57 §

Digitaalisen turvallisuuden politiikka

D/1416/07.01.03.00.02/2017

Perusteluosa

Päijät-Hämeen hyvinvointiyhtymän digitaalisen turvallisuuden politiikka (liite 1) korvaa Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän syksyllä 2012 voimaan astuneen tietoturvallisuuspolitiikan. Samalla tarkastelukulma on entistä laajempi perinteisen tietoturvapolitiikan sijaan. Liitteen 1 mukainen dokumentti on valmisteltu yhteistyössä ulkopuolisten asiantuntijoiden kanssa (RD Velho Oy, entinen Relator Oy). He haastattelivat mm. osaa johtoryhmän jäsenistä syksyllä 2018 ja asia käsiteltiin kuntayhtymän johtoryhmässä 12.3.2019, jossa päätettiin em. politiikan esittämistä kuntayhtymän hallituksen hyväksyttäväksi.

Digitaalisella turvallisuudella on olennainen merkitys yhtymän toiminnassa. Digitaalisessa muodossa olevien tietojen, niiden käsittelyssä käytettävien järjestelmien, yhtymän teknisen ja fyysisen infrastruktuurin sekä informaation käsittelyprosessien turvallisuus on välttämätön edellytys ja tärkeä mahdollistaja yhtymän toiminnalle.

Päijät-Hämeen hyvinvointiyhtymän toimintaympäristössä tulee tapahtumaan merkittäviä muutoksia lähivuosina. Nämä muutokset edellyttävät yhtymältä määrätietoista, suunnitelmallista ja ennakoivaa reagointia. Digitaalisen turvallisuuden varmistaminen on yksi tärkeä osatekijä tässä kokonaisuudessa.

Digitaalisen turvallisuuden politiikka sisältää tietoturvallisuuteen, tietosuojaan, kyberturvallisuuteen, riskienhallintaan sekä toiminnan jatkuvuuteen liittyviä ylätason linjauksia, jotka ohjaavat niihin liittyvien käytännön prosessien suunnittelua.

Digitaalisella turvallisuudella on merkittävä vaikutus potilas- ja asiakasturvallisuuteen ja se kytkeytyy läheisesti kaikkiin toimintaprosesseihin sekä tekniseen infrastruktuuriin, laitteisiin ja järjestelmiin.

Digitaalisen turvallisuuden politiikka koskee koko Päijät-Hämeen hyvinvointiyhtymän toimintaa. Lisäksi politiikka koskee yhtymän yhteistyökumppanien toimintaa siinä laajuudessa, kun ne osallistuvat

yhtymän vastuulla olevien palveluiden tuottamiseen.

Digitaalisen turvallisuuden politiikka ei sellaisenaan sovellu maakunnallisen tason digitaalisen turvallisuuden politiikaksi, mutta se on tarvittaessa laajennettavissa kattamaan koko maakunnan toiminta. (Huom. Luku 1.1 on kirjoitettu ennen maaliskuun 2019 valtakunnallisia tapahtumia).

Digitaalisen turvallisuuden kehittämisen keskeisimmät aihepiirit ovat prosessien yhdenmukaistaminen ja digitalisointi, turvallinen hankintaprosessi, ratkaisujen turvallisuus sekä henkilöstön osaamisen kehittäminen. Digitaalisen turvallisuuden kehittämistä tukevat yhteistoimintamallit, verkostojen hyödyntäminen sekä kehittämisen mittaaminen ja havaittuihin puutteisiin reagointi hyvissä ajoin.

Liitteenä	Digitaalisen turvallisuuden politiikka 1.0
Esittelijä	Vt. toimitusjohtaja Veli Penttilä
Päätösehdotus	Hallitus päättää hyväksyä Päijät-Hämeen hyvinvointikuntayhtymän digitaalisen turvallisuuden politiikan.
Päätös	Ehdotus hyväksyttiin yksimielisesti.
Asian valmistelija / Lisätietojen antaja	Tietoturvapäällikkö Antti-Olli Taipale
Toimenpiteet	Ote: Antti-Olli Taipale, Petri Pekkala
Muutoksenhaku	Oikaisuvaatimusohje

PÄIJÄT-HÄMEEN
hyvinvointiyhtymä

Digitaalisen turvallisuuden politiikka

Hallitus 25.03.2019 - §

Yhteistyötoimikunta 21.03.2019

Johtoryhmä 12.03.2019

Tietohallinnon ohjausryhmä 21.02.2019

Sisältö

1 Johdanto

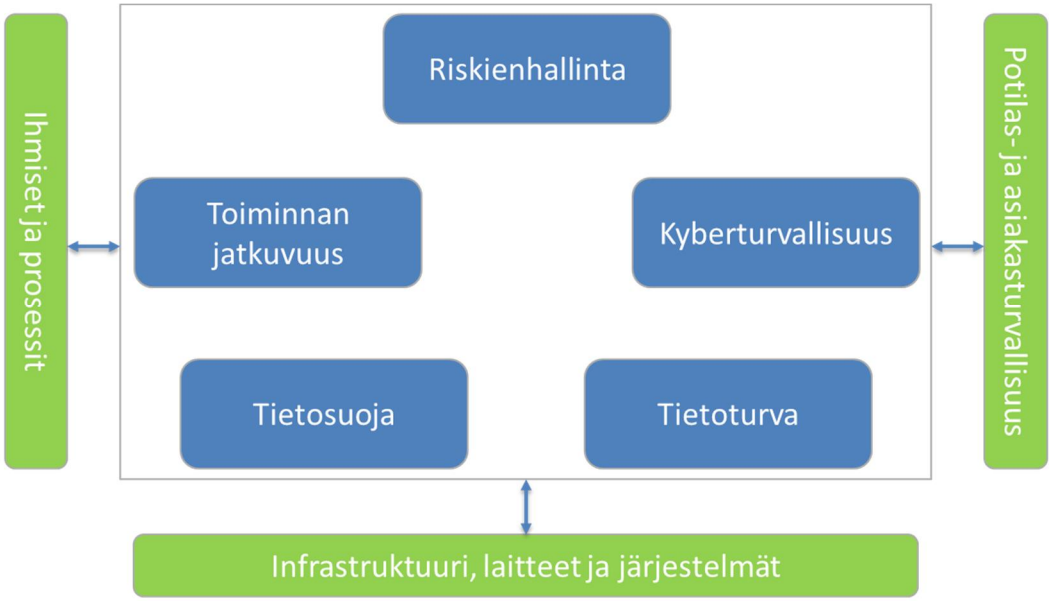
Tämä Päijät-Hämeen hyvinvointiyhtymän digitaalisen turvallisuuden politiikka korvaa Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän syksyllä 2012 voimaan astuneen tietoturvallisuuspolitiikan. Samalla tarkastelukulma on entistä laajempi perinteisen tietoturvapolitiikan sijaan.

Digitaalisella turvallisuudella on olennainen merkitys yhtymän toiminnassa. Digitaalisessa muodossa olevien tietojen, niiden käsittelyssä käytettävien järjestelmien, yhtymän teknisen ja fyysisen infrastruktuurin sekä informaation käsittelyprosessien turvallisuus on välttämätön edellytys ja tärkeä mahdollistaja yhtymän toiminnalle.

Yhtymän ylin johto on sitoutunut digitaaliseen turvallisuuteen ja sen jatkuvaan kehittämiseen. Turvallisuus tulee ottaa asianmukaisesti huomioon kaikessa päivittäisessä toiminnassa sekä toiminnan kehittämisessä.

Digitaalisen turvallisuuden politiikka sisältää tietoturvallisuuteen, tietosuojaan, kyberturvallisuuteen, riskienhallintaan sekä toiminnan jatkuvuuteen liittyviä ylätason linjauksia, jotka ohjaavat niihin liittyvien käytännön prosessien suunnittelua.

Digitaalisella turvallisuudella on merkittävä vaikutus potilas- ja asiakasturvallisuuteen ja se kytkeytyy läheisesti kaikkiin toimintaprosesseihin sekä tekniseen infrastruktuuriin, laitteisiin ja järjestelmiin.



Kuva 1, digitaalinen turvallisuus

1.1 Politiikan soveltamisala

Digitaalisen turvallisuuden politiikka koskee koko Päijät-Hämeen hyvinvointiyhtymän toimintaa. Lisäksi politiikka koskee yhtymän yhteistyökumppanien toimintaa siinä laajuudessa, kun ne osallistuvat yhtymän vastuulla olevien palveluiden tuottamiseen.

Päijät-Hämeen hyvinvointiyhtymän digitaalisen turvallisuuden politiikka ei sellaisenaan sovellu tulevan maakunnan digitaalisen turvallisuuden politiikaksi, mutta se on laajennettavissa kattamaan koko maakunnan toiminta. Tulevan maakunnan tehtävistä tämä politiikka kattaa vain sosiaali- ja terveydenhuollon, kun maakunnalla on tehtäväaloja yhteensä 26. Toisaalta toiminnan laajuudella mitattuna sosiaali- ja terveydenhuolto on selvästi suurempi kuin muut tehtäväalat yhteensä.

Maakuntatason digitaalisen turvallisuuden politiikassa tulee ottaa huomioon erityisesti seuraavia asioita:

- Kokonaisturvallisuuden varmistaminen maakunnan (palveluiden järjestäjä) sekä palveluiden tuottamiseen osallistuvien eri organisaatioiden välisessä yhteistyössä
- Tulevan maakunnan digitaalisen turvallisuuden johtamisen organisointi
- Maakunnan vastuulla olevien eri tehtäväalojen ominaispiirteet ja synergiaedut
- Eri tehtäväaloilla hyödynnettävät kansalliset ratkaisut
- ”Pienien” tehtäväalojen oikeasuhtainen huomioon ottaminen kokonaisuuden ohjauksessa

Muutosprosessin turvallisuus järjestämisvastuun siirtyessä kunnista ja kuntayhtymistä maakuntiin edellyttää hyvin hallittua uuden toiminnan suunnittelua, riittävää kehittämisresursointia, ennakoivaa ja kattavaa tiedottamista, IT-muutoshallintaosaamista sekä aktiivista toimimista yhteistyöverkostoissa muutoksessa mukana olevien eri toimijoiden välillä.

1.2 Digitaalisen turvallisuuden tavoitteet

Digitaalista turvallisuutta ohjaa lainsäädännön, viranomaisten, asiakkaiden, potilaiden, yhteistyökumppanien sekä yhtymän johdon digitaaliselle turvallisuudelle asettamat vaatimukset.

Digitaalisen turvallisuuden tavoitteena on varmistaa tietojen sekä niihin liittyvien digitaalisten palveluiden saatavuus, luottamuksellisuus ja eheys riskilähtöisesti ottaen huomioon myös toiminnan jatkuvuuden vaatimukset poikkeustilanteissa. Lisäksi digitaalisen turvallisuuden tavoitteena on tukea ja mahdollistaa eri osapuolten yhteistoimintaa sekä uudenlaisten digitaalisten palveluiden käyttöönottoa.

