Tietoturvapolitiikka

Sisällysluettelo

Käsitteet

Kiistämättömyys	Ilmentää sitä, että tiedon lähettäjä tai vastaanottaja tai tietoon liittyvä tapahtuma voidaan varmistaa luotettavasti myös jälkikäteen.
Kyberturvallisuus	Tietoturvallisuuden alalaji, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Sosiaali- ja terveydenhuollon kyberturvallisuuteen varautuminen tarkoittaa sitä, että keskeisten toimintojen osalta on tehty suunnitelma, jonka mukaan harjoitellaan säännöllisesti.
Käytettävyys	Tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana.
Tietoturvapolitiikka	Organisaation johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Tietoturvapolitiikka ja –strategia ovat osa organisaation toiminta- ja tietohallintopolitiikkaa.
Tietoturvallisuus = tietoturva	Hallinnollisia ja teknisiä toimenpiteitä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Käytettävyys tarkoittaa sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvallisuus on riskienhallintaa ja osa organisaation turvallisuutta.
Tietosuoja	Toimenpiteet, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä. Yksityisyyttä suojataan muun muassa estämällä tietojen valtuudeton saanti, säilyttämällä tietojen luottamuksellisuus ja suojaamalla henkilötietojen valtuudeton tai henkilöä vahingoittava käyttö.
Tiedonhallintayksikkö	Viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti.
Tietovarantojen yhteentoimivuus	Tietojen hyödyntämistä ja vaihtoa eri tietojärjestelmien välillä siten, että tietojen merkitys ja käytettävyys säilyvät.
Todentaminen (autentikointi)	Varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta, alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.

1. Johdanto

Tietoturvapolitiikka on Kainuun hyvinvointialueen johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Tietoturvapolitiikan avulla vaikutetaan omalta osaltaan siihen, että Kainuun hyvinvointialueen strategiassa määritelty visio, toiminta-ajatus, arvot ja palvelut toteutetaan laadukkaasti ja turvallisesti.

Tietojen turvaaminen on olennainen osa Kainuun hyvinvointialueen toiminnan turvallisuutta. Tietojärjestelmät tukevat hyvinvointialueen toimintaa sen tuottaessa toiminta-ajatuksensa mukaisia erikoissairaanhoidon, perusterveydenhuollon, sosiaalitoimen ja pelastustoimen palveluita. Kainuun hyvinvointialueen tietoturvapolitiikan tarkoituksena on yhdenmukaistaa tietosuoja- ja tietoturvakäytäntöjä alueellisesti sekä vahvistaa tietojenkäsittelyn tietoturvan perustaso, organisointi, vastuut ja seurantamenetelmät.

Tämä Tietoturvapolitiikka-asiakirja on hyvinvointialueen johdon hyväksymä tietoturvan hallinnollinen ohje, jonka liitteissä on nostettu esille tietoturvaan liittyviä erityiskysymyksiä, jotka toimivat työohjeina. Hyvinvointialueella on lisäksi tietoturvapolitiikkaa tarkentavia tietoturvaan liittyviä käytäntöjä, prosesseja ja ohjeita. Tietoturvapolitiikka tarkistetaan ja arvioidaan vuosittain tai merkittävien muutosten yhteydessä.

Turvattavia tietoja ovat sekä manuaalisessa että sähköisessä muodossa olevat tiedot. Erityistä huomiota kiinnitetään sosiaali-, terveydenhuollon- ja pelastustoimen toiminnan kannalta kriittisiin tietojärjestelmiin sekä niiden sisältämiin tietoihin. Tietoaineistot sisältävät potilaisiin, asiakkaisiin, työntekijöihin, pelastustoiminnan kohteisiin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava tehokasta, virheetöntä ja varmaa.

Kainuun hyvinvointialueelle on tärkeää, että tietoturvallisuustyön päämääränä on organisaation lakisääteisten palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa, ja että potilas/asiakas voi luottaa hänen tietojensa olevan turvassa, oikeita ja vain hoitoon/asiakassuhteeseen osallistuvien saatavissa, ja että niitä käsitellään kaikissa vaiheissa asianmukaisesti. Tietojen käsittely perustuu hoito/asiakassuhteeseen tai muuhun asialliseen yhteyteen, jonka perusteena on virka- tai työtehtävien hoito. Luottamuksellisuus ja yksityisyyden suoja toteutuvat myös henkilöstöasioiden käsittelyssä.

