POHJOIS-SAVON HYVINVOINTIALUE

Tietoturvallisuuden, tietosuojan ja henkilörekisterien vastuut

Tietoturva- ja tietosuojapolitiikka liite 3

POHJOIS-SAVON HYVINVOINTIALUE

Sisällys

1 Dokumentin tarkoitus ja rakenne

Tämän dokumentti on Pohjois-Savon hyvinvointialueen (jatkossa hyvinvointialue) tietoturva- ja tietosuojapolitiikan liite 3.

Luku 2. kuvaa hyvinvointialueen tietoturva- ja tietosuojatehtävät, vastuut sekä organisoinnin. Luku 3. kuvaa tiedonhallintalain mukaiset tehtävät. Luku 4. kuvaa henkilörekisterien vastuut.

Tämä dokumentti tarkentaa KYSin toimintaohjeen (OHJE-2017-00606) mukaisia vastuita tietoturvan ja tietosuojan osalta.

2 Tietoturva- ja tietosuojatehtävät

Tässä luvussa kuvataan tehtävien tarkkuudella yksittäisten työntekijöiden, viranhaltijoiden ja toimielinten roolit hyvinvointialueen tietoturvallisuuden ja tietosuojan toteuttamisessa.

2.1 Hyvinvointialueen ylin johto (aluevaltuusto, aluehallitus)

- varmistaa, että hyvinvointialueella on tietoturvallisuuden ja tietosuojan hallintajärjestelmä, ja sitä ylläpidetään ja parannetaan jatkuvasti.
- päättää tietoturvallisuuden ja tietosuojan hallintajärjestelmän rajauksista ja soveltamisesta.
- varmistaa, että tietoturvallisuuden ja tietosuojan hallintajärjestelmä saavuttaa halutut tulokset.
- edellyttää, että koko hyvinvointialueen henkilökunta, opiskelijat, toimittajat, luottamushenkilöt ja muut sidosryhmät toimivat tietoturvallisesti hyvinvointialueen olemassa olevien politiikkojen, periaatteiden ja ohjeiden mukaisesti.
- ohjaa henkilöstöä tietoturvallisuuden ja tietosuojan hallintajärjestelmän vaikuttavuuden kehittämiseen.
- varmistaa, että hyvinvointialueella tunnistetaan keskeinen EU-tasoinen, kansallinen ja erityisesti sosiaali- ja terveysalan tietoturvallisuuteen ja tietosuojaan liittyvä lainsäädäntö.
- määrittää hyvinvointialueen ja sen toimintaympäristön tietoturvallisuuden tason.
- tunnistaa tietoturvallisuuden ja tietosuojan hallintajärjestelmän kannalta olennaiset sidosryhmät ja näiden sidosryhmien asettamat tietoturvallisuutta ja tietosuojaa koskevat vaatimukset.
- sitoutuu tietoturvallisuutta ja tietosuojaa koskevien periaatteiden ja vaatimusten täyttämiseen.
- varmistaa, että tietoturvallisuustavoitteet asetetaan ja tietoturvan kehittämissuunnitelmat laaditaan ja että ne ovat yhdenmukaisia hyvinvointialueen strategian kanssa.

- varmistaa, että tietoturva- ja tietosuojapolitiikka laaditaan ja sitä ylläpidetään säännöllisesti.
- varmistaa, että tietoturvallisuuden ja tietosuojan hallintajärjestelmän vaatimukset yhdistetään hyvinvointialueen kaikkeen toimintaan.
- määrittelee tietoturvallisuuteen ja tietosuojaan liittyvät roolit ja vastuut sekä tietoturvallisuuden ja tietosuojan tarvitsemat resurssit.
- huolehtii riittävistä resursseista tietoturvallisuuden ja tietosuojan toteuttamiseen, ylläpitoon ja kehittämiseen.
- valvoo, että tietoturvallisuus ja tietosuoja on organisoitu hyvinvointialueen toimipaikoissa ja yksiköissä.
- varmistaa, että hyvinvointialueella on edellytykset toimia tietoturvallisuuteen tai tietosuojaan liittyvissä poikkeama-, loukkaus-, erityis- ja kriisitilanteissa.
- viestii tietoturvallisuustavoitteiden ja tietoturva- ja tietosuojapolitiikan lakisääteisten velvoitteiden noudattamisen ja jatkuvan parantamisen tärkeydestä.
- varmistaa, että hyvinvointialueella on toimiva tietoturva- ja tietosuojariskien arviointiprosessi, jolla tunnistetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden menettämiseen liittyvät riskit ja riskeillä on nimetyt omistajat.
- päättää hyväksyttävästä riskitasosta.
- raportoi tietoturvallisuudesta osana sisäistä valvontaa.
- tekee sisäisiä auditointeja suunnitelluin aikavälein tietoturvallisuuden hallintajärjestelmän osalta.
- katselmoi tietoturvallisuuden ja tietosuojan hallintajärjestelmän suunnitelluin aikavälein varmistaakseen, että se on edelleen soveltuva, asianmukainen ja vaikuttava.
- ryhtyy toimenpiteisiin väärinkäytöstapauksissa.
- määrittää millainen pätevyys hyvinvointialueella eri rooleissa työskentelevillä tai sen lukuun toimivilla henkilöillä täytyy olla tietoturvan ja tietosuojan suhteen.

2.2 Johtajaylilääkäri

- vastaa potilasrekisteristä ja arkistotoimesta sekä myöntää rekisteritiedon käyttöluvat.

