Yhteistoimintamenettely 17.9.2012
Henkilöstöjaosto 17.9.2012
Hyväksytty johtokunta 24.9.2012 § 106

Tietoturva- ja tietosuojapolitiikka

Suupohjan peruspalvelu-liikelaitoskuntayhtymä

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

Sisällys:

1. JOHDANTO

Tietoturva- ja tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan liikelaitoskuntayhtymän tietoturvan ja tietosuojan toteuttamisessa ja kehittämisessä. Tietoturvatyö on osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutuminen varmennetaan vuosittain tietoturvaorganisaation raportoinnilla johdolle ja toimintakertomukseen tulevalla maininnalla suoritetuista toimenpiteistä.

Tietoturva- ja tietosuojapolitiikkaa täydentävät henkilöstön tietoturvaohjeet sekä palvelualueittain ja vastuualueittain annetut tietojen käsittelyä koskevat määräykset ja ohjeet. Tietoturva- ja tietosuojapolitiikkaa ja sen perusteella annettuja ohjeita ja määräyksiä noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia liikelaitoskuntayhtymän palveluksessa olevia viranhaltijoita, työntekijöitä ja luottamushenkilöitä. Liikelaitoskuntayhtymän ulkopuolisten toimijoiden ja toimittajien tulee myös sitoutua noudattamaan tietoturva- ja tietosuojapolitiikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsylle liikelaitoskuntayhtymän tietojärjestelmiin ja niiden tietoaineistoihin.

Johtokunnan hyväksymä tietoturva- ja tietosuojapolitiikka sekä sitä täydentävät henkilöstön tietoturvaohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle.
Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi. Se on asiakirjana julkinen ja saatavissa liikelaitoskuntayhtymän ulkoisilta ja sisäisiltä verkkosivuilta.

Tietoturva- ja tietosuojapolitiikan tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon liikelaitoskuntayhtymän tietoturvan kehittämisessä.

Asiakastietojen turvallinen käsittely korostuu entisestään siirryttäessä asiakastietojen sähköiseen käsittelyyn sekä alueellisiin ja kansallisiin yhteisjärjestelmiin. Terveydenhuoltolain mukaisesti Etelä-Pohjanmaan sairaanhoitopiirin julkisen terveydenhuollon yksiköt ovat muodostaneet yhteisen Etelä-Pohjanmaan potilastietorekisterin, jossa potilastietoja voidaan käyttää yli organisaatiorajojen ilman potilaan suostumusta. Potilastietojärjestelmästä saa kuitenkin hakea ainoastaan hoidettavan potilaan tietoja työtehtävien hoitamiseksi tarvittavassa laajuudessa. Lisäksi tietoturvatason yhtenäistäminen edellyttää tietojärjestelmien yhteensovittamista alueen julkisessa terveydenhuollossa. Näiden vaatimusten täyttyminen on huomioitava liikelaitoskuntayhtymän tietoturvaperiaatteissa.

Liikelaitoskuntayhtymä on päättänyt liittyä kansalliseen KanTa-palveluun, johon sisältyy sähköinen potilastiedon arkisto (eArkisto) ja reseptikeskus (eResepti). Edellytyksenä liittymiselle on Sosiaali- ja terveysministeriön asettamien kansallisten auditointivaatimusten täyttyminen. Liikelaitoskuntayhtymän tietoturvaperiaatteissa on huomioitu nämä auditointivaatimukset ja periaatteet toteutetaan asteittain siten, että ne toteutuvat eReseptin osalta liityttäessä kansalliseen sähköiseen reseptipalveluun ja kaikkien potilastietojen osalta viimeistään liityttäessä eArkistoon.

2. TIETOTURVA JA TIETOSUOJA

Seuraavassa kuvataan tietoturvan ja tietosuojan käsitteellinen sisältö. Jatkossa esityksessä käytetään termejä tietoturva ja tietoturvallisuus käsittäen sekä tietoturvan että tietosuojan.

