



KANGASALAN KUNNAN SOSIAALI JA TERVEYSKESKUKSEN TIETOTURVAPOLITIikka

Hyväksytty: Sosiaali- ja terveystieteiden lautakunta 1.11.2011 § 85

1. JOHDANTO

Tietojenkäsittely tukee Kangasalan kunnan sosiaali- ja terveystieteiden palvelujen tuottamista, ja palveluiden tehokkuus riippuu osaltaan tietojenkäsittelystä. Tietoaineistot sisältävät asiakkaisiin, potilaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava tehokasta, virheetöntä ja varmaa. Sähköisen tietojenkäsittelyn tietoturvasuunnitelma ja -ohjeet ovat yhteiset Pirnet-kuntien kesken.

Tietoturvasuunnitelma määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita toimintayksikössä noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Tietoturvasuunnitelmaa täydentävät **tietoturvasuunnitelma** sekä yksityiskohtaiset määräykset ja ohjeet.

Tietoturvasuunnitelmaa ohjaavat seuraavat periaatteet:

- Tietoturva ja tietosuojat ovat Suomen lainsäädännön mukaisesti osa organisaatiomme päivittäistä toimintaa ja koskevat koko toimintaa ja henkilöstöä.
- Asiat pitää tehdä tietoturvallisesti, jolla tarkoitetaan tiedon suojaamista monenlaisilta uhkilta tarkoituksena varmistaa toiminnan jatkuvuus, minimoida toiminnalliset riskit sekä maksimoida toiminnan ja investointien tulos.
- Tietoturva- ja tietosuojat-asiat huomioidaan välineriippumattomasti.
- Paperiset asiakirjat, sähköiset tietovarannot, tietoverkot, tietotekniset laitteet, tietojärjestelmät ja niihin liittyvät palvelut on suojattava normaali- että poikkeusoloissa.
- Tietoturvallisuuden saavuttamiseksi pitää toteuttaa turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatorakenteista 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 on varmistettava, että tietoturvamääräykset ja ohjeet koulutetaan tai perehdytetään henkilöstölle.
- Tietoturvaan liittyvä ohjaus, valvonta ja seuranta pitää organisoida.

2. KATTAVUUS

Kangasalan kunnan sosiaali- ja terveystieteiden lautakunnan vahvistama tietoturvasuunnitelma kattaa toimintayksikön kaikki toimintaan liittyvät tietojen käsittelyt tehtävät.



Jokaisen sosiaali- ja terveystakeskuksen viranhaltijan, työntekijän ja luottamushenkilön sekä tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapoliittikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Sosiaali- ja terveydenhuollon ulkopuolisten toimijoiden, toimittajien ja muiden tahojen tulee myös sitoutua noudattamaan tätä tietoturvapoliittikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsyyllle toimintayksikön tietojärjestelmiin ja niiden tietoaisteistoihin.

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 tietoturvapoliittikan 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 terveystakeskus vastaa osana tietoturvatyötä myös asiakas- ja potilastietoja sisältävien asiakirjojen suojaamiseen liittyvästä tietoturvatyön suunnittelusta ja toteuttamisesta.

5. ORGANISOINTI JA VASTUUT

Tietoturvaa johtaa ja valvoo **Kangasalan sosiaali- ja terveystakeskunta. Kangasalan kunnan sosiaali- ja terveystakeskunta** päättää sosiaali- ja terveystakeskuksen kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvastavaan ja tietosuojavastavaan. Poti-



lastietojen tietoturvasta vastaa **johtava ylilääkäri** ja sosiaalitoimen tietoturvasta vastaa toimistosihteeri.

Tietoturvavastaava vastaa oman alueensa tietoturvatyön kokonaisuudesta toimintayksikön johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Tietoturvavastaavan valtuudet ja velvollisuudet pitää määrittellä. Hän vastaa myös tietoturva-asioista tiedottamisesta sosiaali- ja terveyskeskuksen 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.

Auditointikriteerien mukaan tietosuojavastaavalla tulee olla kirjallinen toimenkuva. Tietosuojavastaavan tehtävänä on toimia rekisterinpitäjän erityisasiantuntijana henkilötietojen hyvän käsittelytavan ja mahdollisimman korkeatasoinen tietosuojan saavuttamiseksi. Hänen tehtävänä on tukea henkilökuntaa tietosuoja-asioissa ja auttaa toteuttamaan rekisterinpitäjälle määrätyt henkilötietolain mukaiset velvoitteet.

Sosiaali- ja terveyskeskuksen keskeisten toimintojen turvanäkemyksiä edustaa **tietoturvaryhmä**, jonka asettaa **sosiaali- ja terveysjohtaja**. Tietoturvaryhmälle tulee nimetä puheenjohtaja ja sihteeri. Ryhmän jäsenet vastaavat oman vastuualueensa tietoturvaprosessin asioiden valmistelusta. Tietoturvaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi. Tietoturvaryhmän kokoonpano on organisaatiokohtainen.

Jokaisella tietojärjestelmällä on **omistajayksikkö** ja **vastuuhenkilö**. Tietojärjestelmän vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointinnettelyn) määrittely sekä käyttöoikeuksien myöntäminen ja valvonta. Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja 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 raportoisesta esimiehelleen tai tietoturvavastavalle.

6. TIETOTURVAN TOTEUTUS

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



Toimintayksikön tietoturvaperiaatteet perustuvat 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 **tietoturvasuunnitelmassa**. 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 määrittäminen tapahtuu säännöllisesti suoritettavilla turvallisuusanalyysillä.

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

Käyttäjien toimintaa ohjataan tietoturvasuunnitelmaan sisältyvillä käytösäännöillä 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 tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietoturvavastaavalle.

Yksikön esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään.

Tietoturvavastaavan tehtävänä on seurata ja valvoa Kangasalan kunnan tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.