1.3 Termit ja määritelmät

Tässä luvussa on määritelty keskeisimmät tässä politiikassa käytetyt termit. Määrittelyt perustuvat pääosin Turvallisuuskomitean laatimaan kyberturvallisuuden sanastoon. http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Termien kuvauksia on lyhennetty ja muokattu alkuperäisestä dokumentista luettavuuden parantamiseksi. Lisäksi termien määrittelyssä on hyödynnetty muita lähteitä niissä tapauksissa, kun päälähteessä ei ole ollut vastaavaa määritelmää.

Digitaalinen turvallisuus: tarkoittaa tässä dokumentissa digitaalisen toimintaympäristön sekä siihen liittyvien toimintaprosessien turvallisuutta sisältäen tietosuojan, tietoturvallisuuden, kyberturvallisuuden, jatkuvuudenhallinnan sekä riskienhallinnan.

Eheys: tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa.

Hyökkäyspinta-ala: organisaation hyökkäyspinta-ala on organisaatiosta esiin nousevien ICT- ja käytännön toimintaan liittyvien inhimillisten riskien summa. Se kattaa koko infrastruktuurin, kuten verkot, ohjelmistot, verkkosovellukset, laitteet sekä ymmärryksen näiden kohteiden välisistä keskinäisistä yhteyksistä, käyttötavoista ja tiedon kulusta.

Jatkuvuudenhallinta: on organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa.

Jatkuvuudenhallinta on organisaation ylimmän johdon hyväksymää strategista ja operatiivista toimintaa, jolla organisaatio varautuu hallitsemaan häiriötilanteet ja jatkamaan toimintaa ennalta määritellyllä hyväksyttävällä tasolla.

Kyberturvallisuus: tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja turvallisuuden vaikutusta niiden toimintoihin.

Luottamuksellisuus: tarkoittaa sitä, ettei kukaan sivullinen saa tietoa.

Riski: on määritelmän mukaan epävarmuuden vaikutus tavoitteisiin. Riski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä. Riski on tässä yhteydessä aina kielteinen, ei-toivottu tapahtuma tai seuraus.

Saatavuus: tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana.

Suojattava kohde: on organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta. Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, laite, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema.

Tietosuoja: järjestelyt, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen.

Tietoturva: järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.

Yhtymä: tarkoittaa tässä dokumentissa Päijät-Hämeen hyvinvointiyhtymää.

2 Nykytila ja visio

2.1 Nykytila ja haasteet

Yhtymä

Päijät-Hämeen hyvinvointiyhtymä tarjoaa perusterveydenhuollon palveluita, erikoissairaanhoidon palveluita, perhe- ja sosiaalipalveluita sekä ikääntyneiden palveluita ja kuntoutusta. Lisäksi yhtymä tarjoaa ympäristöterveydenhuollon (terveydensuojelu ja eläinlääkintä) palveluita.

Yhtymä on käynnistetty nopealla aikataululla vuoden 2017 alusta lukien, minkä seurauksena sekä toimintamalleissa että teknisissä ratkaisuissa on vielä kahden toimintavuoden jälkeen epäyhtenäisyyttä. Organisaatio on toimintakulttuurien kehittämisen osalta vielä nuori, joten yhtenäistämisen kautta on mahdollista muuttaa sekä toimintatapoja että teknologiaa helpommin kuin vakiintuneemmassa tilanteessa.

Tekniset ratkaisut

Yhtymän nopeatahtinen käynnistys on jättänyt kehitettävää perustoiminnoissa. Verkko- ja palvelinympäristön integrointi on kesken. Myös sopimustilanteeseen liittyvät haasteet ovat vaikeuttaneet asioiden kuntoon saattamista.

Potilastietojärjestelmän (Lifecare) uuden version käyttöönotto on aiheuttanut yhtymälle merkittäviä vaikeuksia vuoden 2018 aikana, mikä on osaltaan hidastanut osaltaan kehitystä ja kehittämistä. Yhtymä on mukana 2M-IT:n kautta Keski-Suomen sairaanhoitopirin vetämässä uuden asiakas- ja potilastietojärjestelmän kehittämishankkeessa. Myös muita toiminnan kannalta merkittäviä kehittämishankkeita on käynnissä, kuten uuden intranetin sekä asiakkaiden sähköisen sisääntuloportaalin kehittäminen.

Yhteensä yhtymässä on käytössä useita satoja erilaisia tietojärjestelmiä ja laitteita. Yksittäisten järjestelmien turvallisuuden taso ja elinkaaren vaihe vaihtelevat. Järjestelmien välillä on monenlaisia integraatioita, mutta eri järjestelmien ja laitteiden muodostama kokonaisuus ei ole yhtenäinen. Yhtymässä tehdään aktiivisesti arkkitehtuurityötä eri järjestelmien muodostaman kokonaisuuden hallitsemiseksi.

Toimintamallit

Eri toimintayksiköissä sekä yksittäisten toimintayksiköiden sisällä on käytössä erilaisia toimintamalleja. Erilaiset tavat hoitaa samoja asioita vaikeuttavat toimintaa palvelevien

turvallisten digitaalisten ratkaisujen kehittämistä. Nykyisissä toimintamalleissa ei ole myöskään otettu huomioon kaikkia digitalisaation tarjoamia mahdollisuuksia hoitaa asioita tehokkaammin.

Henkilöstö

Kaikki henkilökunnan jäsenet allekirjoittavat tietoturva- ja tietosuojasitoumuksen ja ovat tietoisia turvallisuuteen liittyvistä velvollisuuksista. Lisäksi on turvallisuuteen liittyviä ohjeita, viestintää, koulutuksia ja perehdyttämistä.

Hajanaisista ohjeista, vaihtelevista käytännöistä ja epäyhtenäisestä yhtymärakenteesta johtuen tietoturvallisuuteen liittyvä kokonaisuus on henkilöstölle haastava. Turvallisuuteen liittyvät näkökohdat jäävät monissa tilanteissa toissijaisiksi, eikä niitä mielletä samalla tavalla tärkeiksi, kuten esimerkiksi potilasturvallisuuteen liittyviä asioita.

Hankintaprosessi

Hankinnoissa ja käyttöönotoissa on olemassa keskitettyjä prosesseja, joilla esimerkiksi varmistetaan hankintojen arkkitehtuurinmukaisuus ja turvallisuus ennen niiden käyttöönottoa. Monet hankinnat kuitenkin tehdään ensisijaisesti yksittäisen yksikön näkökulmasta, eikä hankinnoissa oteta riittävän ajoissa eikä riittävän laajasti huomioon yhteiskäyttöisyyttä ja turvallisuutta. Lisäksi sopimustenhallintaan liittyvää käytännön toimintaa ei ole keskitetty, eikä sitä ole resursoitu riittävästi.

Digitaalisen turvallisuuden hallinta

Digitaalisen turvallisuuden varmistamiseksi tehdään töitä useissa eri yksiköissä. Käytössä on useita erilaisia menettelyitä digitaalisen turvallisuuden varmistamiseksi.

Digitaalisen turvallisuuden hallintaan liittyviä toimenpiteitä eri yksiköiden välillä ei koordinoida systemaattisesti tällä hetkellä. Joitakin digitaalisen turvallisuuden hallintaan liittyviä prosesseja on määritelty, mutta kokonaisuutena digitaalisen turvallisuuden hallintaan liittyvä työskentely on vielä luonteeltaan reaktiivista.

Lisäksi arkistotoimea ei ole riittävissä määrin nivottu mukaan digitalisaation mahdollisuuksien hyödyntämiseen ja uuden kehittämiseen yhteistyössä tietohallinnon ja eri toimialojen toiminnan kehittäjien kanssa. Arkistotoimen kokemusta asiakirjojen koko elinkaaren hallinnasta tulee entistä paremmin hyödyntää kehitettäessä digitaalisen turvallisuuden hallintaa.

2.2 Muutokset toimintaympäristössä

Vallitsevat megatrendit ennustavat huomattavaa muutosta Päijät-Hämeen hyvinvointiyhtymän toimintaympäristöön lähivuosina. Muutos on käynnissä parhaillaan ja se on väistämätöntä. Yhtymä ei voi vaikuttaa näiden muutosten toteutumiseen.

Nämä muutokset edellyttävät yhtymältä määrätietoista, suunnitelmallista ja ennakoivaa reagointia. Digitaalisen turvallisuuden varmistaminen on yksi keskeinen osatekijä tässä kokonaisuudessa. Seuraavassa on kuvattu tärkeimpiä yhtymän strategiassa ja turvallisuusympäristössä tunnistettuja muutostrendejä:

- Maakunnan väestö ikääntyy ennätyksellisen nopeasti. Ikääntyminen lisää palveluiden tarvetta. Käytettävissä olevat taloudelliset resurssit eivät kuitenkaan kasva vastaavasti.
- Suomen sote-markkinat jaetaan uudestaan. Sote-organisaatioiden tulee olla kilpailukykyisiä sekä tuottavuuden että palveluiden laadun osalta pärjätäkseen kilpailussa.
- Teknologia mahdollistaa parempaa palvelua ja tuottavuutta. Palveluiden ja palveluprosessien digitalisointi on osa tätä kehitystä. Teknologian ja digitalisaation avulla saavutettava tuottavuuden kasvu on välttämätön edellytys toiminnallisten ja kilpailullisten tavoitteiden saavuttamiseksi.
- Yhteistyö eri sote-toimijoiden välillä kasvaa. Teknologiset ratkaisut on toteutettava siten, että ne mahdollistavat turvallisesti tietojen vaihdon eri toimijoiden välillä.

- Itsepalvelun ja kotona tapahtuvan hoidon merkitys kasvaa. Palveluiden käytön on oltava turvallista myös ei-turvallisissa käyttöympäristöissä.
- Informaation merkitys hoitoprosessin osana sekä päätöksenteon tukena kasvaa. Yhtymän tulee hyödyntää tehokkaasti ja turvallisesti sekä olemassa olevia ulkoisia tietoaineistoja että yhtymän vastuulla olevia asiakas- ja potilastietoja.
- Digitaalisen toimintaympäristön turvallisuusuhat ja hyökkäyspinta-ala kasvavat. Yhtymän tulee hallita suunnitelmallisesti ja kattavasti digitaaliseen turvallisuuteen liittyviä riskejä.

2.3 Visio tavoitetilasta

Päijät-Hämeen hyvinvointiyhtymä on ihmisläheinen, digitaalinen ja turvallinen!

Päijät-Hämeen hyvinvointiyhtymä tarjoaa laadukkaita sosiaali- ja terveydenhuollon palveluita kohtuulliseen hintaan. Palveluiden asiakaskokemus on tärkeä ja palvelut ovat helposti saatavilla myös etänä. Palveluiden tuottavuuden ja asiakaspalvelun parantamisessa integroiduilla digitaalisilla palveluilla on keskeinen rooli.

Palveluiden tuottamisessa on käytössä yhdenmukaiset toimintamallit sekä yhtymän sisällä että yhteistyökumppaneiden kanssa. Toimintamallit on suunniteltu kokonaan digitaalisista lähtökohdista ja niissä on otettu huomioon digitalisaation tarjoamat mahdollisuudet tehostaa työskentelyä, hyödyntää tietoaineistoja ja palvella asiakkaita.

Digitaalisen turvallisuuden hallinnassa on käytössä tietoturvastandardeja ja kansallisia ohjeistoja soveltava hallintamalli, jonka avulla voidaan varmistaa ja osoittaa digitaaliselle turvallisuudelle asetettujen vaatimusten täyttyminen. Hallintamallin keskeisinä periaatteina ovat riskilähtöisyys ja jatkuva parantaminen.

