Österbottens välfärdsområde
Pohjanmaan hyvinvointialue

Tietoturvapolitiikka

Pohjanmaan hyvinvointialueen kuntayhtymä

Hallitus x.x.2021 § xx

Voimaantulo 1.1.2022

Sisällysluettelo

Pohjanmaan hyvinvointialueen kuntayhtymän tietoturvapolitiikka 3
1. Johdanto 3
2. Tietoturvallisuuden merkitys organisaatiolle 3
3. Tietoturvallisuuden määritelmä ja tavoitteet 4
4. Tietoturvatoimintaa ohjaavat tekijät 4
5. Tietoturvallisuuden organisointi ja vastuut 5
6. Tietoturvallisuuden toteutuminen käytännössä 5
7. Tiedon ja tietojärjestelmien käyttö 6
8. Tietojen luokittelu 6
9. Tietoturvaosaaminen ja -tietoisuuden ylläpito 7
10. Tietoturvallisuudesta tiedottaminen 7
11. Tietoriskien hallinta 7
12. Toiminta häiriötilanteissa ja poikkeusoloissa 7
13. Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely 8
14. Tietoturvallisuuden kehittäminen 8
15. Valvonta ja rikkomusten seuraamukset 9
Liite 1 Keskeiset käsitteet 10
Liite 2 Tietoturvallisuuden osa-alueet 12

Pohjanmaan hyvinvointialueen kuntayhtymän tietoturvapolitiikka

1. Johdanto

Kuntayhtymän palveluiden perustana ovat asiakkaiden tarpeet. Palveluiden tuottaminen perustuu tietoon sekä sen käsittelyyn kuntayhtymän toimintaympäristöissä. Kuntayhtymän palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

Kuntayhtymän strategian visiossa Pohjanmaalla on innovaatiokykyä sekä yhdistetty sosiaali- ja terveydenhuolto, jonka vaikuttavuus on erinomainen. Tavoitteiden saavuttaminen edellyttää laajaa digitalisaatiota sekä tietoturvallisuuden kaikkien osa-alueiden, kokonaisarkkitehtuurin ja yhteentoimivuuden laajaa huomioimista jo suunnitteluvaiheessa.

Tässä tietoturvapolitiikassa määritellään kuntayhtymän 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 kuntayhtymän organisaatiota, sen työntekijöitä ja luottamushenkilöitä sekä niitä kuntayhtymän sidosryhmien edustajia, jotka työnsä tai toimeksiantojensa puitteissa käsittelevät kuntayhtymän omistamaa tai hallinnoimaa tietoa. Tietoturvapolitiikka kattaa kuntayhtymän omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2. Tietoturvallisuuden merkitys organisaatiolle

Viimeaikaiset 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 kuntayhtymässä tulee tunnistaa sen toiminnan kannalta elintärkeät palvelutehtävät ja määritellä niiden turvaamiseksi riittävät tietoturvaperiaatteet. Tietoturvallisuuden toteutumista tukevat kuntayhtymän käytännöt ja ohjeistukset, joita on muun muassa tietosuojapolitiikka sekä sisäisen valvonnan ja riskienhallinnan ohjeistuksessa.

3. Tietoturvallisuuden määritelmä ja tavoitteet

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 kuntayhtymän tietosuojapolitiikassa.

4. Tietoturvatoimintaa ohjaavat tekijät

Kuntayhtymän 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).

Kuntayhtymän ylimmän johdon tehtävänä on ohjata tietoturvallisuuden kehittämistä strategisella tasolla yhdessä tietohallintojohtajien ja muiden tietoturvasta vastaavien kanssa.

5. Tietoturvallisuuden organisointi ja vastuut

Tietoturvallisuutta johtaa kuntayhtymän johtaja. Hänen kanssaan ylin vastuu tietoturvallisuudesta on kuntayhtymän hallituksella, joka päättää kuntayhtymän kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista.

Tietoturvallisuuden kehittämisestä, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä kuntayhtymässä vastaavat tietohallintojohtajat johdolta saamiensa valtuuksien ja resurssien puitteissa. Jokainen kuntayhtymän tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. Kukin kuntayhtymän tietojärjestelmien ja niiden sisältämien tietojen omistaja vastaa tietojensa ja tietojärjestelmiensä suojaamisesta. Yksityiskohtainen kuvaus vastuista on tarkemmin kuntayhtymän tietoturvasuunnitelmassa.

6. Tietoturvallisuuden toteutuminen käytännössä

Tietoturvallisuuden toteuttamisen perusta on tämä kuntayhtymän johdon hyväksymä kirjallinen tietoturvapolitiikka. Jokaiselle kuntayhtymän henkilökunnan jäsenelle ja tietojärjestelmien käyttäjälle annetaan siihen pohjautuvat ohjeet.

Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka sisältää hallinnollisia, fyysisiä ja teknisiä ratkaisuja. Tietoturvapolitiikan pohjalta laaditaan kuntayhtymän tietoturvasuunnitelma sekä käyttäjän, tietojärjestelmävastaavan ja tietohallinnon tietoturvaohjeet.

