KALLIO
peruspalvelukuntayhtymä

Peruspalvelukuntayhtymä Kallio

TIETOTURVAPOLITIIKKA

Yhtymähallitus 10.4.2014 § 41

Johdanto

Tiedon käsittely on oleellinen osa Peruspalvelukuntayhtymä Kallion toimintaa ja palveluiden tuottamista.

Tietojenkäsittelyn tehokkuus, toimintakyky, turvallisuus ja virheettömyys ovat keskeisiä tekijöitä palvelutuotannon tehokkuudelle ja laadulle. Käytettävät tietoaineistot sisältävät usein asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava.

Tiedon turvaaminen on oleellista koko organisaation toiminnan kannalta. Tietoturvan hyvä hallinta edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja riittävää resursointia erilaisten uhkatilanteiden varalta. Tietoturvan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää.

Tietoturvapolitiikka on Peruspalvelukuntayhtymä Kallion johdon kannanotto tietoturvan toteuttamiseen. Se määrittelee ne yleisperiaatteet, tavoitteet, joita noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Vastuut määräytyvät kuntayhtymän hallintosäännön mukaisesti.

Peruspalvelukuntayhtymä Kallion yhtymähallituksen vahvistama tietoturvapolitiikka kattaa kuntayhtymän kaikkeen toimintaan liittyvät tietojenkäsittelyn. Jokaisen Peruspalvelukuntayhtymä Kallion viranhaltijan, työntekijän ja luottamushenkilön sekä toimintayksikön tietojen ja tietojärjestelmien käyttäjän on tunnettava tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeistuksia ja määräyksiä.

Organisaation ulkopuolisten toimijoiden tulee myös sitoutua noudattamaan tätä tietoturvapolitiikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsylle toimintayksikön tietojärjestelmiin ja niiden tietoaineistoihin. Ostopalveluasiakkaiden ja muiden sidosryhmien välisissä sopimuksissa ja tietoturvakäytäntöjen toteuttamisessa vähimmäisvaatimuksena on tämä politiikka ja siihen liittyvät ohjeet.

Tietoturva ja tietosuoja

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvaan kuuluvat tietoturvan organisointi, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Hyväksytyn tietoturvapolitiikan mukainen tietoturva sisältyy luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa toimintayksikön yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käsittelemiseltä. Tietosuojaan kuuluvat yksityisten henkilöiden yksityisyydensuoja sekä sitä turvaavat oikeudet ja edut henkilötietoja käsiteltäessä. Sosiaali- ja terveyspalveluita tuottavan toimintayksikön tietosuojaa ohjaavat voimakkaasti asiakastietojen käsittelystä säädetyt lait ja määräykset.

Tietosuojapolitiikka liittyy kiinteänä osana Peruspalvelukuntayhtymä Kallion tietoturvapolitiikkaan.

Tietoturvan tavoitteet

Peruspalvelukuntayhtymä Kallion tietoturvatyön tavoitteena on turvata kuntayhtymän toimintaa tukevien tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, havaita ja estää tietojen ja

tietojärjestelmien luvaton käyttö, tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen sekä minimoida niistä mahdollisesti aiheutuvat vahingot.

Tietoturvatason tulee mukautua tilanteen, palvelun, standardien ja lakien edellyttämiin vaatimuksiin. Lähtökohtana on, että kuntayhtymän tiedot ja tietojärjestelmät suojataan asianmukaisesti sekä normaali että poikkeusoloissa hallinnollisin ja teknisin toimenpitein. Terveydenhuollon toimintayksikkönä Peruspalvelukuntayhtymä Kallio vastaa osana tietoturvatyötä myös potilasasiakirjojen ja potilastietoja sisältävien muiden asiakirjojen suojaamiseen liittyvästä tietoturvatyön suunnittelusta ja toteuttamisesta.

Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Tietoturvatyön tavoitteena on sisällyttää hyväksytyn tietoturvapolitiikan ja sitä täydentävien tietoturvaperiaatteiden ja –ohjeiden mukainen tietoturva luonnollisena osana kaikkeen kuntayhtymän toimintaan. Tämä tarkoittaa henkilökunnan, yhteistyökumppaneiden ja alihankkijoiden sitouttamista Peruspalvelukuntayhtymä Kallion tietoturvakäytäntöihin ja vastuuttamista huolehtimaan käsiteltävien tietojen tietoturvasta.