1.1 Tietoturvapolitiikan velvoittavuus

Tietoturvaan liittyvä lainsäädäntö ja tietoturvapolitiikka sekä sitä tarkentavat tietoturvakäytännöt ja ohjeet koskevat kaikkia Kainuun hyvinvointialueen toiminnoissa työskenteleviä ja hyvinvointialue velvoittaa kaikkia työntekijöitä noudattamaan niitä.

Soveltuvilta osin ne ulotetaan myös luottamushenkilöiden sekä yhteistyö- että sopimuskumppaneiden ja muiden sidosryhmien noudatettavaksi. Mikäli yhteistyön puitteissa käsitellään luottamuksellisia tietoja, tietoturvaan liittyvät vastuut ja käytännöt on kirjattava yhteistyökumppanin kanssa tehtäviin sopimuksiin.

1.1 Tavoite

Tietoja käsitellään Kainuun hyvinvointialueella yhdenmukaisten tietosuoja- ja tietoturvaperiaatteiden mukaisesti. Tällä turvataan potilas- ja asiakastyön mahdollisimman sujuva ja häiriötön toiminta sekä hyvinvointialueen oma operatiivinen toiminta.

Tietoturvallista organisaatiota rakennetaan eri toimijoiden yhteistyössä muodostaman jatkuvan riskienhallintaprosessin avulla. Tavoitteena on turvata perustehtävän häiriötön ja laadukas toteuttaminen. Tämän päämäärän saavuttamiseksi:

- Kaikkien tietoja käsittelevien henkilöiden on ymmärrettävä tietojen käsittelyn periaatteet: mitä, missä tarkoituksessa ja milloin tietoa saa käsitellä ja käyttää sekä ymmärtää ja huomioida potilaan/asiakkaan halu ja oikeudet kieltää tietojensa käsittely tietyissä tilanteissa.
- Johdon sitoutuminen ja organisaation koko henkilöstön tietoturvatietoisuus on oltava hyvä. Kaikki ymmärtävät tietoturvan merkityksen sekä tehtävänsä ja velvollisuutensa tietoturvallisuuden ylläpidossa.
- Tietosuoja- ja tietoturvaperiaatteita toteutetaan hyvinvointialueen kaikessa toiminnassa.
- Tietojen luottamuksellisuuden, eheyden ja saatavuuden vaatimus toteutuu kaikessa tietojenkäsittelyssä ja se mahdollistaa tietoturvallisen asioinnin ja tietojen käytön.

1.2 Säädösten ja muiden vaatimusten täyttäminen

Kainuun hyvinvointialueen tietojenkäsittelyn ja sen turvaamisen periaatteet noudattavat kansallisia ja kansainvälisiä tietoturvallisuutta koskevia säädöksiä, standardeja, terveydenhuollon auditointivaatimuksia ja suosituksia, sekä Pelastustoimen säädöksiä ja suosituksia. Näistä keskeisimpiä ovat julkisuuslaki, laki hyvinvointialueesta, laki potilaan asemasta ja oikeuksista, laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, laki asiakas- ja potilastietojen sähköisestä käsittelystä, arkistolaki, tiedonhallintalaki, tietosuojalaki pelastuslaki, laki julkisen hallinnon turvallisuusverkkotoiminnasta, sekä Euroopan unionin tietosuojadirektiivi ja -asetus. Kaikessa toiminnassa noudatetaan hyvää tietojenkäsittelytapaa, velvoitteita ja sopimuksia.

Tietoturvallisuutta koskevat määräykset ovat keskeisiä ja velvoittavia. Velvoitteissa korostetaan salassapidon, vaitiolovelvollisuuden ja yksityisyyden suojan toteutumista sekä tietoturvallisuuden, tietosuojan, hyvän tietojenkäsittelytavan ja laadun merkitystä.

Hallinnollisten dokumenttien ja niiden tuottamiseen liittyvien prosessien osalta noudatetaan Sähke2-normia sähköisten asiakirjallisten tietojen käsittelyn, hallinnan

ja säilyttämisen osalta siinä vaiheessa, kun se on tietojärjestelmien puolesta toteutettavissa.

1.3 Tarkoitus

Tietoturvatoimilla estetään tietojen luvaton käyttö ja haltuunotto. Suuri osa hyvinvointialueella käsiteltävästä tiedosta on luottamuksellista, arkaluonteista sekä salassa pidettävää ja voi paljastuttuaan rikkoa yksityisyyden suojaa. Tietoturvatoiminnan tavoitteena on vastata siitä, että tieto on oikeaan aikaan, oikeassa paikassa ja eheänä, vain niiden henkilöiden käytettävissä, joilla on siihen laillinen tai työtehtävänsä vaatima valtuutus.

