9.5.2019

Sosiaali- ja terveydenhuollon toimintayksikköjen tietoturvapolitiikka

Hyväksytty: Sosiaali- ja terveyslautakunta, päivämäärä 25.9.2012
Päivitetty: Pia-Maria Sjöström/Solveig Sandvik-Nyberg, päivämäärä 9.5.2019

1. Johdanto

Tietojenkäsittely tukee Pietarsaaren sosiaali- ja terveysviraston toimintayksikön palvelujen tuottamista, ja palveluiden tehokkuus riippuu osaltaan tietojenkäsittelystä. Tietoaineistot sisältävät potilaisiin, asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on Suomen lainsäädännön ja EU:n tietosuoja-asetuksen perusteella suojattava. Tietojenkäsittelyn on oltava tehokasta, virheetöntä ja varmaa.

Tietoturvapolitiikka määrittelee ne periaatteet, toimintatavat, vastuut sekä seurannan ja valvonnan, joita toimintayksikössä noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Tietoturvapolitiikkaa täydentävät **tietosuojan omavalvontasuunnitelma,** joka sisältää vuosittaisen **tietoturvasuunnitelman**, sekä yksityiskohtaiset määräykset ja ohjeet.

Tietoturvapolitiikkaa ohjaavat seuraavat periaatteet:

- Tietoturva ja tietosuoja ovat Suomen lainsäädännön mukaisesti osa organisaatiomme päivittäistä toimintaa ja koskevat koko toimintaa ja henkilöstöä.
- Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista monenlaisilta uhkilta tarkoituksena varmistaa toiminnan jatkuvuus, minimoida toiminnalliset riskit sekä maksimoida toiminnan ja investointien tulos.
- Tietoturva- ja tietosuoja-asiat huomioidaan välineriippumattomasti.
- Paperiset asiakirjat, sähköiset tietovarannot, tietoverkot, tietotekniset laitteet, tietojärjestelmät ja niihin liittyvät palvelut on suojattava sekä normaali- että poikkeusoloissa.
- Tietoturvallisuuden saavuttamiseksi pitää toteuttaa turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista.
- Luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
- Esimiehen ja muun johdon on varmistettava, että tietoturvamääräykset ja ohjeet koulutetaan tai perehdytetään henkilöstölle.
- Tietoturvaan liittyvä ohjaus, valvonta ja seuranta pitää organisoida.

2. Kattavuus

Toimintayksikön sosiaali- ja terveyslautakunnan vahvistama tietoturvapolitiikka kattaa toimintayksikön kaikki toimintaan liittyvät tietojen käsittelyn tehtävät. Jokaisen Pietarsaaren sosiaali- ja terveysviraston viranhaltijan, työntekijän ja luottamushenkilön sekä toimintayksikön tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Toimintayksikön ulkopuolisten terveydenhuollon toimijoiden, toimittajien ja muiden ulkopuolisten tahojen tulee myös sitoutua noudattamaan tätä tietoturvapolitiikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsylle toimintayksikön tietojärjestelmiin ja niiden tietoaineistoihin.

3. Tietoturva

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

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

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

4. Tietoturvatyö

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvatyön päämäärä on turvata toimintayksikön toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Sosiaali- ja terveydenhuollon toimintayksikkö vastaa osana tietoturvatyötä myös potilas- ja asiakasasiakirjojen ja potilas- ja asiakastietoja sisältävien muiden asiakirjojen suojaamiseen liittyvästä tietoturvatyön suunnittelusta ja toteuttamisesta.

5. Organisointi ja vastuut

Tietoturvaa johtaa ja valvoo kaupunginhallitus**.** Kaupunginjohtaja päättää toimintayksikön kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan ja tietosuojavastaavan.