2.3 Biopankin johtaja

- vastaa rekisterien ja tietokantojen ylläpitämisestä, yhdistämisestä ja suojaamisesta
- vastaa yksityisyyden suojan varmistamisesta näytteitä ja niihin liittyviä tietoja käsiteltäessä.

2.4 Johtavat viranhaltijat

Perusterveydenhuollon yksikön ylilääkäri, talousjohtaja, viestintäjohtaja, kiinteistöjohtaja, hallintopäällikkö, ylilääkärit, palvelukeskusjohtaja, osaamiskeskusjohtaja ja muut voimassa olevan toimintaohjeen mukaiset johtavat viranhaltijat.

- toimivat tietojärjestelmien omistajina sovittujen järjestelmien osalta.

2.5 Henkilöstöjohtaja

- omistaa HR-järjestelmät.
- vastaa käyttöoikeusprosessien määrittelystä.
- omistaa käyttövaltuushallinnan järjestelmät.

2.6 Tietohallintojohtaja

Tietohallintojohtaja vastaa tietoturvasta yleisesti, niiltä osin mitä tässä dokumentissa ei ole todettu kuuluvan muiden tahojen vastuulle.

- raportoi tietoturvallisuudesta kuntayhtymän johtoryhmälle (Kujo), kuntayhtymän hallitukselle ja valtuustolle.
- vastaa tietoturvaan liittyvien hankkeiden budjetoinnista, ohjauksesta, valvonnasta ja tuloksellisuudesta.
- vahvistaa tietoturvallisuuteen liittyvät ohjeet.
- vastaa ICT-infrastruktuurin tietoturvallisuudesta ja niiden tietojärjestelmien tietoturvallisuudesta, joiden omistajana toimii.
- osallistuu kansallisen tason yhteistyöhön tietoturvassa.
- tekee toimivaltansa puitteissa päätökset tietoturvapoikkeamatilanteissa.
- vastaa tietoturvaan liittyvästä viestintäsuunnitelmasta ja viestinnästä.
- vastaa, että asiaankuuluviin viranomaisiin ylläpidetään tarkoituksenmukaisia yhteyksiä.
- toimii tiedonhallintaryhmän puheenjohtajana.
- vastaa ICMT-puitesopimuksen ja muiden merkittävien ICMT-sopimusten osalta, että tietoturvallisuus on asianmukaisesti huomioitu ja valvoo toteutumista.
- toimii tietoturvapäällikön esimiehenä ja tekee virkavastuulla tehtävät päätökset tietoturvaan liittyen.

2.7 Tietoturvapäällikkö

- vastaa tietoturvan operatiivisesta johtamisesta hyvinvointialueella.
- vastaa tietoturvaan liittyvien ohjeiden, politiikkojen ja linjausten valmistelusta ja ylläpitämisestä yhteistyössä sidosryhmien kanssa.
- vastaa tietoturvan hallintamallin kehittämisestä ja ylläpidosta.
- vastaa tietoturvariskien hallinnan kehittämisestä ja ylläpidosta.
- suorittaa kehittämistä kansallisessa ja kansainvälisessä yhteistyössä.
- valmistelee tietoturvallisuuteen liittyviä kehittämishankkeita ja budjetointia yhdessä muiden sidosryhmien kanssa.
- ohjeistaa yleiset tietoturvallisuusasiat ja huolehtii, että niistä tiedotetaan ja koulutetaan.
- vastaa tietoturvapoikkeamien seurannasta ja tilastoinnista.
- tiedottaa tietoturvallisuusasioista ja –ongelmista.

- valmistelee tietoturvaan liittyvän viestinnän koko organisaation, sidosryhmien ja erityisesti esimiesten kanssa.
- osallistuu hyvinvointialueen turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tietosuoja ja tietoturvaryhmän jäsenenä, operatiivisen tietoturva- ja tietosuojaryhmän puheenjohtajana.
- osallistuu hyvinvointialueen riskienhallintatyöryhmän toimintaan jäsenenä.
- tiedottaa tietoturvallisuusasioista ja – ongelmista.
- raportoi tietoturvallisuudesta tietohallintojohtajalle ja tietosuoja- ja tietoturvaryhmälle
- vastaa tietoturvaprosessien ja hallintakeinojen osalta seuranta-, mittaus-, analysointi- tai arviointimenetelmien suunnittelusta.
- toimii tietoturvallisuuden asiantuntijana hyvinvointialueen toiminta-alueella, tarvittaessa hankkii lisää asiantuntijapalveluita.
- valvoo, osaltaan että tietoturvallisuusasiat on organisoitu hyvinvointialueen toimipaikoissa ja yksiköissä
- avustaa tietoturvallisuus- ja tietosuojaliitteiden valmistelussa sopimuksiin.
- valvoo, että tietoturva toteutuu hankinnoissa ja projekteissa osana operatiivisen tietoturvaryhmän toimintaa.
- huolehtii, että osaamisyhteisöihin tai muihin turvallisuusasiantuntijaryhmiin ja ammatillisiin järjestöihin ylläpidettään tarkoituksenmukaisia yhteyksiä.

