilötietojen käsittelystä vastaava rekisterinpitäjä, mitä henkilötietoja rekisterissä on, mihin niitä käytetään ja minne tietoja säännönmukaisesti luovutetaan, tietojen suojauksen periaatteet sekä informaatio rekisteröidyn oikeuksista. Lomakkeet, joilla rekisteröity voi esittää rekisteritietojen tarkastuspyynnön, käyttäjälokitietojen selvityspyynnön tai rekisteritietojen korjaamisvaatimuksen ovat saatavilla yksiköistä, kotisivuilta www.kauhajoenvanhaintuki.fi sekä Y-asemalta Y:\Henkilökunta\Tietosuoja.

1.4. Henkilötietojen käyttäminen ja luovuttaminen
Lähtökohtana on, että henkilötietoja sisältävät asiakirjat ovat salassa pidettäviä. Vain asiakkaan kirjallisella suostumuksella tai lainsäädäntöön perustuvalla oikeudella tai velvoitteella, voidaan asiakirjoihin sisältyviä tietoja antaa sivulliselle tai toiselle viranomaiselle.

Kuolleen henkilön osalta asiakirjoista saadaan antaa perustellusta kirjallisesta hakemuksesta tietoja sille, joka tarvitsee niitä tärkeiden etujensa tai oikeuksiensa selvittämistä tai toteuttamista varten. Tietoja voidaan antaa vain siltä osin kuin ne ovat välttämättömiä hakemuksessa esitetyn käyttötarkoituksen kannalta.

2. TIETOJEN KÄSITTELY

Tiedolla tarkoitetaan eri muodoissa tallennettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisessä asiakirjassa, puheessa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai matkapuhelimen muistissa, ääni- tai kuvanauhassa tai vaikkapa yksittäisen ihmisen muistissa. Tietoa on tarkasteltava tiedon koko elinkaaren ajalla, jolloin tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat mm. tiedon luominen, käyttäminen, muuttaminen, tallentaminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen.

2.1. Työhön liittyvät tiedot

- Käsittele tietoja huolellisesti käsittely- tai tallennusvälineestä riippumatta.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä. Varo myös syöttämästä salasanojasi siten, että joku ”näkee” salasanan sormiesi liikkeistä.
- Tallenna tekemäsi työ mahdollisuuksien mukaan palvelimelle, jonka varmuuskopioinnista atk-henkilöstö huolehtii. Vältä tilannetta, jossa asiakirja tai muu aineisto olisi ainoastaan sellaisella laitteella tai tietovälineellä, jonka varmuuskopiointi on epäsäännöllistä.
- Mikäli aineistoa siirretään muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti.
- Varo toimistojärjestelmäsovelluksilla (esim. tekstinkäsittely, taulukkolaskenta, esitysgrafiikka) tehtyjen tiedostojen piiloon jääviä tietoja erityisesti organisaation ulkopuolelle tiedostoja lähettäessäsi.
- Arkaluonteisia tietoja tai henkilötunnuksia ei saa lähettää ulkoisessa sähköpostissa (yhdistyksellä ei ole käytössä salaustekniikkaa). Mikäli joudut lähettämään salassa pidettävää aineistoa kirjeitse, varmista vastaanottajan oikeus tiedon vastaanottamiseen ja tee asiakirjaan salassapitomerkintä.
- Lähetä kirjeposti määrittäen vastaanottaja tarkasti ja käytä tarvittaessa saantitodistusta tai kirjattua kirjettä. Lähetyksen tulee olla hyvin suljetussa kuoressa.
- Faksia käytettäessä asiakirjojen lähetys ja vastaanotto tapahtuu siten, että asiakirjat voi lähettää ja vastaanottaa vain siihen oikeutettu tai oikeutetut henkilöt, ja tiedonsiirrossa kiinnitetään erityistä huomioita asiakirjojen suojaamis- ja huolellisuusvelvoitteeseen.
- Vältä turhaa tulostamista ja kopiointia, koska ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet lisäävät tiedon vääriin käsiin joutumisen vaaraa ja siten turvaamistehtäviä erityisesti säilyttämisen ja hävittämisen osalta.
- Varmista, mihin tulostimeen tulostat. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
- Käytä salassa pidettävien tietojen hävittämiseen silppureita tai hävittämispalveluun kuuluvia keräyssäiliöitä.

