Yhteistyötoimikunta 23.5.2019 § 6
Henkilöstöjaosto 24.5.2019 § 16
Hyväksytty Johtokunta 19.8.2019 § 86

Tietoturva- ja tietosuojapolitiikka

Suupohjan peruspalvelu-liikelaitoskuntayhtymä

Hallintoaukio • PL 100, 61801 KAUHAJOKI • (06) 2413 2000 • www.llky.fi

Sisällys

1. JOHDANTO

Tieto on keskeisessä roolissa organisaatioiden toiminnassa ja palvelutuotannossa. Tiedon tulee olla hyödynnettävissä tarpeen mukaisesti ja tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tietojenkäsittelyn turvallisuus, luotettavuus ja virheettömyys on tärkeää toiminnan jatkuvuuden sekä palveluiden laadun ja tehokkuuden kannalta.

Tietosuoja suojaa ihmisten yksityisyyttä (tunnistettavuutta). Inhimillisenä toimintana tietojenkäsittelyyn liittyy aina riskejä, joita pyritään minimoimaan ohjeistuksilla, koulutuksella ja teknisillä ratkaisuilla. Tietoturvariskeistä pystytään minimoimaan teknisin ratkaisuin vain osa, tärkeintä ovat päivittäisessä tietojenkäsittelyssä tehdyt ratkaisut ja toimenpiteet.

Tietoturva suojaa henkilötietoja ja muita tietoja luvattomalta käytöltä. Tietoturva käsittää keskeisiin toimintoihin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky hallita ennakoivasti uhkia ja tarvittaessa sietää niiden vaikutuksia. Riskien tunnistamisen ja hallinnan sekä vaikutusten minimointi on osa organisaation aktiivista tietoturvan toteuttamista.

Poikkeamatilanteisiin varautumisen ensisijainen vastuu on organisaation ylimmällä johdolla. Johdon on varmistettava tietoturvatyön riittävä resursointi ja seuranta. Johtokunnan hyväksymä tietoturva- ja tietosuojapolitiikka ilmaisee sitoutumisen tietoturvatyöhön ja siihen liittyvien tehtävien organisointiin. Panostaminen tietoturvaan sekä yleisellä että tekniikan tasolla ovat strategisia päätöksiä, joilla vaikutetaan myös organisaation toimintakykyyn. Edut ovat häiriötön toiminta, toiminnan laatu ja positiivisen julkisuuskuvan säilyminen, myös lainsäädäntö edellyttää tietoturvasta huolehtimista. Tietoturvan ja tietotietotekniikan ammattilaisilla on keskeinen merkitys johdon neuvonantajina.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi ja sitä voidaan tarvittaessa täydentää tai päivittää, kuten lainsäädännön tai muiden ohjeistusten muuttuessa.

Tietoturva- ja tietosuojapolitiikka on julkinen asiakirja.

2. TIETOTURVA- JA TIETOSUOJAPERIAATTEET

Tietoturvatyö on osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutuminen varmennetaan vuosittain tietoturvaorganisaation raportoinnilla johdolle ja toimintakertomukseen tulevalla maininnalla tehdyistä toimenpiteistä.

Tietoturva- ja tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan tietoturvallisuuden toteuttamiseksi ja kehittämiseksi, sitä sovelletaan kaikessa toiminnassa ja koko henkilöstöön sekä sidosryhmiin. Tarkoituksena on varmistaa lainmukaiset ja yhdenmukaiset käytännöt.

Tietoturvaperiaatteita noudatetaan kaikissa tiedon elinkaaren vaiheissa ja tämän edistämiseksi tietoturva- ja tietosuojaperiaatteet ovat osa henkilöstön perehdytystä ja koulutusta. Teknisin ratkaisuin varmistetaan toiminnan ja työtehtävän kannalta tarpeellisten tietojen käsittely.

Tietoturvaan kuuluvat lisäksi muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen, tilojen ja toiminnan turvaaminen. Tietoturva kokonaisuutena muodostuu tietoturvasta ja tietosuojasta sekä näiden suunnittelusta ja hallinnasta.

Suupohjan peruspalveluliikelaitoskuntayhtymä on liittynyt kansalliseen KanTa-palveluun, johon sisältyy sähköinen potilastiedon arkisto (eArkisto) ja reseptikeskus (eResepti). Palveluun liittyminen on lakisääteinen ja laatuvaatimuksena on muun muassa Sosiaali- ja terveysministeriön asettamien auditointivaatimusten täyttyminen.

Yksityiskohtaisemmat toimintaohjeet löytyvät Henkilöstön tietoturvaohjeesta ja toimialuekohtaisista lisäohjeista ja määräyksistä. Nämä asiakirjat tulee antaa tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle.

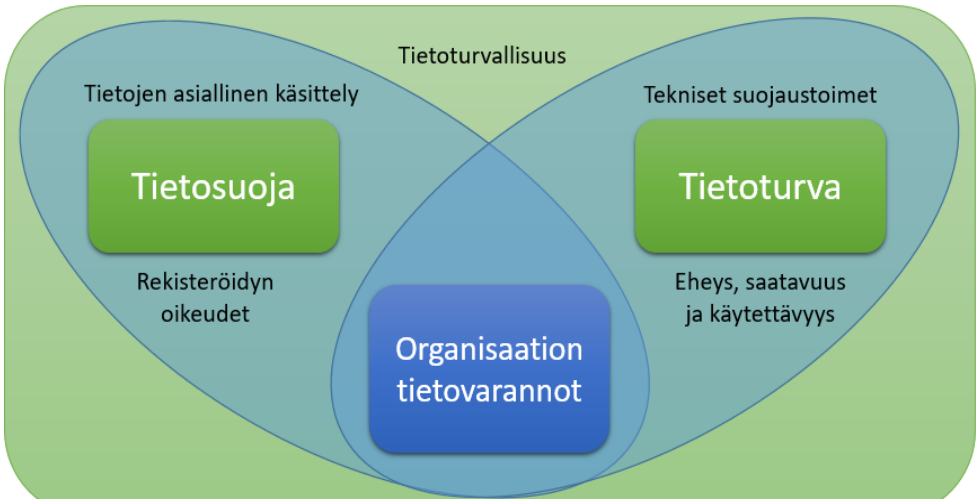
3. TIETOTURVA

Tietoturvasta tulee huolehtia asianmukaisesti ja sillä tarkoitetaan tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Tietoturvasta huolehtiminen on osa organisaation riskienhallintaa, sisäistä valvontaa ja turvallisuusjohtamista. Tietoturvatoimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä.

Tietoturvallisen toiminnan tulee olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella. Tämän tavoitteen toteutuminen edellyttää jokaiselta vastuullista toimintaa ja teknisen ympäristön ja tietoturvallisuuden ohjauksen ajantasaisuutta.