Digitaalisten palveluiden toteuttamista varten on käytössä edistyksellisiä ratkaisuja, jotka mahdollistavat monipuolisten integroitujen palveluiden tuottamisen kustannustehokkaasti ja turvallisesti.

Hankinnoissa ja toimintaprosessien suunnittelussa otetaan huomioon turvallisuusnäkökohdat, digitalisaation tarjoamat mahdollisuudet sekä koko yhtymän tarpeet heti hankinta- ja suunnitteluprosessin alusta alkaen. Turvallisuus varmistetaan systemaattisesti hankintaprosessin eri vaiheissa, ennen käyttöönottoa sekä sen jälkeen koko ratkaisun elinkaaren ajan.

Digitaalisen turvallisuuden seuraamiseksi on käytössä ajantasaiset tilannekuvapalvelut. Seurannan tulosten perustella turvallisuuden tilaa arvioidaan säännöllisesti ja kehitetään havaittujen puutteiden perusteella.

3 Organisointi

3.1 Valtuudet ja vastuut

Digitaalisen turvallisuuden johtaminen ja kehittäminen ovat osa Päijät-Hämeen hyvinvointiyhtymän johtamistoimintaa.

Yhtymän hallitus hyväksyy digitaalisen turvallisuuden politiikan. Yhtymän johtaja vastaa turvallisuuden yleisestä järjestämisestä siten, että turvallisuustyöllä on olemassa riittävät resurssit politiikan mukaisten tehtävien hoitamiseen. Turvallisuustyötä johtaa yhtymän johtaja ja linjajohto johtosäännössä todettujen periaatteiden mukaisesti. Turvallisuustyön johtaminen on osa palvelutuotannon johtamista kaikilla johtamisen tasoilla.

Turvallisuuspalveluita tuottaa turvallisuus- ja tukipalvelut yksikkö, joka vastaa fyysisten turvallisuustoimenpiteiden toteutumisesta yhtymässä yhdessä toimialojen kanssa. Turvallisuus- ja tukipalvelut yksikkö on keskeisessä roolissa yhtymän kokonaisvaltaisen turvallisuuskulttuurin rakentamisessa, ylläpitämisessä ja jatkuvassa kehittämisessä.

Turvallisuuspäällikkö vastaa toimitilaturvallisuudesta, henkilöstöturvallisuudesta sekä varautumisen kehittämisestä.

Tietosuojaryhmän tehtävänä on varmistaa tietosuojan toteutuminen eri toimialoilla lakeja ja asetuksia noudattaen; ohjata ja koordinoida tiedon turvaamisen ja suojaamisen riskienhallintaa; tukea digitaalisen turvallisuuden ylläpitoa ja kehittämistä; tukea henkilöstön osaamisen kehittämistä digitaalisessa turvallisuudessa; ottaa kantaa, linjata ja tarvittaessa ohjeistaa tietosuoja-asioissa; ohjata ja koordinoida EU:n tietosuoja-asetuksen vaatimusten noudattamista sekä raportoida yhtymän johtoryhmälle digitaalisen turvallisuuden tilannekuvasta.

Tietoturvapäällikkö vastaa yhtymän tietoturvallisuuden (tietoturva, tietosuoja, kyberturvallisuus) johtamisesta ja kehittämisestä. Tietoturvapäällikkö vastaa myös tietoturvallisuuteen liittyvien yhtymätasoisten määräysten, ohjeiden ja suositusten antamisesta. Lisäksi tietoturvapäällikön tehtävänä on ohjata ja valvoa yhtymän digitaalisen turvallisuuden politiikan toteutumista sekä johtaa yhtymässä toimivan tietosuojatiimin työtä.

Tietosuojavastaava vastaa lakisääteisen tietosuojavastaavan tehtävien hoitamisesta yhteistyössä rekisterinpitäjien kanssa: Tietosuojavastaava seuraa tietosuojalainsäädännöstä seuraavien velvoitteiden noudattamista yhtymässä, antaa neuvoja tietosuojalainsäädännön mukaisista velvollisuuksista sekä toimii yhteyspisteenä valvontaviranomaisten suuntaan tietosuojaan liittyvissä kysymyksissä.

Tietosuojatiimin tietosuojapartnerit neuvovat, ohjaavat, opastavat ja kouluttavat henkilökuntaa tietosuojakysymyksissä yhteistyössä tietosuojavastaavan kanssa sekä osallistuvat tietosuojan ylläpito- ja kehittämistehtävien toteuttamiseen.

Yhtymän johtoryhmä toimii riskienhallinnan ylimpänä päätöksentekoelimenä yhtymässä.

Riskienhallinnan työryhmä suunnittelee ja ohjaa kokonaisvaltaisesti riskienhallinnan käytännön toimenpiteitä yhtymässä.

Tietohallinnon arkkitehtuuriryhmä vastaa tietojärjestelmien ja infrastruktuurin arkkitehtuurinmukaisuudesta ja turvallisuudesta yhtymässä.

Laiteturvallisuusryhmä huolehtii laitteiden turvallisesta käytöstä niiden koko elinkaaren ajan. Ryhmän vastuulle kuuluvat muun muassa laitteiden turvallisen käytön edellyttämän osaamisen varmistaminen, toiminnan säännöstenmukaisuuden varmistaminen, vaaratilanteiden arvioinnit, vaaratilanteiden toistumisen estämiset, ohjeiden laatiminen, laiteturvallisuudesta tiedottaminen sekä laiteturvallisuuden seuranta.

Potilas- ja asiakasturvallisuudesta vastaa ensisijaisesti palvelua tuottava yksikkö. Lisäksi yhtymässä on potilas- ja sosiaaliasiamiehet, joiden tehtävinä on neuvoa ja avustaa potilaita ja asiakkaita muistutusten teossa, asemaan ja oikeuksiin liittyvissä kysymyksissä sekä edistää muilla tavoin potilaiden ja asiakkaiden oikeuksien toteutumista.

Suurin osa päivittäisestä digitaaliseen turvallisuuteen vaikuttavasta työstä ja päätöksenteosta tehdään hajautetusti eri yksiköissä. Erityisen merkittävä rooli on kaikilla esimiehillä, joiden vastuulla on tukea ja varmistaa työskentelyn turvallisuus päivittäisessä työssä.

3.2 Kehittämistarpeet

Digitaalisen turvallisuuden johtamisen haasteena on eri näkökulmien tasapainoinen huomioon ottaminen siten, että tehtävät päätökset edistävät digitaalisen turvallisuuden kokonaisuutta optimaalisella tavalla.

Nykyinen hierarkkiseen johtamismalliin perustuva digitaalisen turvallisuuden johtaminen ei palvele parhaalla mahdollisella tavalla turvallisuuden kehittämistä. Haasteena on erityisesti useiden eri turvallisuusnäkökohtien yhteensovittaminen muiden toiminnan asettamien

vaatimusten kanssa. Seuraavassa on hahmoteltu keinoja, joilla digitaalisen turvallisuuden johtamista voitaisiin kehittää:

- **Erillisten turvallisuusnäkökohtien koordinointi ja yhteensovittaminen.** Kehitetään nykyisestä toimintamalli ja organisointitapa, joiden avulla eri turvallisuusnäkökohtien yhteensovittaminen onnistuu entistä paremmin. Potilasturvallisuus, henkilöstön turvallisuusosaaminen, tietosuoja, tietoturva, laiteturvallisuus, fyysinen turvallisuus ja toiminnan laatu sisältävät hyvin pitkälle samoja tavoitteita ja keinoja, minkä vuoksi niiden ohjaaminen rinnakkain olisi mahdollista toteuttaa tehokkaasti.
- **Riskilähtöisen turvallisuusjohtamisen jalkauttaminen osaksi päätöksentekoa.** Laaditaan ohjeistus ja riskienarviointimalli, joiden avulla riskienhallinta saadaan mukaan osaksi päätöksentekoprosesseja. Ottamalla riskienhallinta laaja-alaisesti mukaan päätöksentekoprosessiin, voidaan erilaiset digitaaliseen turvallisuuteen liittyvät riskit ”laittaa samalle viivalle”, mikä tarjoaa paremmat edellytykset tehdä turvallisuuden kannalta oikeita päätöksiä.
- **Turvallisuusnäkökulmien jalkauttaminen hankinta- ja suunnitteluprosesseihin**. Turvallisuuteen liittyvät näkökulmat tulee ottaa huomioon toiminnan ja prosessien suunnittelussa sekä niihin liittyvissä hankinnoissa heti alusta alkaen. Turvallisuusnäkökohtien huomioon ottaminen suunnittelun alkuvaiheessa mahdollistaa toiminnan ja turvallisuuden asettamien vaatimusten yhteensovittamisen sekä teknologian tuomien mahdollisuuksien kattavan hyödyntämisen toiminnan kehittämisessä.
- **Eri osapuolten yhteistyö ja tietämyksen jakaminen**. Kehitetään toimintamalleja, joiden avulla eri yksiköissä toimivien henkilöiden sekä yhtymätason välistä yhteistyötä ja tietojen vaihtoa saadaan kehitettyä. Erityisesti tämä huomioidaan resursoitaessa kehityshankkeita ja tiedotettaessa alkavista ja toteutuneista kehittämistoimenpiteistä

4 Linjaukset

4.1 Toimintaprosessit

Toimintaprosessit suunnitellaan digitaalisiksi

Toimintaprosessien suunnittelussa otetaan huomioon digitalisaation mahdollisuudet. Paperipohjaisista tietojenkäsittelyvaiheista pyritään systemaattisesti eroon. Paperimuodossa saatavat aineistot saatetaan sähköiseen muotoon ja tietoaineistojen käsittely paperimuodossa hyväksytään uudistettavissa prosesseissa vain poikkeustapauksissa.

Ajantasainen ja helposti saatavilla oleva informaatio on keskeisessä roolissa yhtymän toiminnassa. Paperimuodossa olevia tietoja ei kyetä tehokkaasti välittämään palveluketjujen eri osapuolille. Siten digitalisaatio on välttämätön edellytys tietojen saatavuuden varmistamisessa. Myös EU:n ISA-ohjelmassa laaditut eurooppalaiset yhteentoimivuusperiaatteet sekä tuleva kansallinen lainsäädäntö (mm. tiedonhallintalaki) ohjaavat organisaatioita vahvasti tähän suuntaan.

Toimintaprosessit suunnitellaan sujuviksi ja lisäarvoa tuottamattomat vaiheet minimoidaan

Toimintaprosesseista poistetaan tarpeettomat ja lisäarvoa tuottamattomat työvaiheet, jotka lisäävät tarvittavaa työtä ja kustannuksia. Suunnittelu toteutetaan asiakas- ja potilastyöhön osallistuvien ammattilaisten ja prosessiasiantuntijoiden yhteistyönä konsultoiden myös turvallisuusasiantuntijoita.

Sujuvat toimintaprosessit parantavat toiminnan turvallisuutta. Toimintaprosessien suunnittelussa voidaan hyödyntää ns. Lean-ajattelua, jonka jatkuvan kehittämisen periaate tukee hyvin myös tietoturvallisuuden hallinnan kehittämistä.

