Österbottens välfärdsområde
Pohjanmaan hyvinvointialue

Tietoturvapolitiikka

Pohjanmaan hyvinvointialue

Aluehallitus 16.1.2023 § xx

Voimaantulo 1.1.2023

Sisällysluettelo

Pohjanmaan hyvinvointialueen tietoturvapolitiikka

1. Johdanto

Pohjanmaan hyvinvointialueen palveluiden perustana on asiakkaiden tarpeet, palveluiden tuottaminen perustuu tietoon sekä sen käsittelyyn Pohjanmaan hyvinvointialueen toimintaympäristössä. Hyvinvointialueen palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

Pohjanmaan hyvinvointialueen strategian ja tavoitteiden saavuttaminen edellyttää laajaa digitalisaatiota sekä tietoturvallisuuden kaikkien osa-alueiden, kokonaisarkkitehtuurin ja yhteentoimivuuden laajaa huomioimista jo suunnitteluvaiheessa sekä jatkuvasti.

Tässä tietoturvapolitiikassa määritellään Pohjanmaan hyvinvointialueen johtamista, palveluita ja toimintoja koskevat tietoturvallisuuden periaatteet, tavoitteet, vastuut ja toteuttamistavat. Tietoturvapolitiikka toimii perustana tietoturvallisuutta koskeville muille ohjeistuksille, joiden tehtävänä on tarkentaa tietoturvapolitiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietoturvapolitiikka koskee koko hyvinvointialueen organisaatiota, sen työntekijöitä ja luottamushenkilöitä, sekä niitä Pohjanmaan hyvinvointialueen sidosryhmien edustajia, jotka työnsä tai toimeksiantojensa puitteissa käsittelevät Pohjanmaan hyvinvointialueen omistamaa tai hallinnoimaa tietoa. Tietoturvapolitiikka kattaa Pohjanmaan hyvinvointialueen omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2. Merkitys organisaatiolle

Viimeaikaiset laajat muutokset, kuten sosiaali- ja terveydenhuollon uudistus sekä useat lainsäädäntömuutokset, kuten Euroopan unionin saavutettavuusdirektiivi ja yleinen tietosuoja-asetus sekä kansallinen tietosuojalaki, tähtäävät tietoturvan, tietosuojan, riskienarvioinnin, kokonaisarkkitehtuurin ja yhteen toimivuuden huomioimiseen suunnittelussa ja sen kautta saatavaan kustannustehokkuuteen ja tietojen käytettävyyteen.

Tietoturvallisuuden toteutumiseksi hyvinvointialueella tulee tunnistaa sen toiminnan kannalta elintärkeät palvelutehtävät ja määritellä niiden turvaamiseksi riittävät tietoturvaperiaatteet. Tietoturvallisuuden toteutumista Pohjanmaan hyvinvointialueella tukevat käytännöt ja ohjeistukset, joita on muun muassa tietoturvasuunnitelma, tietosuojapolitiikka sekä sisäisen valvonnan ja riskienhallinnan ohjeistukset.

3. Määritelmä

Tietoturvallisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen suojaaminen ja turvaaminen siten, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen.

- Luottamuksellisuus (confidentiality): Luottamuksellisen tiedon tunnistaminen ja sen luottamuksellisuuden turvaaminen. Tiedot, tietojärjestelmät ja palvelut ovat vain niihin oikeutettujen saatavilla, eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.
- Eheys (integrity): Tiedon oikeellisuuden, ristiriidattomuuden ja oikeakestoisen säilymisen turvaaminen. Tiedot, tietojärjestelmät ja palvelut ovat oikeita ja eheitä, eivätkä ole muuttuneet tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- Saatavuus (availability): Tiedon oikeiden käyttömahdollisuuksien turvaaminen. Tiedot, tietojärjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä. Pääsynvalvonnalla varmistetaan, että tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa. Todentamisella varmistutaan osapuolten luotettavasta tunnistautumisesta.

Tietosuojaa käsitellään tarkemmin Pohjanmaan hyvinvointialueen tietosuojapolitiikassa.