Tiedon saatavuudella ja käytettävyydellä tarkoitetaan, että tieto on tallennettu sellaisessa muodossa, että se on luettavissa, ymmärrettävissä ja tulkittavissa oikein. Lisäksi tiedon on oltava kattavaa, ajantasaista, oikeellista ja helposti käytettävissä ilman tulkinta- ja väärinkäyttömahdollisuutta.

Tietoturvatoimilla vähennetään ja ennaltaehkäistään tietoturvariskien syntyminen, varmistetaan tietojen saatavuus poikkeuksellisissa olosuhteissa, toiminnan jatkuvuus, asiakkaiden ja potilaiden oikeusturva ja yksityisyyden suoja lainsäädännön ja muiden määräysten edellyttämällä tavalla. Lisäksi varmistetaan tietojen oikeellisuus ja luotettavuus sekä se, että asianosaiset ovat tiedostaneet tietoturvan merkityksen.

1.4 Suojattavat kohteet

Turvattavia tietoja ovat sekä manuaalisessa että sähköisessä muodossa olevat tiedot. Tietoturvapolitiikka kattaa myös vaitiolovelvollisuuden piiriin kuuluvan ja muunkin tiedon, jonka tahtomattaan kuulee, näkee tai lukee.

Erityistä huomiota kiinnitetään organisaation toiminnan kannalta kriittisiin tietojärjestelmiin ja niiden sisältämiin tietoihin. Kriittisiä tietojärjestelmiä ovat asiakas- ja potilastietojärjestelmät sekä talous- ja henkilöstöhallinnon tietojärjestelmät, ja näiden sisältö. Tietojen turvaamisen kannalta on huomioitava myös muut osarekisterit, sekä ulkoiset että sisäiset (esim. kuntayhtymän väestörekisterikanta ja sosiaali- ja terveydenhuollon valtakunnalliset rekisterit). Pitkällä aikavälillä kriittisinä järjestelminä voidaan pitää myös järjestelmiä, joiden sisältämää tietoa ei ole palautettavissa ehkä koskaan, jos niissä oleva tieto tuhoutuu. Suojattavat kohteet luetteloidaan ja priorisoidaan kriittisten kohteiden tunnistamisen perustaksi.

2. Tietoturvallisuuden perustason määrittely

Tietoturvallisuus on laaja toiminnallinen kokonaisuus, jonka keskeisimmät turvallisuustekijät liittyvät ihmisten toimintaan. Tietoturvallisuuden vaikutukset ulottuvat koko organisaatioon ja sen ylläpitäminen on jatkuva prosessi, jota toteutetaan hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Tietoturvallisuuden kehittämistä yksiköissä ja

tietojärjestelmissä ohjaa hyvin toteutettu riskienhallinta. Käyttäjien toimintaa ohjataan toimintaohjeilla sekä tietoturvakoulutuksella. Tietohallinto vastaa tietoturvasääntöjen ylläpitämisestä.

2.1 Tärkeimmät hallinnolliset tietoturvatoimet

2.1.1 Tietoturvallisuus osana kaikkea toimintaa

Hyväksytyn tietosuoja ja -turvapolitiikan mukaiset tietoturvatoimet tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa organisaation yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturva on erityisesti sosiaali- ja terveydenhuollon kriittinen tekijä, koska potilaan ja asiakkaan on luotettava ehdottomasti tietojensa tietosuojaan. Tämä luottamus on palvelun kulmakivi.

Kainuun hyvinvointialueen tietoturvallisuustyön tulee luoda asiakkaille, potilaille ja henkilöstölle luottamus siitä, että salassapito- ja vaitiolovelvollisuus sekä yksityisyyden suoja toteutuvat säädösten mukaisesti. Lisäksi tietoja tulee käsitellä kaikissa vaiheissa huolella ja asianmukaisesti.

2.1.2 Tietojen turvallinen käsittely tietojärjestelmissä ja tietoverkoissa

Kainuun hyvinvointialueen toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta turvataan ja estetään tietojen ja tietojärjestelmien joutuminen ulkopuolisille. Tietojen ja tietojärjestelmien valtuudeton käyttö ja tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen estetään sekä minimoidaan aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin jatkuvuudenhallinnalla.

Lainsäädäntöä ja ohjeistusta tulee seurata jatkuvasti. Muutosten vaikutus on otettava huomioon organisaation tietoturvallisuuden kehittämisessä. Tietoturvallisuutta koskevat määräykset ovat keskeisiä ja velvoittavia. Velvoitteissa korostetaan salassapidon, vaitiolovelvollisuuden ja yksityisyyden suojan toteutumista sekä tietoturvallisuuden, tietosuojan, hyvän tietojenkäsittelytavan ja laadun merkitystä.