2.2. Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

- Ohjaa haastattelu- ja kyselypyynnöt esimiehellesi tai asian vastuuhenkilölle.
- Varo antamasta viattomankin oloisten keskustelujen tai lomakkeiden yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt esimiehellesi tai aineiston vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta.

2.3. Omat tiedot ja yksityisyys

- Käytä henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi (ei työpaikan sähköpostiosoitetta).
- Omia henkilökohtaisia tiedostoja ei pidä tarpeettomasti tallentaa työpaikan matkapuhelimeen, työasemaan tai palvelimelle.
- Kaikki ovat vaitiolovelvollisia toisten viesteistä, jotka on työtehtävissään vahingossa saanut tietoonsa.
- Tukahduta juorut.
- Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, myös sähköpostiliikenteestä ja Internet -selauksesta. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäytöksiin puututaan.

3. TYÖPAIKALLA

3.1. Tietokoneen käyttö

Tietokoneen käyttö sisältää sekä oman työaseman että verkon kautta käytettävien palveluiden käytön.

- Vastaat käyttämästäsi tietokoneesta. Ole siis huolellinen.
- Vain atk-henkilöstö saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää koneisiin ohjelmia.
- Kirjaudu koneelle aina omilla käyttöoikeuksillasi (poikkeuksena hoitaja -tunnus).
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi (Windows-työasemalla paina Ctrl+Alt+Del ja valitse Lukitse tietokone tai Hilkka -potilastietojärjestelmästä poistu Kirjaudu ulos –painikkeesta).
- Samoja levykkeitä, muistitikkuja tai muita tietovälineitä ei saa käyttää työpaikalla ja sen ulkopuolella, jollei ole varmistanut niiden viruksettomuutta.
- Talleta työsi käyttäen välitallennuksia. Älä jätä työtä tallentamatta, kun poistut työpisteestäsi.
- Jos työaseman kiintolevy tai muu tallennusväline esim. muistitikku rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Toimita tallennusväline atk-henkilöstölle hävitettäväksi.

3.2. Käyttöoikeudet ja salasanat

Tietojärjestelmiin tarvitaan käyttöoikeus, joka saadaan esimiehiltä. Käyttöoikeus on henkilökohtainen ja se on yhdistetty juuri sinun henkilöllisyyteesi ja työtehtävääsi. Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttiasi ja tunnuslukuasi.

- Käyttäjätunnukset ovat henkilökohtaisia ja kukin vastaa käyttäjätunnuksellaan tehdyistä toimenpiteistä ja merkinnöistä.
- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi tai PIN -koodejasi toisen henkilön käyttöön – älä edes atk-henkilöstölle. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiisi. Tietojen urkkimista voi tapahtua esim. puhelimitse tai sähköpostilla vääräksi henkilöksi esittäytymällä.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä salasanana. Hyvässä salasanassa voi olla pieniä ja isoja kirjaimia, numeroita ja jopa erikoismerkkejä. Kaikkiin järjestelmiin ei kuitenkaan käy erikoismerkit. Hyvä salasana on sellainen, jonka sinun on helppo muistaa, mutta vaikea ulkopuolisen arvata.
- Älä kirjoita salasanoja muistiin – ainakaan sellaiseen paikkaan, mistä ne ovat helposti löydettävissä.
- Älä käytä organisaation antamaa käyttäjätunnusta ja salasanaa Internetin palveluihin rekisteröityessäsi.
- Mikäli joissain tilanteissa tai järjestelmissä on pakko käyttää yhteistunnuksia, siitä päättää järjestelmän tai tietojen omistaja.
- Työsuhteen päättyessä käyttöoikeudet poistetaan.
- Huolehdi, että tallenteet, asiakirjat, tietovälineet ja muu informaatio tulee organisaation käyttöön. Poista mahdolliset henkilökohtaiset tallenteet.