Tietoturvatyön tavoitteena on ylläpitää kuntalaisten ja eri sidosryhmien luottamusta kuntayhtymän tarjoamiin perinteisiin ja sähköisiin palveluihin sekä niiden tietoturvan, tietosuojan ja yksityisyydensuojan toteutumiseen.

Organisointi ja vastuut

Kokonaisvastuu tietoturvan toteutumisesta on Peruspalvelukuntayhtymä Kallion hallituksella ja kuntayhtymän johtajalla. Tietoturvan organisointi perustuu kuntayhtymän hallintosääntöön.

Kuntayhtymän tietoturvatyön kokonaisuudesta vastaa Hallinto- ja tukipalvelujen toimialajohtaja saamiensa resurssien ja toimintavaltuuksien puitteissa. Hallinto- ja tukipalveluiden toimialajohtaja nimeää tietoturvaryhmän. Tietoturvaryhmä valmistelee tietoturvan linjaukset ja ohjeet Peruspalvelukuntayhtymä Kallion johtoryhmälle toimialajohtajien hyväksyttäväksi ja vastaa tietoturva-asioiden sisäisestä tiedottamisesta kuntayhtymässä.

Kuntayhtymän potilas- ja asiakastietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta vastaavat toimialajohtajat. Toimialajohtajat nimeävät toimialoilleen tietosuojavastaavat.

Kuntayhtymän eri palvelualat vastaavat tietoturvan toteutumisesta omassa toiminnassaan sekä hankkimissaan ostopalveluissa. Palvelualojen johdon ja kuntayhtymään nimettyjen tietoturva- ja tietosuojavastaavien tulee huomioida toiminnan erityispiirteet ja lainsäädäntö sekä selventää tietoturvavastuut omissa yksiköissään.

Jokaiselle tietovarastolle ja tietojärjestelmälle määritetään omistaja, joka vastaa järjestelmänsä toiminnasta ja tietoturvan kehittämisestä ja toteuttamisesta. Omistajien tehtävänä on mm. kartoittaa tietojärjestelmiensä toimintaan liittyvät riskit, huolehtia tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta, pääsyn valvonnasta ja toimintojen jatkuvuudesta. Jokaisesta tietojärjestelmästä laaditaan tarvittavat dokumentit.

Kuntayhtymän työntekijöiden vastuulla on huolehtia siitä, että heidän työtehtävissään käsittelemät, organisaatiolle kuuluvat tiedot jäävät organisaation haltuun ellei niitä muilla määräyksillä ole määrätty hävitettäviksi. Kuntayhtymän lukuun ylläpidettävien tietojen toimittamisesta kuntayhtymälle toimeksiantosuhteen päätyttyä vastaa sopimuksen allekirjoittaja.

Esimiesten tehtävänä on vastata siitä, että työntekijöillä on oikeudet tehtävän edellyttämässä laajuudessa tarvittaviin tietojärjestelmiin ja tietoihin, myös työtehtävien mahdolliset muutokset huomioiden. Työsuhteen päättyessä on huolehdittava käyttöoikeuksien poistamisesta tietojärjestelmiin.

Esimiesten tehtävänä on huolehtia myös siitä, että alaiset saavat riittävän perehdytyksen ja koulutuksen tietoturvaan ja siitä, että työntekijät ymmärtävät tietoturvan merkityksen. Esimiehiltä odotetaan esimerkillistä ja vastuullista tietoturvakäyttäytymistä.

Tietoturvan toteutus

Tietoturvan toteuttamisen perusteena on tässä dokumentissa kuvattu ja kuntayhtymän hallituksen hyväksymä *Peruspalvelukuntayhtymä Kallion tietoturvapolitiikka*. Tietoturvan toteuttamisen lähtökohtana on tietoturvapolitiikan tehokas viestiminen koko organisaatiolle.

Peruspalvelukuntayhtymä Kallion tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin velvoittaviin säädöksiin ja ohjeisiin. Lainsäädännön ja ohjeistusten muutokset otetaan huomioon toimintayksikön tietoturvan kehittämisessä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Käyttäjien toimintaa ohjataan käyttösäännöillä ja toimintaohjeilla sekä tietoturvakoulutuksella.