Toimintamallit suunnitellaan yhdenmukaisiksi ottaen huomioon toiminnan asettamat erityisvaatimukset

Yhtymässä toimitaan pääosin yhdenmukaisesti koko organisaation laajuisesti. Yhdenmukaisuudella tarkoitetaan sitä, että samantyyppiset tehtävät hoidetaan samanlaisilla menettelyillä. Toimintamallien suunnittelussa otetaan huomioon myös toiminnan asettamat erityisvaatimukset. Mahdollisuuksien mukaan toimintamalleja yhdenmukaistetaan myös yli organisaatiorajojen.

Yhdenmukaiset toimintamallit voidaan helpommin suunnitella turvallisiksi ja niitä on selkeämpi ohjeistaa sekä oppia. Yhdenmukaisten toimintamallien digitalisointi on yksinkertaisempaa ja niiden turvallisuus on sujuvampaa varmistaa, koska riskienhallintaa voidaan näin kohdistaa pienempään määrään toimintatapoja. Siten yhdenmukaiset toimintamallit kyetään toteuttamaan turvallisiksi entistä pienemmillä kustannuksilla.

Digitaaliset palvelut rakennetaan yhdenmukaisiksi ja helppokäyttöisiksi

Digitaalisten palveluiden ja järjestelmien käyttöliittymät ja niiden toimintalogiikat toteutetaan yhdenmukaisiksi ja helppokäyttöisiksi. Linjaus koskee niin yhtymän asiakkaille suunnattuja palveluita kuin yhtymän henkilökunnalle ja yhteistyökumppaneille suunnattuja ratkaisuja.

Tätä varten laaditaan ohjeistuksia mahdollisuuksien mukaan yhteistyössä muiden SOTE-organisaatioiden kanssa. Ohjeistuksia noudatetaan niiden digitaalisten palveluiden toteutuksessa, joihin yhtymä voi vaikuttaa. Lisäksi yhtymä pyrkii edistämään eri palveluiden yhdenmukaista suunnittelua yhteistyössä muiden alan organisaatioiden kanssa.

Yhdenmukaiset ja helppokäyttöiset digitaaliset palvelut parantavat asiakaskokemusta, tehostavat henkilökunnan työskentelyä ja pienentävät virhemahdollisuuksia.

Digitalisaatiossa otetaan huomioon tietojen koko elinkaaren hallinta

Digitalisoitaessa toimintaprosesseja otetaan huomioon tietojen koko elinkaari. Tämän varmistamiseksi arkistotoimi tulee ottaa entistä selvemmin mukaan digitalisaation mahdollisuuksien hyödyntämiseen ja uuden kehittämiseen tiiviissä yhteistyössä tietohallinnon ja eri toimialojen toiminnan kehittämisen kanssa.

Arkistotoimen ”linjapaikka” organisaatiossa kuin organisaatiossa tulee olla sellainen, että edellä kuvatun vaatimuksen on käytännössä mahdollista toteutua. Tämä edellyttää erityistä johtamis- ja asiantuntijaosaamista arkistotoimen, tietohallinnon ja digitaalisen kehittämisen saralla. Vain tällaisella modernilla ajattelumallilla voidaan taata kunnollinen koko elinkaaren kattava digitaalinen turvallisuus kaikissa hoito- ja palveluketjuissa.

4.2 Turvallisuusjohtaminen

Turvallisuutta hallitaan suunnitelmallisesti

Digitaalisen turvallisuuden hallinnan prosessit suunnitellaan ja resursoidaan siten, että niitä pystytään toteuttamaan riittävässä määrin turvallisuuden varmistamiseksi. Seurannan tulosten perusteella arvioidaan digitaalisen turvallisuuden eri hallintaprosessien määrällistä ja laadullista riittävyyttä. Hallintaprosessien suunnitelmat täsmennetään vuosittain seurannan tulosten ja aiempien kokemusten perusteella.

Digitaalisen turvallisuuden varmistamisessa on välttämätöntä päästä reaktiivisesta, ad hoc -ongelmaan reagoivasta toimintamallista kohti suunnitelmallista työskentelyä, jossa tunnistetaan ja torjutaan digitaaliseen turvallisuuteen liittyviä uhkia ennakoivasti. Turvallisuustoimenpiteiden suunnittelu sekä suunnitelmien toteutumisen seuranta varmistavat hallitun digitaalisen turvallisuuden kehittymisen.

Turvallisuutta johdetaan riskilähtöisesti

Digitaalisen turvallisuuden varmistavat kontrollit suunnitellaan ja toteutetaan riskilähtöisesti. Yhtymä vastuulla olevien tietojen, järjestelmien ja käsittelyprosessien riskit tunnistetaan, arvioidaan ja käsitellään riskilähtöisesti siten, että jäljelle jäävät riskit ovat hyväksyttävällä tasolla.

Riskienhallinnan avulla voidaan priorisoida turvallisuuden kannalta tärkeät toimenpiteet ja välttää tarpeettomia turvallisuusinvestointeja. Siten riskienhallinta on tärkeä digitaalisen turvallisuuden suunnittelun ja ohjauksen apuväline, joka auttaa toteuttamaan tehokkaasti digitaalista turvallisuutta rajallisilla resursseilla.

Kaikkien prosessien ja hankintojen turvallisuus on varmistettava

Kaikissa toimintaprosesseissa, hankinnoissa ja kehittämisprojekteissa on varmistettava turvallisuus arvioimalla riskit, määrittelemällä turvallisuusvaatimukset ja varmistamalla vaatimusten toteutuminen. Turvallisen toimintaympäristön toteuttaminen edellyttää ensisijaisesti yhteistoimintaa ja aktiivisuutta turvallisuuden varmistamiseksi kaikilta osapuolilta, kuten järjestelmätoimittajilta, palvelutarjoajilta ja yhtymän sisäisiltä toimijoilta.

Yhtymän toimintaan liittyy monia keskenään vuorovaikutuksessa olevia prosesseja ja järjestelmiä. Puutteet niiden digitaalisessa turvallisuudessa voivat johtaa mittaviin ongelmiin sekä asiakas- tai potilasturvallisuuden että yksityisyyden suojan vaarantumiseen.

Turvallisuus otetaan huomioon heti kehittämisprosessin alkuvaiheessa

Turvallisuus rakennetaan sisään jokaiseen järjestelmään ja toimintaprosessiin. Prosessit ja järjestelmät suunnitellaan heti alun alkaen ottaen huomioon turvallisuusvaatimukset sekä erilaiset mahdollisuudet näiden vaatimusten täyttämiseen. Sovelletaan security- ja privacy by default -ajattelua.

Turvallisuuden huomioon ottaminen heti alkuvaiheessa tuottaa parhaan lopputuloksen kokonaisuuden kannalta. Jälkikäteen ”päälle liimattu turvallisuus” johtaa helposti joko liian turvattomiin tai liian vaikeakäyttöisiin ratkaisuihin.

Henkilöstön perehdytetään ja turvallisuusosaamista ylläpidetään jatkuvasti

Yhtymässä huolehditaan koko henkilöstön turvallisuusosaamisesta ja varmistetaan osaamisen riittävä taso ohjeiden, perehdytysten, koulutusten ja seurannan avulla. Turvallisuusosaamista ylläpidetään säännöllisillä lisäkoulutuksilla. Yhtymässä haetaan tehokkaita ratkaisuja henkilöstön turvallisuusosaamisen lisäämiseen.

Henkilöstön turvallinen toiminta on yksi tärkeimmistä digitaalisen turvallisuuden osa-alueista. Hyvätkään tekniset ratkaisut eivät riitä takaamaan turvallisuutta, ellei henkilöstö osaa toimia turvallisesti.

Häiriö- ja poikkeustilanteisiin varaudutaan suunnitelmien ja varajärjestelmien avulla

Järjestelmät ja prosessit arvioidaan niiden saatavuusvaatimusten näkökulmasta. Arvioiden perusteella niille suunnitellaan ja toteutetaan tarpeelliset järjestelyt häiriö- ja poikkeustilanteita varten. Erityisesti otetaan huomioon sellaiset häiriöt ja poikkeustilanteet, joiden vaikutukset ovat laaja-alaiset. Kyky toimia häiriö- ja poikkeustilanteissa varmistetaan poikkeustilanteiden harjoittelulla yhteistyössä sidosryhmien kanssa.

Parhaimmatkaan turvallisuuskontrollit eivät kykene takaamaan täydellistä suojaa häiriöitä ja poikkeustilanteita vastaan, minkä vuoksi on varauduttava myös toimimaan normaalista poikkeavien tilanteiden aikana. Varautuminen poikkeustilanteisiin pienentää tehokkaasti riskien vaikutuksia ja on siten kustannustehokas tapa parantaa organisaation turvallisuutta. Varautumisella on myös merkittävä vaikutus potilas- ja asiakasturvallisuuteen.

Turvallisuutta seurataan, arvioidaan ja parannetaan jatkuvasti

Digitaalisen turvallisuuden toteutuminen ja kehittyminen varmistetaan säännöllisellä seurannalla. Seuranta tehdään sellaisella tarkkuudella, että saadaan selkeä kokonaiskuva turvallisuuden tilanteesta ja turvallisuuden eteen tehdyistä toimenpiteistä kaikilla tärkeimmillä turvallisuuden osa-alueilla. Seurannan tulosten perusteella arvioidaan kehittämistarpeita sekä suunnitellaan ja toteutetaan tarvittavia kehittämistoimenpiteitä säännöllisesti.

4.3 Kehittäminen

Kehittämistoiminta resursoidaan riittävästi

Digitaalisen turvallisuuden kehittämistoimintaan resursoidaan riittävästi ja pitkäjänteisesti sekä osaavia henkilöitä että varoja. Henkilöstöresurssit suunnitellaan siten, että kehittämistoiminta ei vaarannu henkilöiden muiden arkitehtävien johdosta. Kehittämisen resursoinnissa varmistetaan myös, että lyhyen aikavälin taloudelliset paineet eivät vaaranna pitkäjänteistä kehittämistä.

Laajamittainen toiminnan ja palveluiden digitalisointi on yksi keskeinen organisaation tuottavuutta parantava tekijä. Digitaalinen turvallisuus on välttämätön mahdollistaja digitaalisten palveluiden laajamittaiselle hyödyntämiselle. Riittävät investoinnit digitaaliseen turvallisuuteen ovat välttämätön edellytys digitalisaation kautta haettavalle tuottavuuden kasvulle.

Digitaalisen turvallisuuden kehittämisestä tinkiminen ei tuo todellisia säästöjä, vaan siirtää kehittämistoiminnan kustannussäästöt korkeammiksi operatiivisen toiminnan kustannuksiksi myöhemmässä vaiheessa. Väärässä paikassa säästäminen turvallisuuden kustannuksella voi eskaloida täysin ennalta arvaamattomia ja vakavia riskejä nopealla tahdilla digitalisoituvassa yhteiskunnassa.