Tietoturvavastaava vastaa toimintayksikön tietoturvatyön kokonaisuudesta toimintayksikön johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Tietoturvavastaavan valtuudet ja velvollisuudet pitää määritellä. Hän vastaa myös tietoturva-asioista tiedottamisesta toimintayksikön ulkopuolelle ja toimintayksikössä yleisellä tasolla. Tietoturvavastaava vastaa toimintayksikön tietoturvallisuustason määrittelystä ja arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta. Hän vastaa tietoturvan kehittämissuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta toimintayksikössä ja sen ostamissa palveluissa sekä raportoinnista johdolle.

Tietosuojavastaavan tehtävänä on toimia rekisterinpitäjän erityisasiantuntijana henkilötietojen hyvän käsittelytavan ja mahdollisimman korkeatasoinen tietosuojan saavuttamiseksi. Hänen tehtävänään on tukea henkilökuntaa tietosuoja-asioissa ja auttaa toteuttamaan rekisterinpitäjälle määrätyt GDPR:n mukaiset velvoitteet.

Toimintayksikön keskeisten toimintojen tietosuojanäkemyksiä edustaa **tietosuojaryhmä**, jonka asettaa **sosiaali- ja terveysjohtaja**. Tietosuojaryhmälle nimetään puheenjohtaja ja sihteeri. Ryhmän jäsenet vastaavat oman vastuualueensa tietosuojaprosessien asioiden valmistelusta. Tietosuojaryhmä käsittelee tietosuojatyön linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi. Tietosuojaryhmän kokoonpano on organisaatiokohtainen, ja siihen kuuluvat muun muassa tietosuojavastaava, tietoturvavastaava, eri osa-alueiden toiminnasta vastaavat, potilasasiamies, potilas- ja asiakasrekisterien vastuu- ja yhteyshenkilöt sekä potilastietojärjestelmistä vastaavat henkilöt.

Jokaisella tietojärjestelmällä on **omistajayksikkö** ja **vastuuhenkilö**. Vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toiminnalle ja turvallisuudelle asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely sekä käyttöoikeuksien myöntäminen ja valvonta. Tietoturva-asioita koskevien ohjeiden noudattamisesta sekä tiedottamisesta ja tietoturvallisuuden valvonnasta omassa yksikössään vastaa **yksikön esimies**.

Organisaatiossa jokainen toimintayksikön **työntekijä**, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietosuojavastaavalle.

6. Tietoturvan toteutus

Tietoturvan toteuttamisen perusta on tämä sosiaali- ja terveyslautakunnan hyväksymä kirjallinen tietoturvapolitiikka, joka annetaan tiedoksi jokaiselle toimintayksikön työntekijälle ja tietojärjestelmien käyttäjälle.

Toimintayksikön tietoturvaperiaatteet perustuvat eurooppalaisiin, kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin, velvoittaviin säädöksiin, ohjeisiin ja standardeihin.

Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon toimintayksikön tietoturvan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan yksityiskohtaisesti tietosuojan **omavalvontasuunnitelmassa.** Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuusluokka asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille. Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määritteleminen tapahtuu säännöllisesti suoritettavilla turvallisuusanalyyseillä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Ne kuvataan omavalvontasuunnitelmassa ja tarvittaessa käyttöympäristöille ja yksiköille laadituissa erillisissä tietoturvan kehittämissuunnitelmissa.

Käyttäjien toimintaa ohjataan omavalvontasuunnitelmaan sisältyvillä käyttösäännöillä sekä vahvistetuilla ja saatavilla olevilla toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän tietosuojaohjeen ja sitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

7. Tietoturvan seuranta ja valvonta

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietosuojan ja tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietoturva- tai tietosuojavastaavalle.

Yksikön esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään.

Tietosuojavastaavan tehtävänä on seurata ja valvoa Pietarsaaren sosiaali- ja terveysviraston tietojärjestelmien tietosuojan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietosuojan heikkouksien korjaamiseksi. Tietosuojavastaavan tehtävänä on seurata ja valvoa, että henkilötietoja käsitellään Suomen lainsäädännön ja EU:n tietosuoja-asetuksen mukaisesti, sekä toimia tietosuoja-asioiden asiantuntijana.