Organisaation tiedot ja tietojenkäsittelyjärjestelmät ja niiden käyttöympäristöt pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden liitteissä kuvattujen toimenpiteiden avulla.

2.1.3 Tietoturvariskien hallinta

Riskienhallinnan tarkoituksena on mahdollistaa organisaation menestyminen, toiminnan jatkuvuuden takaaminen ja tavoitteiden saavuttaminen. Riskienhallinta on järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan lisäksi organisaation johtamista ja kehittymistä. Jatkuvaa riskienhallintaa tarvitaan tietoturvallisuustoimenpiteiden oikeaan mitoittamiseen.

Kainuun hyvinvointialueella tietoturvariskien hallintaa toteutetaan voimassa olevien ohjeistuksien ja prosessien mukaisesti.

2.1.4 Tiedon ja tietojärjestelmien luokittelu

Organisaatiossa on käytössä tietojen turvallisuusluokitus ja tietojärjestelmien kriittisyysluokitus osana kokonaisarkkitehtuurin tietojärjestelmäsalkkua. Jokaisella tietojärjestelmällä tai sen osalla on yksikäsitteinen omistaja ja/tai haltija.

2.1.5 Tietoturvallisuusasioiden tiedottaminen

Normaaliolojen viestintä (ulkoinen ja sisäinen)
Tietoturvallisuutta koskevista yleisistä asioista tiedottaminen kuuluu hyvinvointialueen tietoturvavastaavalle. Tietosuoja-asioihin liittyvän tiedottamisen hoitaa ensisijaisesti tietosuojavastaava.

Ajankohtaisista tiettyä tietojärjestelmää koskevista merkittävistä tietoturvauhkista sisäisesti tiedottaminen kuuluu kyseisen järjestelmän pääkäyttäjille.

Kriisiviestintä
Kriisiviestintä on viestintää poikkeustilanteissa, joissa organisaation toimintaedellytykset ja/tai maine ovat uhattuina. Kriisi voi vaarantaa tärkeitä yhteiskunnallisia tai muita etuja ja järkyttää normaalia toimintaa, päätöksentekoa ja tiedotuskäytäntöä. Kriisi voi koskea itse organisaatiota (sisäinen kriisi) tai sen toimintaa ja siihen liittyviä palveluja ja palvelujen tuottamisen nopeutta (ulkoinen kriisi).

Kriisiviestinnän tarkoituksena on tiedottaa poikkeustilanteesta henkilöille, joihin tilanteella voi olla vaikutusta. Kriisitilanteiden viestinnästä on ohjeet Kainuun hyvinvointialueen kriisiviestinnän periaatteet -asiakirjassa. Sen mukaan kriisitilanteessa viestinnästä vastaa aina se toimija tai viranomainen, joka johtaa toimintaa.

2.1.6 Henkilökunnan koulutus

Henkilökunnalle annetaan heidän toimintojen edellyttämä tietosuojaan ja tietoturvaan liittyvä koulutus. Näistä järjestetään säännöllisesti organisaation

sisäistä koulutusta ja tarvittaessa myös yksikkökohtaista neuvontaa. Sijaisille, opiskelijoille ja yhteistyökumppaneille tiedotetaan tietosuojasta ja tietoturvasta sekä heitä koskevista säännöistä ja suosituksista.

2.2 Tärkeimmät teknisluontoiset tietoturvatoimet

2.2.1 Toiminnan jatkuvuuden hallintaprosessi

Toiminnan jatkuvuuden hallintaprosessi, jatkuvuussuunnitelma, tulee toteuttaa onnettomuuksien ja turvallisuushäiriöiden (joita voivat aiheuttaa esim. luonnonmullistukset, onnettomuudet, laiteviat ja ilkivalta) aiheuttamien keskeytysten vähentämiseksi hyväksyttävälle tasolle yhdistämällä ehkäiseviä ja palautumista edistäviä turvamekanismeja.
Jatkuvuussuunnitelmia tulee kehittää ja toteuttaa käytännössä varmistamaan, että toimintaprosessit saadaan palautettua toimintaan vaaditussa ajassa. Suunnitelmia tulee pitää yllä ja harjoitella, jotta niistä tulee muiden hallinnollisten prosessien rinnalla integroitunut osa toimintaa.