4. Ohjaavat velvoitteet

Pohjanmaan hyvinvointialueen tietoturvallisuutta velvoittavat ja ohjaavat yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut tietoturvallisuutta ohjaavat velvoitteet, määräykset ja ohjeet, kuten toimittajien kanssa tehdyt turvallisuussopimukset. Lisäksi noudatetaan soveltuvin osin muuta tietoturvaan liittyvää ohjeistusta (mm. JUHTA/VAHTI). Asiakas- ja potilastiedot, joita koskee lakisääteinen arkistointivelvoite, arkistoidaan asianmukaisesti sekä arkistointilaitoksen että SÄHKE 2 kriteerien mukaisiin tallennuspaikkoihin. Tietoturvasuunnitelmaa ohjaa niin THL:n suositukset kuin monet julkiset sosiaali- ja terveysalan toimijat, kuten tietosuojavaltuutettu, sosiaali -ja terveysministeriö, digi- ja väestövirasto ja valtiovarainministeriö.

Pohjanmaan hyvinvointialueen ylimmän johdon tehtävänä on ohjata tietoturvallisuuden kehittämistä strategisella tasolla yhdessä tietohallinnon ja muiden tietoturvasta vastaavien kanssa.

5. Johto ja vastuut

Tietoturvallisuudesta vastaa Pohjanmaan hyvinvointialueen johtaja. Operatiivinen johtovastuu on tietohallintojohtalla. Tietoturvaan liittyvät ohjausdokumentit käsitellään alueellisessa ICT-ohjausryhmässä ja viedään hyväksyttäväksi hallitukseen.

Tietoturvallisuuden kehittämisestä, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä Pohjanmaan hyvinvointialueella vastaa tietohallintojohtaja johtoryhmiltä saamiensa valtuuksien ja resurssien puitteissa.

Pohjanmaan hyvinvointialueen tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. Kukin Pohjanmaan hyvinvointialueen tietojärjestelmien ja niiden sisältämien tietojen omistaja vastaa tietojensa ja tietojärjestelmiensä suojaamisesta. Yksityiskohtainen kuvaus vastuista on tarkemmin Pohjanmaan hyvinvointialueen tietoturvasuunnitelmassa.

6. Koulutus

Tietoturvallisuuden toteuttamisen perusta on tämä Pohjanmaan hyvinvointialueen johdon hyväksymä kirjallinen tietoturvapolitiikka. Jokaiselle Pohjanmaan hyvinvointialueen henkilökunnan jäsenelle ja tietojärjestelmien käyttäjälle annetaan siihen pohjautuvat ohjeet. Henkilökunnan jäsenten ja tietojärjestelmien käyttäjien ohjeet löytyvät Pohjanmaan Hyvinvointialueen intrasta, myös tämä tietoturvapolitiikka on nähtävillä intrassa.

Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka sisältää hallinnollisia, fyysisiä ja teknisiä ratkaisuja. Jokainen Pohjanmaan hyvinvointialueen työntekijä, jonka tehtävät edellyttävät tietoturvaohjeistuksen osaamista, saa opastuksen tietoturvaohjeiden sijainnista sekä tietoturvan organisoinnista perehdytyksen yhteydessä.

Tietoturvaohjeet ovat jokaisen henkilöstöön kuuluvan saatavissa hyvinvointialueen Intranetistä osoitteesta: intra.pohjanmaanhyvinvointi.fi

Tietoturvallisuuden ylläpidosta, kehittämisestä ja johtamisesta vastaaville tulee tarjota mahdollisuus riittävän perus- ja jatkokoulutuksen hankkimiseen. Koulutustarve arvioidaan vuosittain tietohallintojohdon toimesta.

7. Tietoturvasuunnitelma

Tietoturvapolitiikan pohjalta laaditaan Pohjanmaan hyvinvointialueen tietoturvasuunnitelma sekä käyttäjän, tietojärjestelmävastaavan ja tietohallinnon tietoturvaohjeet.

Pohjanmaan hyvinvointialueella on käytössä tietojen ja tietojärjestelmien turvallisuusluokitus. Kullekin turvallisuusluokalle on määritelty vaadittava tietoturvallisuustaso ja sen mukaiset

tietoturvatoimenpiteet. Jokaisella tietojärjestelmällä on oltava omistaja. Järjestelmien omistajista pidetään rekisteriä.

Henkilökunnalle jaetaan heidän toimissaan tarvitsemansa tietoturvallisuusohjeistus ja tietoturvallisuus on osa yleisperehdytystä. Sijaisille, opiskelijoille ja yhteistyökumppaneille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Pohjanmaan hyvinvointialueen jäseniä koulutetaan tietoturvasta tiedottein eri tiedotuskanavissa sekä järjestämällä koulutustilaisuuksia. Pohjanmaan hyvinvointialueen tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen valvonnan keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.

