Tietoturvapolitiikka

Perusturvapalvelut

Versio	Pvm.	Kuvaus	Laatija/laatijat	Hyväksyjä
1.0	9.10.2012	eReseptin käyttöönoton edellyttämä kuvaus terveyskeskuksen tietoturvapolitiikasta	Terveyskeskuksen tietoturvatyöryhmä	Perusturvalautakunta, Petu 09.10.2012 § 96
1.1	01/2015	Tarkistus ja vastuutahojen päivitys	—	—
2.0	1.11.2021	Koko perusturvapalveluiden palvelualaa koskeva tietoturvapolitiikka, joka määrittää noudatettavat periaatteet, toimintatavat ja vastuut	Tietosuojavastaava	Perusturvalautakunta Petu xx.xx.xxxx § xx

SISÄLLYS

LIITTEET

Liite 1. Tietoturvan ja -suojan valvonnan vastuut

KÄSITTEET

Tietoturvapolitiikka	*Organisaation hyväksytty näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta*
Tietoturvallisuus = Tietoturva	*Hallinnolliset ja tekniset toimenpiteet, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus sekä rekisteröidyn oikeuksien toteutuminen. Tietoturvallisuus on riskienhallintaa ja osa organisaation turvallisuutta.*
Tietosuoja	*Toimenpiteet, joiden tarkoituksena on suojata rekisteröidyn oikeuksien ja vapauksien toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.*
Tietoturvatyö	*Tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista, jotta voidaan turvata keskeytymätön toiminta sekä estää tietosuojarikkomukset.*
Henkilötieto	*Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.*
Henkilötietojen erityiset tietoryhmät, arkaluonteiset henkilötiedot	*Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja, tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.*
Henkilötietojen käsittelijä	*Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.*
Kyberturvallisuus	*Toimenpiteet, joilla organisaatio suojaa tarvittavat järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet kyberuhkilta. Esimerkkejä kyberuhista ovat tietojenkalastelut, haittaohjelmat ja palvelunestohyökkäykset*.

1. JOHDANTO

Tietojen, käsittelyprosessien, tietojärjestelmien, teknisen ympäristön sekä toimitilojen turvallisuus on välttämätön edellytys perusturvapalveluiden toiminnalle. Potilas- ja asiakastietojen saatavuus, virhettömyys, ajantasaisuus tukevat perusturvapalveluiden vastuulla olevien sosiaali- ja terveyspalveluien tuottamista. Tietoturvallisuus ja tietosuoja on huomioitava kaikessa toiminnassa jo suunnitteluvaiheessa. Käsiteltävien tietojen arkaluonteisuus ja tietojen suuri määrä edellyttävät tietojen luottamuksellisuuden varmistamista tietojen koko elinkaaren ajan.

Tietojen käsittely vaikuttaa palveluiden tehokkuuteen ja toiminnan sujuvuuteen. Tietoaineistot sisältävät potilaisiin, asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa. Tietoaineistot sisältävät sekä manuaalisessa että sähköisessä muodossa olevaa turvattavaa tietoa. Tietojenkäsittelyn on oltava tehokasta, virheetöntä ja varmaa.

Tietoturvan tärkeyttä lisäävät myös potilaille/asiakkaille sunnattujen sähköisten palveluiden sekä tietojärjestelmien etä- ja mobiilikäytön lisääntyminen, ostopalveluina tuotettavat palvelut sekä palvelutuotannon uudet menetelmät erityisesti pilvipalvelut.

Tietoturvapolitiikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita noudatetaan Euran perusturvapalveluiden tietoturvan toteuttamisessa ja kehittämisessä. Euran perusturvapalveluiden tietoturvatyötä ohjaavat lainsäädäntö, viranomaisohjeet sekä muut mahdolliset vaatimukset.