Toiminnan jatkuvuuden hallintaan tulee sisältyä turvamekanismit riskien havaitsemiseen ja vähentämiseen, niillä tulee rajoittaa uhkan mahdollisen toteutumisen aiheuttamia seurauksia ja niillä tulee varmistaa olennaisen tärkeiden toimintojen nopea palautuminen. Toiminnan jatkuvuussuunnitelmia tulee pitää yllä säännöllisin arvioinnein ja päivityksin tehokkuuden säilymisen varmistamiseksi. Tässä ylläpitotehtävässä tulee huomioida organisaation valmiussuunnitelma ja siellä asetetut vaatimukset tietojärjestelmien ja tiedon saatavilla olosta käyttöympäristö huomioiden.

2.2.2 Tietoturvapäivitykset ja käyttöturvallisuus

Kriittisten komponenttien, palvelinten, työasemien, käyttöjärjestelmien sekä ohjelmistojen turvapäivityksiä varten on palveluntuottajilla toimintasuunnitelma. Päivitystarvetta seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan ennakolta, jos mahdollista. Kriittiset päivitykset asennetaan välittömästi viivytyksettä ja ne dokumentoidaan. Turvapäivitysten asennukset keskitetään ja automatisoidaan mahdollisuuksien mukaan.

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojakopioinnista sekä häiriöraportoinnista.

2.2.3 Käyttäjähallinta

Organisaatio vastaa järjestelmien tietoturvasta ja laadusta yhdessä toimittajien ja palveluntuottajien kanssa sopimusten mukaisesti. Organisaatiossa on yksiselitteisesti määritelty käyttövaltuushallintaprosessi vastuineen ja

poikkeusmenettelyineen. Palveluiden saatavuus, käytettävyys, luotettavuus, hallinnointi ja valvonta on määritelty yhdessä palveluntuottajien kanssa.

Tietojärjestelmien käyttäjähallinta rakentuu henkilötietojen hallinnasta, käyttöoikeuksien ja pääsynhallinnasta, tunnistamisesta, käyttöoikeuksien jakamisesta sekä käyttöoikeuksien seurannasta. Käyttäjähallintaan kuuluvat organisaatiossa yhteisesti sovitut toimintatavat, joiden perusteella tietojärjestelmien käyttöoikeuksia määritellään, luodaan, ylläpidetään ja hyödynnetään.

Käyttäjähallinta perustuu henkilön tehtävään organisaatiossa, roolimäärityksiin, lupiin ja kieltoihin. Tietojärjestelmän käyttäjälle myönnetään tehtävän ja roolin vaatimat oikeudet tietojärjestelmiin. Esimies vastaa henkilöstönsä käyttöoikeuksien hallinnoinnista, niiden myöntämisestä, muuttamisesta ja poistamisesta.

2.2.4 Sisäiset tarkastukset ja poikkeamaraportointi

Lokien muuttumattomuus ja kiistämättömyys tulee taata vaatimustenmukaisesti koko niille määritellyn säilytysajan lainsäädännön vaatimusten mukaisesti. Kansalaisen tiedonsaanti lokitiedoista toteutetaan kansallisten määritysten mukaisesti. Käyttölokin osalta julkisuuslain mukaisen valitusprosessin ollessa kesken, lokitietoja ei saa tuhota talletusajan mahdollisesti päättyessä.

Tietojärjestelmien poikkeustilanteiden hallinnan edellyttämien toimien suunnitelmat sisällytetään toipumissuunnitelmaan. Ohitustilanteet merkitään erilliseen luetteloon ja hätäkorjaustilanteiden jälkeen palataan normaalien käyttöoikeuksien ja käyttöoikeusprosessin mukaiseen toimintaan

Kainuun hyvinvointialueella tehdään potilas- ja asiakastietojen käytön valvontaa lokivalvonnalla ja muilla tarvittavilla menetelmillä.

Tietoturvapoikkeamista, haitallisista ja toimintaa vaarantavista tapahtumista raportoidaan kaikilla tasoilla viivytyksettä poikkeamien hallintaprosessin (HaiPro) mukaisesti ja prosessi on kuvattu organisaation tietoturvallisuutta käsittelevissä kokonaisarkkitehtuurikuvauksissa.

2.2.5 Viestien ja dokumenttien välittäminen

Viestit ja dokumentit välitetään luokitusten vaatimin salausmenettelyin. Viestinvälityksen tietosuojaa koskevat vaatimukset ja vastuut on määritelty organisaation ja viestinvälitysoperaattorin välisissä sopimuksissa sekä tietoturvallisuutta käsittelevissä kokonaisarkkitehtuurikuvauksissa.

Palveluja ulkoistettaessa huolehditaan Suomen lainsäädännön ja palvelutoiminnan vaatimustenmukaisesta luottamuksellisen aineiston käsittelystä siten, että tiedot eivät voi joutua sivullisten käsiin.

