Yhteistoimintamenettely 17.9.2012
Henkilöstöjaosto 17.9.2012
Hyväksytty johtokunta 24.9.2012 § 107

Henkilöstön tietoturvaohjeet

Suupohjan peruspalvelu-liikelaitoskuntayhtymä

Hallintoaukio • PL 100, 61801 KAUHAJOKI • (06) 2413 2000 • www.llky.fi

Sisällys:

1. JOHDANTO

1.1. Yhteinen vastuu tietoturvallisuudesta

Tietoturvallisuus perustuu lainsäädäntöön ja normiohjaukseen. Liikelaitoskuntayhtymässä tietoturvan toteuttamisen perustana on johtokunnan hyväksymä tietoturva- ja tietosuojapolitiikka, joka annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle. Tietoturva- ja tietosuojapolitiikan tietoturvaperiaatteita noudatetaan kaikessa tietojen käsittelyyn liittyvässä toiminnassa.
Vastuu tietoturvallisuudesta, siihen liittyvästä osaamisesta ja annettujen ohjeiden ja määräysten noudattamisesta kuuluu omalta osaltaan jokaiselle, myös sinulle.

Nämä henkilöstön tietoturvaohjeet täydentävät tietoturva- ja tietosuojapolitiikkaa ja antavat sinulle käytännön neuvoja ja ohjeita tietoturvallisuuden toteuttamiseen omassa työssäsi.
Palvelujohtajat vastaavat palvelualueensa henkilötietojärjestelmien rekistereistä ja antavat henkilötietojen ja asiakirjojen käsittelystä ja menettelytavoista palvelualuekohtaisia ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja.
Esimiehet vastaavat tietoturvan ja tietosuojan toteutumisesta, ohjeiden noudattamisesta, tiedottamisesta ja valvonnasta omassa yksikössään. Esimies huolehtii, että jokainen työntekijä on tutustunut liikelaitoskuntayhtymän tietoturva- ja tietosuojapolitiikkaan sekä henkilöstön tietoturvaohjeisiin ja on tehnyt asiakirjojen, tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen ennen tietojärjestelmän käyttöluvan hakemista. Lisäksi esimies huolehtii, että henkilöstö suorittaa tietoturvan ja tietosuojan verkkokoulutuksen tietosuojavastaavan ohjeistuksen mukaisesti sekä osallistuu muuhun tietoturva- ja käyttökoulutukseen.
Tietosuojavastaavalla ja tietoturvavastaavalla on liikelaitoskuntayhtymän ylimmän johdon antama valtuutus ja velvollisuus tehdä tietojärjestelmien ja tietojen käsittelyn tietoturvallisuuden ja tietosuojan seurantaa ja valvontaa sekä ryhtyä toimenpiteisiin havaittujen heikkouksien parantamiseksi ja ongelmatilanteiden selvittämiseksi. Heidän apunaan toimii tietoturvatyöryhmä.

Tämä tietoturva- ja tietosuojaohje on tarkoitettu liikelaitoskuntayhtymän koko henkilöstölle, luottamushenkilöille, sen toimeksiannosta työskenteleville (esim. palvelun toimittajat) ja sen tietojärjestelmiä tai toimitiloja säännönmukaisesti käyttäville henkilöille (esim. opiskelijat ja harjoittelijat).

Tietoturva- ja tietosuojapolitiikka sekä henkilöstön tietoturvaohjeet ovat saatavissa sekä liikelaitoskuntayhtymän sisäisiltä verkkosivuilta L:\tietoturva\ohjeet että ulkoisilta verkkosivuilta www.llky.fi.
Lopussa oleva tietoturvan ja tietosuojan huoneentaulu on tallennettuna sisäisillä verkkosivuilla L:\tietoturva\ohjeet\huoneentaulu.doc, josta se on tulostettavissa jokaisen työyksikön ja työpisteen seinälle ohjeeksi.

1.2. Miksi tietoturvallisuus on tärkeää?

Tietoturvatoimenpiteillä turvataan yksilön, yhteisön ja yhteiskunnan etuja. Tietoturvallisuusjärjestelyjen tarkoituksena on, että tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyvät riskit ovat hallinnassa. Käytännössä tämä merkitsee mm. sitä, että osa tiedoista ja tietojärjestelmistä pidetään vain niiden käyttöön oikeutettujen saatavilla. Tällöin sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään.

Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muidenkaan vahinkojen ja tapahtumien seurauksena.
Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin kun niitä tarvitaan. Sähköisen asioinnin yleistyessä on lisäksi entisestään korostunut vaatimus, että asioinnin osapuolet tunnistetaan luotettavasti ja että asiointitapahtumien olemassaolo ja sisältö voidaan jälkikäteenkin todistaa.

Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön inhimillisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki – ei siis vain tekniikka vaan myös jokapäiväiset toimintatapamme ja asenteemme.

1.3. Vaitiolovelvollisuus ja salassapito

Kaikkia liikelaitoskuntayhtymän työntekijöitä koskee vaitiolovelvollisuus ja asiakirjojen salassapitovelvollisuus, joka perustuu lainsäädäntöön sekä liikelaitoskuntayhtymän omiin määräyksiin ja ohjeisiin.

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. potilas- ja 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 potilaan hoitoon osallistumattomat henkilöt. Salassa pidettäviä tietoja käsitellessä on noudatettava erityistä huolellisuutta ja tietoja saa luovuttaa ainoastaan asiakkaan tai potilaan kirjallisella suostumuksella tai erityislainsäädännön nojalla.

Uudet vakinaiset työntekijät, sijaiset, harjoittelijat ja opiskelijat allekirjoittavat vaitiolo- ja salassapitositoumuksen tietojärjestelmien käyttölupahakemuksen yhteydessä. Vaitiolo- ja salassapitovelvollisuus jatkuvat palvelussuhteen tai tehtävän hoitamisen päätyttyäkin.

1.4. Henkilötietorekisteriä koskevat asiakkaan ja potilaan oikeudet

Jokaisella on oikeus saada tieto itseään koskevista asiakirjoista. Siten potilaalla ja asiakkaalla on oikeus saada myös itseään koskevia salassa pidettäviä tietoja. Lisäksi henkilöllä voi 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. Alaikäistä lasta koskeviin rekisteritietoihin voi olla oikeus lapsen huoltajalla, jollei laissa ole toisin säädetty. Edunvalvojan edustusvallan ulottaminen täysi-ikäisen päämiehen henkilöä koskeviin asioihin ei tavallisesti ole tarpeen, koska päämies voi itse päättää henkilöä koskevasta asiasta. Mikäli päämies ei tilansa vuoksi kykene ymmärtämään asian merkitystä, hän tarvitsee edunvalvontaa myös henkilöä koskevassa asiassa.
Tieto voidaan jättää antamatta vain, jos sen antaminen on vastoin erittäin tärkeää yleistä, yksityistä tai lapsen etua.

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.
Asianosaisen oikeudesta tiedonsaantiin tehdään aina viranhaltijapäätös, johon tyytymätön asianosainen voi tehdä oikaisuvaatimuksen liikelaitoskuntayhtymän johtokunnalle. Mikäli oikaisuvaatimus hylätään, voi oikaisuvaatimuksentekijä valittaa Vaasan hallinto-oikeuteen.

Liikelaitoskuntayhtymän jokaisesta henkilörekisteristä tulee laatia rekisteri- ja tietosuojaseloste, jotka ovat yleisesti saatavilla toimipaikoista ja yhtymän internet-sivuilta ja sisäisiltä verkkosivuilta L:\tietoturva\rekisteriselosteet. 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 toimipaikoissa, yhtymän internet-sivuilla ja sisäisillä verkkosivuilla L:\tietoturva\lomakkeet.

1.5. Henkilötietojen käyttäminen ja luovuttaminen

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

Asiakas- ja potilastietojen turvallinen käsittely korostuu entisestään siirryttäessä asiakastietojen sähköiseen käsittelyyn sekä kansallisten ja alueellisten tietojärjestelmien yhteiskäyttöön.