2.8 Tietosuojavastaava

- antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat niiden Tietosuoja-asetuksen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten mukaisia velvollisuuksia.
- seuraa, että noudatetaan Tietosuoja-asetusta, muita unionin tai jäsenvaltion tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset.
- antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta Tietosuoja-asetuksen 35 artiklan mukaisesti.
- tekee yhteistyötä valvontaviranomaisen kanssa;
- toimii valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien tietosuoja-asetuksen 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

Tietosuojavastaava on nimetty Kuntayhtymän johtoryhmässä:

- tietosuoja- ja tietoturvaryhmän puheenjohtajaksi.
- Pohjois-Savon hyvinvointialueen tutkimuseettisen toimikunnan pysyväksi asiantuntijaksi.

Tietosuojavastaava toimii lisäksi:

- Pohjois-Savon alueellisessa tietosuojatyöryhmässä puheenjohtajana.
- Itä-Suomen Biopankin ohjausryhmän asiantuntijana ja kommentoi tutkimusten tietosuojaa.

2.9 Kehittämispäällikkö (tietohallinto)

- vastaa hyvinvointialueen yleisen ICT-infrastruktuurin (tietoverkot, toimialueet, päätelaitteet, konesaliratkaisut) tietoturvallisuuden kehittämisestä ja siihen liittyvästä budjetoinnista.
- valvoo, että tietosuoja- ja tietoturva toteutuu hankinnoissa ja projekteissa osana operatiivisen tietoturvaryhmän toimintaa.
- osallistuu hyvinvointialueen turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin operatiivisen tietoturva- ja tietosuojaryhmän jäsenenä.
- vastaa tietovälineiden käsittelyn ohjeistuksesta.
- vastaa keskitetyn pääsynhallinnan (IDM) periaatteista ja toteutuksesta.

2.10 Hankinnasta vastaava ja projektipäällikkö (hankinnat ja projektit)

Tässä luvussa kuvatut vastuut perustuvat Tietoturvan- ja tietosuojan arvioprosessi -ohjeessa kuvattuihin tehtäviin.

- vie päätöksiä ja linjauksia vaativat asiat operatiivisen tietoturva- ja tietosuojaryhmän käsittelyyn ja omistajan päätöksentekoon kuvatun prosessin mukaisesti.
- varmistaa, että hankinta tai projekti dokumentoidaan ohjeistuksen mukaan asianhallintajärjestelmään omalle asialleen.
- varmistaa, että hankinnan tai projektin kohde kuvataan.
- varmistaa, että hankinnalle tai projektilla on tietoturva- ja tietosuojavaatimukset.
- varmistaa, että tietoturva ja tietosuojavaatimukset toteutetaan projektissa tai hankinnassa.
- varmistaa, että riskiarvio tehdään ja tallennetaan riskienhallinnan järjestelmään.
- varmistaa, että mahdollisiin sopimuksiin tulee mukaan tietosuoja ja tietoturvaehdot -liite ja käsittelytoimien kuvaus (tarvittaessa).
- varmistaa, että käsittelytoimien kuvaus tehdään ja tallennetaan asianmukaisesti (tarvittaessa).
- tietosuojavaikutusten arviointi tehdään ja tallennetaan asianmukaisesti (tarvittaessa).
- varmistaa, että tietosuojaseloste tehdään (tarvittaessa).
- varmistaa, että uhkamallinnus tilataan palveluntoimittajalta, uhkamallinnusdokumentit tallennetaan asianhallintajärjestelmään ja järjestää uhkamallinnustyöpajan palveluntoimittajan kanssa (tarvittaessa).
- varmistaa, että tietojärjestelmäsalkku päivitetään (tarvittaessa).
- varmistaa, että omavalvontasuunnitelma päivitetään (tarvittaessa).
- tilaa tarvittaessa teknisen tietoturvatarkastuksen palveluntoimittajalta ja tallentaa syntyneen raportin asianmukaisesti (tarvittaessa).

- varmistaa, että A ja B-luokan tietojärjestelmistä on valmistajan antamat ohjeet niiden käyttöön liittyen, kuten myös CE-merkityistä lääkintälaitteista. Nämä ohjeet ovat talletettava osaksi dokumentaatiota ja saatettava käyttäjien saataville.
- varmistaa, että A tai B luokan järjestelmä löytyy Valviralle ilmoitettujen tietojärjestelmien rekisteristä (ilman tätä järjestelmää ei voida ottaa käyttöön).
- huolehtii, että sovitut (tietoturva- ja tietosuoja) kontrollit ja muut asiat otetaan käyttöön.

2.11 Tietohallintopäällikkö

- toimii tiedonhallintaryhmän puheenjohtajana.
  - toimii konfiguraationhallintatietokannan ja tietojärjestelmäsalkun omistajana. Huolehtii, että nämä toimivat myös suojattavan omaisuuden luettelona, jossa määritellään mm. kriittisyys.

2.12 Palvelussuhdepäällikkö

- varmistaa, että hyvinvointialueen henkilökunta, opiskelijat, toimittajat, luottamushenkilöt ja muut sidosryhmät ymmärtävät velvollisuutensa ja ovat sopivia heille harkittuihin tehtäviin.
- huolehtii, että työntekijöiden ja vuokratyöntekijöiden kanssa tehdyissä sopimuksissa on eriteltävä työntekijän tai vuokratyöntekijän vastuut tietoturvallisuudesta.
- ilmaisee sopimuksissa tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättymisen tai muuttumisen jälkeen.

2.13 Turvallisuuspäällikkö

- vastaa työntekijöiden turvallisuusselvityksistä sovituissa tehtävissä.
- vastaa turvallisuusselvitykset ja tarkastukset ovat oikeassa suhteessa toiminnallisiin vaatimuksiin, käsiteltävän tiedon luokitukseen ja oletettuihin riskeihin.
- vastaa fyysisestä turvallisuudesta.