2.2.6 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmän toimivuus käsitellään johtoryhmässä ja johto päättää tarvittavista muutoksista. Teknisten tietoturvallisuuskuvausten tietosuojasta vastaa tietohallintojohtaja.

3. Tietoturvatyön organisointi ja tehtävät

Tietojen turvaaminen ja tietosuojan toteuttaminen ovat osa johtamistoimintaa. Käytännön tietoturvatoimia hallinnoi ja hoitaa nimetty hyvinvointialueen tietoturvallisuusorganisaatio. Toimintaan kuuluvat päivittäisten toimien ohella tietojen turvaamismenettelyjen määrittely ja ylläpito, työhön osoitettujen riittävien resurssien turvaaminen sekä välineistön ja toimenpiteiden turvallisuudesta ja tietoturvaominaisuuksista huolehtiminen.

3.1 Kainuun hyvinvointialueen tietoturvaorganisaatio

Hyvinvointialueenjohtaja nimeää tietoturva- ja tietosuojatyöryhmän jäsenet, joita ovat jokaisen toimialueen tietoturvan ja tietosuojan vastuuhenkilöt sekä muut henkilöt, joiden työtehtäviin hyvinvointialueen tietoturva- ja tietosuoja-asiat olennaisesti kuuluvat.

Hyvinvointialueen työntekijöiden työtehtäviin voi kuulua tietoturvaan liittyviä tehtäviä, vaikka he eivät kuuluisikaan varsinaiseen tietoturvaorganisaatioon. Tietoturva on koko organisaation asia ja hyvinvointialueen jokainen työntekijä vastaa omalta osaltaan tietoturvallisuuden toteutumisesta.

3.2 Tietoturvatehtävät ja organisointi

Tietoturvaorganisaatio sekä tietohallinto huolehtivat, ylläpitävät ja valvovat koko organisaation tietoaineiston tietoturvaa omien vastuualueidensa mukaisesti.

Hyvinvointialueen aluehallitus

Hyvinvointialueen aluehallitus hyväksyy tietoturvapolitiikan.

Hyvinvointialueenjohtaja

Hyvinvointialuejohtaja vastaa tietoturvallisuuden sekä tietosuojan järjestämisestä sekä kehittämisestä.

Johtoryhmä

Hyvinvointialueen johtoryhmän jäsenet vastaavat kukin omalta osaltaan tietoturvapolitiikan noudattamisesta omassa toiminnassaan.

Johdon tulee osoittaa sitoutumisensa tietoturvallisuuden hallintajärjestelmän luomiseen, käyttöönottoon, käyttöön, valvontaan, katselmointiin, ylläpitoon ja parantamiseen:

- määrittelemällä tietoturvaperiaatteet
- varmistamalla, että tietoturvatavoitteet asetetaan ja tietoturvasuunnitelmat laaditaan kaikissa toimijaorganisaatioissah
- määrittelemällä tietoturvallisuuteen liittyvät roolit ja vastuut

- viestimällä organisaatiolle tietoturvatavoitteiden ja tietoturvapolitiikan noudattamisen, niihin liittyvien lakisääteisten velvoitteiden noudattamisen ja jatkuvan parantamisen tärkeydestä
- huolehtimalla siitä, että käytettävissä on riittävät resurssit tietoturvallisuuden hallintajärjestelmän kehittämiseen, toteuttamiseen, käyttöön ja ylläpitoon
- päättämällä hyväksyttävästä riskitasosta

Tuotannon hallinto- ja tukipalveluiden toimialuejohtaja

Tuotannon hallinto- ja tukipalveluiden toimialuejohtaja vastaa hyvinvointialueen tietoturvallisuuden johtamisesta ja koordinoinnista.

Tietohallintojohtaja

Tietohallintojohtaja vastaa tietojärjestelmien operatiivisesta toiminnasta tietoturvallisella tavalla. Tietohallintojohtaja vastaa tietoliikenteen ja muun tekniikan järjestämisestä tietoturvallisella tasolla.