Tietoturva koostuu:

- **Tiedon luottamuksellisuudesta**, eli siitä, että tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla eivätkä ne päädy ulkopuolisten tietoon
- **Tiedon eheydestä,** joka tarkoittaa tietojen muuttumattomuutta tai säilyvyyttä laitteisto- tai järjestelmävian tai inhimillisen toiminnan vuoksi
- **Tiedon saatavuudesta,** jolloin tieto on oikeutettujen henkilöiden saatavilla tai käytettävissä silloin kun niitä tarvitaan.
- **Todentamisesta ja kiistämättömyydestä**, joilla tarkoitetaan käyttäjän todentamista ja käyttäjien tietojen käytön kiistämätöntä todistamista



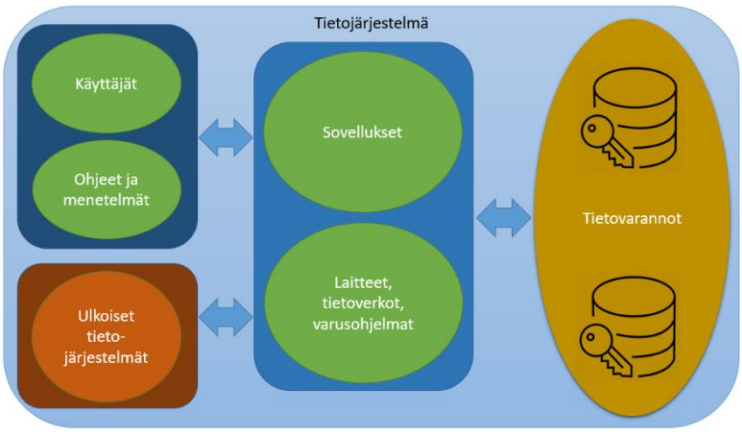
Kuva 1: Tietoturvallisuus

Tietoturvatoimien päämääränä on turvata toiminnalle tärkeiden järjestelmien, tietoverkkojen sekä palveluiden keskeytymätön toiminta sekä varmistaa tiedon olevan saatavilla ja hyödynnettävissä siihen oikeutetuille riittävän esteettömästi, vaivattomasti ja nopeasti. Luottamuksellisiin tietoihin pääsy ja tietojen tahaton tai tahallinen tuhoaminen tai vääristyminen pyritään tietoturvatoimenpitein estämään. Samalla varmistetaan, että tietoja käsitellään lakien, asetusten ja sopimusten mukaisesti. Näiden toteutumisessa tärkeä osa on henkilöstön koulutus ja sitoutuminen hyvän tietoturvan toteuttamiseen.

Tietojärjestelmien teknisen ympäristön ja ohjelmistojen sekä laitteiden ylläpito on ulkoistettu, yhtiö vastaa sopimuksen mukaisesti tietoturvan toteutumisesta lain ja asetusten sekä rekisterinpitäjän ohjeiden mukaisesti.

3.1. Tietojärjestelmä

Tietojärjestelmä on kokonaisuus joka koostuu tietovarannoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, tietojen käyttöä määrittävistä ohjeista, käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Tietojärjestelmään kuuluu oleellisena osana käsiteltävien tietojen turvallisuus ja tietoturvan yleinen hallinta ja valvonta. Poikkeama missä tahansa kokonaisuuden osassa merkitsee häiriötä järjestelmän toiminnassa.



Kuva 2: Tietojärjestelmä

Tärkeitä periaatteita tietoturvan toteutuksessa ovat:

- Kaikki organisaation hallussa olevat tiedot, sähköiset tai manuaaliset, sekä tietovälineet ja laitteet ovat organisaation omaisuutta ja niitä tulee käsitellä ohjeiden mukaisesti,
- Tietojen säilytystä ohjaavat arkistolaki sekä erilliset ohjeet ja asetukset.
- Henkilöstön kouluttaminen ja ohjeistuksen ajantasaisuus.
- Kirjalliset tietoturvaohjeet, jotka annetaan tiedoksi jokaiselle työntekijälle ja jotka ovat saatavilla intranetissä.
- Tietoturvasta annettujen ohjeiden noudattaminen ja jokaisen työntekijän vastuu toiminnastaan.

3.2. Tietoturvan hallinnolliset periaatteet

Hallinnollinen tietoturva on tietoturvatoimintojen johtamista ja organisointia, sillä tarkoitetaan tietoturvatoimien, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Tavoitteena on sekä tietoturvan toteutuminen että johdon ja henkilöstön sitoutuminen sen suunnitelmalliseen hoitamiseen ja kehittämiseen.

Hallinnollinen tietoturva pyrkii ennakoimaan riskit sekä arvioimaan ja hallitsemaan riskien mahdollisia vaikutuksia.

Hallinnollisen tietoturvan periaatteet:

- Suupohjan peruspalveluliikelaitoskuntayhtymä noudattaa toimintaansa ohjaavia lakeja ja asetuksia sekä kehittää toimintaansa viranomaissuositusten, valtakunnallisten tietojärjestelmäpalveluiden asettamien tietoturvavaatimusten ja tietoturvakäytäntöjen mukaiseksi.
- Tietoturva huomioidaan organisaation ja eri osapuolten välisissä sopimuksissa ja tietoturva- ja tietosuojapolitiikka tuodaan näille toimijoille tiettäväksi.
- Tietoturvaan liittyvillä tehtävillä on omat vastuuhenkilöt, jotka tiedotetaan organisaatiossa työskenteleville ja sidosryhmille. Vastuuhenkilöillä on resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät. Vastuuhenkilöistä tarkemmin luvussa Vastuut ja organisointi.
- Tietoturvan eri osa-alueiden tilannetta seurataan säännöllisesti raporteilla ja valvontajärjestelmillä sekä erikseen tehtävillä riskikartoituksilla. Havaintojen pohjalta tehdään tarvittaessa tietoturvan kehittämissuunnitelma, jonka johto hyväksyy.
- Tietoturvatietämyksen ajan tasalla pysymisestä huolehditaan koulutuksen, tiedotuksen, ohjeistuksen ja motivoinnin keinoin.
- Palveluiden hankinnoissa edellytetään tiedon käsittelyyn liittyvien suojatoimien, vastuiden ja teknisten tietoturvavastuiden sisältyvän palvelusopimuksiin, lisäksi on huomioitava henkilötietojen käsittelystä sopiminen silloin kun palveluun liittyy henkilötietojen käsittelyä. Palveluntuottajan on toimitettava tarvittavat dokumentit ja pidettävä ne ajan tasalla.
- Ohjelmistojen ja laitteiden tarjouspyynnöissä ja hankinnoissa edellytetään voimassa olevien standardien ja säännösten noudattamista ja ennen hankintapäätöksiä tehtyä tietoturvallisuusnäkökohtien arviointia.

3.3. Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöiden toimista johtuvien ja heihin kohdistuvien tietoturvauhkien hallintaa. Tavoitteena on luotettava ja tehtäväänsä soveltuva henkilöstö, joka tuntee oman roolinsa mukaisesti hänelle asetetut tietoturvallisuusvaatimukset. Henkilöstön ja organisaatiolle ostopalveluita tuottavien henkilöiden ja toimijoiden tulee noudattaa tietoturvallisia toimintatapoja tehtävässään.