2.14 Tietosuoja ja tietoturvaryhmä

- arvioi omalta osaltaan tietosuojan ja tietoturvan toteutumista ja tunnistaa siihen liittyviä riskejä.
- tarjoaa laaja-alaista asiantuntemusta tietosuojan ja tietoturvan toteuttamiseen liittyviin ajankohtaisiin aiheisiin.
- edistää tietosuojakäytänteiden rakentamista ja toteuttamista sekä rekisteröityjen oikeuksien turvaamista.

2.15 Operatiivinen tietoturva- ja tietosuojaryhmä

- toimii tietoturvan- ja tietosuojan hallintamalleja kehittävänä, toimeenpanevana ja valvovana ryhmänä.

- edistää omalta osaltaan tietoturvallisuuden hallintamallin suunnittelua ja jatkuvaa operointia (soveltaen ISO 27001 standardia, tiedonhallintalautakunnan suosituksia ja muita alan parhaita käytänteitä, sekä regulaatiota).
- valmistelee esityksiä tietoturvan sekä tietosuojan politiikoiksi, periaatteiksi ja linjauksiksi, sekä niiden ajan tasalla pitämiseksi.
- valmistelee ja ylläpitää tietoturva- ja tietosuojavaatimukset.
- tunnistaa puuttuvia ja puutteellisia ohjeita, raportoi niistä omistajille, tekee esityksiä ohjeista ja osallistuu niiden laatimiseen.
- tekee poikkeamapäätökset hyvinvointialueen tietoturva- ja tietosuojavaatimuksista. Päätöksissä huomioiden asianmukaisen riskitason (ottaen huomioon kompensoivat tietoturvakontrollit).
- auttaa tunnistamaan ja hallitsemaan tietoturvaan ja tietosuojaan liittyviä riskejä asianmukaisesti.
- seuraa teknisen tietoturvan tilannetta, kuten IPS/IDS, haittaohjelmat, päivitysten asennusten tilanne, palvelunestohyökkäykset, haavoittuvuudet ja muut poikkeamat.
- kehittää tietoturvaan liittyvää raportointia yhdessä Istekin kanssa.
- ryhmä yhdistää mm. Istekki, KTK, SOTE-ISAC luomat tietoturvan tilannekuvat hyvinvointialueen tilannekuvaksi ja analysoi riskitasoa hyvinvointialueen toiminnalle sekä ydintavoitteille.
- ryhmä raportoi korkeat riskit välittömästi tietohallintojohtajalle, johtajaylilääkärille ja/tai kyseisen rekisterin omistajalle. Matalammat riskit raportoidaan osana muuta raportointia.
- ryhmässä tehdään tietoturva-arvioissa tunnistettujen riskien analysointi ja niiden merkityksen arviointi ja niiden merkityksen arviointi hyvinvointialueen toiminalle ja ydintavoitteille.
- tietoturva-arvioiden löydöksien perusteella antaa suositeltavat riskienhallintatoimet (järjestelmien, tietojen, prosessien tai projektien omistajille).
- ryhmä arvioi Istekin ja muiden toimittamien tietoturva-arvioiden ja tietoturvapalveluiden laatua.
- ryhmä arvioi tapahtuneiden henkilötietojen tietoturvaloukkausten perusteella tarvittavia toimenpiteitä ja antaa näistä suosituksia.

2.16 Arkistopäällikkö

Arkistopäällikön johdolla toimivan arkistotoimen tehtävänä on varmistaa asiakirjojen käytettävyys ja säilyminen, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää tarpeeton aineisto. Arkistotoimen vaatimukset on otettava huomioon arkistonmuodostajan tieto- ja asiakirjahallinnossa, siksi asiakirja- ja tietohallinnon suunnittelu ja toteutus tapahtuvat arkistotoimen ja tietohallintoyksikön yhteistyönä.

- johtaa kuntayhtymän arkistotointa ja arkistonmuodostusta.
- vastaa kuntayhtymän pysyvästi säilytettävistä asiakirjoista.
- vastaa kuntayhtymän arkistotoimen suunnittelusta, ohjauksesta ja valvonnasta.

- laatii ja ylläpitää kuntayhtymän arkistonmuodostussuunnitelman.
- suunnittelee ja toteuttaa asiakirja- ja tiedonhallinnan yhdessä tietohallinnon kanssa.
- osallistuu organisaation tietoturvaan ja -suojaan liittyvien asioiden suunnitteluun ja kehittämiseen sekä ohjeiden laatimiseen ja ylläpitoon.
- osallistuu hyvinvointialueen turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tietoturva –tietosuoja -työryhmän jäsenenä.
- on tarvittaessa yhteydessä valvontaviranomaisiin.