Esimerkiksi terveydenhuoltolain mukaisesti Etelä-Pohjanmaan yhteisen potilastietorekisterin tietoja voidaan käyttää rekisteriin kuuluvien julkisen terveydenhuollon yksiköiden välillä, joita ovat:
Etelä-Pohjanmaan sairaanhoitopiirin kuntayhtymä
JIK-peruspalveluliikelaitoskuntayhtymä
Kuntayhtymä Kaksineuvoinen
Kuusiokuntien terveysyhtymä
Lapuan terveyskeskus
Järvi-Pohjanmaan yhteistoiminta-alue
Seinäjoen terveyskeskus
Suupohjan peruspalveluliikelaitoskuntayhtymä
Alueen kunnallinen työterveyshuolto

Etelä-Pohjanmaan yhteisen potilastietorekisterin tietoja voidaan käyttää ilman potilaan suostumusta, jotta potilastietojen käyttö voidaan toteuttaa joustavasti potilaan hoidon turvaavalla tavalla. Potilastietoja käytetään ainoastaan työtehtävissä potilaan hoidon järjestämisen ja toteuttamisen yhteydessä. Potilas voi halutessaan kieltää tietojensa käytön kokonaan toisessa potilastietorekisteriin kuuluvassa terveydenhuollon yksikössä. Potilas voi myös erikseen kieltää potilastietojensa käytön hätätilanteessa.
Yksityisiltä tai Etelä-Pohjanmaan sairaanhoitopiirin alueen ulkopuoliselta julkiselta toimintayksiköltä pyydettyihin ja annettuihin potilastietoihin tarvitaan edelleen potilaan kirjallinen suostumus.
Suostumuksen rajoitus tai kielto estää potilaskertomustietojen lähettämisen esim. jatkohoitopaikkaan tai yksityislääkärille. Tällöin potilas itse vastaa tietojensa välittämisestä.

Tieto sosiaalihuollon asiakkuudesta tai potilaana olosta on itsessään salassa pidettävä tieto, jota ei voida antaa ilman henkilön antamaa suostumusta.

Salassa sairastaminen on henkilön esittämä tahto, jolloin myöskään neuvonta tai potilastoimisto ei yhdistä asianomaiselle puheluja tai opasta vieraita hänen luokseen.

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. ASIANHALLINTA JA TIETOJEN KÄSITTELY

Asianhallinta tarkoittaa liikelaitoskuntayhtymän toimintaprosesseihin sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista ja arkistointia. Asiakirjallisen tiedon laadukas hallinta edellyttää, että käsittelykäytännöt on suunniteltava huolellisesti ja suojaaminen varmistettava ja että asiakirjallisen tiedon alkuperäisyys, eheys, luotettavuus ja käytettävyys taataan.

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

- Selvitä itsellesi tietojen ja asiakirjojen luokittelu ja siihen liittyvät käyttöä, luovutusta ja käsittelyä koskevat säännöt ja rajoitukset. Asiakirjahallinnon ohje sekä arkistonmuodostussuunnitelma ohjaavat tietoaineiston luokittelua, käsittelyä, säilyttämistä ja hävittämistä koko sen elinkaaren ajan.
- Mikäli laadit salassa pidettävää asiakirjaa, vastaat tehtäviesi mukaisesti myös sen luokittelusta ja merkinnästä.
- Käsittele tietoja huolellisesti käsittely- tai tallennusvälineestä riippumatta.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. 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 (yhtymällä ei ole käytössä salaustekniikkaa). Mikäli joudut lähettämään salassa pidettävää aineistoa kirjeitse, varmista vastaanottajan oikeus tiedon vastaanottamiseen ja tee asiakirjaan salassapitomerkintä. Lähetä kir-