Turvallisuusvaatimukset otetaan huomioon hankinnoissa ja sopimuksissa

Kaikissa hankinnoissa otetaan suunnitelmallisesti huomioon turvallisuusvaatimukset. Turvallisuusvaatimusten unohtaminen voi johtaa ongelmiin käyttöönottovaiheessa, estää hankinnan järkevän integroinnin osaksi kokonaisuutta ja pahimmillaan vaarantaa potilas- ja asiakasturvallisuuden. Lisäksi hankintatoimessa tulee riittävästi panostaa juridiseen sekä tietosuoja- ja sopimuksenhallinnalliseen osaamiseen.

Hankinnoissa otetaan huomioon koko organisaation tarpeet

Hankinnoissa otetaan huomioon koko organisaation tarpeet sekä yhtymän tietojenkäsittely-ympäristön asettamat vaatimukset. Hankinnan vaatimuksia määriteltäessä otetaan huomioon kaikki ne tahot, joihin hankinta vaikuttaa tai jotka voisivat hyödyntää kyseistä hankintaa.

Erillisiä yksikkökohtaisia hankintoja voidaan tehdä vain niissä tapauksissa, kun hankinta on luonteensa johdosta selkeästi yksikkökohtainen. Niissäkin tapauksissa tulee yhteistyössä hankintatoimen kanssa suunnitella etukäteen, miten hankinta sovitetaan yleisiin ja yhtymän hankintasäännöksiin sekä digitaaliseen ympäristöön.

Yksikkökohtaiset hankinnat, joissa ei ole otettu huomioon yhteisiä vaatimuksia ja yhteiskäyttömahdollisuuksia johtavat helposti päällekkäisiin investointeihin, yhteentoimimattomaan kokonaisuuteen ja sitä kautta korkeampiin kustannuksiin. Tällainen toimintatapa voi myös aiheuttaa ennalta arvaamattomia riskejä.

Merkittävät hankinnat tehdään yhteistyössä kansallisen tason ja muiden maakuntien kanssa

Merkittävät digitalisaatiota tukevat investoinnit, kuten asiakas- ja potilastietojärjestelmät, suuret uudenlaista teknologiaa hyödyntävät ratkaisut sekä kansallisella tasolla toteutettavat ratkaisut pyritään hankkimaan yhteistyössä muiden julkishallinnon toimijoiden kanssa, kuten esimerkiksi maakuntien ja kansallisten toimijoiden välisinä yhteishankkeina.

Hankintayhteistyöllä voidaan säästää sekä hankintojen hinnassa että hankintoihin vaadittavassa valmistelutyössä. Lisäksi yhteiset hankinnat helpottavat yhteistyötä ja parantavat tietojen vaihdettavuutta eri osapuolten välillä.

Uudet ratkaisut ja toimintaprosessit testataan riittävästi ja huolellisesti

Kaikki käyttöönotettavat uudet ratkaisut ja toimintaprosessit testataan riittävästi ennen niiden käyttöönottoa. Testaamalla varmistetaan sekä ratkaisun turvallisuus että soveltuvuus käytännön toimintaprosesseihin. Testaamisessa tulee hyödyntää erillisiä testausympäristöjä ja varmistaa testauksessa käytettävien henkilötietoja sisältävien tietoaineistojen käsittelyn turvallisuus koko aineiston elinkaaren ajan.

Laajemmissa hankinnoissa testaus suunnitellaan kokonaisuutena ottaen huomioon sekä toimittajan että yhtymän itse suorittamat testaukset. Soveltuvin osin osana testausprosessia voidaan hyödyntää toimittajan etukäteen suorittamia ja dokumentoimia testaustuloksia, jotka osoittavat ratkaisun toimivuuden.

Yhtymän tulee riittävästi ja hyvissä ajoin resursoida joko omia tai ulkoisen kumppanin asiantuntijoita mukaan testaamisen eri vaiheisiin. Eri testausvaiheissa havaitut huomiot ja näkökannat tulee arvioida riippumattomien ja ulkopuolisten erityisasiantuntijoiden avustuksella. Uuden ”digitaalisen ratkaisun” tai järjestelmän käyttöönoton kynnyksellä projektin tai asianomistajan tulee tehdä yhteistyössä toimittajan ja muiden asiaan kuuluvien tahojen kanssa riittävän kattava hyväksymistestaus.

Muutokset ohjeistetaan, koulutetaan ja viestitään

Toimintaprosesseihin, järjestelmiin ja palveluihin liittyvät muutokset pitää viestiä, ohjeistaa ja kouluttaa kattavasti. Uudet ratkaisut määritellään ja suunnitellaan ottaen aina huomioon ratkaisuja käyttävät ihmiset sekä työprosessit, joihin ne liittyvät.

Ennen uusien ratkaisujen käyttöönottoa ne ohjeistetaan ja koulutetaan siten, että kaikilla käyttäjillä on edellytykset käyttää niitä turvallisesti. Viestinnän avulla varmistetaan kaikkien osapuolten tietoisuus muutoksista ja uusista ratkaisuista. Muutosten aikatauluja suunniteltaessa otetaan huomioon myös muut muutokset siten, ettei suunnitella liikaa muutoksia liian lyhyelle aikavälille.

Ihmisten ohjeistaminen ja kouluttaminen ovat keskeisiä tekijöitä kaikissa onnistuneissa käyttöönotoissa. Puutteellisesti hoidettu koulutus voi johtaa vakaviin virheisiin järjestelmien käytössä, hidastaa työskentelyä ja kuormittaa henkilöstöä tarpeettomasti.

4.4 Digitaaliset palvelut

Vältetään lukittautumista yksittäiseen teknologiaan

Digitaalisen turvallisuuden kehittäminen on mahdollista sekä toiminnan että teknologian kautta. Koska teknologiat vaihtuvat erilaisilla sykleillä, tulee pitkällä aikavälillä välttää lukittautumista minkään tietyn teknologian käyttäjäksi. Turvallisen teknologia-arkkitehtuurin näkökulmasta on ensisijaisen tärkeää, että arkkitehtuuri mahdollistaa teknologisten ratkaisujen muuttamisen joustavasti.

Selkeytetään eri osapuolten vastuut

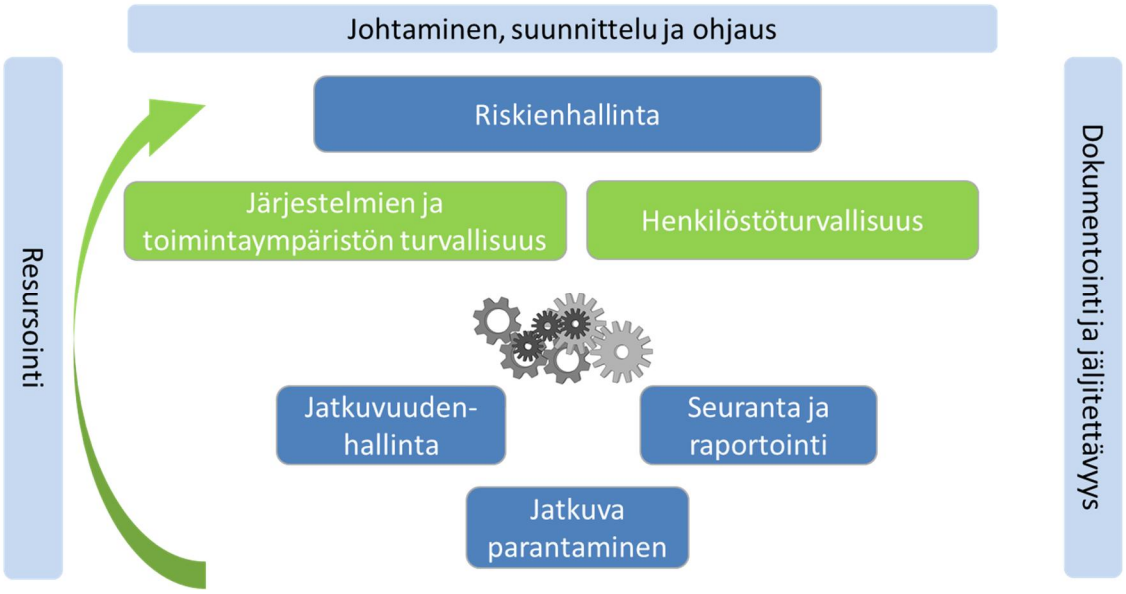
Digitaalisten palveluiden hankinnassa vastuu turvallisuusratkaisujen toteuttamisesta on sekä toimittajalla että tilaajalla. Toimittaja ei voi vastata asiakkaan ympäristöön liittyvistä ratkaisuista, joihin toimittajalla ei ole vaikutusmahdollisuutta. Toisaalta toimittaja on vastuussa järjestelmän sisäisestä turvallisuudesta sekä siitä, että turvallisuuteen liittyvät rajoitteet tulevat selkeästi kommunikoitua tilaajalle. Hankintojen tietoturvallisuuden kehittäminen edellyttääkin ensisijaisesti sekä vaatimustenhallinnan että hankintaprosessin vastuiden ja niihin liittyvien velvollisuuksien kehittämistä.

Hyödynnetään valmiita vaatimusjoukkoja ja yhteistyötä

Digitaalisten palveluiden turvallisuuden varmistaminen on laaja ja monivaiheinen prosessi, jossa kannattaa hyödyntää mahdollisuuksien mukaan valmiita vaatimusmäärittelyitä, muiden organisaatioiden kokemuksia vastaavista hankinnoista sekä yhteistyöverkostoja, kuten esimerkiksi Huoltovarmuuskeskuksen Kyberterveys -hanketta ja Julkisen hallinnon digitaalisen turvallisuuden johtoryhmää (Vahti). Koska samat vaatimukset toistuvat enemmän tai vähemmän samankaltaisina eri hankinnoissa, on perustelua kehittää työkaluja helpottamaan tietoturvallisuusvaatimusten hallintaa, käyttöä ja niiden todentamista.

5 Digitaalisen turvallisuuden hallinta

Digitaalisen turvallisuuden hallinta koostuu joukosta prosesseja, joiden avulla luodaan edellytyksiä sekä ohjataan, seurataan ja varmistetaan digitaalisen turvallisuuden toteutumista. Oheisessa kuvassa sekä seuraavissa alaluvuissa on eritelty tärkeimpiä digitaalisen turvallisuuden hallintaan liittyviä prosesseja.



Kuva 2, digitaalisen turvallisuuden hallinta

5.1 Resursointi, johtaminen ja dokumentointi

Resursointi

Ylin johto varmistaa, että digitaalisen turvallisuuden hallinnan eri tehtäviin nimetyillä henkilöillä on tosiasialliset mahdollisuudet suoriutua tehtävistään asetettujen vaatimusten puitteissa. Resursointi perustuu aiempien vuosien työmäärän ja havaittujen muutostarpeiden perusteella muodostettuun arvioon tarvittavista resursseista. Lisäksi ylin johto varmistaa, että digitaalisen turvallisuuden kehittämiseen käytettävissä olevat resurssit ovat riittävät suhteessa digitaaliselle turvallisuudelle asetettuihin vaatimuksiin.

Digitaalisen turvallisuuden hallinta ei toteudu, jos eri rooleissa työskentelevillä henkilöillä ei ole riittävästi aikaa vaadittujen tehtävien hoitamiseen. Toisaalta digitaalisen turvallisuuden hallinta tuo oikein toteutettuna systemaattisuutta ja tehokkuutta työskentelyyn, mikä pienentää resurssien kokonaistarvetta. Siten digitaalinen turvallisuus edellyttää lisäresursointia alkuvaiheessa, mutta pidemmällä aikavälillä resurssien tarve pienentyy toiminnan tehostumisen myötä.