Pelkkä henkilöstölle suunnattu ohjeistus ei yksinään riitä kattamaan lain velvoitteita, vaan henkilökunnan koulutus ja valmennus on tärkeä osa henkilökunnan tietoturvallisuustietoisuuden ylläpidossa. Erityisesti se on tärkeää uusien järjestelmien, ohjeiden ja lainsäädännön yhteydessä. Koulutuksessa ja ohjeistuksissa tulee huomioida eri kohderyhmien tarpeet.

Henkilöstöturvallisuuden periaatteet

- Esimiehet vastaavat henkilökunnan perehdyttämisestä tietoturvan vaatimuksiin ja annettujen tietoturvaohjeiden ja käytäntöjen noudattamisesta sekä tietoturvan ja tietosuojan verkkokoulutuksen suorittamisesta.
- Henkilöstön tehtäväkuvauksia ylläpidetään ja niiden perusteella myönnetään tehtävän edellyttämät henkilökohtaiset käyttöoikeudet järjestelmiin.
- Jokainen työntekijä ja viranhaltija sitoutuu noudattamaan tietoturvatyöryhmän hyväksymää, liitteen 1. mukaista salassapitovelvoitetta.
- Käyttöoikeudet myönnetään esimiehen ilmoittamien työtehtävien mukaisesti.
- Käyttöoikeuden myöntäminen edellyttää henkilöllisyyden luotettavaa varmistamista.
- Tietojärjestelmien käyttäjistä ylläpidetään rekisteriä, josta ilmenee yksilöintitietojen lisäksi käyttäjän työrooli. Ostopalveluiden tuottajista tai muista organisaation tietojärjestelmiä käsittelevistä, kuten opiskelijoista, edellytetään vastaavan kuvauksen ylläpitoa.

- Työnkuvissa on huolehdittu, ettei synny tilanteita tai käyttöoikeuksia, jotka mahdollistavat tietojen käsittelyn ilman toisen työntekijän mahdollisuutta kontrolloida käsittelyä (vaaralliset työyhdistelmät).
- Organisaation toiminnan kannalta kriittisten järjestelmien vastuuhenkilöillä on nimetyt varahenkilöt.
- Henkilökuntaa koulutetaan tietoturva-asioissa säännöllisesti. Osallistumista koulutukseen ja tietotasoa tietoturvan vaatimuksista seurataan yleisellä tasolla ja tulokset raportoidaan vastuuhenkilöille. Tietosuojavastaava huolehtii verkkokoulutuksen ylläpidosta, seurannasta ja raportoinnista.
- Tietoturvaohjeiden noudattamisen seuranta ja käyttölokivalvonta on säännöllistä ja suunnitelmallista. Tietoturvarikkomukset käsitellään seuranta- ja valvontasuunnitelman mukaisesti. Väärinkäytösten varalle on laadittu seuraamusjärjestelmä.
- Työtehtävien päättyessä tietojärjestelmien käyttöoikeudet ja valvomaton pääsy tiloihin, joissa on yhteys suojattuun tietojärjestelmäympäristöön, päättyvät tehtävien loppuessa.
- Tietoturvaperiaatteiden tiedottaminen sopimuskumppaneille ja sopimusten ajantasaisuus sekä sopimuskumppaneiden tietoturvallisuudesta varmistuminen.

3.4. Fyysinen tietoturva

Fyysinen tietoturva sisältää ne keinot, joilla pyritään suojaamaan organisaation hallussa olevia tietoja ja tietovarantoja fyysisten uhkien, kuten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja luvattomien tai rikollisten toimien seurauksilta. Fyysisen tietoturvan suunnittelussa kartoitetaan ja huomioidaan tärkeimmät suojattavat kohteet ja varmistetaan teknisten järjestelmien toiminta.

Fyysisen tietoturvan periaatteet

- Tilojen lukitseminen
    - Avaimet ovat henkilökohtaisia ja niiden haltijat on rekisteröity
    - Kulunvalvonta
    - Henkilön tunnistaminen ennen pääsyä tiloihin
- Työtehtävään oikeutettua tietoa käytetään vastuullisesti.
- Tärkeiden palveluiden ja prosessien keskeytymättömän toiminnan varmistaminen sekä häiriöihin varautuminen.
- Jatkuvuus- ja toipumissuunnitelmat
- Paikallisverkon käytönvalvonta
- Kameravalvonta
- Kiinteistöturvallisuus, joita ovat mm. paloturvallisuus, kosteudelta ja vedeltä suojaaminen, sähköhäiriöihin varautuminen ja pelastussuunnitelma.

3.5. Tietoaineiston turvallisuus

Tietoaineistoturvallisuudella varmistetaan asiakirja- ja tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito sen elinkaaren kaikissa vaiheissa. Säädösten mukaisesti taltioidut tiedot säilyvät ja ovat saatavissa käyttötilanteen edellyttämässä ajassa, tarkoituksenmukaisessa muodossa ja järjestyksessä ja tietojen hävittäminen tapahtuu säädösten mukaisesti.

Tietojen saatavuus ja käytettävyys varmistetaan teknisin toimin ja estetään tietojen tahaton tai tahallinen tuhoutuminen tai vääristyminen. Teknisillä toimilla pyritään varmistamaan toiminnan

jatkuvuus häiriöttä ja varaudutaan mahdollisista häiriöistä toipumiseen. Samalla varmistetaan mahdollisen sähköisen asioinnin saatavuus, luotettavuus ja kiistämättömyys, joka tarkoittaa sähköisen asioinnin toimintaprosessin huolellista suunnittelua.

Tiedon tallennusmuodosta riippumatta pyritään turvaamaan tietoaineistojen käytettävyys, eheys ja luottamuksellisuus muun muassa seuraavin toimin:

- Henkilökunnan edellytetään tuntevan henkilötietojen käsittelyä ohjaavat ja rajoittavat normit sekä tietojen ja asiakirjojen luokittelu julkisuus- ja salassapitosäännösten mukaisesti.
- Henkilökunnan valmiuksia ylläpidetään ja kehitetään perehdytyksellä, koulutuksella ja tietoturvaohjeistuksin.
- Henkilö- ja potilastietojen käsittelyn edellytyksenä on käyttäjän tehtävästä johtuva asiayhteys asiakkaaseen tai häntä koskeviin tietoihin.
- Henkilö- ja potilastietojen käsittelystä on laadittu palvelualuekohtaisia ohjeita, jotka esim. tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja.
- Tietoaineisto säilytetään arkistonmuodostussuunnitelman mukaisesti. Suunnitelma on laadittu arkistosäädöksiä ja kansallisia tehtäväluokituksia noudattaen.
- Tietoaineiston säilytys luottamuksellisena, eheänä ja muuttumattomana on huomioitu tiedon koko elinkaaren ajalla sen lopulliseen hävittämiseen saakka.
- Tietoaineiston tiedonsaanti- tarkastus- ja korjaamisoikeuden toteuttamista varten on sovittu palvelusta vastaavat henkilöt ja prosessin toteuttamistapa on kuvattu.
- Tietoaineiston käyttämisestä tai luovuttamisesta laskutus-, tilastointi-, raportointi-, kehittämis- ja tutkimustarkoituksiin on annettu ohjeet.
- Valtakunnallisten tietojärjestelmäpalvelujen kautta saatavia tietoja saa käsitellä vain henkilökohtaisilla käyttäjätunnuksilla tai varmennekortilla tunnistautunut henkilö. Tietoaineistojen käyttöä seurataan säännöllisesti ja seurannan periaatteet on käsitelty YT-menettelyn mukaisesti työntekijöiden kanssa.
    - Näiden ohjeiden annosta ja ylläpidosta vastaa kyseinen palvelujohtaja.
- Henkilörekisterin perustamisen ja henkilötietojen käsittelyn tulee olla perusteltua rekisterinpitäjän toiminnan kannalta.
    - Rekisteristä tehdään seloste käsittelytoimista ja tarpeen mukaan vaikutustenarviointi sekä tietosuojaseloste.
- Asiakirjahallinnon ohjeissa on ohjeita tietojen luokittelusta, säilyttämisestä ja hävittämisestä sekä tietojen luovuttamisesta.

Näitä toimia sovelletaan tietoaineiston koko elinkaaren ajan, tiedon syntymisestä sen hävittämiseen.

3.6. Laitteistoturvallisuus

Laitteistoturvallisuudella suojataan organisaation laitteistojen elinkaarta ja turvallista käyttöä, siihen kuuluvat laitteiston asennuksen, suojauksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja sopimukset sekä laitteistojen turvallinen poisto niiden elinkaaren lopussa.

Laitteiden elinkaareen liittyvien palvelusopimusten tulee olla ajan tasalla ja laitteiston elinkaaren päättyessä on huolehdittava tietojen asianmukaisesta tuhoamisesta. Erityisesti tämä koskee tilanteita, joissa ulkoinen palveluntarjoaja huolehtii organisaation laitteista ja järjestelmistä. Tietojärjestelmätoimittajilla ja tietoinfrastruktuurin ylläpitäjällä on omat vastuunsa laitteistoturvallisuuden osalta ja nämä tulee huomioida hankinnoissa ja sopimuksissa.

Laitteistoturvallisuuden periaatteet

- Hankittavien laitteistojen tulee olla kokonaisarkkitehtuurin mukaisia tai muuten yhteensopivia tietojärjestelmäympäristön sekä tietoverkon kanssa. Hankinnat, asennukset ja käytöstä poistot on keskitetty.
- Laitteisto valitaan huomioiden sen käyttöikä ja tietojärjestelmävaatimusten muutoksiin vastaavuus arvioidaan kohtuulliseksi. Lisäksi huomioidaan varaosien, huollon ja vararatkaisujen saatavuus.
- Palvelutoiminnan jatkuvuuden ja palvelutasovaatimusten kannalta kriittiset työasemat sekä oheislaitteet on tunnistettu, näille on järjestetty katkojen aikainen sähkönsyöttö ja riittävä palvelutaso ylläpidossa.
- Kriittisten palvelimien, verkkolaitteiden ja muiden laitteiden kriittisyys johdetaan niissä ylläpidettävien ohjelmistojen ja työasemien kriittisyyden perusteella. Kriittisille laitteistoille taataan katkoton sähkönsyöttö ja ylläpidon korkea palvelutaso.
- Teknisillä toimilla pyritään varmistamaan toiminnan jatkuvuus häiriöttä ja varaudutaan mahdollisista häiriöistä toipumiseen. Samalla varmistetaan mahdollisen sähköisen asioinnin saatavuus, luotettavuus ja kiistämättömyys, joka tarkoittaa sähköisen asioinnin toimintaprosessin huolellista suunnittelua.

3.7. Ohjelmistoturvallisuuden periaatteet

Pääsynhallinnalla ja sen suunnittelulla estetään tietoaineiston, ohjelmien ja järjestelmien luvaton käyttö. Ohjelmistojen tietoturvaan kiinnitetään huomiota jo niiden hankintavaiheessa, jolloin varmistutaan ohjelmistojen tietoturvasta ja vaatimustenmukaisuudesta. Käyttäjät perehdytetään ohjelmistojen käyttöön.

Ohjelmistohankinnat ja kehittäminen perustuvat toiminnan tarpeisiin. Uuden ohjelman hankinnan edellytys on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja arkkitehtuurin kanssa. Lisäksi tulee huomioida EU:n yleisen tietosuoja-asetuksen asettamat vaatimukset.

Huomioitavia asioita ohjelmistoturvallisuuden kannalta ovat:

- Käyttäjähallinta
- Tukipalvelut
- Haittaohjelmien torjunta
- Varmistukset
- Ylläpito
- Jäljitettävyys
- Lisenssien hallinta
- Yhteensopivuus
- Tietoturvallinen asennus

3.8. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus pyrkii varmistamaan viestinnän häiriöttömyyden, tiedonsiirtoyhteyksien käytettävyyden, tiedonsiirron suojaamisen ja salauksen sekä käyttäjien tunnistamisen. Tietoliikenneturvallisuus kattaa tietoverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan, jonka tuloksena ovat turvatut ja luotettavat tiedonsiirtoyhteydet.

Tietoliikenneturvallisuuden periaatteet:

- Erityisluonteisia ja salassa pidettäviä tietoja ei lähetetä salaamattomia yhteyksiä käyttäen organisaation sisällä eikä sen ulkopuolelle.
- Etäyhteydet on toteutettu suojattuna ja vahvaa tunnistusta käyttäen.
- Tietoliikennelokia ja käyttöhäiriöitä valvotaan.
- Tietojärjestelmäympäristö on suojattu palomuurein, joiden toimintaa valvotaan.
- Työtehtäviin tarkoitettujen järjestelmien ja portaalien yhteydet ovat salattuja.
- Tietosuojaa koskevat vaatimukset on määritelty sopimuksin.

3.9. Käyttöturvallisuus

Käyttöturvallisuus tarkoittaa turvallisen käytön toimintaolosuhteita, tekniikan toimivuuden valvontaa, käytön ja lokien valvontaa, ohjelmistotukea, ylläpitoa ja huollon turvallisuustoimenpiteitä, varmuuskopiointia sekä häiriöraportointia.

Tietoturva on suuressa määrin käyttäjien toiminnasta riippuvaista. Tietoturvan perustana on osaava ja sitoutunut henkilöstö sekä ajantasaiset ohjeistukset, joita toiminnassa noudatetaan. Tietojen oikeudeton käyttö estetään tietojen käsittelyn suunnittelulla ja käyttöoikeuksien hallinnalla..