Tietoturvan tavoitteena on turvata ja suojata tietoa, tietojärjestelmiä, tietojenkäsittelyä ja tiedonvälitystä. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, käytettävyydestä ja saatavuudesta. Tietoturvan hallintaan liittyvät tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, tietojen käsittelyn valvonta, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Sekä arkistotoimella että tietohallinnolla on yhteisenä tavoitteena tietojen saatavuuden ja käytettävyyden turvaaminen. Tiedon käytettävyydellä ja saatavuudella tarkoitetaan, että tieto on tallennettu siten ja sellaisessa muodossa, että se on luettavissa, ymmärrettävissä, tulkittavissa oikein, kattava, ajantasainen, oikeellinen ja muuten käyttökelpoinen vaadittavalla tavalla ja helppokäyttöisesti ilman tulkinta- ja väärinkäyttömahdollisuutta. Tiedon, tietojärjestelmän ja palvelun on oltava saatavilla ja hyödynnettävissä siihen oikeutetuille riittävän esteettömästi, vaivattomasti ja nopeasti vaaditulla tavalla ja vaadittuna aikana.

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista, jonka päämääränä on turvata liikelaitoskuntayhtymän toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoaminen tai vääristyminen sekä minimoida aiheutuvat ongelmat. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen. Suojautuminen kattaa sekä riskien toteutumista ehkäisevät toimenpiteet, toiminnan jatkuvuutta suojaavat toimet että poikkeustilanteita varten laadittujen valmiussuunnitelmien mukaiset toimet.

Tietosuoja on oleellinen osa tietoturvallisuutta ja liikelaitoskuntayhtymän palvelutoiminnan kannalta kriittinen tekijä, sillä suurin osa yhtymässä käsiteltävästä tiedosta on luottamuksellista, arkaluonteista sekä salassa pidettävää ja voi paljastuttuaan rikkoa yksityisyyden suojan ja luottamuksen yhtymän palvelutoimintaa kohtaan.

Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Tietojen ja tietojärjestelmien käyttöä seurataan ja väärinkäytöksiin puututaan.

Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä. Väärien, vanhentuneiden ja virheellisten tietojen käsittely on kielletty, ja näiden oikaiseminen on tehtävä tarpeen mukaan.

Tietoja voivat käyttää ainoastaan niitä työssään tarvitsemat henkilöt ja työtehtävänsä suorittamisen edellyttämässä laajuudessa. Tietoja voi luovuttaa ainoastaan henkilön itsensä suostumuksella tai lainsäädännön nojalla.

3. TIETOTURVAPERIAATTEET

3.1. Hallinnollinen turvallisuus

Hallinnollinen tietoturvallisuus on organisaation tietoturvatoimintojen johtamista ja organisointia tavoitteena sekä tietoturvallisuuden toteutuminen että johdon ja henkilöstön sitoutuminen tietoturvallisuuden suunnitelmalliseen kehittämiseen ja hoitamiseen.

Hallinnollisella tietoturvallisuudella tarkoitetaan tietoturvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Tuloksena on kuvaus tietoturvallisuustoiminnan periaatteista, tietoturvatyön järjestelyistä, organisoinnista, arvioinnista, ylläpidosta ja kehittämisjärjestelmästä. Hallinnollisessa tietoturvallisuudessa määritellään kunkin tietoturvatyöhön osallistuvan vastuut, tehtävät ja toimivaltuudet. Lisäksi määritetään resurssit sekä tietoturvatyölle että tietoturvan ohjeistukselle, koulutukselle, valvonnalle ja raportoinnille.

Hallinnollisen tietoturvallisuuden periaatteet:
- LLKY noudattaa sitä sitovia lakeja ja asetuksia sekä kehittää toimintaansa vastaamaan voimaan tulevia toimialan viranomaissuosituksia, valtakunnallisten tietojärjestelmäpalveluiden asettamia tietoturvavaatimuksia ja tietoturvakäytäntöjä.
- LLKY:llä on johtokunnan hyväksymä kirjallinen tietoturva- ja tietosuojapolitiikka, jossa ilmaistaan sitoutuminen tietoturvatyöhön ja tietoturvatyön organisointi.
- LLKY:llä on johtokunnan hyväksymät henkilöstön tietoturvaohjeet, jotka ohjeistavat tietoturva- ja tietosuojapolitiikan mukaisiin tietoturvakäytäntöihin.
- Tietoturvaan ja tietosuojaan liittyvillä tehtävillä on nimetyt vastuuhenkilöt, jotka ovat organisaatiossa työskentelevien ja sidosryhmien vastuuhenkilöiden tiedossa. Vastuuhenkilöillä on resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät.
- Tietoturvan eri osa-alueilla seurataan tietoturvatilannetta säännöllisesti raporteilla ja valvontajärjestelmillä sekä erikseen tehtävillä riskikartoituksilla. Havaintojen pohjalta tehdään tarvittaessa tietoturvan kehittämissuunnitelma, jonka johto hyväksyy.
- Keskeisistä tietoturvallisuusasioista annetaan ohjeet. Tietoturvallisuustietämyksen ajan tasalla pysymisestä huolehditaan säännöllisen koulutuksen, tiedotuksen, ohjeistuksen ja motivoinnin keinoin.
- Palveluiden hankinnoissa edellytetään, että tiedon käsittelyyn liittyvät suojaustoimet, vastuut ja tekniset tietoturvavastuut sisältyvät ostopalvelusopimuksiin. Palveluiden tuottajilta edellytetään sovittua palvelutasoa vastaavaa tietoturvatasoa. Palvelun tuottajalta edellytetään kuvausta palvelun tietoturvatasosta sekä tietoturvapoikkeamien valvonta-, havaitsemis-, ilmoittamis- ja käsittelykäytännöistä. Palvelun tuottajalta edellytetään, että se pitää organisaatiolle toimitetut dokumentit ajantasaisina, ja että se raportoi ostopalveluun liittyvistä tietoturvapoikkeamista.
- Ohjelmistojen ja laitteiden tarjouspyynnöissä ja hankinnoissa edellytetään voimassa olevien standardien noudattamista ja ennen hankintapäätöksiä tehtyä tietoturvallisuusnäkökohtien arviointia.