Johtaminen, suunnittelu ja ohjaus

Digitaalisen turvallisuuden hallinta on systemaattista toimintaa. Vuositasolla suunnitellaan digitaalisen turvallisuuden hallintaan liittyvät tehtävät, työmäärät, aikataulut ja vastuut. Suunnitelmat laaditaan kirjallisesti. Suunnitelmat kytketään yhtymän toiminnan suunnittelun vuosikelloon tai vastaavaan yhtymätasoisen toiminnan kehittämisen kokonaisuuden tarkasteluun.

Suunnitelmia täsmennetään tarpeen mukaan vuoden aikana. Osa digitaaliseen turvallisuuteen liittyvästä työstä voi olla ennalta suunnittelematonta reagointia tilanteen kulloinkin edellyttämällä tavalla.

Dokumentointi

Kaikki erilaiset digitaaliseen turvallisuuteen liittyvät asiat, kuten suunnitelmat, tehdyt toimenpiteet, häiriötilanteet, tietoturvaloukkaukset ja seurantatiedot dokumentoidaan. Dokumentointi tehdään systemaattisesti ja suunnitelmallisesti siten, että jälkikäteen pystytään osoittamaan sekä digitaalisen turvallisuuden toteutuminen että tehdyt turvallisuustoimenpiteet.

Dokumenttien hallinnan kannalta yhteiset seikat, kuten nimeämis- ja versiointikäytännöt suunnitellaan keskitetysti. Kunkin digitaalisen turvallisuuden hallinnan prosessin yhteydessä täsmennetään syntyvän dokumentaation yksityiskohdat ja sisällöt. Dokumentointi voi toteutua eri muodoissa ja koostua sekä järjestelmissä olevista tiedoista että erillisistä tiedostoista.

Systemaattisen dokumentoinnin merkitys on keskeinen sekä digitaalisen turvallisuuden kehittämisessä että mm. lakisääteisen tietosuoja-asetuksen edellyttämän osoitusvelvollisuuden toteuttamisessa.

5.2 Riskienhallinta, järjestelmät, toimintaympäristö ja henkilöstö

Riskienhallinta

Riskienhallinta koostuu joukosta prosesseja, joiden avulla varmistetaan, että digitaaliseen turvallisuuteen liittyvät riskit ovat hyväksyttävällä tasolla. Riskienhallinta koostuu seuraavista riskienhallintaan sisältyvistä tai siihen läheisesti liittyvistä tehtävistä:

- Suojattavien kohteiden hallinta sisältäen digitaalisen turvallisuuden kannalta merkityksellisten tietojen, järjestelmien, laitteiden ja käsittelyprosessien tunnistamisen ja luokittelun
- Digitaaliseen turvallisuuteen liittyvien vaatimusten hallinta
- Digitaaliseen turvallisuuteen liittyvien riskien tunnistaminen ja arviointi
- Digitaaliseen turvallisuuteen liittyvien riskien käsittely ja jäännösriskien hyväksyminen.

Digitaaliseen turvallisuuteen liittyvien riskien hallinta toteutetaan osana muita yhtymän hallintaprosesseja. Riskienhallinta sisällytetään kaikkiin yhtymän prosesseihin, joiden yhteydessä tehdään merkittäviä digitaaliseen turvallisuuteen liittyviä päätöksiä.

Digitaalisen turvallisuuden kannalta olennaiset suojattavat kohteet tunnistetaan ja luokitellaan yhteistyössä tietohallinnon arkkitehtuurityöryhmän kanssa. Riskienhallinnassa hyödynnetään koko yhtymän yhteisiä riskienhallintaprosesseja ja riskienarvioinnissa arvioidaan digitaalisesta turvallisuudesta aiheutuvia riskejä myös asiakas- ja potilasturvallisuuden näkökulmista.

Digitaaliseen turvallisuuteen liittyvää riskienhallintaa toteutetaan yhtymässä suunnitelmallisesti siten, että kaikki toiminnan, potilas- ja asiakasturvallisuuden kannalta tärkeiden kohteiden riskit on käsitelty ja arvioitu ottaen huomioon myös henkilötietojen käsittelyyn liittyvät tietosuojanäkökohdat. Tarvittaessa riskit käsitellään myös tietosuojaryhmässä.

Riskienhallintaa tehdään myös havaittujen poikkeamien yhteydessä. Poikkeamien arvioinnin perusteella suunnitellaan korjaavia toimenpiteitä tietoturvallisuuden hallintakeinoihin ja tarvittaessa myös riskienhallintaprosessiin.

Riskienhallintaa toteutetaan yhdenmukaisen menetelmän avulla, joka ohjeistetaan kaikille, joiden kuuluu työssään arvioida riskejä. Riskienhallinnan käytännön toteutusta ja seurantaa varten hankitaan tarkoituksenmukaiset tekniset työkalut.

Järjestelmien ja toimintaympäristön turvallisuus

Yhtymän toimintaympäristö koostuu lukuisista erilaisista järjestelmistä, laitteista, muusta digitaalisesta infrastruktuurista ja fyysisestä toimintaympäristöstä. Koko tämän toimintaympäristön turvallisuuden varmistaminen on digitaalisen turvallisuuden hallinnan keskeinen tehtävä yhdessä henkilöstön turvallisuuden varmistamisen kanssa. Tärkeässä roolissa on myös järjestelmäasiantuntijoiden ja ICT-partnereiden työn tekemisen johtaminen erilaisissa tilanteissa, projekteissa ja ylläpitotyössä riippumatta siitä, että onko asiantuntijatyö ulkoistettu kumppaneille vai hoidetaanko se omana tietohallinnon työnä.

Yhtymän toimintaympäristön turvallisuuden varmistaminen ei ole erillinen prosessi, vaan se koostuu useista muista tässä politiikassa kuvatuista prosesseista ja toimenpiteistä, joista keskeisimmät ovat:

- Prosessit, joilla varmistetaan hankintojen ja käyttöönottojen turvallisuus
- Turvallisuuden varmistaminen muutostilanteissa
- Systemaattinen riskienhallinta sisältäen uusien digitaaliseen turvallisuuteen liittyvien riskien tunnistamisen
- Häiriöhallinnan yhteydessä tehtävä häiriön syyn arviointi ja juurisyyn poisto.

Toimintaympäristön kokonaisturvallisuus riippuu tulevaisuudessa entistä enemmän ympäristön eri osien yhteen toimivuudesta sekä toimintaprosessien turvallisuudesta. Siten kaikki toimintaympäristön turvallisuuteen liittyvät tarkastelut tehdään laaja-alaisesti ottaen huomioon kaikki muut kohteet, joihin turvallisuusongelma saattaa vaikuttaa.

Henkilöstöturvallisuus

Henkilöstöturvallisuuden prosessien avulla varmistetaan yhtymän henkilöstön sekä yhtymälle palveluita tuottavien muiden organisaatioiden henkilöiden työskentelyn turvallisuus. Henkilöstöturvallisuus kattaa koko yhtymässä työskentelyn elinkaaren. Yhtymän vastuulla olevien luottamuksellisten tietojen salassapitovelvollisuus jatkuu myös sen jälkeen, kun henkilö on lopettanut työskentelyn yhtymän palveluksessa.

Ennen työsuhteen alkua tehtävien taustatarkastusten ja työsuhteen alkaessa allekirjoitettavan ”Tietoturva- ja tietosuojasitoumuksen” avulla varmistetaan työntekijän soveltuvuus ja sitoutuminen turvallisuuteen. Työsuhteen päättyessä varmistetaan, että henkilö tietää salassapitovelvollisuuksien jatkumisen myös työsuhteen tai toimeksiannon päättymisen jälkeen.

Laajin henkilöstöturvallisuuden osa-alue on työsuhteen aikana tehtävät toimenpiteet, joiden avulla varmistetaan, että yhtymälle työskentelevät henkilöt ovat tietoisia digitaaliseen turvallisuuteen liittyvistä vastuista ja niihin liittyvistä velvoitteista. Yhtymässä henkilöstön turvallista työskentelyä varmistetaan seuraavilla keinoilla:

- Turvallisuusohjeilla, joissa on kuvattu, miten eri tilanteissa tulee toimia.
- Koulutusaineistoilla, joiden avulla henkilöstö voidaan kouluttaa ja perehdyttää turvallisuuteen.
- Perehdytyksillä, joiden avulla uudet henkilöt sekä tehtäviä vaihtavat henkilöt perehdytetään yleisiin ja tehtäväkohtaisiin turvallisuusohjeisiin ja käytäntöihin.
- Säännöllisillä koulutuksilla, joiden avulla ylläpidetään turvallisuusosaamista yhtymässä.
- Osaamistasotesteillä, joiden avulla varmistetaan tietoturva- ja tietosuojaohjeiden osaaminen ja selvitetään osaamiseen liittyviä puutteita.
- Tehtyjen virheiden seurannalla, jonka avulla selvitetään osaamiseen liittyviä puutteita.
- Säännöllisellä viestinnällä ja kohdennetulla tiedottamisella, joilla varmistetaan riittävä tietoisuus digitaalisen turvallisuuden merkityksestä ja siihen liittyvistä käytännöistä.
- Johdon esimerkillä ja viestinnällä, joilla varmistetaan henkilöstön oikea asenne turvallisuuteen.

- Esimiesten ja avainhenkilöiden työskentelyllä, jolla tuetaan turvallisuusosaamisen jalkauttamista päivittäiseen työhön.
- Potilas- ja asiakastiedon käytön asiakasaloitteisella- ja omavalvonnalla.
- Kurinpitoprosessilla, jonka mukaisesti käsitellään havaitut väärinkäytökset.

Lisäksi työsuhteen päättyessä varmistetaan kaikkien työntekijän hallussa ja käytössä olleiden resurssien (esimerkiksi avaimet, laitteet, käyttäjätunnukset jne.) pois ottaminen sekä niiden käytöstä poistaminen työntekijän hallusta. Keskeinen vastuu tästä on työntekijän esimiehillä.

5.3 Jatkuvuudenhallinta, seuranta ja jatkuva parantaminen

Jatkuvuudenhallinta

Jatkuvuudenhallinnan avulla varmistetaan, että yhtymän toiminta voi jatkua riittävän turvallisesti myös poikkeustilanteissa. Koska toiminnan häiriöttömyyden 100% varmistaminen ei ole mahdollista kohtuullisilla kustannuksilla, on asianmukaisesti hoidettu jatkuvuuden hallinta välttämätöntä riittävän turvallisuuden varmistamiseksi.

Jatkuvuuden hallinnan varmistamiseksi yhtymässä toteutetaan seuraavat toimenpiteet:

- Määritellään digitaalista turvallisuutta poikkeustilanteissa koskevat vaatimukset.
- Laaditaan suunnitelmat poikkeustilanteiden hoitamista varten sisältäen turvallisuuden varmistamisen poikkeustilanteiden yhteydessä.
- Varmistetaan kyky toimia turvallisesti poikkeustilanteissa katselmointien ja testausten avulla.