3.3. Internet ja sähköposti

Internet ja sähköposti ovat hyviä työvälineitä sekä tiedon hakuun että yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa tai Internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa.

- Internet ja sähköposti on työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintään yksityistä sähköpostiosoitettasi. Älä anna työsähköpostiosoitettasi ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä.
- Arkaluonteisia ja muita salassa pidettäviä tietoja ei saa lähettää ulkoisen sähköpostin välityksellä, siinäkään tapauksessa, että asiakas tai potilas itse on pyytänyt tietojaan sähköpostitse. Myös viestit, jotka paljastavat asiakassuhteen ovat kiellettyjä.
- Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana. Pääsääntöisesti käytäntönä on, että sähköpostiin laitetaan automaattivastaus -toiminto, joka ohjaa lähettäjän ottamaan yhteyttä nimettyyn sijaiseen.
- Mikäli saat toiselle henkilölle kuuluvan sähköpostiviestin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite

- Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia). Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä, vaan ilmoita asiasta atk-henkilöstölle.
- Älä välitä ketjukirjeitä ja muuta roskapostia eteenpäin. Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se kannattaa tuhota heti. Jos viestiin vastaa, tietää roskapostittajasähköpostiosoitteesi toimivaksi ja jatkaa roskapostien lähettämistä ja lisäksi välittää osoitteesi myös muille roskapostittajille.
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa ja se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiotoimintoa, jos haluat estää jakelulistalla olevien osoitteiden näkymisen vastaanottajille.
- Vältä turhien sähköpostien lähettämistä. Esimerkiksi joulutervehdysten lähettäminen kuormittaa sekä sähköpostijärjestelmää että vastaanottajan sähköpostilaatikkoa.
- Suuret liitetiedostot kuormittavat sähköpostijärjestelmää, joten niitä ei pidä säilyttää turhaan ja on vältettävä viestittelyketjuja, joissa liitetiedostot kulkevat tarpeettomasti mukana.
- Sähköposti on epävarma tallennuspaikka. Siirrä tärkeät liitetiedostot verkkopalvelimelle varmuuskopioinnin turvaamiseksi.
- Työsuhteen päättyessä sähköpostiosoite poistetaan, poista mahdolliset henkilökohtaiset viestit.

3.4. Toimitilojen turvallisuus

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja tietokonelaitteita säilytetään ja käsitellään asianmukaisesti turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan ja vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden.

- Suuntaa tietokoneesi näyttö niin, ettei asiakas näe ruutua.
- Tarkista työpisteeseesi tullessasi, ettei mitään asiatonta ole tapahtunut poissaolosi aikana.
- Pyri käyttämään vierailuihin neuvottelutiloja.
- Huolehdi, ettei tauko- tai neuvottelutiloissa ole esillä asiaankuulumatonta materiaalia. Vastaavasti neuvottelun päättyessä huolehdi, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyjä luottamuksellisia aineistoja tai muistiinpanoja.
- Säilytä tieto ja laitteet turvassa, mahdollisuuksien mukaan lukitussa kaapissa ja huoneessa.
- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Huolehdi laitteiden ja tallennusvälineiden asianmukaisesta säilyttämisestä.
- Noudata ”puhtaan pöydän” periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.

- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai muihin yhdistyksen toimitiloihin.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi.
- Ohjaa vieraat tai ”eksyneet” henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä suljettuina pidettäväksi tarkoitettuja ovia auki.