Tietoturvavastaava

- valmistelee tietoturvallisuuteen liittyviä kehittämishankkeita yhdessä muiden tietoturvaorganisaatioon kuuluvien henkilöiden kanssa
- ohjeistaa tietoturvallisuusasiat ja huolehtii, että niistä tiedotetaan ja koulutetaan
- vastaa tietoturvapoikkeamien seurannasta ja tilastoinnista
- tiedottaa tietoturvallisuusasioista ja -ongelmista
- valmistelee tietoturvaan liittyvän kommunikoinnin koko organisaation, sidosryhmien ja erityisesti esimiesten kanssa
- vastaa tietoturvatietoisuuden ja osaamistason seurannan toteuttamisesta.
- osallistuu hyvinvointialueen turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tarvittaessa turvallisuusasioita käsittelevän ryhmän jäsenenä
- raportoi tietoturvallisuuden tilasta ja kehittämistarpeista sekä tietoturvavastaavan toiminnasta tietosuoja- ja tietoturvatyöryhmälle sekä hyvinvointialueen johdolle
- osallistuu tietoturvapoikkeamien vakavuusasteiden määrittelytyöhön
- toimii tietoturvallisuuden asiantuntijana hyvinvointialueen toiminta-alueella, tarvittaessa tekee esityksiä asiantuntijapalveluiden hankkimisesta
- valvoo, että tietoturvallisuusasiat on organisoitu hyvinvointialueen toimipaikoissa ja yksiköissä

Arkistopäällikkö/tietosuojavastaava

Hyvinvointialueen arkistopäällikkö toimii organisaation tietosuojavastaavana. Tietosuojavastaavan tehtävänä on toimia rekisterinpitäjän apuna organisaation erityisasiantuntijana ja antaa asiantuntijatukea organisaation henkilöstölle. Tietosuojavastaava avustaa myös organisaation johtoa tietosuojan suunnittelussa ja toimeenpanossa sekä saavuttamaan hyvän henkilötietojen käsittelytavan ja korkean tietosuojan tason.

- vastaa tietosuojaohjeiden tekemisestä ja päivittämisestä
- toimii tietosuojan itsenäisenä ja riippumattomana erityisasiantuntijana hyvinvointialueen toiminta-alueella
- tukee, ohjaa ja opastaa henkilökuntaa ja rekisteröityjä tietosuoja-asioissa
- kehittää ja edistää tietosuojaa organisaatiossa
- ohjeistaa tietosuoja-asiat ja huolehtii, että niistä tiedotetaan ja koulutetaan henkilökuntaa
- osallistuu hyvinvointialueen tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tietosuoja- ja tietoturvatyöryhmän jäsenenä
- seuraa ja valvoo henkilö- ja potilastietojen käsittelyä ja suojaamista ja suojausmenetelmiä sekä raportoi niihin liittyvistä epäkohdista tietosuoja- ja tietoturvatyöryhmälle
- suunnitella ja toteuttaa tietojärjestelmien lokiseurantaa eli käytönvalvontaa
- osallistuu organisaation henkilötietojen käsittelyä koskevaan suunnittelutoimintaan
- toimii yhdyssiteenä valvontaviranomaisiin
- raportoi organisaation johdolle ja tietosuoja- ja tietoturvatyöryhmälle tietosuojan tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta) sekä tietosuojavastaavan toiminnasta
- toteuttaa organisaation johdon osoittamia muita tietosuojaa tukevia tehtäviä
- seuraa ja valvoo tietosuojan toimivuutta ja vastaa, että organisaation selosteet henkilötietojen käsittelytoimista on tehty EU:n tietosuoja-asetuksen mukaisesti.

Arkistopäällikön johdolla toimivan arkisto- ja tietosuojapalveluiden vastuulla on varmistaa asiakirjojen käytettävyys, säilyminen ja lainmukainen säilyttäminen. Asiakirja- ja tietohallinnon suunnittelu ja toteutus tapahtuvat arkisto- ja tietosuojapalveluiden ja tietohallintoyksikön yhteistyönä huomioon ottaen sekä arkistotoimeen että tietoturvaan kohdistuvat vaatimukset.

Lisäksi arkistopäällikkö:

- osallistuu organisaation tietoturvaan ja -suojaan liittyvien asioiden suunnitteluun ja kehittämiseen sekä ohjeiden laatimiseen ja ylläpitoon
- osallistuu hyvinvointialueen turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tietosuoja- ja tietoturvatyöryhmän jäsenenä
- on tarvittaessa yhteydessä valvontaviranomaisiin
- tietosuoja-asioiden ohjaus ja neuvonta (henkilökunta, asiakkaat)

Tietoturva- ja tietosuojatyöryhmä

Hyvinvointialuejohtaja nimeää tietoturva- ja tietosuojatyöryhmän jäsenet, joita ovat jokaisen tulosalueen tietoturvan ja tietosuojan vastuuhenkilöt sekä muut henkilöt, joiden työtehtäviin hyvinvointialueen tietoturva- ja tietosuoja-asiat olennaisesti kuuluvat.