Käyttöturvallisuuden periaatteet:

- Henkilötietojärjestelmien käyttäjillä on henkilökohtainen, yksilöivä käyttäjätunnus.
- Käyttäjällä on työtehtävänsä mukainen käyttöoikeus järjestelmään.
- Työtehtävien mukaiset käyttöoikeudet on määritelty johdon hyväksymässä tehtäväkuvauksessa käyttöturvallisuus huomioiden.
- Käyttökoulutus ja tehtävien mukaisen käytön opetus kuuluu perehdytykseen.
- Henkilöstön tietoturvaohjeisiin on koottu ohjeita ja neuvoja tietojen, tietojärjestelmien ja työvälineiden turvalliseen käyttöön.
- Salassa pidettävien tietojen käytölle edellytys on asiayhteys käyttäjän ja rekisteröidyn välillä. Tahaton käyttö pyritään estämään informoinnilla, teknisillä ratkaisuilla ja selkeillä tehtäväkuvauksilla.
- Käyttöoikeuksien myöntämisen periaatteet on dokumentoitu.
- Käyttöoikeuksien myöntöperusteista vastaavat palvelujohtajat.
- Käyttöoikeuksien haltijoista pidetään rekisteriä, jonka säilytysaika on 12 vuotta käyttöoikeuksien päättymisestä.
- Käytöstä kerätään lokitiedot, joiden avulla käyttö voidaan jäljittää yksilötasolle.
    - Säännöllisessä lokivalvonnassa syntyvät raportit säilytetään 5 vuotta.
    - Käyttölokitietojen selvityspyynnöt ja niiden lokiseurantaraportit säilytetään 12 vuotta.
    - Toimenpiteisiin johtaneiden tapausten selvitykset ja raportit säilytetään 12 vuotta.

3.10. Liikkuva työ

Liikkuva työ tarkoittaa kaikkea organisaation toimitilojen ulkopuolella tehtävää työtä. Erityisesti on huolehdittava puhelinten ja muiden mobiililaitteiden käytön turvallisuudesta sekä tietojen salassa pidon toteutumisesta kaikissa tilanteissa. Kaikessa organisaation toimitilojen ulkopuolella tehtävässä työssä on noudatettava tietoturvallisuuden vaatimuksia.

Mobiililaitteisiin ja niiden käyttöön liittyy vastaavia uhkia kuin kiinteämmin asennettuihin laitteisiin, joten niiden käytössä noudatetaan soveltuvin osin samoja turvallisuusohjeita. Huomioitavaa on kuitenkin se, että näitä laitteita käytetään ja kuljetetaan organisaation toimitilojen ulkopuolella, jolloin tarvitaan erityistä huolellisuutta.

Liikkuvan työn käytäntöjä on selvitetty tarkemmin henkilöstön tietoturvaoppaassa.

3.11. Seuranta, valvonta ja raportointi

Tietoturvan kehittäminen ja ylläpito vaativat jatkuvaa seurantaa. Tähän kuuluvat tietoturvan valvonta sekä poikkeamien raportointi ja tilastointi.

Suunnitellusti toteutettu seuranta, josta tiedotetaan henkilökunnalle, vaikuttaa ennaltaehkäisevästi ja auttaa havaitsemaan poikkeamatilanteet mahdollisimman nopeasti. Seurannan toteuttaminen on sekä automaattista että eri henkilöiden toteuttamaa valvontaa.

Henkilötietojen käsittelyn osalta noudatetaan erillistä valvontasuunnitelmaa, jonka mukaisesti valvontaa ja seurantaa tehdään säännönmukaisesti ja suunnitelmallisesti. Lisäksi valvontaa tehdään rekisteröidyn pyynnöstä tai työntekijän ilmoituksen perusteella.

4. TIETOSUOJA

Tietosuoja on olennainen osa yleistä tietoturvaa. Tietosuoja määrittelee henkilön yksityisuuden suojaamista ja sillä turvataan oikeuksia, tietoja ja luottamusta. Tietosuojan lähtökohtana on suojata henkilöiden perusoikeudet ja -vapaudet sekä erityisesti henkilötiedot ja varmistaa yksityisyyden suoja.

Tietosuojaa ja sen vaatimuksia määrittelee 25.5.2018 voimaan tullut EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, joka velvoittaa rekisterinpitäjän suunnittelemaan ja osoittamaan henkilötietojen käsittelyn lainmukaisuuden.

Suojaamistoimet kattavat kaiken tiedon käsittelyn, siirron ja säilytyksen, riippumatta niiden tallennusmuodosta tai niihin kohdistuvan uhan luonteesta. Uhat voivat olla tahallisia tai tahattomia, kuten tietojen urkinta, huolimattomuus, järjestelmäviat, tapaturmat tai luonnonkatastrofit.

Rekisterinpitäjän tulee seurata tietojen käyttöä ja puuttua havaitsemaansa asiattomaan käyttöön, myös työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietoturvaongelmista. Tietojen luvattomasta käytöstä saattaa seurauksena olla oikeudellisia seurauksia tai erilaisia työnantajan menettelyjä, riippuen tilanteen vakavuudesta. Näitä toimenpiteitä kuvataan liitteissä kaksi ja kolme sekä käyttölokien seuranta- ja valvontasuunnitelmassa.

Henkilötietojen turvallinen käsittely korostuu alueellisten ja kansallisten yhteisjärjestelmien käytössä.

Terveydenhuoltolain mukaisesti Etelä-Pohjanmaan sairaanhoitopiirin julkisen terveydenhuollon yksiköt ovat muodostaneet yhteisen Etelä-Pohjanmaan potilastietorekisterin, jossa potilastiedot ovat terveydenhuollon käytettävissä yli organisaatiorajojen ilman potilaan suostumusta. Potilastietojärjestelmää saa käyttää vain hoidettavan potilaan tietojen hakuun ja vain siinä laajuudessa kuin se työtehtävän hoitamiseksi on tarpeen.

Sosiaalihuollossa, ympäristöpalveluissa ja hallinnossa noudatetaan samoja tietoturvallisuuden periaatteita kuin muussakin henkilötietojen käsittelyssä, alan erityislainsäädäntö huomioiden.

4.1. Henkilötietojen kerääminen ja käsittely

EU:n yleinen tietosuoja-asetus ja kansallinen lainsäädäntö määrittelevät henkilötietojen keräämistä ja käsittelyä, tietojen käytön tulee aina perustua lakeihin ja asetuksiin sekä olla tarkoituksenmukaista sekä suunniteltua. Henkilötietoja käsitellään siinä laajuudessa kuin se on tarpeen palvelun tai työtehtävän kannalta ja käsittelytoimet suunnitellaan ja määritellään tiedon elinkaari huomioiden. Henkilötietojen käyttö on sallittua vain lainsäädännön nojalla tai henkilön suostumuksen perusteella. Tietojen säilytys ja käyttö tulee toteuttaa siten, ettei ulkopuolisten ole mahdollista saada niitä tietoonsa. EU:n yleinen tiesuoja-asetus määrittelee tiedon keräämiselle ja säilyttämiselle tarpeellisuusvaatimuksen, jonka mukaisesti tarpeetonta henkilötietoa ei tule kerätä, käsitellä tai säilyttää.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi ja käyttöä valvotaan. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella.