4. LIIKKUVA TYÖ, ETÄTYÖ JA MATKATYÖ

4.1. Liikkuva työ ja mobiililaitteet

Liikkuvan työn välineisiin ja niiden käyttöön liittyy vastaavia uhkia kuin kiinteästi asennettuihin, joten kyseeseen tulevat soveltuvin osin samat turvallisuusohjeet. Kun välineitä lisäksi kuljetetaan ja käytetään työpaikan toimitilojen tarjoamien turvatoimien ulkopuolella, tarvitaan erityistä huolellisuutta.

- Huolehdi työnteossa käyttämiesi kannettavien tietokoneiden, matkapuhelinten ja älypuhelimien turvallisuudesta. Älä säilytä niissä ylimääräistä tietoa. Käytä tietojen salausta mahdollisuuksien mukaan.
- Huolehdi, että matkapuhelimessasi on päällä PIN -kysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat PIN -koodit.

4.2. Etätyö ja etäkäyttö

Etätyöllä tarkoitetaan muualla kuin vakituisessa toimipisteessä suoritettavaa työtä. Etäkäyttö on tietoteknisten palvelujen käyttöä etäyhteyden kautta. Käyttöympäristöt vaihtelevat (esim. langattomat verkkoyhteydet) eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys.

- Etätyö on sallittua vain, jos siitä on tehty erillinen sopimus esimiehen kanssa. Muista, että kaikkea työtä ei voi tehdä tietoturvallisesti etätyönä. Tunnista nämä työt. Joidenkin järjestelmien etäkäyttö on estetty.
- Kiinnitä kaikessa toiminnassasi huomiota tietoturvallisiin menettelytapoihin. Noudata soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi varsinaisessa toimipisteessä.
- Huolehdi, että etätyössä käyttämäsi laitteisto, käyttäjätunnukset ja salasanat ovat vain sinun hallussasi ja tiedossasi.
- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta. Etätyö on rajattava aineistoon, jonka paljastuminen ei vaaranna tietoturvallisuutta.
- Huolehdi tietoaineistosi varmuuskopioinnista sekä turvallisesta säilytyksestä ja hävittämismenettelystä.

4.3. Matkatyö

- Vältä puhumasta luottamuksellisia työasioita julkisilla paikoilla ja kulkuvälineissä.
- Mikäli työskentelet tietovälineellä julkisessa kulkuvälineessä, varmistu, etteivät kanssamatkustajat näe käsittelemiäsi tietoja ja asiakirjoja. Varo myös aiheettomien langattomien yhteyksien aktivoitumista koneeseesi.
- Säilytä tieto ja laitteet turvassa. Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Niitä ei saa jättää autoon näkyvälle paikalle tai säilyttää autossa yön yli.
- Vältä julkisten päätteiden (esim. kirjastot, nettikahvilat) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään.

5. ONGELMATILANTEET

5.1. Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa

- Ilmoita aina välittömästi tietosuojarikkomuksista tai tietosuojaan liittyvistä puutteista esimiehelle tai tietosuojavastaavalle. Tietoturvarikkomusta lieventää merkittävästi, mikäli rikkomuksen tehnyt henkilö on välittömästi ottanut yhteyttä esimieheensä sekä tietosuojavastaavaan eikä käytä missään olosuhteissa väärin saamaansa tietoa.
- Ilmoita aina välittömästi haittaohjelmista (esim. virukset, madot tai troijalaiset) ja muista tietoturvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista omalle esimiehelle tai tietoturvavastaavalle.
- Mikäli hallussasi oleva laite tms. katoaa tai varastetaan, ilmoita siitä välittömästi yksikön esimiehellesi oman vastuusi rajaamiseksi.

5.2. Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa

- Älä hätiköi.
- Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki. Kirjoita ylös tekemisesi.
- Ota yhteyttä tietosuojavastaavaan tai atk-henkilöstöön. Auta tutkinnassa.
- Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.
- Harkiten ja turhaa ylireagointia välttäen, on varoitettava tahoja, joilla voi olla sama vaaratilanne.