jeposti määrittäen vastaanottaja tarkasti ja käytä tarvittaessa saantitodistusta tai kirjattua kirjettä. Lähetyksen tulee olla hyvin suljetussa kuoressa.
- Telefaksia 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 (itse hankittu, työnantajasta riippumaton) sähköpostiosoitettasi.
- 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 käyttäjänä omasta koneestasi. Ole siis huolellinen.
- Vain atk-henkilöstö saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää koneisiin ohjelmia.
- Kirjaudu koneelle aina omilla käyttöoikeuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi (Windows-työasemalla paina Ctrl+Alt+Del ja valitse Lukitse tietokone) tai yhteiskäytössä olevalla Effica-työasemalla kirjaudu ulos käyttäjävaihdon kautta.
- 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.
- Tallenna kaikki tärkeä tieto sellaisen verkkopalvelimen levylle, josta atk-henkilöstö ottaa säännöllisesti varmuuskopiot.
- Jos työaseman kiintolevy tai muu tallennusväline esim. muistitikku rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Toimita tallennusväline atk-henkilöstölle hävitettäväksi.
- Kirjaudu ulos sekä ohjelmistoista että koneeltasi ja sammuta tietokoneesi työpäivän päättyessä. Poikkeuksista ohjeistetaan erikseen.

3.2. Käyttöoikeudet, salasanat ja varmennekortit

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

- Käyttäjätunnukset ja varmennekortit ovat henkilökohtaisia ja kukin vastaa käyttäjatunnuksellaan tehdyistä toimenpiteistä ja merkinnöistä.
- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, varmennekorttiasi 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 ja työnantajakohtaiset varmennekortit (esim. VRK:n henkilökortti ja toimijakortti) luovutetaan rekisteripisteeseen. 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. Sähköpostin ja internetin käyttö vaativatkin käyttäjältä huolellisuutta.

- Internet ja sähköposti on työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintään yksityistä sähköpostiosoitettasi. Älä anna työsähköpostiosoitettasi ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä.
- Työasemien ja –työajan käyttäminen ns. chat -keskustelutoimintaan tietoverkoissa on kielletty.
- Facebook, IRC-Gallerian ym. vastaavien sivujen käyttäminen on sallittua ainoastaan työtehtävien hoitamisessa esimiehen luvalla.
- Käytä vain sellaisia internet-palveluita, jotka tiedät asiallisiksi.
- Ohjelmien lataus internetin kautta on liikelaitoskuntayhtymässä kokonaan kielletty. Atk-henkilöstö asentaa kaikki tarvittavat ohjelmat. Mikäli työtehtäviesi perusteella lataat ohjelmia, pyri aina varmistumaan ohjelmiston ja lähteen luotettavuudesta.
- 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 asiakas- tai potilassuhteen ovat kiellettyjä.
- Liikelaitoskuntayhtymän sisäinen sähköposti on siten vahvasti suojattu, että arkaluonteisten tietojen lähettäminen on pakottavassa tilanteessa mahdollista, mutta edellyttää erityistä huolellisuutta.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan liikelaitoskuntayhtymän sähköpostijärjestelmään. Sitä ei saa ohjata tai jatkolähettää liikelaitoskuntayhtymän sähköpostijärjestelmän ulkopuolelle.
- Muista, että viranomaisella on velvollisuus käsitellä virkasähköposti.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat, vireille saatettavat asiat liikelaitoskuntayhtymän hallinnon tai toimipaikkojen virallisiksi määritettyihin sähköposteihin. Virallinen sähköposti tulee kirjata vastaanotetuksi ja arkistoida.
- Muista, että vastaat henkilökohtaiseen sähköpostiin tulevasta työpostista virkavelvollisuuksien mukaisesti.

- Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana virkavelvollisuuksien mukaisesti. Pääsääntöisesti käytäntönä on, että sähköpostiin laitetaan automaattivastaus –toiminto, joka ohjaa lähettäjän ottamaan yhteyttä nimettyyn sijaiseen tai sopivaan organisaatio-osoitteeseen.
- 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.
- Ole terveen epäluuloinen sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Myös virukset voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä. Varo ns. ”kalasteluviestejä”, joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin.
- 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 roskapostittaja sähköpostiosoitteesi 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 ja –laatikko poistetaan. Siirrä virkapostisi työnantajan käyttöön ja 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 asiakaspalvelupisteessä ja -tilanteessa tietokoneesi näyttö harkitusti – onko tarkoitus, että tiedot näkyvät asioijalle vai ei?
- Noudata kulunvalvonnasta annettuja ohjeita.