Tietoturvapolitiikka on kaikkia sitova ja se toimii perustana tietoturvasuunnitelmalle ja muille tietoturvaa koskeville toimintaohjeille ja -suunnitelmille, joiden tehtävänä on tarkentaa ja täydentää tietoturvapolitiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

2. TIETOTURVAN TAVOITTEET JA PERUSPERIAATTEET

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen suojaamista hallinnollisilla ja teknisillä toimenpiteillä. Tietoturvallisuuden perusperiaatteena on perusturvapalveluiden vastuulla olevien palveluiden jatkuvuuden turvaaminen kaikissa olosuhteissa. Tietoturvallisuus näkyy laadukkaana, avoimena ja häiriöttömänä toimintana sekä osaltaan varmistaa potilaille/asiakkaille tarjottavien palveluiden luotettavuuden.

Euran perusturvapalveluiden tietoturvatavoitteet ovat seuraavat:

1. **Tietoturvan hallinta ja suunnittelu**
   - Tietoturvatoiminta on suunnitelmallista, systemaattista ja kattavaa
   - Tietoturvallisuuden suunnittelussa ja hallinnassa huomioidaan tietojen luottamuksellisuus, eheys ja saatavuus
     - Luottamuksellisuuden avulla varmistetaan, että tiedot ovat vain ja ainostaan

niihin oikeutettujen tahojen käytettävissä.
    - Eheyden avulla varmistetaan, että tiedot ovat luotettavia, virheettömiä, kattavia ja ajantasaisia.
    - Saatavuuden avulla varmistetaan, että tiedot ovat käytettävissä toiminnan kannalta oikeaan aikaan, viivytyksettä ja häiriöittä.

2. **Tietoturvan kattavuus**
    - Peruturvapalveluiden tietoturvapolitiikka kattaa kaikkeen toimintaan liittyvät tietojen käsittelyn tehtävät.
    - Henkilöstöltä, luottamushenkilöiltä sekä yhteistyö- ja sopimuskumppaneilta edellytetään tietoturvallista työskentelyä.
    - Henkilöstöltä, luottamushenkilöiltä sekä yhteistyö- ja sopimuskumppaneilta edellytetään tietoturva- ja tietosuojaohjeistusten sekä aiheeseen liittyvää lainsäädännön noudattamista.
    - Henkilöstön tietoturvallista työskentelyä tuetaan selkeillä ohjeistuksilla, helppokäyttöisillä tietoturvaratkaisuilla, perehdytyksillä ja koulutuksilla.

3. **Riskit ja kehittäminen**
    - Euran perusturvapalveluiden vastuulla olevien tietojen, järjestelmien ja käsittelyprosessien riskit tunnistetaan, arvioidaan ja käsitellään.
    - Tietoturvallista organisaatiota rakennetaan eri toimijoiden kanssa yhteistyössä jatkuvan riskienhallintaprosessin kautta.

4. **Seuranta, häiriöt ja jatkuvuus**
    - Palveluiden saatavuus ja toiminnan jatkuvuus varmistetaan sekä normaalitilanteessa että poikkeusoloissa.
    - Tietoturvan toteutumista varmistetaan säännöllisellä arvioinnilla, seurannalla ja harjoittelulla.
    - Tietoturvaan liittyviä kehittämistoimenpiteitä toteutetaan jakuvan parantamisen periaatteen mukaisesti

3. ORGNISOINTI JA VASTUU

Tietoturvaa johtaa ja valvoo **Euran Perusturvalautakunta**. Se hyväksyy Euran perusturvapalveluiden tietoturvapolitiikan ja siihen tehtävät muutokset perusturvapalveluiden esityksen perusteella. **Perusturvajohtaja** toimii potilas- ja asiakasrekisterien vastuuhenkilönä ja vastaa potilas- ja asiakastietojen käsittelyn lainmukaisuudesta

Euran kunnassa toimii kunnanjohtajan nimittämä **tietosuojatyöryhmä**. Työryhmä ylläpitää ja kehittää tietoturvallisuutta, luo yleisiä kaikkia koskevia periaatteita, antaa niihin liittyviä tarkentavia ohjeita sekä osallistuu tietoturvaa koskevien ratkaisujen ja ohjeistusten suunnitteluun. Työryhmässä on edustus myös perusturvapalveluiden palvelualueelta.