5.3. Tietoturvarikkomusten seuraamukset

- Rikkomuksesta tiedotetaan aina esimiehelle.
- Kaikki tietoturvarikkomukset käsitellään asianmukaisesti ja johtoryhmän hyväksymän seuranta- ja valvontasuunnitelman mukaisesti.
- Jos kyseessä on toistuva tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin. Tietoturvarikkomuksesta seuraa varoitus ja sen perusteella on mahdollista

- purkaa työsuhde. Käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin. Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

6. TIETOTURVALLISUUTEEN KESKEISESTI LIITTYVÄT SÄÄDÖKSET

Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Suomen perustuslaki (731), 10 § ja 12 §
- Laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki), 1 §, 3§, 10 §, 5. luku, 6. luku ja 7. luku
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Arkistolaki (821/1994)
- Henkilötietolaki (523/1999)
- Terveydenhuoltolaki (1326/2010)
- Laki potilaan asemasta ja oikeuksista (785/1992, potilaslaki)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009, potilasasiakirja-asetus)
- Laki sähköisestä lääkemääräyksestä (61/2007, eReseptilaki)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000, sosiaalihuollon asiakaslaki)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (1227/2010, asiakastietolaki)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki terveydenhuollon ammattihenkilöistä (559/1994, ammattihenkilölaki)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Rikoslaki (39/1889), 34. luku ja 38. luku
- Vahingonkorvauslaki (41/1974)

7. TIETOTURVAN JA TIETOSUOJAN HUONEENTAULU

- Tietoturvallisuudesta huolehtiminen kuuluu kaikille, myös sinulle. Seuraa tietoturvallisuuteen liittyviä tiedotteita, tutustu ohjeisiin ja osallistu sinulle tarjottuun koulutukseen. Toimi saamiesi ohjeiden mukaisesti.
- Käytä tietoaineistoja ja työvälineitä vain työtehtäviesi hoitamiseen. Käsittele tietoja huolellisesti välineestä riippumatta – olipa tiedon välittäjänä sitten henkilö, tietokone, paperi, puhelin tai telekopio.
- Tietoja tulee suojata sen käsittelyvaiheissa; luomisessa, käyttämisessä, muuttamisessa, tallentamisessa, siirtämisessä, jakelussa, kopioinnissa, arkistoinnissa ja tuhoamisessa.
- Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanoja toisen henkilön käyttöön – älä edes atk-henkilöstölle, koska he eivät niitä tarvitse. Vaihda salasanat riittävän usein ja heti, kun epäilet niiden paljastuneen.
- Älä anna kenenkään nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluontoista tietoa tai kun syötät käyttäjätunnuksia ja salasanoja. Älä anna ulkopuolisen käyttää tietokonettasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi tai yhteiskäytössä olevilla kirjaudu ulos käyttäjävaihdon kautta. Työpäivän päättyessä kirjaudu tietojärjestelmästä ulos ja sammuta työasemasi. Noudata ns. puhtaan pöydän periaatetta. Älä säilytä työpöydällä salassa pidettävää aineistoa.
- Älä jätä asiakasta tai vierasta yksin tai valvomatta työhuoneeseesi tai muihin yhdistyksen tiloihin.
- Älä asenna ohjelmistoja tai tee niihin asennusmuutoksia, ellei tämä kuulu työtehtäviisi.
- Tallenna tekemäsi työ verkkopalvelimen levylle, mistä tiedot varmistetaan keskitetysti. Mikäli siirrät aineistoa muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti.
- Muista, että organisaation laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnyt tietoverkossa aina yhdistyksen edustajana.
- Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemistasi uhkista ja suojauspuutteista välittömästi omalle esimiehelle, tietosuojavastaavalle tai atk-henkilöstölle. Heidän velvollisuutensa on ryhtyä tarvittaviin toimenpiteisiin.