Jokaisen kuntayhtymän tietoverkkojen ja tietojärjestelmien käyttäjän tulee noudattaa hyväksyttyjä tietoturvaperiaatteita ja –ohjeita, joiden noudattamiseen jokainen käyttäjä sitoutuu allekirjoittamalla käyttäjäsitoumuksen työ- tai toimeksiantosopimuksen yhteydessä.

Näiden ohjeistusten tuntemus ja käyttäjäsitoumuksen allekirjoittaminen on edellytys tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöoikeuksien saamiselle. Esimiesten tehtävänä on valvoa tietoturvaohjeiden noudattamista ja tietoturvan toteutumista yksiköissään ja työntekijöiden keskuudessa.

Käytännön teknisestä tietoturvasta ja sen ohjeistuksesta vastaavat osaltaan palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. Palvelusopimuksissa huomioidaan tietoturvaan liittyvät vaatimukset, velvoitteet, häiriötilanteiden toimintamallit ja määritellään vastuuhenkilöt läpi koko palveluketjun.

Palvelutuottajan vastuulla on raportoida tietoturvaan kohdistuvista merkittävistä riskeistä välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille. Jokaisen työntekijän velvollisuus on ilmoittaa havaitsemistaan tietoturvaan liittyvistä puutteista tai väärinkäytöksistä esimiehelleen tai toimialan tietosuojavastaavalle.

Jokaiselle kuntayhtymän tietojärjestelmälle on nimetty omistaja, joka osaltaan vastaa tietojärjestelmän tietoturvan toteutumisesta. Järjestelmän omistajuuteen liittyvät tiedot dokumentoidaan rekisteri- ja tietojärjestelmäselosteessa..

Koulutus ja ohjeistus

Tietoturvakoulutusta järjestetään yksittäisinä koulutustapahtumina tai tietoiskutyyppisinä tilaisuuksina. Henkilöstön jatkuvaa osaamista ylläpidetään sähköisen koulutusympäristön avulla. Koulutuksen tarkoituksena on ylläpitää riittävä tietoturvaosaaminen muistuttaen säännöllisesti tietoturvan tärkeydestä.

Koulutus on pakollinen koko henkilöstölle osana jokaisen työntekijän henkilökohtaisia vaatimuksia ja osaamisen kehittämissuunnitelmaa. Koulutuksen hyväksytystä suorittamisesta tulostuu todistus, joka oikeuttaa käyttöoikeuksien saamiseen tietojärjestelmiin.

Tietoturvan käsikirja sisältää kaiken oleellisen tiedon tietoturvan ylläpitämisessä. Tietoturvan käsikirja on Kallion sisäisessä intrassa.

Tietoturvan seuranta ja valvonta

Tietoturvapolitiikan ja –ohjeiden noudattamisen valvonta on tärkeä osa kuntayhtymän sisäistä valvontaa.

Tietoturvaryhmä ja kuntayhtymän johtoryhmä seuraavat teknisen ja hallinnollisen tietoturvan toteutumista. Hallinnollisen ja teknisen valvonnan menetelmät on kuvattu erillisissä ohjeissa.

Käyttäjien ja tietojärjestelmien ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai toimialan tietosuojavastaavalle.

Esimiesten tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään ja raportoida tietoturvaloukkauksista tietosuojavastaavalle.

ICT-palveluiden tuottajilla on velvollisuus raportoida säännöllisesti tietoturvaan liittyvistä palvelutasojen täyttymisestä ja riskeistä tietoturvavastaavalle.

Tietosuojavastaavien tehtävänä on valvoa kuntayhtymän potilas- ja asiakastiedon käsittelystä säädetyn lain ja ohjeistusten toteutumista ja ryhtyä toimenpiteisiin havaittujen tietosuojan heikkouksien korjaamiseksi.

Tietoturvavastaavien tehtävänä on seurata ja valvoa kuntayhtymän tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

Tiedottaminen

Tietoturva-asioihin liittyvästä sisäisestä tiedottamisesta vastaa tietosuojavastaavat yhteistyössä tietoturvatyöryhmän kanssa. Ensisijainen sisäisen viestinnän tiedotuskanava on kuntayhtymän intranet.

Ulkoinen tiedottaminen toteutetaan kuntayhtymän viestintäsuunnitelman mukaisesti.