Hyvinvointialue varmistaa, että myös palveluntuottajat sopimuksellisesti sitoutuvat siihen, että hankittava tietojenkäsittelyjärjestelmä tai -palvelu täyttää sisäänrakennetun ja oletusarvoisen tietosuojan vaatimukset. Rekisterinpitäjän velvollisuuksien ja rekisteröidyn oikeuksien toteutuminen huomioidaan ja varmistetaan jo tietojärjestelmän määrittelyssä ja toteutuksessa.

8. Tietojärjestelmät

Pohjanmaan hyvinvointialueen henkilöstönsä käyttöön luovuttamat laitteet, ohjelmistot, tietojärjestelmät sekä tieto on tarkoitettu työtehtävien hoitamiseen. Pohjanmaan hyvinvointialueen tietojärjestelmäympäristössä saa käyttää ainoastaan kuntayhtymän hallituksen ja tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja. Asennustyöt suorittaa 2M-IT tai Pohjanmaan hyvinvointialueen kanssa sopimussuhteessa olevat toimijat, kuten ICT- palveluntuottajat sekä järjestelmä- ja laitetoimittajat. Hyvinvointialueen ja näiden toimijoiden välisissä sopimuksissa tulee huomioida tietoturvaan ja tietosuojaan liittyvät vastuut ja velvoitteet.

9. Tietojärjestelmien käyttö

Jokainen Pohjanmaan hyvinvointialueen henkilöstöön kuuluva sitoutuu tietojen ja tietojärjestelmien tietoturvalliseen ja ohjeiden mukaiseen käyttöön allekirjoittamalla tätä koskevan sitoumuksen. Vastaavasti sitoumus edellytetään niiltä Pohjanmaan hyvinvointialueen luottamushenkilöiltä, joille sallitaan oikeus käyttää Pohjanmaan hyvinvointialueen omistamia tietojärjestelmiä.

Pohjanmaan hyvinvointialueen omistamat tietojärjestelmät tunnistetaan ja niille nimetään omistajaksi organisaatioyksikkö, jonka vastuulla on tietojärjestelmän käyttövaltuushallinta.

Tietoturvallinen toimintatapa kuvataan tarkemmin tietoturvaohjeissa. Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi.

10. Tietojen luokittelu

Pohjanmaan hyvinvointialueen omistamat tiedot luokittelee se, joka tiedon omistaa. Tietojen luokittelu perustuu lakiin viranomaisten toiminnan julkisuudesta (julkisuuslaki, 621/1999) sekä Pohjanmaan hyvinvointialueen antamiin tarkempiin ohjeisiin lain soveltamisesta. Julkisuuslain mukaiset luokat ovat julkinen, ei- julkinen ja salassa pidettävä.

Pilvipalveluiden käytössä tulee huomioida, että luokittelematonta tietoa ei saa viedä pilvipalveluun.

11. Viestintä

Tietoturvallisuuteen liittyvä henkilöstön tiedottaminen ajankohtaisasioista, ohjeista ja poikkeamatilanteista tehdään pääsääntöisesti sähköpostin ja lähiesimiehen välityksellä. Jokainen esimies on velvollinen seuraamaan ja varmistamaan, että henkilöstö seuraa tiedotteita.

Teknistä tietoturvaa (esim. virustorjunta, palomuurit ja roskapostisuodatus) tuottavien ulkopuolisten ICT- palveluntuottajien kanssa sovitaan kirjallisesti poikkeamatilanteiden tiedotusmenettelyistä ja yhteyshenkilöistä palvelusopimuksia tehtäessä.

12. Riskienhallinta

Tietoriskien hallinnan perustana on niiden tunnistaminen ja vaikutusanalyysin muodostaminen sekä tarvittavista toimenpiteistä päättäminen riskien hallitsemiseksi. Pohjanmaan hyvinvointialueen tietojen turvaamistoimet mitoitetaan riskien mukaisesti yhteistyössä tiedon omistajan ja tietohallinnon kanssa.

13. Resilienssi, jatkuvuus ja palautuminen

Pohjanmaan hyvinvointialueen käytössä olevista tietojärjestelmistä ja palveluista on määriteltävä ja kuvattava suojattavat kohteet. Suojattavat kohteet on priorisoitava.

