Julkinen tietoturvapolitiikka

Johdanto

Tässä tietoturvapolitiikan julkisessa osassa kuvataan Vankiterveydenhuollon yksikön tietoturvapolitiikan päämäärä ja yleiset linjaukset. Lisäksi kerrotaan mikä taho vastaa mistäkin toiminnosta ja kuvataan toteutuksen organisointi.

Tietoturvalla tarkoitetaan seuraavien asioiden varmistamista:

- tiedon luottamuksellisuus
- tiedon eheys
- tiedon käytettävyys

Määritelmä

Tämä dokumentti kuvaa tietoturvan perusvaatimukset Vankiterveydenhuollon yksikössä. Se luo pohjan toiminnan suunnittelulle ja jalkauttamiselle eri toimipisteisiin valtakunnallisesti. Politiikan julkisen osan lisäksi on kirjoitettu sisäiset osuudet, jotka kattavat tietoturvan luottamukselliset osa-alueet. Nämä osat eivät ole julkisia.

Tietoturvallisuuden kehittäminen

Vankiterveydenhuollon yksikössä toteutetaan ja kehitetään terveydenhuollon tietoturvallisuutta jatkuvasti seuraavien kriteerien mukaisesti:

- Suomen lakien ja asetusten mukaisesti
- Euroopan parlamentin ja neuvoston tietoturva-asetukset huomioiden
- Sosiaali- ja terveysministeriön säädöksiä ja ohjeita noudattaen
- Terveyden ja hyvinvoinnin laitoksen ohjeistamana
- Vankiterveydenhuollon yksikön tietoturvan hallintamallin mukaisesti
- riskilähtöisesti ja skenaariopohjaisesti, tilannekuva huomioiden
- vuosittain katselmoiden
- terveydenhuollon henkilökunnan näkemykset huomioiden
- potilaiden etua ajatellen

Tietoturvapolitiikka katselmoidaan Vankiterveydenhuollon yksikön omavalvonnan vuosikellon mukaisesti. Tietoturva- ja tietosuojapolitiikka, riskienhallintaprosessi sekä Vankiterveydenhuollon yksikön visio, missio ja arvot muodostavat yhtenäisen kokonaisuuden.

Tietoturvapolitiikan päämäärä

Tärkeimpänä päämääränä on Vankiterveydenhuollon yksikkö toimintojen jatkuvuuden turvaaminen muuttuvissa olosuhteissa, myös kriisin aikana.

Tarkoituksenmukainen ja tehokas tietoturva mahdollistaa:

- sellaisten tietoteknisten ratkaisujen toiminnan, jotka mahdollistavat Vankiterveydenhuollon yksikön lakisääteisen perustehtävän suorittamisen
- prosesseissa ja palveluissa käytettävien tietojen eheyden, etenkin henkilö- ja potilastiedon osalta
- luottamuksellisuuden kaikissa olosuhteissa

Tämän politiikka luo perustan Vankiterveydenhuollon yksikön tietojärjestelmien turvallisuudelle ja tietojenkäsittelyn luottamuksellisuudelle. Potilastietojärjestelmän ja muiden digitaalisten toimintojen tuottaman ja käsittelemän datan turvaaminen on olennainen osa vastuullista toimintaamme. Potilaat ja viranomaiset edellyttävät meiltä luottamuksellisuutta ja salassa pitoa.

Tietojenkäsittelyn ja sähköisten asiointipalveluiden kasvu jatkuu. Tietoturvaa koskeva lainsäädäntö lisääntyy ja monimutkaistuu, etenkin potilastiedon sähköistä käsittelyä ja tiedonsiirtoa koskien. Jokaisen työntekijän on noudatettava Vankiterveydenhuollon yksikön tietoturvapolitiikkaa, annettuja ohjeistuksia, sekä kansallisia määräyksiä ja voimassa olevaa lainsäädäntöä. Lisäksi terveydenhuollon alaa koskevat eettiset käytännöt.

Tietoturvan toteuttamisen menetelmät

Riskien arviointi

Tietoturvariskejä arvioidaan säännöllisesti. Prosessissa huomioidaan Vankiterveydenhuollon yksikön perustehtävien suorittamiseen kohdistuvaa uhkaa tai vaikutusta. Riskiarviointi laaditaan aina uuden tietojärjestelmän vaatimusmäärittelyn yhteydessä. Jos toiminnan kriittisyyteen tulee muutoksia, tehdään riskiarviointi.

Tietojen luokittelu ja käsittely

Vankiterveydenhuollon yksikön käytössä tietojen luokittelumenetelmä, jossa ohjeistetaan, miten tiedot tulee luokitella ja määritellään tietoturvakontrollit eri luokkiin kuuluvan tiedon käsittelylle. Vankiterveydenhuollon yksikkö noudattaa Valtioneuvoston asetusta tietoturvallisuudesta valtionhallinnossa sekä lakia sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä.

Potilas- ja henkilötietojen käsittely

Tietosuojapolitiikassa ja erillisissä ohjeistuksissa määritellään, miten potilas- ja henkilötietoja käsitellään Vankiterveydenhuollon yksikössä.

Vankiterveydenhuollon yksikön järjestelmäkehityksessä on työvaiheita, joissa analysoidaan potilas- ja henkilötietojen käsittelyn tietosuojavaatimukset ja luodaan tarvittavat tietoturvamekanismit. Tietoturvatasot määrittelevät valtionhallinnon viranomaisille tietoturvallisuuden minimitason, joka on toteutettava kaikissa yksiköissä, toiminnoissa ja tietojärjestelmissä.

Tekninen toteutus suunnitellaan siten, että se vastaa tiedonkäsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot ja tietoturvakäytännöt riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi.