3.2. Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstön toimista aiheutuvien ja heihin kohdistuvien tietoturvauhkien hallintaa. Henkilöstöturvallisuustyön tulos on luotettava ja tehtäviinsä soveltuva henkilöstö, joka tuntee itselleen asetetut tietoturvavaa-

timukset omaan toimenkuvaansa ja rooliinsa liittyen. Oman ja ostopalveluita organisaatiolle tuottavan henkilöstön tulee tuntea tiedonsaantioikeutensa, käyttöoikeutensa, sijaisuus- tai muihin työtä koskeviin järjestelyihin liittyvät toimet, oma tietosuojansa sekä velvollisuutensa ja oikeutensa työsuhteen alkaessa ja päättyessä.

Henkilöstötietoturvallisuuden periaatteet:
- Uuden henkilöstön perehdytykseen kuuluu henkilöstön tietoturvaohjeiden läpikäyminen sekä tietoturvan ja tietosuojan verkkokoulutuksen suorittaminen. Ennen tietojärjestelmän käyttöoikeuksien myöntämistä allekirjoitetaan asiakirjojen, tietojen ja tietojärjestelmien vaitiolo- ja salassapitositoumus.
- Henkilöstön tehtäväkuvauksia ylläpidetään siten, että niistä on johdettavissa tehtävien edellyttämät henkilökohtaiset tietojärjestelmien käyttöoikeudet.
- Tietojärjestelmien käyttäjistä pidetään ajantasaista rekisteriä, josta ilmenee käyttäjän yksilöintitietojen lisäksi käyttäjärooli. Ostopalveluiden tuottajien henkilöistä tai muuten organisaation tietojärjestelmiä käsittelevistä (esim. harjoittelijat ja opiskelijat) edellytetään vastaavien tehtäväkuvauksien ylläpitoa käyttäjärekisteriä varten.
- Käyttöoikeuden saaminen alueelliseen tai valtakunnalliseen tietojärjestelmäpalveluun edellyttää työntekijän henkilöllisyyden luotettavaa varmistamista tai henkilökohtaisen varmennekortin myöntämistä.
- Organisaation toiminnan kannalta kriittisten tietojärjestelmien vastuuhenkilöillä on nimetyt varahenkilöt.
- Työnkuvissa on huolehdittu, ettei synny tilanteita tai käyttöoikeuksia, jotka mahdollistavat tietojen käsittelyn ilman toisen työntekijän mahdollisuutta kontrolloida käsittelyä (vaaralliset työyhdistelmät).
- Esimiehet vastaavat siitä, että henkilökunta on selvillä tietoturvavaatimuksista ja noudattaa annettuja tietoturvaohjeita ja käytäntöjä.
- Työntekijät saavat säännöllisesti tietoturvakoulutusta. Tietämystasoa ja osallistumista koulutukseen seurataan ja tulokset raportoidaan organisaation vastuuhenkilöille. Tietosuojavastaava huolehtii tietoturvan ja tietosuojan verkkokoulutuksen ylläpidosta, seurannasta ja raportoinnista.
- Tietoturvaohjeiden noudattamisen seuranta ja käyttölokivalvonta on suunnitelmallista ja säännöllistä. Tietosuojarikkomukset käsitellään seuranta ja valvontasuunnitelman mukaisesti. Väärinkäytösten varalle on laadittu sanktiojärjestelmä.
- Työtehtävien loppumiseen liittyvät järjestelyt on ohjeistettu siten, että tietojärjestelmien käyttöoikeudet ja valvomaton pääsy tiloihin, joissa on yhteys suojattuun tietojärjestelmäympäristöön, päättyvät tehtävien loppuessa.