- Tarkista työpisteeseesi tullessasi, ettei mitään asiatonta ole tapahtunut poissaolosi aikana.
- Pyri käyttämään vierailuihin neuvottelutiloja.
- Huolehdi, ettei 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 yhtymän toimitiloihin.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi.
- Ohjaa vieraat tai ”eksyneet” henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä yhtymän toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten 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.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin (esim. PIN-kyselyt, Bluetooth-asetukset, sovellusten lataaminen).
- Huolehdi, että matkapuhelimessasi on päällä PIN-kysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat PIN-koodit.
- Huolehdi tietojen varmuuskopioinnista ja/tai tarvittaessa synkronoinnista muuhun tietojärjestelmään.

4.2. Etätyö ja etäkäyttö

Etätyöllä tarkoitetaan muualla kuin vakituisessa toimipisteessä suoritettavaa työtä. Etäkäyttö on tietoteknisten palvelujen käyttöä etäyhteyden kautta. Käyttöym-

päristöt 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 ao. vastuuhenkilölle 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 tietoturvavastaavaan 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 johtokunnan 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 työ- tai virkasuhde. 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, potilas-asiakirja-asetus)
- Laki sähköisestä lääkemääräyksestä (61/2007, eReseptilaki)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000, sosiaali-huollon 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 kunnallisesta viranhaltijasta (304/2003)
- Laki terveydenhuollon ammattihenkilöistä (559/1994, ammattihenkilölaki)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Rikoslaki (39/1889), 34. luku ja 38. luku
- Vahingonkorvauslaki (41/1974)

Ajantasainen lainsäädäntö on Finlex -tietokannassa, ks. www.finlex.fi

Suupohjan peruspalvelu-
liikelaitoskuntayhtymä

TIETOTURVAN JA TIETOSUOJAN HUONEENTAULU

1. Tietoturvallisuudesta huolehtiminen kuuluu kaikille, myös sinulle. Seuraa tietoturvallisuuteen liittyviä tiedotteita, tutustu ohjeisiin ja osallistu sinulle tarjottuun koulutukseen. Toimi saamiesi ohjeiden mukaisesti.

2. Käytä tietoaineistoja ja työvälineitä vain työtehtäviesi hoitamiseen. Käsittele tietoja huolellisesti välineestä riippumatta – olipa tiedon välittäjänä sitten henkilö, tietokone, paperi, puhelin tai telekopio.

3. Tietoja tulee suojata sen käsittelyvaiheissa; luomisessa, käyttämisessä, muuttamisessa, tallentamisessa, siirtämisessä, jakelussa, kopioinnissa, arkistoinnissa ja tuhoamisessa.

4. 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.

5. Älä anna kenenkään nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluontoista tietoa tai kun syötät käyttäjätunnuksia ja salasanoja. Älä anna ulkopuolisen käyttää tietokonettasi.

6. Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi tai yhteiskäytössä olevilla kirjaudu ulos käyttäjävaihdon kautta. Työpäivän päättyessä kirjaudu tietojärjestelmästä ulos ja sammuta työ-asemasi. Noudata ns. puhtaan pöydän periaatetta. Älä säilytä työpöydällä salassa pidettävää aineistoa.

7. Älä jätä asiakasta tai vierasta yksin tai valvomatta työhuoneeseesi tai muihin liikelaitoskuntayhtymän tiloihin.

8. Älä asenna ohjelmistoja tai tee niihin asennusmuutoksia, ellei tämä kuulu työtehtäviisi.

9. Tallenna tekemäsi työ verkkopalvelimen levylle, mistä tiedot varmistetaan keskitetysti. Mikäli siirrät aineistoa muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti.

10. Muista, että organisaation laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnyt tietoverkossa aina yhtymän edustajana.

11. Ilmoita aina tietoturvallisuuteen liittyvistä ongelmatilanteista ja havaitsemis-tasi uhkista ja suojauspuutteista välittömästi omalle esimiehelle, tietosuoja-vastaavalle, tietoturvavastaavalle tai atk-henkilöstölle. Heidän velvollisuutensa on ryhtyä tarvittaviin toimenpiteisiin.

Suupohjan peruspalveluliikelaitoskuntayhtymä
Hallintoaukio • PL 100, 61801 KAUHAJOKI • (06) 2413 2000 • fax. (06) 2413 2009 • www.llky.fi