Resilienssi koostuu tietoturvan organisaation kehittämisen tuloksena, jonka olennaisena osana on jatkuvuuden varmistaminen. Tietojärjestelmien varmuuskopiot tulee testata ja niiden toiminta on varmistettava simuloidussa häiriötilanteessa. Jatkuvuussuunitelma päivitetään vuosittain.

Palautuminen koostuu organisaation kyvystä palautua häiriötilanteesta. Roolit, varahenkilöjärjestelyt, varajärjestelmäjärjestelyt sekä ohjelmistojen varaversion käyttö tulee varmistaa, jotta toimintaan ei tulisi muutoksia häiriöissä.

14. Tietoturvan kehitys

Operatiivinen kehitysvastuu on tietohallintojohtajalla. Tietoturvaan liittyvät ohjausdokumentit hyväksytään ICT-ohjausryhmässä poislukien tietoturvapolitiikka, jonka hyväksyy hallitus.

Tietoturvallisuuden kehittämisestä, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä Pohjanmaan hyvinvointialueella vastaa tietohallintojohtaja hallitukselta saamiensa valtuuksien ja resurssien puitteissa.

Tietohallintojohtajalla on Pohjanmaan hyvinvointialueella ylimmän johdon antama valtuutus ja velvollisuus tehdä Pohjanmaan hyvinvointialueen tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen tietoturvallisuuden heikkouksien parantamiseksi.

Pohjanmaan hyvinvointialueen tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen noudattaen seuraavia periaatteita:

SUUNNITTELU – Hyvinvointialueen hallitus ja tietoturvasta vastaavat tuottavat analyysien ja arvioiden perusteella politiikkoja, periaatteita ja suunnitelmia. Tälle vaiheelle vaatimuksia asettavat mm. lainsäädäntö, riskienhallinnan tulokset, vaatimukset (sopimukset, asiakkaat ja sidosryhmät) sekä toimintaolosuhteet.

TOTEUTUS - Edellisen vaiheen päätökset ja suunnitelmat otetaan käyttöön, tiedotetaan ja jalkautetaan niin henkilökunnalle kuin yhteistyökumppaneille ja asiakkaille.

SEURANTA - Suoritetaan tietoturvallisuuden teknistä valvontaa ja raportointia sekä arvioidaan, ratkaisevatko toteutetut toimenpiteet tunnistettuja tietoturvariskejä ja vähenivätkö ne suunnitellulle tasolle. Teknistä tietoturvaa operoi 2M-IT.

MUUTOSHALLINTA - Toteutetaan muutoshallintaprosessin mukaista normaalia muutoshallintaa seurantavaiheen tuloksista opitun perusteella.

15. Velvoitteet työntekijöille ja käyttäjille

Jokainen Pohjanmaan hyvinvointialueen työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta ja velvollinen noudattamaan Pohjanmaan hyvinvointialueen johdon hyväksymiä käyttösääntöjä ja tietoturvaohjeita. Hyvinvointialueen työntekijällä on tietosuoja- ja tietoturva-asioihin liittyvä valvontavastuu. Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista HaiPro - tietoturvailmoituksen avulla tai ottamalla yhteyttä 2M-IT:n Servicedeskiin. Tietoturvallisuudesta annettujen ohjeiden toteutumisesta vastaa kukin

toimintayksikkö. Yksiköiden esihenkilöt vastaavat, että yksiköissä on riittävä tietämys tietojärjestelmien käyttämisestä ja annetuista ohjeista.

16. Tietoturvarikkomukset

Tietojen ja tietojärjestelmien käyttöä valvotaan olemassa olevien lakien ja asetusten mukaisesti huomioiden yksityisyyden suoja työelämässä. Kaikki tietoturvarikkomukset käsitellään asianmukaisesti mm. Pohjanmaan hyvinvointialueen potilasrekisterin tietosuojaohjeessa tarkemmin kuvatulla tavalla.

Kun tietosuojarikkomuksista tulee epäily, selvityspyyntö lähetetään esimiehelle. Hän pitää kuulemistilaisuuden ja kirjaa muistion. Kyseisen erikoisalan johtava lääkäri tai viime kädessä hallintoylilääkäri tekee asiasta päätöksen seuraamustaulukkoa käyttäen. Em. rikkomuksen perusteella on mahdollista myös aloittaa palvelussuhteen päättymismenettelyn käynnistys. Tietoturvarikkomuksesta voi seurata myös rikosoikeudellinen vastuu ja tutkimuspyyntö poliisille.