3.3. Fyysinen turvallisuus

Fyysinen tietoturvallisuus on toimitilojen suojaamista siten, että tiedon käsittely ja siinä tarvittava tekniikka on suojattu fyysisten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja joutumiselta luvattomien tai rikollisten toimien kohteeksi sekä varmistetaan teknisten järjestelmien toiminta.

Fyysisen tietoturvallisuuden periaatteet:
- Asiaton pääsy toimintayksikön tai sen palveluntuottajan tiloihin, joissa on pääsy suojattuun tietojärjestelmäympäristöön, estetään valvonnalla ja pitämällä lukittuna tilat, joissa ei ole henkilökuntaa tai kameravalvontaa. Tilojen avaimet ovat henkilökohtaisia ja avainten haltijoista pidetään rekisteriä.
- Tietoteknisten laitteiden sijoittelussa on huomioitu vesi-, lämpö- ja tulivahinkojen riski. Palvelinten ja muiden järjestelmään kuuluvien laitteiden ja tiedonsiirtoverkon

suojaus ja valvonta ulkoisilta uhkilta vastaa tietojärjestelmien kriittisyyttä palvelutoiminnan hoidossa. Varmuuskopiot on sijoitettu fyysisesti eri palotiloihin.
- Sähkönsyöttö ja varautuminen sähkönsyötön katkoksiin tietojärjestelmän laitteille ja tiedonsiirtoverkolle vastaa ohjelmistojen kriittisyyttä palvelutoiminnan hoidossa.
- Tietojärjestelmille ja kriittisille työasemille on tehty jatkuvuus- ja toipumissuunnitelmat.
- Paikallisverkon käytönvalvonta on järjestetty.

3.4. Laitteistoturvallisuus

Laitteistoturvallisuustyön tulos on päätelaitteiden, palvelimien ja muiden tiedon käsittelyssä käytettävien laitteiden tarkoituksenmukaisuus, käytettävyys ja saatavuus sekä toiminnan tarpeita tyydyttävä toiminta.

Laitteistotietoturvallisuuden periaatteet:
- Kaikki hankittavat laitteistot ovat kokonaisarkkitehtuurin mukaisia tai muuten yhteensopivia organisaation tietojärjestelmäympäristön sekä tiedonvälitysverkoston kanssa. Hankinnat, asennukset ja käytöstä poistot hoidetaan keskitetysti.
- Laitteisto valitaan siten, että sen käyttöikä ja vastaavuus tietojärjestelmävaatimusten muutoksiin arvioidaan kohtuulliseksi. Laitteistoja hankittaessa otetaan huomioon varaosien, huollon ja vararatkaisujen saatavuus.
- Työasemista ja oheislaitteista, esim. tulostimista, on tunnistettu kriittiset laitteet palvelutoiminnan toteuttamisen jatkuvuuden sekä palvelutasovaatimusten kannalta. Kriittisille laitteille on järjestetty katkojen aikainen sähkönsyöttö ja riittävä palvelutaso ylläpidossa.
- Palvelimien, verkon ja muiden laitteiden kriittisyys johdetaan niissä ylläpidettävien ohjelmistojen ja työasemien kriittisyyden perusteella. Kriittisille laitteistoille taataan katkoton sähkön syöttö ja korkea palvelutaso ylläpidossa.

3.5. Ohjelmistoturvallisuus

Ohjelmistoturvallisuus käsittää käyttöjärjestelmien, varusohjelmistojen sekä sovellusten suojausominaisuudet, näiden ylläpidon ja päivityksen sekä valvonta- ja lokimenettelyt. Ohjelmistoturvallisuustyön tulos on ohjelmistojen käytettävyys, saatavuus ja toimivuus sekä se, että käytössä olevat ohjelmistot suojaavat sisältämänsä tiedon asetettujen vaatimusten mukaisesti.