Perusturvapalveluiden tietoturvavastaava vastaa palvelualueen tietoturvatyön kokonaisuudesta toimintayksikön johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Hän vastaa myös tietoturvaan liittyvästä tiedottamisesta perusturvapalveluiden ulkopuolelle ja toimintayksikössä yleisellä tasolla. Perusturvapalveluiden tietoturvavastaavana

toimii johtava lääkäri.

Perusturvapalveluiden tietosuojavastaavan tehtävänä on tietosuojan toteutumisen seuranta, kehittäminen, edistäminen ja ohjaaminen. Tietosuojavastaava valmistelee ja ylläpitää tietosuoja- ja tietoturvaohjeita sekä vastaa lokiselvityksistä. Hän raportoi tietosuojan valvonnasta. Kunnanjohtaja on viranhaltijapäätöksellä (25/00.00.01/2021) nimennyt perusturvapalveluiden tietosuojavastaavan.

Tietohallinto koordinoi tietojärjestelmien ja niiden käytön tietoturvan ja teknisen toteutuksen suunnittelua, toteutumista ja raportointia sekä vastaa laitteistojen tietoturvasta. Tietohallinto toimii yhdessä palveluntuottajien kanssa teknisenä asiantuntijana tietoturvaa koskevissa kysymyksissä.

Järjestelmien pääkäyttäjät ja vastuuhenkilöt määrittelevät ja vastaavat tietojärjestelmien ja sovellusten tieturvasta, palvelutasosta, käyttöoikeuksista, varmistamisesta, kehittämisestä ja käytöstä. Tietojärjestelmien pääkäyttäjät vastaavat käyttöoikeuksien myöntämisestä esimiesten välittämien tietojen perusteella. Käyttöoikeuksien myöntämisessä noudatetaan vähimpien oikeuksien periaatetta eli käyttäjille myönnetään vain ne oikeudet, joita he työssään tarvitsevat. Käyttöoikeudet tulee myös poistaa, mikäli niiden tarve on poistunut esimerkiksi työntekijän lopettaessa tietyt työtehtävät. Esimiesten tehtävänä on välittää tarvittavat tiedot tietojärjestelmien pääkäyttäjille.

Vastuualuepäälliköt vastaavat vastuualueensa tietoturvallisuuden kokonaisuudesta ja tukevat tietoturvan jatkuvaa kehittämistä ja ylläpitämistä. **Esimiehet** vastaavat siitä, että henkilöstö ja työssäoppijat yms. ovat käynyt vaadittavan koulutuksen sekä saaneet riittävän perehdytyksen ja ohjauksen tietoturvaan ja -suojaan liittyen. Esimiehet vastaavat omien työyksikköidensä osalta tietoturvaan liittyvästä ohjeistamisesta, tiedottamisesta ja valvonnasta ja raportoinnista sekä tietoturvan ja -suoja HaiPro-ilmoitusten laatimisesta sekä niiden käsittelystä.

Jokainen **työntekijä**, tietoja käsittelevä, tietojärjestelmien ja tietoverkkojen ylläpitäjä ja käyttäjä on palvelussuhteesta riippumatta omalta osaltaan vastuussa voimassa oleva lainsäädännön noudattamisesta, tietojen käsittelystä ja viestintävälineiden tietoturvallisesta käytöstä annettujen ohjeiden mukaisesti.

Jokainen työntekijä on havaitsemistaan tahattomista tai tahallista tietosuojarikkomuksista tai riskeistä velvollinen raportoimaan HaiPro-järjestelmään. Lisäksi hänen tulee ilmoittaa asiasta esimiehelleen sekä tietoturva- tai tietosuojavastaavalle. Vastuut on kuvattu kootusti liitteen 1. taulukossa

4. TIETOTURVAN TOTEUTUS

Tietoturvan toteuttamisen perusta on tämä perusturvalautakunnan hyväksymä kirjallinen tietoturvapolitiikka, joka annetaan tiedoksi jokaiselle toimintayksikön työntekijälle ja tietojär-jestelmien käyttäjälle.