2.17 Yksiköiden esimiehet

- vastaavat yksiköidensä tietoturvallisuudesta ja tietosuojasta.
- huolehtivat, että kaikki työntekijät toimivat tietoturvallisesti hyvinvointialueen olemassa olevien politiikkojen, periaatteiden ja ohjeiden mukaisesti esimerkiksi suorittamalla säännöllisiä katselmointeja.
- seuraavat tietoturvan ja tietosuojan osaamista sekä koulutusten suorittamista.
- vastaavat, että henkilöstö tuntee tietoturvallisuuden ja tietosuojan perusasiat, kuten tietoturvapolitiikan ja tämän vastuudokumentin.
- tukevat tietoturvan ja tietosuojan jatkuvaa ylläpitämistä ja kehittämistä.
- toteuttavat ja organisoivat tietoturva- ja tietosuojaorganisaation määrittelemät tietoturvallisuus ja tietosuojatoimenpiteet yksikössään.
- suunnittelevat, budjetoivat ja organisoivat yksikkönsä tietoturvallisuustoimenpiteet.
- huolehtivat, että keskeisille järjestelmille on nimetty omistajat ja vastuuhenkilöt yhteistyössä tietohallinnon kanssa.
- hoitavat yksikkönsä yleiset tietoturvallisuus- ja tietosuoja-asiat.
- raportoivat tietoturvallisuusongelmista ja tietosuojarikkomuksista sekä yksikkönsä. johdolle, että tietosuojavastaavalle hyvinvointialueen ohjeistuksen mukaisesti.

2.18 Jokainen työntekijä

Jokainen työntekijä vastaa omalta osaltaan tietoturvallisuuden ja tietosuojan toteutumisesta voimassa olevan lainsäädännön ja tietoturvallisuudesta ja tietosuojasta annettujen politiikkojen, periaatteiden ja ohjeiden mukaisesti. Jokaisen työntekijän on oltava tietoinen tietoturva- ja tietosuojapolitiikasta, periaatteista ja ohjeista.

Jokaisen työntekijän tulee raportoida heti havaitsemistaan tahattomista tai tahallisista tietoturva- ja tietosuojapoikkeamista ja/tai henkilötietojen tietoturvaloukkauksista turvallisuudesta linjavastuussa olevalle esimiehelle. Lisäksi tulee ilmoittaa erillisen ohjeistuksen mukaan. Mikäli kyse on parhaillaan meneillään olevasta tilanteesta, kuten haittaohjelma tai tunnusten luovuttaminen tietojen kalastelun seurauksena, tulee olla välittömästi yhteydessä Istekki Oy:n asiakaspalveluun (mihin vuorokaudenaikaan tahansa).

Hyvinvointialueella käytetään vaaratapahtumien raportointijärjestelmänä HaiPro-järjestelmää. Vaaratapahtumalla tarkoitetaan potilaan turvallisuuden vaarantavaa tapahtumaa, joka aiheuttaa tai voi aiheuttaa haittaa potilaalle. Ilmoitus tehdään nimettömänä, ja ilmoituksen tekee se, joka havaitsee vaaratapahtuman. HaiPro-järjestelmään ilmoitetaan kaikki haittatapahtumat sekä läheltä piti –tapahtumat. Tämä koskee myös tietoturvaan ja tietosuojaan liittyvää vaaratapahtumaa, joka aiheuttaa tai voi aiheuttaa haittaa potilaalle.

Jokainen työntekijä voi ilmoittaa havaitsemistaan mahdollisista tietoturvapuutteista tai kehittämiskohteista tietoturvapäällikölle ja vastaavasti tietosuoja-asioissa tietosuojavastaavalle.

Ylemmän tason vastuiden lisäksi jokaisella käyttäjällä ja työntekijällä on vastuu omasta toiminnastaan. Henkilötietoja ja muuta salassa pidettävää tietoa on käsiteltävä huolellisesti ja lainsäädännön sekä hyvinvointialueen tai muiden viranomaisten antamien ohjeiden mukaisesti.

Tietoturvarikkomukset ja henkilötietojen tietoturvaloukkaukset käsitellään tapauskohtaisesti. Joissakin tapauksissa tahallinen tai törkeän huolimaton toiminta voi johtaa työoikeudellisiin seurauksiin (huomautus, varoitus, työ- tai virkasuhteen päättäminen) ja tapaus-kohtaisesti rikosoikeudellisiin toimenpiteisiin.

2.19 Prosessien, tietoaineistojen, tietovarantojen, tietojärjestelmien, laitteistojen ja palveluiden omistajat

Kaikille prosesseille, tietoaineistoille, tietovarannoille, tietojärjestelmille ja laitteistoille, sekä hyvinvointialueen omille ja ulkoistetuille palveluille on määritelty omistajat sekä vastuuhenkilöt. Nämä omistajat ja vastuuhenkilöt kirjataan ja ylläpidetään tietojärjestelmien osalta tietojärjestelmäsalkussa. Tietojärjestelmäsalkkuun merkitään myös tietojärjestelmän kriittisyystaso.

Prosessin, henkilötietorekisterin, tietojärjestelmän omistaja vastaa:

- tietoturvallisuudesta ja tietosuojasta koko elinkaaren ajan voimassa olevan lainsäädännön ja Pohjois-Savon hyvinvointialueen tietoturva- ja tietosuojapolitiikkojen, periaatteiden ja ohjeiden mukaisesti.
- tietojärjestelmään sisältyvien rekisterien oikeellisuudesta ja lainmukaisuudesta, kuten henkilörekisterilaissa mainitun rekisterinpitäjän velvollisuuksista.
- lokienhallinnasta lainsäädännön mukaisesti.
- että hankinta/palvelusopimuksissa on mukana asianmukaiset tietoturva ja tietosuojavaatimukset sekä liitteet. Omistaja valvoo näiden toteutumista.
- tietojärjestelmäsalkun tietojen oikeellisuudesta ja päivittämisestä.
- riskit arvioidaan mahdollisissa muutostilanteissa ja määräajoin.
- tietojärjestelmän ohjeet ovat saatavilla ja ajantasaiset.