Ohjelmistotietoturvallisuuden periaatteet:
- Ohjelmistohankinnat ja kehittäminen perustuu toiminnan lähtökohdista todettuihin tarpeisiin. Uuden ohjelman hankinnan edellytys on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja kokonaisarkkitehtuurin kanssa. Hankinnat, ohjelmistojen asennukset ja käytöstä poistot hoidetaan keskitetysti.
- Ohjelma tai sen versio hyväksytään käyttöön vasta, kun se on testattu tulevassa ympäristössään ja todettu tilausta vastaavaksi teknisesti ja toiminnallisesti. Käyttöönotto perustuu hyväksyttyyn käyttöönottosuunnitelmaan, jossa kuvataan myös mahdollisten ongelmien luokittelu, korjausmenettelyt ja niiden vasteaika.
- Valtakunnallisten tietojärjestelmäpalveluiden kanssa asioiva ohjelmisto tulee olla testattu hyväksyttävästi valtakunnallisen palvelun järjestäjän edellyttämällä tavalla ja järjestelmä todettu kansallisten auditointivaatimusten mukaiseksi.

- Ohjelmistoille on määritelty selkeät käyttötarkoitukset siten, että käyttäjä tietää mitä ohjelmistoa hänen tulee käyttää eri tehtävissä ja tarkoituksissa. Ohjelmistojen yhteistoiminnallisuus on varmistettu ja tietoaineisto pysyy eheänä ilman erillisiä käyttäjän toimia tallennusvaiheessa tai tietoa haettaessa.
- Alueellisen tai valtakunnallisen tietojärjestelmäpalvelun kautta luovutetun tiedon käsittely ohjelmistolla on mahdollista vain henkilölle, joka on nimenomaisesti saanut käyttöoikeuden katsoa luovutettua tietoa tai luovuttaa organisaation tietoja.
- Ohjelmistojen toimivuuden valvonta ja ylläpidon palvelutaso vastaavat niiden määriteltyä kriittisyyttä palvelutoiminnalle.
- Salattuja tietoja sisältävistä ohjelmistoista on dokumentti, jossa kuvataan ohjelmiston suojaus haittaohjelmilta ja asiattomalta tunkeutumiselta sekä suojauksen valvonta.
- Ohjelmistossa käsiteltävien tietojen tietoturva vastaa tietoaineistojen kriittisyyttä ja määriteltyä elinkaarta. Ohjelmistoilla on jatkuvuus- ja toipumissuunnitelma.
- Ohjelmistojen ylläpitoa varten avatut etäyhteydet ovat suojattuja ja sanomaliikenne salattua. Etäyhteyden käyttö edellyttää luotettavaa tunnistautumista. Ohjelmiston ylläpitotoimien laajuus sekä niistä riippuvat hyväksymiskäytännöt ja ajoitus on sovittu ja dokumentoitu. Poikkeamista sovituista malleista seurataan ja siihen puututaan.
- Työasemien ja palvelinten käyttöjärjestelmien sekä ohjelmistojen turvapäivityksiä varten on toimintasuunnitelma. Päivitystarvetta seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan.

3.6. Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan häiriötöntä viestintää, tiedonsiirtoyhteyksien käytettävyyttä, tiedonsiirron suojausta ja salausta, käyttäjien tunnistusta ja verkon varmistamista. Tietoliikenneturvallisuustyön tulos on turvatut tiedonsiirtoyhteydet. Työ kattaa tietoliikenneverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan.

Tietoliikenneturvallisuuden periaatteet:
- Organisaation tietojärjestelmäympäristö on suojattu palomuurilla, jota valvotaan. Palomuuri sallii vain määritellyn liikenteen järjestelmiin. Yhteydet ulkoisiin järjestelmiin ja portaaleihin ovat vahvasti salattuja.
- Arkaluonteisia ja salassa pidettäviä tietoja ei lähetetä organisaation sisällä eikä organisaatiosta ulos salaamattomina eikä suojaamatonta yhteyttä pitkin. Tietosuojaa koskevat vaatimukset ja vastuut on määritetty viestinvälityspalvelua koskevissa sopimuksissa. Etäyhteydet on toteutettu suojattuna ja vahvaa tunnistautumismenetelmää käyttäen.
- Tietoliikennelokia ja käyttöhäiriöitä seurataan säännöllisesti.