Tietoturvapoliitiikkaa ja tietoturvallisuuskäytäntöjä ja -periaatteita sekä ohjeita noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia Euran kunnan/perusturvapalveluiden palveluksessa olevia henkilöitä ja luottamushenkilöitä. Tietoturvapoliitiikkaa ja

tietoturvallisuuskäytäntöjä noudatetaan myös kaikessa ulkopuolisten yhteistyökumppanien kanssa tapahtuvassa toiminnassa.

Käyttäjien toimintaa ohjataan toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän salassapito- ja käyttäjäsopimuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

5. TIETOTURVAN SEURANTA JA VALVONTA

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvan puutteista, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta HaiPro-ilmoituksella sekä lisäksi asiasta tulee ilmoittaa esimiehelle sekä tietoturva- tai tietosuojavastaavalle.

Tietoturva- ja tietosuojavastaavalla ja esimiehillä on valtuudet tehdä tietoturvallisuuteen liittyviä tarkastuksia omien vastuualueidensa osalta ja ryhtyä tarvittaviin toimenpiteisiin ongelmakohtien ratkaisemiseksi.

Tietojärjestelmien käytöstä kertynyttä tietoa sekä järjestelmien käyttöä seurataan. Perusturvapalveluissa tehdään sisäistä valvontaa potilas- ja asiakastietoja sisältävien sekä muiden henkilötietoja sisältävien järjestelmien käytöstä.

Sisäisellä valvonnalla tarkoitetaan kaikkia niitä toimenpiteitä ja menetelmiä, joilla pyritään henkilötietojen asianmukaiseen ja luottamukselliseen käyttöön. Valvonta toteutetaan käyttälokien seuranta- ja valvontasuunnitelman mukaisesti.

6. TIETOTURVARIKKOMUKSET JA SANKTIOT

Tietoturvaohjeiden sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti ennalta määritellyn prosessin mukaisesti. Havaitut tietoturvallisuuteen liittyvät rikkomukset käsitellään ensin tietosuojavastaavan, tietoturvavastaavan ja lähiesimiehen johdolla. Tietoturvarikkomusten mahdollisiin seuraamuksiin sovelletaan Tietoturva- ja tietosuojarikkomusten seuraamustaulukkoa. Rikosoikeudellisen lainsäädännön piiriin kuuluvat rikkomukset ilmoitetaan aina poliisille.

Liite 1. Tietoturvan ja -suojan valvonnan vastuut

Roolit Euran perusturvapal-velussa	**Tehtävä ja vastuu**
Perusturvajohtaja	Potilas- ja asiakasrekisterien vastuuhenkilö Vastaa asiakas- ja potilastietojen käsittelyn lainmukaisuu-desta
Johtava lääkäri	Tietoturvan vastuuhenkilö Vastaa käyttäjäkohtaisista käyttöoikeuksista erikoistilan-teissa
Tietosuojavastaava	Tietoturvan valvonta, ohjeistus, toteutumisen seuranta ja koulutus Tietosuoja/tietoturvaohjeiden valmistelu ja ylläpito Valvonnan raportointi
Tietohallinto	Tietojärjestelmien, verkkojen ja laitteistojen tietoturvan asiantuntijavastuu.
Esimies	Tietosuojan valvonta yksikössä
Työntekijä	Toimii tietosuojan edellyttämällä tavalla Noudattaa tietoturva- ja tietosuojaohjeita Ilmoittaa tietoturvauhkista ja poikkea-mista Osallistuu tietoturva/tietosuojakou-lutuksiin
Potilasasiamies	Potilaan neuvonta ja avustaminen Neuvoo potilasta ja henkilökuntaa Välittää tarvittaessa lokitarkastuspyynnöt tietosuojavastaa-valle
Tietosuojatyöryhmä	Avustaa tietosuojavastaavaa ja johtoa erilaisissa toi-missa, kuten esim. tietoturvan ohjaus, neuvonta, kehittä-minen, koulutuksen järjestäminen,