Tietoturvallisuuden ja tietosuojan varmistamiseksi hankinnoissa ja projekteissa hyvinvointialueella toteutetaan ICMT-hankintojen ja projektien osalta tietoturvan ja tietosuojan-arvioprosessi. Tämä prosessi on kuvattu erillisessä ohjeessa. Prosessissa varmistetaan tietoturvallisuus ja tietosuoja riskiarvioiden ym. menettelyjen avulla. Tähän tietoturva ja tietosuoja-arvioprosessiin liittyen omistaja vastaa mm:

- hankintaan tai projektiin liittyvien päätösten tekemisestä.
- riskihallinnasta ja riskien sekä hallintakeinojen seurannasta ja päivittämisestä.

Tulee huomioida, että tietoturvallisuuden ja tietosuojan varmistaminen on jatkuva prosessi, jota tulee hankinnan ja käyttöönoton lisäksi tehdä koko elinkaaren ajan. On myös mahdollista, että hankinnalla tai projektilla on eri omistaja, kuin jatkossa projektin lopputuloksella (esimerkiksi tietojärjestelmä). Näiden välille tulee varmistaa sujuva vastuiden siirto.

Hyvinvointialueelle on laadittu jatkuvuussuunnitelma/ toipumissuunnitelma toiminnan jatkuvuuden turvaamiseksi normaaliolosuhteiden poikkeustilanteiden sekä eriasteisten poikkeusolojen varalle. Lisäksi kunkin kriittisen tietojärjestelmän omistaja on velvollinen laatimaan ja ylläpitämään varajärjestelmäsuunnitelmaa.

3 Tiedonhallintalain mukaiset tehtävät

Laki julkisen hallinnon tiedonhallinnasta 906/2019 (tiedonhallintalaki) mukaisista tehtävistä tietoturvaan liittyen ovat jaettu seuraavasti. Tässä luvussa ei kuvata muita tiedonhallintalain mukaisia tehtäviä, kuin tietoturvaan liittyvät ja hyvinvointialueen toimintaan soveltuvat.

3.1 Tietoturvapäällikkö:

2 § mukainen määrittely; tässä ja muussa laissa säädettyjen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuiden kuvaaminen. (tämä dokumentti toteuttaa tämän).

4 § mukainen tietoturvallisuustoimenpiteiden kuvaaminen.

4 § mukaisesti ajantasaiset ohjeet tietoturvallisuustoimenpiteistä.

13 § mukainen toimintaympäristön tietoturvallisuuden tilan seuranta.

13 § mukainen tietojenkäsittelyyn kohdistuvien riskienhallinnan ja tietoturvallisuustoimenpiteiden mitoituksen malli eli tietoturva- ja tietosuojariskienhallinnan periaatteet.

3.2 Turvallisuuspäällikkö:

12 § mukaisesti tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta.

Lisäksi 4 § mukaisesta poikkeusoloihin varautumisesta.

3.3 Prosessien, tietoaineistojen, tietovarantojen, tietojärjestelmien, laitteistojen ja palveluiden omistajat sekä vastuuhenkilöt:

13 § mukaisesti on varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

13 § mukaisesti on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti omistamansa prosessien, tietoaineistojen, tietovarantojen, tietojärjestelmien, laitteistojen ja palveluiden osalta.

14 § mukaisesti on varmistettava tietojensiirron salaaminen yleisessä tietoverkossa, jos siirrettävät tiedot ovat salassa pidettäviä.

15 § mukaisesti on toteuttava seuraavat tietoturvallisuustoimenpiteet omistamansa prosessien, tietoaineistojen, tietovarantojen, tietojärjestelmien, laitteistojen ja palveluiden osalta:
1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;
2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;
3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;
4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;
5) tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;
6) tietoaineistot voidaan tarvittavilta osin arkistoida.

16 § mukaisesti on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina.

17 § mukaisesti on huolehdittava, että tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

3.4 Tietohallintojohtaja:

17 § mukaan viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

Tietohallintojohtaja on keskitetyn lokienhallinnan ja lokienhallinnan arkkitehtuurin omistaja.

4 Henkilörekisterien vastuut

4.1 Johdanto

Tässä osassa määritellään rekisterihallinnon ja henkilötietorekisterien vastuut ja menettelytavat. Rekisterihallinnolla tarkoitetaan EU:n yleisessä tietosuoja-asetuksessa rekisterinpitäjälle ja henkilötietojen käsittelijälle säädettyjen tehtävien ja vastuiden määrittämistä sekä rekistereitä koskevien päätöksentekovaltuuksien määrittämistä Pohjois-Savon hyvinvointialueella. Henkilörekisterillä tarkoitetaan samaan käyttötarkoitukseen varten kerättyjä/samassa käyttötarkoituksessa käsiteltäviä henkilötietoja. Ohjeen kohderyhmänä ovat erityisesti johtavat viranhaltijat, henkilörekistereiden vastuuhenkilöt ja rekisteriasioita hoitavat henkilöt.