3.7. Käyttöturvallisuus

Käyttöturvallisuus kattaa turvallisen käytön toimintaolosuhteet, tekniikan toimivuuden valvonnan, käyttöoikeudet, käytön ja lokien valvonnan, ohjelmistotuen, ylläpidon ja huollon turvallisuustoimenpiteet, varmuus- ja suojakopioinnin sekä häiriöraportoinnin.
Käyttöturvallisuustyön tulos on hallittu tietoaineiston käsittely, jossa tietojen käyttäjä on suojattu tietämättömyyden, osaamattomuuden, tahattomien virheiden ja vahin-

kojen sekä tahallisten tekojen aiheuttamilta tilanteilta, joissa käyttäjä voisi syyllistyä tietojen asiattomaan tai oikeudettomaan käsittelyyn.

Käyttöturvallisuuden periaatteet:
- Tietojärjestelmien käyttökoulutus ja tehtävien mukaisen käytön opetus kuuluu jokaisen käyttäjän perehdytykseen. Käyttäjien osaamista seurataan ja tulokset huomioidaan henkilöstön koulutuksessa.
- Henkilöstön tietoturvaohjeisiin on koottu ohjeita ja neuvoja tietojen, tietojärjestelmien ja työvälineiden tietoturvalliseen käyttöön.
- Asiayhteys käyttäjän ja rekisteröidyn välillä on aina salassa pidettävien tietojen käytön edellytys. Tahaton käyttö ilman asiayhteyttä estetään informoinnin, teknisten järjestelmien ja tehtäväkuvien selventämisen avulla.
- Henkilötietoja sisältävän tietojärjestelmän käyttäjällä tulee olla henkilökohtainen ja yksilöivä käyttäjätunnus ja vain omassa tiedossa oleva salasana tai varmennekortti tai vastaava tunnistautumisväline.
- Käyttöoikeuksien myöntämisen periaatteet on dokumentoitu ja niiden noudattamista valvotaan. Käyttöoikeuksien haltijoista pidetään rekisteriä, jota säilytetään 12 vuotta.
- Käytöstä kerätään lokitiedot, joiden avulla käyttö voidaan jäljittää yksilötasolle. Säännöllisessä lokivalvonnassa syntyvät raportit säilytetään 5 vuotta. Käyttölokitietojen selvityspyynnöt ja niiden lokiseurantaraportit säilytetään 12 vuotta. Samoin 12 vuotta säilytetään toimenpiteisiin johtaneiden tapausten selvitykset ja raportit.

3.8. Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella varmistetaan asiakirja- ja tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito elinkaaren kaikissa vaiheissa. Tietoaineistoturvallisuustyön tulos on tietoaineistojen hallinta siten, että säädösten mukaisesti taltioidut tiedot säilyvät ja ovat saatavissa käyttötilanteen edellyttämässä ajassa, tarkoituksenmukaisessa muodossa ja järjestyksessä sekä hävitetään säädösten mukaisesti.

Tietoaineistoturvallisuuden periaatteet:
- Henkilö- ja potilastietojen käsittelyn edellytys on käyttäjän tehtävistä johtuva asiayhteys asiakkaaseen tai potilaaseen tai häntä koskeviin tietoihin. Henkilökuntaa sitoo vaitiolo- ja salassapitovelvollisuus.
- Sähköisessä muodossa olevia ja valtakunnallisten tietojärjestelmäpalveluiden 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.
- Henkilökunnan edellytetään tuntevan henkilötietojen käsittelyä ohjaavat ja rajoittavat normit sekä tietojen ja asiakirjojen luokittelu julkisuus- ja salassapitosäännösten mukaisesti. Perehdytyksen, koulutuksen ja tietoturvaohjeistuksen avulla ylläpidetään ja kehitetään henkilökunnan valmiuksia.
- Henkilö- ja potilastietojen käsittelystä ja menettelytavoista on laadittu palvelualuekohtaisia ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja. Näiden ohjeiden annosta ja ylläpidosta vastaa kyseinen palvelujohtaja.
- Asiakirjahallinnon ohjeseen sisältyy ohjeistoa tietojen luokittelusta, säilyttämisestä ja hävittämisestä sekä tietojen luovuttamisesta.