Kuntayhtymässä otetaan käyttöön tietojen ja tietojärjestelmien turvallisuusluokitus. Kullekin turvallisuusluokalle on määritelty vaadittava tietoturvallisuustaso ja sen mukaiset tietoturvatoimenpiteet. Jokaisella tietojärjestelmällä tai sen osalla on oltava yksikäsitteinen omistaja. Tietoturvallisuuden toteuttamista ohjaavat dokumentit ovat vahvistettuja ja asianomaisten kohderyhmien saatavissa.

Henkilökunnalle jaetaan heidän toimissaan tarvitsemansa tietoturvallisuusohjeet. Sijaisille, opiskelijoille ja yhteistyökumppaneille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Yleensäkin kuntayhtymän jäsenten tietoturvallisuustietoisuutta lisätään tiedottein ja kirjoituksin eri tiedotuskanavissa sekä järjestämällä koulutustilaisuuksia. Kuntayhtymän tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen valvonnan keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.

Kuntayhtymä varmistaa, että myös palveluntuottajat sopimuksellisesti sitoutuvat siihen, että hankittava tietojen käsittelyjärjestelmä tai -palvelu täyttää sisäänrakennetun ja oletusarvoisen tietosuojan vaatimukset. Rekisterinpitäjän velvollisuuksien ja rekisteröidyn oikeuksien toteutuminen on huomioitava ja varmistettava jo tietojärjestelmän määrittelyssä ja toteutuksessa.

7. Tiedon ja tietojärjestelmien käyttö

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

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

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

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

8. Tietojen luokittelu

Kuntayhtymän omistamat tiedot luokittelee se, joka tiedon omistaa. Tietojen luokittelu perustuu lakiin viranomaisten toiminnan julkisuudesta (julkisuuslaki, 621/1999) sekä kuntayhtymän 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.

9. Tietoturvaosaaminen ja -tietoisuuden ylläpito

Jokainen kuntayhtymän työntekijä, jonka tehtävät edellyttävät tietoturvaohjeistuksen osaamista, saa opastuksen tietoturvaohjeiden sijainnista sekä tietoturvan organisoinnista kuntayhtymässä.

Tietoturvaohjeet ovat jokaisen henkilöstöön kuuluvan saatavissa kuntayhtymän Intranetistä.

Tietoturvallisuuden ylläpidosta, kehittämisestä ja johtamisesta vastaaville tulee tarjota mahdollisuus riittävän perus- ja jatkokoulutuksen hankkimiseen.

10. Tietoturvallisuudesta tiedottaminen

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.

11. Tietoriskien hallinta

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

12. Toiminta häiriötilanteissa ja poikkeusoloissa

Kuntayhtymän käytössä olevista tietojärjestelmistä ja palveluista on määriteltävä ja kuvattava suojattavat kohteet. Näiden toipumis- ja jatkuvuussuunnitelmissa tulee huomioida tietoturvallisuuteen kohdistuvat uhat ja toiminta poikkeamatilanteissa (esim. palvelunestohyökkäysten vaikutus). Suojattavat kohteet on priorisoitava.

13. Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Tietohallintojohtajilla on kuntayhtymän ylimmän johdon antama valtuutus ja velvollisuus tehdä kuntayhtymän tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen tietoturvallisuuden heikkouksien parantamiseksi.

Jokainen kuntayhtymän työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta ja velvollisia noudattamaan kuntayhtymän johdon hyväksymiä käyttösääntöjä ja tieto-turvaohjeita. Kuntayhtymän 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 pää- ja vastuukäyttäjät vastaavat, että yksiköissä on riittävä tietämys tietojärjestelmien käyttämisestä ja annetuista ohjeista.

14. Tietoturvallisuuden kehittäminen

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

SUUNNITTELU – Kuntayhtymän johto 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.

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

15. Valvonta ja rikkomusten seuraamukset

Tietojen ja tietojärjestelmien käyttöä valvotaan olemassa olevien lakien ja asetusten mukaisesti huomioiden yksityisyyden suoja työelämässä. Kaikki tietoturvarikkomukset käsitellään asianmukaisesti mm. kuntayhtymän potilasrekisterin tietosuojaohjeessa tarkemmin kuvatulla tavalla. Tietoturvarikkomusta lieventää merkittävästi, mikäli rikkomuksen tehnyt henkilö on välittömästi rikkomuksen huomattuaan ottanut yhteyttä esimieheensä sekä tietoturva- tai tietosuojavastaavaan, eikä käytä missään olosuhteissa väärin saamaansa tietoa. Tietoturvarikkomuksesta seuraa kurinpidollisia toimenpiteitä johtajaylilääkärin erikseen vahvistetun ohjeesta mukaisesti ja em. rikkomuksen perusteella on mahdollista myös päättää työ- tai virkasuhde. Tietoturvarikkomuksesta voi seurata myös rikosoikeudellinen vastuu.

Liite 1 Keskeiset käsitteet

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

Liite 2 Tietoturvallisuuden 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.