Keskeinen osa jatkuvuudenhallintaa on riittävä harjoittelu. Yhtymän kyvykkyyttä toimia vaatimusten mukaisesti erilaisissa häiriö- ja poikkeustilanteissa tulee harjoitella säännöllisesti ja kattavasti. Harjoittelun avulla saavutetaan seuraavia hyötyjä:

- Rutiinien kehittyminen poikkeustilanteisiin
- Vastuiden ja päätöksenteon selkeyttäminen
- Prosessien ja dokumentoinnin puutteiden tunnistamien ja korjaaminen.

Häiriöhallinta

Osana jatkuvuudenhallinnan kokonaisuutta on häiriöiden hallinnan prosessi, jonka avulla käsitellään suunnitelmallisesti havaitut digitaaliseen turvallisuuteen liittyvät häiriötilanteet. Systemaattinen häiriöhallintaprosessi auttaa havaitsemaan ja ratkaisemaan häiriöt tehokkaasti ja pienentämään häiriöistä seuraavia haittoja.

Häiriöhallintaprosessi sisältää seuraavat vaiheet:

- Häiriön havaitseminen ja ilmoittaminen
- Häiriön arviointi ja päätöksenteko arvion perusteella
- Häiriövaste – eli häiriön edellyttämien välittömien toimenpiteiden toteutus
- Häiriöviestintä ja ilmoitukset viranomaisille
- Häiriöstä oppiminen – eli häiriön taustalla olevien syiden tunnistaminen ja kehittämistoimenpiteiden käynnistäminen syiden poistamiseksi.

Mikäli häiriö arvioidaan erityisen vakavaksi, käynnistetään vakavien häiriötilanteiden käsittelyprosessi.

Seuranta ja raportointi

Turvallisuuden seurantaa varten määritellään seurattavat kohteet, mittarit ja tavoitearvot. Seurannan käytännön toteuttamiseksi määritellään vastuut ja prosessit pyrkien mahdollisimman helppoon ja automaattiseen seurantatiedon keräämiseen.

Seurantatiedot kootaan yhteen ja raportoidaan määräajoin. Raportoinnissa pyritään seurantakohteittain esittämään seuraavia näkökulmia:

- Kohteen turvallisuuden tila esitettynä mitattujen arvojen ja tavoitearvojen avulla
- Kohteen turvallisuuden muutokset ja trendit
- Vertailutietoja muiden yksiköiden ja toimijoiden tietojen avulla
- Sanalliset arviot, joilla täydennetään numeerisia tietoja
- Ehdotukset kehittämistoimenpiteistä.

Seurantaa ja raportointia kohdistetaan sekä digitaalisen turvallisuuden toteutumiseen että tehtyihin toimenpiteisiin. Seurattavat kohteet valitaan siten, että niiden avulla saadaan kokonaiskuva yhtymän turvallisuudesta.

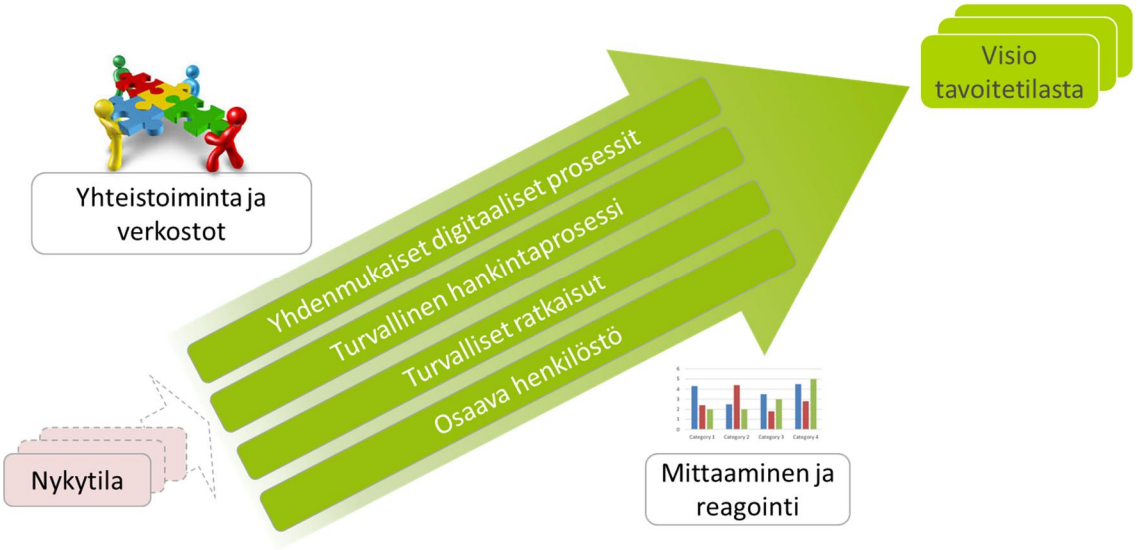
Jatkuva parantaminen

Digitaalista turvallisuutta sekä sen hallintaa kehitetään jatkuvasti havaittujen puutteiden, seurannan tulosten ja tunnistettujen riskien perusteella. Eri tilanteissa vaadittavat kehittämistoimenpiteet voivat vaihdella yksittäisestä välittömästi suoritettavasta toimenpiteestä aina laajamittaiseen kehittämisprojektiin.

6 Digitaalisen turvallisuuden kehittäminen

Digitaalisen turvallisuuden kehittäminen on jatkuva prosessi, jonka avulla yhtymän digitaalista turvallisuutta kehitetään vaiheittain kohti visiota tavoitetilasta. Kehittämistyö koostuu eri projekteista, jotka suunnitellaan ja aikataulutetaan vuositasolla laadittaviin digitaalisen turvallisuuden kehittämissuunnitelmiin.

Digitaalisen turvallisuuden kehittämisen keskeisimmät aihepiirit ovat prosessien yhdenmukaistaminen ja digitalisointi, turvallinen hankintaprosessi, toteutettavien ratkaisujen turvallisuus sekä henkilöstön osaamisen kehittäminen. Digitaalisen turvallisuuden kehittämistä tukevat yhteistoimintamallit, verkostojen hyödyntäminen sekä kehittämisen mittaaminen ja havaittuihin puutteisiin reagointi.



Kuva 3, digitaalisen turvallisuuden kehittäminen.

6.1 Yhteistoiminta ja verkostot

Digitaalisen turvallisuuden onnistunut toteuttaminen edellyttää useiden erityyppisten vaatimusten huomioon ottamista. Tämä edellyttää organisointia siten, että kaikki ne osapuolet, joita kehittämisprojekti tai hankinta koskee pääsevät vaikuttamaan. Tällaisia osapuolia ovat:

- Yhtymän kokonaisarkkitehtuurista ja ratkaisujen yhteen toimivuudesta vastaava tietohallinto
- Kaikki ne substanssiyksiköt, joiden toimintaan kehittämisprojekti vaikuttaa
- Organisaation turvallisuuden eri näkökulmista vastaavat tahot
- Sidosryhmät ja asiakkaat.

Kehittämisprojektin omistajan vastuulla on huolehtia siitä, että eri osapuolet ovat riittävästi edustettuna ja, että eri osapuolten näkökulmat otetaan asianmukaisesti huomioon. Ennen projektin käynnistämistä on arvioitava mahdollisuus kehittää tai hankkia ratkaisu yhteistyössä ulkoisten sidosryhmien kanssa.

Yhteistoiminnan tavoitteena on kehittää mahdollisimman hyvin organisaation kokonaisetua palvelevia ratkaisuja, välttää päällekkäisiä investointeja sekä varmistaa että lopputulos on turvallisuuden, käytettävyyden ja yhteentoimivuuden kannalta optimaalinen.

Yhtymässä kehitetään hankinta ja projektinhallintamenettelyt, joiden avulla yllä kuvatut yhteistoimintatavoitteet saadaan käytännössä toteutettua.

6.2 Yhdenmukaiset digitaaliset prosessit

Toimintaprosessit yhdenmukaistetaan ennen niitä tukevien digitaalisten ratkaisujen kehittämistä. Yhdenmukaistamisella tarkoitetaan erityisesti sitä, ettei samoja asioita tehdä usealla eri tavalla.

Toimintaprosessit suunnitellaan digitaalisiksi ennen niitä tukevien ratkaisujen kehittämistä. Prosessien digitalisointi tarkoittaa tässä yhteydessä sitä, että paperimuodossa toteutettavat vaiheet muutetaan digitaalisiksi.

Prosessien yhdenmukaistaminen ja digitalisointi voidaan toteuttaa seuraavan vaiheistuksen mukaisesti:

1. Tunnistetaan yhdenmukaistettavat ja digitalisoitavat prosessit ja käytännöt. Tällaisia voivat olla esimerkiksi:
    - Henkilöiden tunnistamiseen liittyvät prosessit
    - Käyttöoikeuksien hallintaan liittyvät prosessit
    - Tietojen kirjaamisen menettelyt
    - Väliaikaiseen tietojen tallentamiseen liittyvät menettelyt
    - Olemassa olevan informaation hakemiseen ja hyödyntämiseen liittyvät menettelyt
    - Tietojen vaihtoon eri palvelutuottajien kanssa käytettävät prosessit
    - Lokitietojen keruuseen ja seurantaan liittyvät menettelyt.
2. Ideoidaan ja suunnitellaan prosessit eri osapuolten yhteistyössä ottaen huomioon turvallisuusnäkökulmat heti kehittämistyön alkuvaiheessa
3. Toteutetaan tarvittavat digitaaliset ratkaisut.

Prosessien yhdenmukaistamisen syynä ovat sekä kustannukset että turvallisuus. Mikäli käytössä on useita toisistaan poikkeavia prosesseja, on niiden omaksuminen vaikeampaa ja niitä tukevien tietojärjestelmäratkaisujen kehittäminen kalliimpaa.

Prosessien kattavan digitalisoinnin perusteena ovat kustannus- ja turvallisuusnäkökulmat. Osittain digitalisoidut prosessit ovat usein monimutkaisia ja kalliita toteuttaa sekä helposti alttiita erilaisille tietoturvauhkille. Täysin digitalisoitu toimintaprosessi mahdollistaa huomattavasti paremman tietojen saatavuuden. Tässä yhteydessä on myös syytä tarkastella jatkuvuuden näkökulmaa – digitaalisia ratkaisuja täydentäviä paperipohjaisia toimintatapoja saatetaan väliaikaisesti tarvita normaalista poikkeavissa tilanteissa.

6.3 Turvallinen hankintaprosessi

Jokaisessa hankinnassa ja kehittämisprojektissa tulee varmistaa digitaalisen turvallisuuden toteutuminen. Varmistaminen edellyttää seuraavien vaiheiden toteuttamista:

- Digitaaliseen turvallisuuteen liittyvien vaatimusten määrittely. Hankinnoissa hyödynnetään valmiita vaatimuspohjia, joiden avulla täsmennetään hankintaa koskevat yksityiskohtaiset vaatimukset
- Vaatimusten toteutumisen varmistaminen, joka voi sisältää katselmointeja, toimittajan suorittamia testauksia sekä yhtymän suorittamia testauksia
- Turvallinen käyttöönottoprosessi
- Kehitettävän ratkaisun turvallisen käytön edellyttämien käyttö- ja toimintaohjeiden olemassaolon varmistaminen
- Käyttäjien ja pääkäyttäjien perehdyttäminen
- Perehdytys-, koulutus-, häiriöhallinta- ja seurantaprosessien täydentäminen tarvittaessa uuden ratkaisun osalta.