- Tietoaineiston säilytys tapahtuu arkistonmuodostussuunnitelman mukaisesti, joka on laadittu arkistosäädöksiä ja kansallisia tehtäväluokituksia noudattaen. Tietoaineiston säilyminen luottamuksellisena, eheänä ja muuttumattomana on huomioitu tiedon koko elinkaaren aikana aineiston lopulliseen hävittämiseen asti.
- Henkilörekisterin perustaminen ja henkilötietojen käsittely tulee olla asiallisesti perusteltua rekisterinpitäjän tehtävän ja toiminnan kannalta. Rekisteristä laaditaan rekisteri- ja tietosuojaseloste.
- Tietoaineiston lakisääteisen tiedonsaantioikeuden käytön, tarkastusoikeuden ja tiedon korjaamisvaatimuksen toteuttamista varten on sovittu palvelusta vastaavat henkilöt ja kuvattu prosessin toteuttamistapa.
- Tietoaineiston käyttämisestä tai luovuttamisesta laskutus, tilastointi-, raportointi-, kehittämis- ja tutkimustarkoituksiin on annettu ohjeet.

4. ORGANISAATIO, VASTUUT ja TOIMIVALTUUDET

Tietoturvallisuus on koko liikelaitoskuntayhtymän yhteinen asia. Tietoturvallisuudesta vastaa **johtokunta** ja sitä johtaa **liikelaitoskuntayhtymän johtaja**. Vastuu on riippumatonta siitä, onko joitakin organisaation toimintoja ulkoistettu. Johtokunta päättää yhtymän kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista sekä toimivaltuuksista. Johtokunnan hyväksymä tietoturva- ja tietosuojapolitiikka on tietoturvan toteuttamisen perusta.
Johtokunta on päätöksellään 14.5.2012 § 63 asettanut tietosuojavastaavan, tietoturvavastaavan ja tietoturvatyöryhmän, hyväksynyt tietosuojavastaavan ja tietoturvavastaavan toimenkuvat sekä valtuuttanut liikelaitoskuntayhtymän johtajan nimeämään tietosuojavastaavan, tietoturvavastaavan ja tietoturvatyöryhmän.

Tietosuojavastaavan tehtävänä on asiantuntijana auttaa ylintä johtoa velvoitteittensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu suunnittelutoimintaan, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutuksen toteutukseen. Tietosuojavastaavan tehtävänä on seurata ja valvoa henkilötietojen käsittelyä ja suojausmenettelyä, tukea ja ohjata henkilökuntaa ja rekisteröityjä tietosuoja-asioissa, toimia yhdyssiteenä valvontaviranomaisiin sekä raportoida johdolle tietosuojan tilasta ja kehittämistarpeista.
Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä ja ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa erillisen johtokunnan hyväksymän seuranta- ja valvontasuunnitelman mukaisesti.
Tietosuojavastaavan toimenkuvassa on tarkempi kuvaus tehtävistä ja oikeuksista.

Tietoturvavastaava toimii tietoturvallisuuden asiantuntijana ja tietoturvan kehittäjänä. Tietoturvavastaava laatii tietoturvallisuussuunnitelman, jossa määritetään tietojärjestelmien vaatimukset, turvaluokitukset, turvallisuustoimenpiteet ja niiden teknisen toteutuksen. Tietoturvavastaava koordinoi ja valvoo käyttöoikeuksien jakoa ja hallintaa. Lisäksi hän edistää tietoturvatietoutta toimintayksiköissä ja niiden ostamissa palveluissa, seuraa ja valvoo tietoturvan toteutumista sekä raportoi johdolle tietoturvan tilasta ja kehittämistarpeista.
Tietoturvavastaavalla on oikeus ylläpitää käyttöoikeusrekistereitä, valvoa tietoturvaa teknisin keinoin, toimia tietosuojavastaavan apuna käyttölokivalvonnan teknisessä toteutuksessa ja ryhtyä toimenpiteisiin tietoturvan ongelmatilanteissa.
Tietoturvavastaavan toimenkuvassa on tarkempi kuvaus tehtävistä ja oikeuksista.

Tietosuojavastaavan ja tietoturvavastaavan apuna toimii **tietoturvatyöryhmä**. Työryhmään kuuluvat ainakin tietosuojavastaava, tietoturvavastaava, palvelualuejohtajat, henkilöstöpäällikkö ja hallintopäällikkö. Tietoturvatyöryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi, huolehtii tietoturvallisuusperiaatteiden toteuttamisesta, seuraa tietoturvan eri vastuualueiden suunnitelmien, ohjeiden, selosteiden ja lomakkeiden laadintaa sekä ottaa tarvittaessa kantaa käytäntöihin ja kehittämishankkeisiin. Lisäksi työryhmä seuraa tietoturvallisuustilannetta.