4.2 Rekisterihallinnon vastuut ja tehtävät

4.3 Henkilörekisterit ja niiden vastuutahot

Pohjois-Savon hyvinvointialueen kuntayhtymällä on
seuraavat keskeiset koko hyvinvointialueen kattavat henkilörekisterit ja niiden vastuutahot:

Rekisteri	Vastuuhenkilö
Asiakaspalauterekisteri	Toimialajohtaja, palvelut ja asiakkuudet
Itä-Suomen biopankki	Biopankin johtaja
Hallinnollisten potilasasioiden rekisteri	Johtajaylilääkäri
Hallintoasioiden rekisteri	Hallintojohtaja
Henkilöstö- ja palkkahallinnon rekisteri (sis. työajan seurannan)	Henkilöstöjohtaja
Henkilöstö- ja palkkahallinnon rekisterin lokirekisteri	Henkilöstöjohtaja

Rekrytointirekisteri	Henkilöstöjohtaja
Tietoallas	Johtajaylilääkäri
Luottamushenkilörekisteri	Hallintojohtaja
Potilasasiamiesten asiakasrekisteri	Johtajaylilääkäri
Potilasrekisteri	Johtajaylilääkäri
Potilasrekisterin lokirekisteri	Johtajaylilääkäri
Tartuntatautirekisteri	Tartuntataudeista vastaava ylilääkäri
Sidonnaisuusrekisteri	Reviisori
Taloushallinnon henkilörekisterit	Talousjohtaja
Tieteellisen tutkimustoiminnan rekisterit	Tutkimus- ja innovaatiojohtaja
Viestintäjärjestelmien rekisteri (intranet, internet)	Viestintäjohtaja
Kameravalvonnan rekisteri (pois lukien hoidolliset potilasvalvontakamerat)	Turvallisuuspäällikkö
Kulunvalvontarekisteri	Kiinteistönpitopäällikkö
Valmiustoiminnan henkilörekisteri	Turvallisuuspäällikkö

4.4 Henkilörekisterin vastuuhenkilön tehtävät

Kohdassa 2.1 mainituilla vastuuhenkilöillä on seuraavat Tietosuoja-asetuksessa säädetyt velvoitteet:

Dokumentointivelvoite	Henkilörekisteristä on ylläpidettävä kirjallista 30 artiklan mukaista selostetta käsittelytoimista.
Informointivelvoite	Henkilörekisteristä on laadittava kirjallinen 12 artiklan mukainen informointi, joka on oltava esim. potilaiden, henkilökunnan ja muiden rekisteröityjen saatavilla esim. intranetissä ja internet-sivulla. Informoinnissa tulee kertoa, miten rekisteröity voi käyttää asetuksessa olevia oikeuksiaan kuten esim. tehdä tarkastuspyynnön.
Rekisterin yhteyshenkilö	Vastuuhenkilö nimeää henkilörekisterin yhteyshenkilön, jonka tehtävät ovat seuraavat:

	valmistelee rekisterin informoinnin vastuuhenkilölle ja huolehtii siitä, että informointi pysyy ajan tasalla, toimii rekisterin yhteyshenkilönä silloin, kun rekisteröity haluaa käyttää oikeuksiaan, toimii käytännön yhteyshenkilönä, kun tietosuojavastaava tai valvontaviranomainen pyytää selvityksiä tai tietoja valmistelee tietosuoja-asetuksen 24 artiklan mukaisen riskien ja vaikutusten arvioinnin
Rekisteröidyn oikeuksien toteuttaminen	Vastuuhenkilö huolehtii siitä, että rekisteröidyillä on mahdollisuus käyttää tietosuoja-asetuksessa säädettyjä oikeuksiaan kuten esimerkiksi • oikeus saada pääsy tietoihin tai • mahdollisuus oikaista virheelliset tiedot tai • poistaa rekisterin käyttötarkoituksen kannalta turhat tiedot Vastuuhenkilö käsittelee ja tekee päätökset seuraavista rekisteröidyn vaatimuksista - oikeus vastustaa henkilötietojen käsittelyä - oikeus rajoittaa henkilötietojen käsittelyä - oikeus tulla unohdetuksi
Käsittelyn riskien arvioiminen ja tietosuojaa koskeva vaikutustenarviointi sekä ennakkokuuleminen	Henkilörekisteristä on laadittava kirjallinen tietosuoja-asetuksen 24 artiklan mukainen riskiarvio: Mikäli riskiarvio osoittaa, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuu todennäköisesti korkea riski, tulee laatia artiklan 35 mukainen tietosuojaa koskeva vaikutustenarviointi. Mikäli vaikutustenarviointi osoittaa, että riskejä ei saada omin toimin laskettua on toteutettava 36 artiklan mukainen ennakkokuuleminen. Riskiarvio/ vaikutustenarviointi tarkastetaan säännöllisesti ja aina silloin, kun henkilörekisteriin kohdistuu merkittäviä muutoksia (esim. järjestelmän tai ohjelmiston versiopäivitykset,

	käyttöoikeuksien olennainen 4 laajentaminen, uusien ominaisuuksien tai teknologioiden käyttöönotto).
Rekisterin käyttöoikeuksien määrittäminen	Vastuuhenkilö hyväksyy vastuullaan olevan henkilörekisterin käyttöoikeuksien yleisperiaatteet.
Hyvinvointialueen oikeuksien turvaaminen sopimuksissa	Henkilörekistereitä koskevissa sopimuksissa on määritettävä tietosuoja-asetuksen mukaiset vastuut. Henkilötietojen käsittelijän kanssa on aina tehtävä sopimus henkilötietojen käsittelystä ja sen ehdoista. Tässä on hyödynnettävä aina kun mahdollista hyvinvointialueen mallisopimuksia. Jos henkilötietoja käsitellään ETA-alueen ulkopuolella, tulee varmistaa laillinen siirtomekanismi tarvittavine lisätoimineen.