Tietosuoja huomioidaan eri sidosryhmien kanssa toimiessa. Sopimuksia tehtäessä varmistutaan tietosuoja-asetuksen vaatimusten täyttymisestä ja henkilötietojen käsittelystä sovitaan EU:n yleisen tietosuoja-asetuksen mukaisesti.

Rekisteröidyllä on oikeus tarkistaa itseään koskevat tiedot järjestelmästä sekä saada halutessaan tieto siitä, kuka hänen tietojaan on käsitellyt. Lisätietoa rekisteröidyn oikeuksien käytöstä voi kysyä tietosuojavastaavalta.

Suomessa henkilötietojen käsittelyä ohjaa ja valvoo tietosuojavaltuutettu, joka käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröidyn oikeuksien toteutumisesta. Yhteyshenkilönä organisaation ja tietosuojavaltuutetun välillä toimii tietosuojavastaava.

Henkilötietojen käsittelystä on saatavissa tarkempaa tietoa nettisivuiltamme tai info-pisteiltä saatavista tietosuojainformointiasiakirjoista tai tietosuojavastaavalta.

5. TIETOTURVARISKEIHIN VARAUTUMINEN

Tietoturvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle. LLKY:n on arvioitava tietoturvallisuusuhat ja varauduttava tietoturvallisuuden poikkeamatilanteisiin.

Tietoturvallisuuden merkittävin tekijä on aina ihminen. Laitetason ratkaisuilla voidaan vaikuttaa tietoturvallisuuteen vain rajallisesti. Henkilöstön mahdollinen osaamattomuus, huolimattomuus tai välinpitämättömyys aiheuttavat merkittävimmän uhan organisaation tietoturvallisuudelle. Uhkia aiheuttavat myös mahdolliset tietoisesti tehdyt väärinkäytökset, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset ja haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat.

Henkilöstön osaaminen ja tietoisuus ovat suuressa roolissa tietoturvallisuuden toteutumisessa ja kouluttaminen sekä tietoisuuden lisääminen tietoturvallisuudesta ovat merkittäviä tekijöitä uhkien pienentämisessä.

Esimiesten vastuulla on huolehtia henkilökunnan perehdyttämisestä, jolla on merkittävä rooli tietoturvan ymmärtämisessä ja osaamisen lisäämisessä sekä ohjeiden noudattamisessa.

5.1. Riskien arviointi

Tietoturvallisuuden riskejä arvioitaessa on huomio kiinnitettävä erityisesti tietojen käsittelyn sisältämiin riskeihin. Riskejä syntyy aina kun tietoja käsitellään, erityisesti silloin, jos tietoja on tarpeen siirtää. Riskejä ovat myös tietojen vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen, luvaton luovuttaminen tai tietoihin oikeudettomasti pääseminen.

Järjestelmien luokittelu tapahtuu niiden kriittisyyden mukaan. Järjestelmien turvajärjestelyt tarkastetaan säännöllisesti ja tarvittaessa niiden toimivuus testataan.

Tyypillisiä tietoon kohdistuvia riskejä ovat:

- Tietoon pääsy on hankalaa, hidasta tai se ei onnistu.
- Tieto päätyy ulkopuolisten tietoon.
- Tieto ei ole käyttökelpoista puutteen tai virheen vuoksi tai tieto on hävinnyt.
- Tieto ei ole käytettävissä.

Tietoturvallisuuteen kohdistuvien riskien yleisiä aiheuttajia:

- Henkilöstön tai ulkopuolisten henkilöiden virheet tai tahallinen toiminta voivat vaarantaa tietojärjestelmän toiminnan tai tiedon laadun tai järjestelmän toiminnan.
- Tietojen käsittely julkisten verkkojen kautta tai muilla kuin organisaation laitteilla, kuten esim. etätyössä on mahdollista, on tietoturvallisuuden kannalta suurempi riski, kuin työskentely organisaation toimipisteessä ja organisaation laitteilla.
- Tietojen siirrossa tai yhteyksien käyttöoikeuksien määrittelyssä tapahtuvat virhetilanteet.
- Viat ja häiriötilanteet, kuten laite-, ohjelma-, tietokanta-, ja tietoliikenneviat sekä ympäristöriskit kuten sähkökatkot.
- Hallintatoimet ovat puutteelliset.

5.2. Riskienhallintasuunnitelma

Tietoturvallisuusriskejä tulee arvioida ja hallita riskienhallinnan ohjeistuksen mukaisesti ja tietoturvallisuuden suurimmat riskit tulee sisällyttää organisaation riskienhallintasuunnitelmaan.

Tietoturvallisuuden riskienhallinnan arvioinnissa ja riskeihin varautumisessa avustaa tietosuojavastaava.

5.3. Tietoturvallisuusriskin toteutuminen

Jokaisella on velvollisuus ilmoittaa havaitsemistaan tietoturvallisuuteen kohdistuvista uhista tai rikkeistä. Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation tietovarantoihin ja palveluihin kohdistuu uhka, joka vaarantaa tiedon ja palvelun eheyden, luottamuksellisuuden tai saatavuuden.

Tietosuojavastaavalla ja tietoturvavastaavalla on johdon antama valtuutus ja velvollisuus tehdä tietojärjestelmien ja tietojen käsittelyn tietoturvallisuuden ja tietosuojan seurantaa ja valvontaa sekä ryhtyä toimenpiteisiin havaittujen heikkouksien parantamiseksi ja ongelmatilanteiden selvittämiseksi. Tarvittaessa tapauksista raportoidaan myös organisaation johdolle.

Havainnon tietoturvapoikkeamasta voi tehdä kuka tahansa, kuten organisaation työntekijä, tietojärjestelmän ylläpitäjä tai ulkopuolinen henkilö. Tällöin on tilanne huomioiden otettava yhteys tietosuojavastaavaan, tietohallintoon, esimieheen tai muuhun vastuuhenkilöön. Työntekijän velvollisuus on viedä asia eteenpäin, mikäli esimerkiksi asiakas siitä hänelle ilmoittaa.

Mikäli kyse on henkilötietoihin kohdistuneesta riskistä, tulee arvioida tapahtuneen vakavuus ja se, tuleeko tapahtuneesta tehdä ilmoitus tietosuojavaltuutetulle ja rekisteröidyille. Kyseinen ilmoitus edellyttää aina tilanteen arvioinnin.

Tarkemmat toimintaohjeet löytyvät Käyttölokien seuranta- ja valvontasuunnitelmasta.