6.4 Turvalliset ratkaisut

Digitalisoituvassa toimintaympäristössä ratkaisuihin kohdistuu uudenlaisia turvallisuushaasteita. Alla on kuvattu ratkaisujen turvallisuuteen vaikuttavia näkökohtia, jotka tulee ottaa huomioon määriteltäessä hankittavien järjestelmien, laitteiden ja palveluiden turvallisuusvaatimuksia:

- Digitaalisten palveluiden käyttöympäristöjen muutos. Pyritään ratkaisuihin, jotka ovat turvallisia, vaikka fyysistä turvallisuutta ei voida taata, kuten kotiin vietävät järjestelmät.
- Varaudutaan kasvaviin resurssitarpeisiin turvallisuuden ylläpitämisessä. Päivitettäviä laitteita ja järjestelmiä tulee olemaan jatkuvasti enemmän ja niiden suojaaminen vaatii enemmän työtä. Ratkaisut suunnitellaan mahdollisimman helposti ja keskitetysti ylläpidettäviksi.
- Kehitetään turvallisuuden valvontaan liittyviä ratkaisuja, jotka tukevat sekä automaattista havainnointia että jälkikäteistä ongelmien selvittämistä. Esimerkkeinä tällaisista ratkaisuista ovat keskitettyyn lokitietojen valvontaan ja analysointiin tarkoitetut SIEM-järjestelmät (Security Information and Event Management) sekä keskitetyt kyberturvallisuuden valvomoratkaisut, CSOC (Cyber Security Operations Center).
- Arkkitehtuurissa vältetään suuria yksittäisiä, hankalasti vaihdettavissa olevia järjestelmiä ja korostetaan mikropalveluarkkitehtuureja, joissa yksittäisiä komponentteja voidaan vaihtaa helpommin.

6.5 Osaava henkilöstö ja kumppanit

Osana digitaalisen turvallisuuden kehittämistä tulee varmistaa, että kaikilla työntekijöillä on riittävät edellytykset toimia turvallisesti hyödynnettäessä uudenlaisia digitaalisia toimintaympäristöjä.

Lähtökohtana turvalliselle työskentelylle digitaalisissa toimintaympäristöissä on henkilöstön riittävä tietoisuus ja osaaminen turvallisuusasioista. Niiden varmistaminen on kuvattu luvun 5.2 kohdassa ”Henkilöstöturvallisuus”.

Tämän lisäksi jokaisen uuden järjestelmän ja toimintaprosessin käyttöönoton yhteydessä varmistetaan sitä hyödyntävien henkilöiden riittävä osaaminen ohjeistamalla ja perehdyttämällä henkilöt uuden ratkaisun käyttöön ja käytön turvallisuusseikkoihin.

Osaamisen kehittämistä varten hankitaan tarvittavassa laajuudessa erilaisia teknisiä ratkaisuja, kuten verkkokoulutus- ja itseopiskeluympäristöjä sekä osaamisen testaukseen liittyviä työkaluja.

Varmistetaan ulkoisten kumppanien asiantuntijoiden osaamisen taso yhteistyösopimusten ja työn jatkuvan seurannan kautta. On erityisen tärkeää pitää koordinointilangat riittävästi omissa tilaajan käsissä, vaikka varsinainen operatiivinen tekeminen olisi ulkoistettu kumppaneille.

6.6 Mittaaminen ja reagointi

Osana digitaalisen turvallisuuden kehittämistä toteutetaan systemaattinen seuranta ja mittaaminen digitaalisen turvallisuuden toteutumisesta yhtymän toiminnan eri osa-alueilla. Seurannan ja mittaamisen avulla varmistetaan, että kehittämistoiminnan avulla on saavutettu halutut tulokset.

Kehittämistoimintaan liittyvä mittaaminen ja seuranta voidaan toteuttaa osana digitaalisen turvallisuuden hallinnan seurantaprosesseja, joita on kuvattu 5. luvussa ”Digitaalisen turvallisuuden hallinta”.

Koska digitaalisen turvallisuuden kehittäminen on hyvin merkittävä osa digitaaliseen turvallisuuteen tehtävää kokonaispanostusta, kannattaa digitaalisen turvallisuuden seurannassa ja mittaamisessa painottaa uusia toimintaprosesseja ja uusia digitaalisia ratkaisuja.

7 Yhteenveto

Digitaalisen turvallisuuden politiikka sisältää tietoturvallisuuteen, tietosuojaan, kyberturvallisuuteen, riskienhallintaan sekä toiminnan jatkuvuuteen liittyviä ylätason linjauksia, jotka ohjaavat niihin liittyvien käytännön prosessien suunnittelua. Tämä politiikka korvaa Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän syksyllä 2012 voimaan astuneen tietoturvallisuuspolitiikan.

Digitaalisen turvallisuuden tavoitteena on varmistaa tietojen sekä niihin liittyvien digitaalisten palveluiden saatavuus, luottamuksellisuus ja eheys riskilähtöisesti ottaen huomioon myös toiminnan jatkuvuuden vaatimukset poikkeustilanteissa.

Päijät-Hämeen hyvinvointiyhtymän toimintaympäristössä tulee tapahtumaan merkittäviä muutoksia lähivuosina. Nämä muutokset edellyttävät yhtymältä määrätietoista, suunnitelmallista ja ennakoivaa reagointia. Digitaalisen turvallisuuden varmistaminen on yksi tärkeä osatekijä tässä kokonaisuudessa.

Tavoitetilassa Päijät-Hämeen hyvinvointiyhtymä on ihmisläheinen, digitaalinen ja turvallinen. Palveluiden tuottamisessa on käytössä yhdenmukaiset toimintamallit sekä yhtymän sisällä että yhteistyökumppaneiden kanssa. Toimintamallit on suunniteltu kokonaan digitaalisista lähtökohdista ja niissä on otettu huomioon digitalisaation tarjoamat mahdollisuudet tehostaa työskentelyä, hyödyntää tietoaineistoja ja palvella asiakkaita.

Digitaalisen turvallisuuden hallinnassa on käytössä tietoturvastandardeja ja kansallisia ohjeistoja soveltava hallintamalli, jonka avulla voidaan varmistaa ja osoittaa digitaaliselle turvallisuudelle asetettujen vaatimusten täyttyminen. Hallintamallin keskeisinä periaatteina ovat riskilähtöisyys ja jatkuva parantaminen.

Digitaalisen turvallisuuden kehittäminen on jatkuva prosessi, jonka avulla yhtymän digitaalista turvallisuutta kehitetään vaiheittain kohti visiota tavoitetilasta. Kehittämistyö koostuu monista eri projekteista, jotka suunnitellaan ja aikataulutetaan vuositasolla laadittaviin digitaalisen turvallisuuden kehittämissuunnitelmiin.

Digitaalisen turvallisuuden kehittämisen keskeisimmät aihepiirit ovat prosessien yhdenmukaistaminen ja digitalisointi, turvallinen hankintaprosessi, ratkaisujen turvallisuus sekä henkilöstön osaamisen kehittäminen. Digitaalisen turvallisuuden kehittämistä tukevat yhteistoimintamallit, verkostojen hyödyntäminen sekä kehittämisen mittaaminen ja havaittuihin puutteisiin reagointi hyvissä ajoin.

OIKAISUVAATIMUSOHJEET **Liitetään pöytäkirjanotteeseen**
Päijät-Hämeen hyvinvointikuntayhtymä Kunnallisasiat

Oikaisuvaatimus-oikeus	Päätökseen tyytymätön voi tehdä kirjallisen oikaisuvaatimuksen. Oikaisuvaatimuksen saa tehdä se, johon päätös on kohdistettu tai jonka oikeuteen, velvollisuuteen tai etuun päätös välittömästi vaikuttaa (asianosainen) sekä kunnan jäsen.

Oikaisuvaatimus-viranomainen	Viranomainen, jolle oikaisuvaatimus tehdään ja sen yhteystiedot **Toimielin:** **Päijät-Hämeen hyvinvointikuntayhtymän hallitus** **Postiosoite:** **Keskussairaalankatu 7, 15850 Lahti** **Puh.:** **(03) 819 11** **Sähköpostiosoite:** **kirjaamo@phhyky.fi** **Aukioloaika:** **klo 9-15**
Oikaisuvaatimusaika ja sen alkaminen	Oikaisuvaatimus on tehtävä 14 päivän kuluessa päätöksen tiedoksisaannista ennen viraston aukioloajan päättymistä. Kunnan jäsenen katsotaan saaneen päätöksestä tiedon, kun pöytäkirja on asetettu yleisesti nähtäväksi. Annettaessa päätös asianosaiselle tiedoksi hänen suostumuksellaan sähköisenä viestinä hänen katsotaan saaneen päätöksestä tiedon kolmantena päivänä viestin lähettämisestä, jollei muuta näytetä. Muuta tiedoksiantotapaa käytettäessä asianosaisen katsotaan saaneen päätöksestä tiedon, jollei muuta näytetä, seitsemän päivän kuluttua kirjeen lähettämisestä, saantitodistuksen osoittamana aikana tai erilliseen tiedoksisaantitodistukseen merkittynä aikana. Oikaisuvaatimusaika taloudellisin ja tuotannollisin perustein tehdystä irtisanomista koskevasta päätöksestä alkaa kulua vasta irtisanomisajan päättymisestä.

Pöytäkirjan nähtäväksi asettaminen	**Pvm:** 1.4.2019
Kuntalain 95 §:n 1 momentin mukainen erityistiedoksianto asianosaiselle	Asianosainen: tietoturvapäällikkö Antti-Olli Taipale, tulosaluejohtaja Petri Pekkala ☒ Annettu tiedoksi sähköisesti, pvm: ☐ Lähetetty tiedoksi kirjeellä, joka on annettu postin kuljettavaksi, pvm: (kuntalaki 95 §) Tiedoksiantaja: ☐ Luovutettu asianosaiselle Paikka ja pvm: _____ Vastaanottajan allekirjoitus ☒ Muulla tavoin, miten Tweb 1.4.2019
Oikaisuvaatimuksen sisältö ja sen toimittaminen	Oikaisuvaatimuksesta on käytävä ilmi vaatimus perusteluineen sekä sen tekijä ja yhteystiedot. Oikaisuvaatimus on toimitettava oikaisuvaatimusviranomaiselle oikaisuvaatimusajan kuluessa ennen sen viimeisen päivän virka-ajan päättymistä riippumatta tavasta, jolla se toimitetaan. Jos oikaisuvaatimusajan viimeinen päivä on pyhäpäivä, itsenäisyyspäivä,

	vapunpäivä, joulu- tai juhannusaatto tai arkilauantai, saa oikaisuvaatimuksen toimittaa ensimmäisenä sen jälkeisenä arkipäivänä. Omalla vastuulla oikaisuvaatimuksen voi lähettää postitse tai lähetin välityksellä. Postiin oikaisuvaatimus on jätettävä niin ajoissa, että se ehtii perille oikaisuvaatimusajan viimeisenä päivänä ennen viraston aukioloajan päättymistä.