17. Keskeistä tietoturvaan liittyvää käsitteistöä

Tietoturva

Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta.

Tietosuoja

Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

Tietoturvapolitiikka

Johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnittelu

Suunnitteluprosessi, johon kuuluu muun muassa uhka-analyysi, perusturvallisuuden määrittely sekä toipumisvalmiuden ja poikkeusolojen valmissuunnittelu, ja jonka tuloksena on tietoturvasuunnitelmia, -linjauksia ja - ohjeistoja.

Tietoaineistoturvallisuus

Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Eheys

Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Käytettävyys

Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Luottamuksellisuus

Henkilötietojen käsittely tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä

18. Tietoturvan osa-alueet

Hallinnollinen turvallisuus

Hallinnollinen tietoturva koostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista ja valvonnasta.

Ohjelmistoturvallisuus

Käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella säilytetään asiakirjojen, tietueiden ja tiedostojen luottamuksellisuus sekä estetään tietojen tuhoutuminen tai tahaton muuttuminen. Oleellista on myös tallenteiden suojaaminen ja oikeanlainen säilyttäminen. Tietoaineistoturvallisuuteen liittyvät tiedon jatkuva varmistaminen, asianmukainen säilytys sekä hävittäminen.

Käyttöturvallisuus

Käyttöturvallisuutta ovat mm. salasanat, käytössä olevien ohjelmien osaaminen ja virustentorjunta. Annettujen käyttöoikeuksien tulee olla mukautettu työtehtäviin. Käyttöturvallisuus koostuu järjestelmien turvallisista käyttöperiaatteista, tietojenkäsittelytapahtumien valvonnasta sekä jatkuvuuden turvaamisesta. Laitteiden käyttövarmuus on myös käyttöturvallisuutta. Laaditaan ns. toipumissuunnittelu, jonka avulla varmistetaan toiminnan jatkuminen jonkun yllättävän tilanteen ilmaantuessa.

Laitteistoturvallisuus

Tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.

Fyysinen turvallisuus

Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden. Fyysinen turvallisuus koostuu monesta eri osatekijästä, turvallisuuden perusta kuitenkin luodaan jo rakennusvaiheessa.

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella pyritään varmistamaan tietoturvan perustavoitteet eli verkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Keskeisenä tavoitteena on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus. Tieto-liikenneturvallisuudessa on kyse kaikista niistä toimenpiteistä, joilla varmistetaan tietojen turvallisuus tiedon liikkuessa järjestelmän sisällä tai organisaatioiden välillä.

Henkilöstöturvallisuus

Henkilöstöturvallisuuden tavoite on, ettei työntekijä tietämättömyyden, huonon motivaation tai pahantahtoisuuden vuoksi pääse muuttamaan tai tuhoamaan tietoa, tai mahdollista jonkun ulkopuolisen käyttämään sitä. Henkilöstöturvallisuuden pääpaino on riskien välttäminen ennakkoon ja synnyn estäminen.

19. Yhteenveto

Hyvinvointialueen tietoturvaa ohjaa tietoturva- ja tietosuojapolitiikka ja se kehittyy jatkuvasti. Järjestelmämuutokset luovat kompleksisen kokonaisuuden, jossa järjestelmäomistajilla on yhä enenevissä määrin vastuu huomioida tietoturva kaikissa kehitys- ja tuotantoympäristöissä. Käyttäjän ja työntekijän vastuu kasvaa myös, etenkin yhä hienovaraisempien tietoturvahyökkäysten kasvaessa, jolloin tietoturvatietoisuus on olennaisessa osassa. Koko organisaation tulee yhdessä kehittää tietoturvaa ja vastuiden muuttuminen organisaatiomuutoksissa tulee ottaa huomioon. Resilienssi ja sen testaaminen tulee myös ottaa huomioon.

20. Liitteet

Tässä kuvataan dokumentissa listatut liitetiedostot.

1. Tietoturvasuunnitelma, sijainti: Versio 1.0 Sijainti: OVPH Tietohallinto
2. Tietosuojapolitiikka, sijainti: Versio 1.0 Sijainti: OVPH Intra
3. Riskiarvio: Versio 1.0 Sijainti: OVPH Tietohallinto