5.4. Tietoturvallisuusrikkomusten seuraamukset

Tietoturvallisuusrikkomuksista säädetään työsopimuslaissa sekä viranhaltijalaissa. Henkilötietoihin kohdistuvien rikkomusten osalta asiaa säätää lisäksi EU:n yleinen tietosuoja-asetus sekä muut kansalliset lait ja asetukset.

Tietoturvallisuuslainsäädäntöä ja organisaation tietoturva- ja tietosuojapolitiikkaa sekä näiden perusteella annettuja ohjeita vastaan rikkominen tiedotetaan aina esimiehelle. Seurauksena rikkomuksista, niiden vakavuuden mukaisesti, voi olla käyttöoikeuteen kohdistuvia rajoituksia, palvelussuhteeseen vaikuttavia seuraamuksia sekä rikoslaissa määriteltyjä seuraamuksia. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin.

Seuraamuksia arvioitaessa on toimintaa tarkasteltava kokonaisuutena, jonka yhtenä osana tietoturvallisuusrikkomus on, ja jonka vaikutukset ja seuraukset arvioidaan aina tapauskohtaisesti. Arvioinnissa käytetään apuna käyttölokien seuranta- ja valvontasuunnitelman liitteenä olevaa seuraamustaulukkoa. Arviointi tehdään yhteistyössä tietosuojavastaavan ja esimiehen/palvelujohtajan/henkilöstöpäällikön kanssa.

6. VASTUUT JA ORGANISOINTI

Tietoturvallisuus on organisaation yhteinen asia ja se koskettaa koko henkilöstöä.

Toiminnassa noudatetaan lakeja ja asetuksia, toimintaa kehitetään vastaamaan kulloinkin voimaan tulevia toimialan viranomaissuosituksia sekä lakeja. Havaittuihin väärinkäytöksiin tai tietojen päätymiseen ulkopuolisten tietoon suhtaudutaan vakavasti ja niihin puututaan.

Johtokunta kantaa ylintä vastuuta tietoturvallisuudesta. Johtokunnan alaisuudessa toimintaa johtaa liikelaitoskuntayhtymän johtaja. Vastuu on riippumatonta siitä, onko toimintoja ulkoistettu. Johtokunta päättää organisaation kokonaistietoturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimivaltuuksista. Johtokunnan hyväksymä tietoturva- ja tietosuojapolitiikka on tietoturvallisuuden toteuttamisen perusta. Johtokunta on päätöksellään 14.5.2012 § 63 asettanut tietosuojavastaavan, tietoturvavastaavan ja tietoturvatyöryhmän, hyväksynyt tietosuojavastaavan ja tietoturvavastaavan toimenkuvat sekä valtuuttanut liikelaitoskuntayhtymän johtajan nimittämään tietosuojavastaavan, tietoturvavastaavan ja tietoturvatyöryhmän.

Tietosuojavastaava auttaa organisaation johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu suunnittelutoimintaan, valmistelee ohjeita ja ylläpitää niitä sekä kouluttaa tietosuoja-asioita henkilöstölle. Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa ja seuraa sekä valvoo henkilötietojen käsittelyä ja suojausmenettelyä. Tietosuojavastaavaa tulee tiedottaa suunnitelluista henkilötietojen käsittelyistä tai näihin suunnitelluista muutoksista. Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Lisäksi tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä sekä ryhtyä jatkotoimenpiteisiin tietosuoja ongelmatilanteissa johtokunnan hyväksymän seuranta- ja valvontasuunnitelman mukaisesti. Organisaation velvollisuus on ottaa tietosuojavastaavan riittävän aikaisessa vaiheessa mukaan henkilötietojen käsittelyä koskevaan suunnittelutoimintaan. Organisaation johto on vastuussa tietosuojavastaavan työn mahdollistamisesta asianmukaisesti.

Tietoturvavastaava toimii tietoturvallisuuden asiantuntijana ja tietoturvan kehittäjänä. Tietoturvavastaava laatii tietoturvallisuussuunnitelman, jossa määritellään tietojärjestelmien vaatimukset, turvaluokitukset, turvallisuustoimenpiteet ja niiden tekninen toteutus. Tietoturvavastaava koordinoi ja valvoo tietoturvan toteutumista sekä raportoi johdolle tietoturvan tilasta ja kehittämistarpeista. Tietoturvavastaavalla on oikeus ylläpitää käyttöoikeusrekisteriä, valvoa tietoturvaa teknisin keinoin, toimia tietosuojavastaavan apuna käyttölokivalvonnan teknisessä toteutuksessa ja ryhtyä toimenpiteisiin tietoturvan ongelmatilanteissa.

Tietoturvatyöryhmä toimii tietosuojavastaavan ja tietoturvavastaavan apuna tietoturvallisuuden toteuttamisessa ja suunnittelussa. Työryhmään kuuluvat liikelaitoskuntayhtymän johtaja, tietosuojavastaava, tietoturvavastaava, palvelualuejohtajat, henkilöstöpäällikkö ja hallintopäällikkö. Tietoturvatyöryhmä käsittelee tietoturvallisuuden linjaukset ja ohjeet ennen niiden esittämistä johdolle hyväksyttäviksi, huolehtii tietoturvallisuusperiaatteiden toteuttamisesta, seuraa tietoturvallisuuden eri vastuualueiden suunnitelmien, ohjeiden, selosteiden ja lomakkeiden laadintaa sekä ottaa tarvittaessa kantaa käytäntöihin ja kehittämishankkeisiin. Tietoturvatyöryhmä seuraa organisaation tietoturvallisuustilannetta.

Palvelujohtajat vastaavat oman palvelualueensa tietoturvallisuudesta ja päättävät kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimivaltuuksista sekä tietoturvallisuutta koskevasta sisäisestä ja ulkoisesta tiedottamisesta. Palvelujohtajat vastaavat palvelualueensa henkilötietojärjestelmien rekistereistä, tietosuojaselosteiden olemassaolosta ja rekistereiden vastuuhenkilöiden nimeämisestä. Lisäksi palvelujohtajat huolehtivat vaikutustenarvioinnin tekemisestä omalla palvelualueellaan sekä selosteen käsittelytoimista ajantasaisuudesta. Palvelujohtajat antavat henkilötietojen ja asiakirjojen käsittelystä ja menettelytavoista palvelualuekohtaisia ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja. Asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen arkistonmuodostussuunnitelman mukaisesti.

Esimiehet vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta yksiköittäin, tiedottamisesta sekä valvonnasta ja henkilötietojen lainmukaisesta käytöstä. Esimies vastuulla on huolehtia henkilöstön tutustumisesta tietoturva- ja tietosuojapolitiikkaan sekä henkilöstön tietoturvaohjeisiin ja salassapitositoumusten allekirjoittamisesta ennen käyttölupahakemusten tekemistä. Tietosuojavastaava avustaa näissä tarpeen mukaan ja osallistuu tietoturvallisuuden arviointiin ja kehittämiseen sekä valvoo tietojen käyttöä. Esimiesten vastuulla on henkilökunnan tietoturvan- ja tietosuojan verkkokoulutuksen suorittaminen tietosuojavastaavan ohjeistuksen mukaisesti. Asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen arkistonmuodostussuunnitelman mukaisesti.