VAITIOLO- JA SALASSAPITOSITOUMUS

Asiakirjojen, tietojen ja tietojärjestelmien käsittely- ja käyttöoikeudet annetaan vain tämän sitoumuksen allekirjoittaneelle. Sitoumus tehdään vakinaisen työsuhteen alkaessa ja sijaisten, opiskelijoiden ja harjoittelijoiden kanssa ensimmäisen palvelussuhteen alkaessa tai palvelussuhteen luonteen muuttuessa. Sitoumus tehdään myös luottamushenkilöiden ja vapaaehtoistyöntekijöiden kanssa.

Lainsäädännön ja annettujen ohjeiden noudattaminen
Jokainen työntekijä vastaa oman toimintansa tietoturvallisuudesta ja lainsäädännön, annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.

Kauhajoen Vanhaintuki ry:n tietosuojaselosteet sekä tietoturvaohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle. Tietosuojaselosteet ja -ohjeet löytyvät Kauhajoen Vanhaintuki ry:n Y-asemalta Y:\Henkilökunta\Tietosuoja sekä kotisivuilta www.kauhajoenvanhaintuki.fi, lisäksi paperiversiona jokaisesta yksiköstä. Esimies huolehtii, että uusi työntekijä tutustuu tietoturvan ja tietosuojan materiaaliin osana työhön perehdytystä.

Vaitiolo- ja salassapitositoumus
Työntekijänä sitoudun olemaan käyttämättä, ilmaisematta tai luovuttamatta palvelussuhteen aikana asiakkaisiin, henkilötietoihin sekä liike- ja ammattisalaisuuksiin liittyviä salassa pidettäviä tietoja, riippumatta siitä, miten tai mihin tieto on tallennettu tai millä tavalla tieto on saatu (kirjallisesti, suullisesti tai havainnoimalla). Tietojen luovutuksen tulee perustua aina asiakkaan kirjalliseen suostumukseen tai erityislainsäädäntöön.

Sitoudun noudattamaan seuraavia tietosuojaperiaatteita:

- Salassapito- ja vaitiolovelvollisuus koskee minua palvelussuhteeni aikana ja sen jälkeen.
- Noudatan erityistä huolellisuutta käsitellessäni salassa pidettäviä tietoja esim. puhelin- ja käytäväkeskusteluissa sekä taukotiloissa niin, etteivät ne kantaudu sivullisten tietoon.
- Pidän salassa kaikki tietooni saamani arkaluonteiset tiedot, esimerkiksi henkilön sairautta, tutkimusta, hoitoa, taloudellista asemaa tai sosiaalisia etuuksia koskevat tiedot.
- Käsittelen vain työtehtävieni edellyttämiä tietoja. En käsittele esimerkiksi omia, työtovereiden, lähiomaisten tai naapureiden tietoja, mikäli työtehtäväni eivät sitä sillä hetkellä edellytä.
- Vastaan käyttäjätunnuksillani tapahtuvasta tietojen käytöstä.
- Vastaan käytössäni olevasta tietokoneesta, puhelimesta tai muusta laitteesta niin, ettei laite ja siinä olevat tiedot joudu vääriin käsiin.
- Olen tietoinen, että tietojärjestelmissä käyntini ja siellä tehdyt tapahtumat kirjautuvat lokitiedostoihin, niitä valvotaan ja epäillystä väärinkäytöstä raportoidaan esimiehelleni.
- Olen tietoinen, että tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta on lainsäädännössä rangaistava teko. Rangaistavaa menettelyä henkilörekisteritoiminnassa koskevat säännökset sisältyvät henkilötietolakiin ja rikoslakiin.

Olen perehtynyt tietoturvaohjeisiin. Olen lukenut tämän sitoumuksen ja minulle on selvitetty sen sisältö ja merkitys. Tätä sitoumusta on laadittu kaksi samansisältöistä kappaletta, yksi kummallekin osapuolelle.

Työntekijä _____ Hetu _____

Työyksikkö _____ Nimike _____

_____ _____

Pvm ja työntekijän allekirjoitus Pvm ja esimiehen allekirjoitus