Tietoturvavaatimukset

Terveydenhuollon tietojärjestelmiä säätelevät kansalliset määräykset ja vaatimukset. Tietojärjestelmien hankinnoissa on aina mukana tietosuoja- ja tietoturvavaatimukset, joita tarjoajien on noudatettava. Vaatimustenmukainen tietoturvan taso voidaan tarvittaessa todentaa sisäisin ja ulkoisin auditoinnein. Lisäksi terveydenhuollon Vankiterveydenhuollon yksikköä valvovat useat eri viranomaiset, jotka tekevät valvontakäyntejä Vankiterveydenhuollon yksikön toimipisteisiin.

Tietoturvakoulutus

Vankiterveydenhuollon yksikkö toteuttaa säännöllisiä toimenpiteitä, joiden avulla ylläpidetään ja parannetaan työntekijöiden tietoturvallisuusosaamista.

Näitä ovat:

- läsnäolo- ja verkkokoulutukset sekä interaktiiviset harjoitukset
- ajantasainen ohjekirjasto intranetissä ja muistutukset hyvistä tietoturvakäytännöistä sähköpostitse
- huijausviesti- ja kyberhyökkäyssimulaatiot
- kohdennettu tietoturvakoulutus, joka on suunniteltu terveydenhuollon alalle ja räätälöity ammattiryhmien mukaan

Valvonta ja seuranta

Tietojärjestelmien toimintaa valvotaan jatkuvasti ja automatisoidusti. Valvontaa toteuttavat henkilöt ovat lain mukaan vaitiolovelvollisia työssään käsittelemistä tiedoista. Kaikki henkilökunta on läpäissyt turvallisuusselvityksen. Myös tietojärjestelmätoimittajiin sovelletaan samoja sääntöjä.

Tietoturvatilanteesta raportoidaan omavalvonnan sekä sisäisten ja ulkoisten tarkastusten yhteydessä. Teknistä tietoturvaa arvioidaan jatkuvasti ja tärkeimpiin ympäristöihin tehdään erillisiä tietoturvatarkastuksia.

Tietoturvapoikkeamien käsittely

Vankiterveydenhuollon yksiköllä on menettelytavat ja palvelut tietoturvapoikkeamien havaitsemiseksi. Mahdollisten tietoturvaloukkauksien käsittelyyn ja raportointiin on määritellyt toimintamallit. Henkilökunta ilmoittaa poikkeamista matalalla kynnyksellä ja heidät opastetaan käyttämään ilmoitusjärjestelmää.

Tietoturvarikkomukset

Tietoturvarikkomukseksi lasketaan tietoturvapolitiikan ja -ohjeistuksen vastainen toiminta. Vankiterveydenhuollon yksikkö on määritellyt menettelytavat rikkomustilanteille ja henkilökunta on tietoinen säännöistä.

Vastuut ja organisointi

Tietoturvapolitiikan hyväksyy Vankiterveydenhuollon yksikön johtoryhmä. Tietoturvapolitiikka kattaa Vankiterveydenhuollon yksikön toiminnot kaikissa toimipisteissä Suomessa. Henkilöstön on noudatettava politiikkaa. Vankiterveydenhuollon yksikön yksiköt huolehtivat toteutuksen tarvittavasta resursoinnista.

Yksikön johtaja vastaa siitä, että Vankiterveydenhuollossa on toimiva tietoturva osana riskienhallintajärjestelmää. Tietoturvan toteuttamisessa hänellä on apunaan Vankiterveydenhuollon yksikön riskienhallintatoiminnot ja IT- henkilökunta, sekä tulosohjaajan tietohallintopalvelut. Tarkoitusta varten perustettu omavalvontatyöryhmä käsittelee ja seuraa tietoturvariskejä sekä päätettyjen riskienhallintatoimenpiteiden toteutumista.

Vastuu sovittujen toimenpiteiden toteuttamisesta on Vankiterveydenhuollon yksikön toiminnanohjauksessa. Nimetty tietoturva-asiantuntija koordinoi tietoturvaprosesseja yksikön johtoryhmässä hyväksyttyjen tavoitteiden mukaisesti. Hän järjestää käytännön toteutuksen ja tarvittavat asiantuntijaresurssit IT-palveluntarjoajilta. Tietoturva-asiantuntija johtaa tietoturvariskien tunnistamista ja hallintatoimenpiteiden määrittämistä.

Jokainen Vankiterveydenhuollon yksikön työntekijä tunnistaa tietoturvaan liittyvät riskit ja reagoi niihin. Jokainen voi kääntyä tietoturva-asiantuntijan puoleen ja kysyä neuvoa epäselvään tilanteeseen.

Tietoturvan hallinta

Tietoturvan hallintamalli on osa Vankiterveydenhuollon yksikön riskienhallintaa, johon kuuluvat mm. potilasturvallisuus, työturvallisuus ja muita kokonaisturvallisuuden osa-alueita. Vankiterveydenhuollon yksikön johtoryhmän alainen omavalvontatyöryhmä seuraa ja arvioi Vankiterveydenhuollon yksikön omavalvonnan, sisäisen tarkastuksen ja riskienhallintajärjestelmien tehokkuutta. Johtoryhmä käsittelee yksikön merkittävimmät tietoturvariskit ja ajankohtaiset uhat, jotka Tietoturvavastaava esittelee johtoryhmälle tilannekuvan muodossa.

Voimaantulo

Hyväksytty Vankiterveydenhuollon yksikön johtoryhmässä omavalvontatyöryhmän esityksen mukaisesti 15.6.2022. Politiikka tulee voimaan 16.6.2022.