Palvelujohtajat vastaavat oman palvelualueen tietoturvasta ja päättävät siihen kuuluvista kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimivaltuuksista sekä tietosuojaa koskevasta sisäisestä ja ulkoisesta tiedottamisesta. Palvelujohtajat vastaavat palvelualueensa henkilötietojärjestelmien rekistereistä, rekisteriselosteiden olemassaolosta ja rekistereiden vastuuhenkilöiden nimeämisestä. Palvelujohtajat antavat henkilötietojen ja asiakirjojen käsittelystä ja menettelytavoista palvelualuekohtaisia ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja.

Sisäisen tukipalvelun johtajan johdolla toimivalle atk-palveluille on keskitetty erityistä osaamista ja koordinaatiota vaativat tietohallintotehtävät. Atk-palvelut toteuttaa tietojärjestelmien ja niiden käytön tietoturvan teknisen toteutuksen suunnittelun, toteutuksen ja raportoinnin. Jokaisella tietojärjestelmällä on omistajayksikkö, **pääkäyttäjä** ja tarvittaessa erillisiä **vastuukäyttäjiä**. He vastaavat tietojärjestelmien toiminnasta, hoidosta, turvallisuudesta ja käytön riittävästä ohjeistuksesta sekä tietojärjestelmäselosteiden laadinnasta.

Hallintopäällikön johdolla toimivan arkistotoimen vastuulla on varmistaa asiakirjojen käytettävyys, säilyminen ja lainmukainen luovuttaminen ja säilyttäminen arkistonmuodostussuunnitelman mukaisesti. Arkistotoimi vastaa myös liikelaitoskuntayhtymän rekisterihallinnon käytännön toteutuksen koordinoinnista siten, että rekistereiden perustaminen, ylläpito ja lakkauttaminen on suunnitelmallista, luetteloitua ja rekisterit arkistolainsäädännön mukaisesti säilytettyjä ja poistettuja. Pääosa henkilörekistereistä ylläpidetään sähköisissä tietojärjestelmissä. Tietojärjestelmistä ylläpidetään erikseen tietojärjestelmäluetteloa, joka toimii tietojärjestelmäselosteena. Vastuuhenkilöinä ovat tietoturvavastaava ja hallintopäällikkö. Hankinta- ja sopimusvastaavana hallintopäällikkö vastaa siitä, että tietoturvallisuusnäkökohdat arvioidaan hankinnoissa ja tietosuojatoimet ja tietoturvavastuut sisältyvät ostopalvelusopimuksiin.

Esimiehet vastaavat tietoturvan ja tietosuojan toteutumisesta, henkilörekistereiden lain mukaisesta käytöstä, ohjeiden noudattamisesta sekä tiedottamisesta ja valvonnasta omassa yksikössään. Esimies huolehtii, että henkilöstö on tutustunut liikelaitoskuntayhtymän tietoturva- ja tietosuojapolitiikkaan sekä henkilöstön tietoturvaohjeisiin ja tehnyt asiakirjojen, tietojen ja tietojärjestelmien vaitiolo- ja salassapitositoumuksen ennen tietojärjestelmien käyttöluvan hakemista. Lisäksi esimies huolehtii, että henkilöstö suorittaa tietoturvan ja tietosuojan verkkokoulutuksen tietosuojavastaavan ohjeistuksen mukaisesti.

Jokainen **työntekijä**, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa oman toimintansa tietoturvallisuudesta ja annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.

5. TIETOTURVALLISUUDEN ONGELMATILANTEET

Jokainen työntekijä on velvollinen raportoimaan tietoturvaan liittyvistä uhista ja poikkeamista esimiehelleen ja/tai tietosuojavastaavalle tai tietoturvavastaavalle. Tietoturvalainsäädäntöä ja liikelaitoskuntayhtymän tietoturva- ja tietosuojapolitiikkaa sekä sen perusteella annettuja ohjeita ja määräyksiä vastaan havaitut rikkomukset tiedotetaan aina esimiehelle.

Jos kyseessä on toistuva tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin johtokunnan hyväksymän käyttölokien seuranta- ja valvontasuunnitelman mukaisesti. Tietoturvarikkomuksesta seuraa varoitus ja sen perusteella on mahdollista purkaa työ- tai virkasuhde. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin. Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

Tietosuojavastaavalla ja tietoturvavastaavalla on liikelaitoskuntayhtymän ylimmän 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. He raportoivat tarvittaessa tapauksista myös organisaation johdolle.