4.5 Henkilörekistereitä koskevat erityistehtävät

4.5.1 Hyvinvointialueen johtaja

- antaa rekisterinpitoa ja käyttövaltuushallintaa koskevat yleisohjeet ja määrittää henkilörekistereitä koskevat vastuut.

4.5.2 Johtajaylilääkäri

- antaa kirjalliset ohjeet potilasasiakirjojen laatimisesta ja tietoturvallisesta käsittelystä
- määrittää potilastietoja koskevat yleiset käyttövaltuushallinnan periaatteet
- huolehtii siitä, että potilasrekisterin informointi on julkaistu internetsivulla ja intranetissä
- toimii potilasrekisterin kokonaisuuden vastuuhenkilönä (mukaan lukien kaikki hoidolliset potilastietojärjestelmät ja rekisterit).
- käsittelee potilastietojen osalta useita hyvinvointialueen tulosyksiköitä tai tulosalueita koskevat tietosuojaa koskevat hallintoasiat sekä useita tulosyksiköitä tai tulosalueita koskevat virheiden oikaisuvaatimukset tai tietojen poistovaatimukset valvontaviranomaisilta saapuvat tietosuojaa koskevat hallintoasiat.

4.5.3 Henkilöstöjohtaja

- toimii kaikkien henkilöstöhallintoa palvelevien henkilörekistereiden vastuuhenkilönä
- nimeää henkilöstöhallinnon rekisteriasioita hoitavat henkilöt.
- antaa henkilöstöasioita koskevien tietojen kirjaamista ja käsittelyä koskevat yleisohjeet.
- vahvistaa henkilöstöä koskevien rekistereiden käyttöoikeuksien myöntämisen periaatteet tietoturvapolitiikan ja käyttövaltuushallinnan ohjeistusten mukaisesti.

4.5.4 Hallintojohtaja (hallintopäällikkö)

- toimii kaikkien hallintotoiminnan henkilörekistereiden vastuuhenkilönä (mm. luottamushenkilörekisteri, asiankäsittelyjärjestelmä).
- nimeää yleishallinnon rekisteriasioita hoitavan henkilön antaa hallintoasioita koskevien tietojen kirjaamista ja käsittelyä koskevat yleisohjeet (asiakirjahallinnon ja päätöksenteon ohjeet).
- vahvistaa yleishallinnon rekistereiden käyttöoikeuksien myöntämisen periaatteet.

4.5.5 Palvelukeskusjohtaja

- on tulosyksikkönsä tai tulosalueensa henkilörekistereiden vastuuhenkilö (esim. erikoisalakohtaiset laaturekisterit).
- vahvistaa oman yksikkönsä potilashoitoon liittyvien henkilörekistereiden käyttöoikeuksien myöntämisperiaatteet noudattaen yleisiä tietoturva- ja tietosuojapolitiikan ja johtajaylilääkärin vahvistamia käyttöoikeuslinjauksia.

4.5.6 Tartuntataudeista vastaava ylilääkäri

- vastaa potilasrekisterin osana tartuntatautilain (2227/2016, 36–38 §) velvoittamista rekistereistä. Tunnistetietoja säilytetään vain niin kauan kuin se on käyttötarkoituksen vuoksi välttämätöntä ja tapauskohtaiset rekisterit hävitetään heti kun ne eivät ole tartunnan torjunnan kannalta välttämättömiä.

4.5.7 Tutkimus- ja innovaatiojohtaja ja tutkimuksista vastaavat henkilöt

- vastaa tutkimusta ja opetusta koskevista hyvinvointialueen laajuisista henkilörekistereistä kuten esimerkiksi tieteellisten tutkimusprojektien hallintajärjestelmästä (eTutkija tai vastaava). Tutkimuksissa tulee nimetä johtava tutkija , joka huolehtii tutkimustoiminnan ohjeistuksen mukaisesti tutkimuksessa tapahtuvan henkilötietojen käsittelyn dokumentoinnista, riskiarviosta ja rekisteröityjen informoinnista. Tutkijalähtöisissä tutkimuksissa rekisterinpitäjyys arvioidaan tapauskohtaisesti. Ennen tutkimuslupapäätöksen hyväksymistä tutkimusluvan myöntävä viranhaltija varmistaa, että tutkimusrekisteristä on tehty asianmukainen seloste ja riskien arviointi.

4.5.8 Biopankin johtaja

- nimeää rekisteriasioita hoitavan henkilön.
- vastaa siitä, että suostumus-, koodi- sekä näyte- ja tietorekistereistä laaditaan informoinnit ja ne julkaistaan Biopankin internet-sivulla.
- vastaa siitä, että tietojen luovutukset tapahtuvat lainsäädännön mukaisesti.

4.5.9 Tietohallintojohtaja

- huolehtii siitä, että hyvinvointialueen tietohallinnon ylläpitämät henkilötietoja sisältävät tietojärjestelmät ja palvelut toteutetaan tietoturvallisesti.
- toimii AD-käyttäjähakemiston (Active Directory) vastuuhenkilönä.

4.5.10 Tietosuojavastaava

- antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat EU tietosuoja asetuksen ja muiden tietosuojasäännösten mukaisia velvollisuuksia.
- seuraa tietosuoja-asetuksen noudattamista ja raportoi poikkeamista rekistereiden vastuutahoille.
- antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta 35 artiklan mukaisesti.
- tekee yhteistyötä valvontaviranomaisen kanssa; toimii valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

4.6 Sovelletut säädökset

- Euroopan unionin yleinen tietosuoja-asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.
- Tietosuojalaki 2018/1050.