Jokainen työntekijä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhista tai menettelyvirheistä tietosuojavastaavalle. Samoin jokainen työntekijä on omalta osaltaan vastuussa tietoturvallisuuden toteuttamisesta ja määräysten noudattamisesta tehtäviensä hoidossa.

Organisaatiolle palveluja tuottava **kolmannet osapuolet** velvoitetaan noudattamaan organisaation ja lakien määrittelemiä tietoturvallisuusperiaatteita. Asetettavat tulee kuvata sopimuksessa tai sen liitteessä.

Vastuutaho	Tehtävä
Kuntayhtymän johtaja	Johtaa tietoturvallisuutta
Johtokunta	Tietoturvallisuuden kokonaisvastuu. Päättää organisaation kokonaistietoturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimivaltuuksista. Tietoturva- ja tietosuojapolitiikan sekä mobiilipolitiikan hyväksyminen.
Tietosuojavastaava	Auttaa organisaation johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä.
Tietoturvavastaava	Toimii tietoturvan asiantuntijana ja kehittäjänä.
Tietoturvatyöryhmä	toimii tietosuojavastaavan ja tietoturvavastaavan apuna tietoturvallisuuden toteuttamisessa ja suunnittelussa.
Palvelujohtajat	Vastaavat oman palvelualueensa tietoturvan toteuttamisesta ja tiedottamisesta
Esimiehet	Tietoturvan ja tietosuojan toteutuminen yksiköittäin, tiedottaminen sekä valvonta ja vastuu henkilötietojen lainmukaisesta käytöstä
Työntekijät	Velvollisuus noudattaa annettuja ohjeita Velvollisuus ilmoittaa havaitsemistaan tietoturvallisuuden ongelmista

Taulukko 1: Tietoturvallisuuden vastuutahot

7. LISÄTIETOA

Tämä tietoturva- ja tietosuojapolitiikka pohjautuu kansalliseen lainsäädäntöön ja EU:n yleiseen tietosuoja-asetukseen. Lisätietoa löydät mm. seuraavista:

- Organisaation intranet
  - www.intra.net
- Lainsäädäntö
  - www.finlex.fi
  - https://eur-lex.europa.eu/homepage.html?locale=fi
- Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI-ohjeet
  - www.vahtiohje.fi
- Viestintäviraston kyberturvallisuuskeskuksen sivut
  - https://www.viestintävirasto.fi/kyberturvallisuus.html
- Tietosuojavaltuutetun toimisto
  - www.tietosuoja.fi

LIITE 1

SOPIMUS SALASSAPIDOSTA JA VAITIOLOVELVOLLISUUDESTA

Me allekirjoittaneet osapuolet olemme sopineet salassapito- ja vaitiolovelvollisuudesta seuraavaa: Asiakirjojen, tietojen ja tietojärjestelmien käsittely- ja käyttöoikeudet annetaan vain tämän sitoumuksen allekirjoittaneelle. Sitoumus tehdään työsuhteen alkaessa, sijaisten, opiskelijoiden ja harjoittelijoiden kanssa ensimmäisen palvelusuhteen alkaessa tai palvelusuhteen luonteen muuttuessa.

Jokainen työntekijä vastaa oman toimintansa tietoturvallisuudesta ja lainsäädännön, annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.

Työnantajan tietoturva- ja tietosuojaohjeet sekä sitä täydentävä henkilöstön tietoturvaohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle. Esimiehen velvollisuus on uuden työntekijän perehdytyksen yhteydessä läpikäydä henkilöstön tietoturva- ja tietosuojaohjeet.

Vaitiolo- ja salassapitositoumus:
Työntekijänä sitoudun olemaan käyttämättä, ilmaisematta tai luovuttamatta palvelusuhteen aikana asiakkaisiin, potilaisiin, henkilötietoihin sekä liike- ja ammattisalaisuuksiin liittyviä salassa pidettäviä tietoja, riippumatta siitä, miten tai mihin tieto on tallennettu tai millä tavalla tieto on saatu (kirjallisesti, suullisesti tai havainnoimalla) muutoin kuin työtehtävien vaatimassa laajuudessa ja yhteydessä. Tietojen luovutuksen tulee perustua aina asiakkaan tai potilaan kirjalliseen suostumukseen, asiayhteydestä ilmenevään suostumukseen tai lainsäädäntöön.

Sitoudun noudattamaan seuraavia tietosuojaperiaatteita:

- Salassapito- ja vaitiolovelvollisuus koskee minua palvelusuhteeni aikana ja myös sen jälkeen
- Noudatan erityistä huolellisuutta käsitellessäni salassa pidettäviä tietoja
- Pidän salassa kaikki tietooni saamani arkaluonteiset tiedot esim. henkilön sairautta, tutkimusta, hoitoa, taloudellista asemaa tai sosiaalisia etuuksia koskevat tiedot sekä myös asiakkaaksi hakeutumisen ja asiakkuuden olemassaolon sekä turvallisuuteen, tietojärjestelmiin ja kiinteistön liittyvät tiedot.
- Käsittelen vain työtehtävieni edellyttämiä tietoja. En käsittele esim. työkavereiden, lähiomaisten, naapureiden tai julkisuuden henkilöiden tietoja, mikäli työtehtäväni eivät sitä sillä hetkellä edellytä. Omien tietojen käsittely on kiellettyä.
- Vastaan käyttäjätunnuksillani ja/tai varmennekortin tunnuksillani tapahtuvasta tietojen käytöstä.
  Tunnuksia ei saa luovuttaa toisen henkilön käyttöön.
- Vastaan käytössäni olevasta kannettavasta tietokoneesta tai muusta laitteesta niin, ettei laite ja siinä olevat tiedot joudu vääriin käsiin.
- Olen tietoinen, että tietojärjestelmissä käyntini ja siellä tehdyt tapahtumat kirjautuvat lokitiedostoihin ja epäillystä väärinkäytöstä raportoidaan esimiehelleni ja tarvittaessa myös viranomaisille sekä henkilölle, jonka tiedoista on kyse.
- Olen tietoinen, että tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta on lainsäädännössä rangaistava teko. Rangaistavaa menettelyä henkilörekisteritoiminnassa koskevat säännökset sisältyvät henkilötietolakiin ja rikoslakiin. Tietojen oikeudettomasta käytöstä voi seurata rikos-, työ- ja vahingonkorvausoikeudellisia seuraamuksia.

Olen lukenut tämän sitoumuksen ja ymmärrän sen sisällön ja merkityksen.

Paikka ja aika:_____ _____ / _____ 20_____

Työyksikkö:_____

_____ _____
Työntekijän nimi Esimiehen nimi

_____ _____

Työntekijän allekirjoitus

Esimiehen allekirjoitus