- koordinoi hyvinvointialueen tietosuoja- ja tietoturva-asioiden kokonaisuutta
- ohjaa ja valvoo tietoturva-asioiden toteuttamista
- valvoo hyvinvointialueen tietoturvapolitiikan, tietoturvakäytäntöjen ja – periaatteiden sekä -suunnitelman ja -sääntöjen laatimista, toteuttamista ja ajan tasalla pitämistä
- määrittää säännölliset tietoturvatoimenpiteet

- vastaa tietoturvakontrollien valinnasta ja toteutuksen ohjaamisesta yhteistyössä organisaation eri osien kanssa
- seuraa tietoturvallisuustilannetta, -osaamistasoa ja reagoi tarvittaessa havaittuihin ongelmiin ja uhkiin
- valvoo, että tietohallinto on varmistanut tietojärjestelmien toiminnan jatkuvuuden infrastruktuurin ja keskeisten järjestelmien osalta poikkeustilanteita varten
- huolehtii säännöllisestä riski-/uhka-analysoinnin järjestämisen valvomisesta
- vastaa tietoturvan ja tietosuojan auditointien toteuttamisen järjestämisestä
- vastaa tietoturva- ja tietosuojapolitiikan päivityksestä
- määrittelee ja suunnittelee sisäisen valvonnan kohteita.

Tietohallinto

Tietohallinto koordinoi hyvinvointialueen tietojärjestelmien ja niiden käytön tietoturvan ja teknisen toteutuksen suunnittelua, toteutumista ja raportointia. Tietohallinto toimii yhdessä palveluntuottajien kanssa teknisenä asiantuntijana tietoturvaa koskevissa kysymyksissä.

Tietohallinto hoitaa tietohallintolaissa osoitettuja erityistä osaamista ja koordinaatiota vaativia tietohallintotehtäviä. Tietohallintolaissa tietohallinnolla tarkoitetaan tukitoimintoa, jolla turvataan julkisten hallintotehtävien hoitaminen tieto- ja viestintäteknisiä menetelmiä ja keinoja hyväksikäyttäen.

- koordinoi tietoturvaorganisaation toimeksiannosta tietojärjestelmien ja niiden käytön tietoturvan teknisen toteutuksen suunnittelua, toteutumista ja raportointia
- toimii teknisenä asiantuntijana sekä antaa ja järjestää teknistä asiantuntemusta tietoturvaa koskevissa kysymyksissä
- arvioi teknologisen ympäristön muuttuessa suojaamismenettelyiden, kontrollien ja testaamisen ajantasaisena pitämiseen sekä kehittämiseen ja tarvittavien muutosten suunnittelun toteutukseen
- valvoo tietoturvatoimenpiteiden teknistä toteuttamista ja tietoturvakontrollien toteutusta (esim. palomuurien ja virustorjunnan ylläpito, roskapostisuodatus, tietoturvatapahtumien seuranta, kulunvalvonta)
- SOC-tiimi valvoo ja reagoi tietoturvauhkiin ja -poikkeamiin sovittujen käytäntöjen mukaisesti
- vastaa organisaation tietoteknisten toimenpiteiden toteutuksesta

Toimialuejohtajat, järjestämisjohtaja, palvelualuejohtajat ja palveluyksiköiden esimiehet

- vastaavat toimialueensa/palvelualueensa/palveluyksikkönsä tietoturvallisuudesta ja siitä, että henkilöstö tuntee tietoturvallisuuden perusasiat ja ovat käyneet vaadittavat koulutukset
- tukevat tietoturvan jatkuvaa ylläpitämistä ja kehittämistä
- toteuttavat, budjetoivat ja organisoivat yksikkönsä tietoturvallisuus ja tietosuojatoimenpiteet yksiköissään
- huolehtivat, että vaadittavat tietosuoja ja -turva koulutukset on käyty
- tietohallinnon kanssa nimeävät keskeisille järjestelmille vastuuhenkilöt
- raportoivat tietoturvallisuusongelmista ja tietosuojarikkomuksista tietoturva- ja tietosuojavastaavalle ja

- tekevät Haipro-ilmoitukset tietosuojaan ja tietoturvaan liittyvistä riskeistä ja ongelmista.

Turvallisuuspäällikkö

- toimii asiantuntijana organisaation sisäisissä turvallisuusasioissa
- valtuus tehdä turvallisuuteen liittyviä päätöksiä niin työyksikkö- kuin organisaatiotasolla
- tekee yhteistyötä Kainuun hyvinvointialueen ulkopuolisten turvallisuusviranomaisten kanssa
- toimii työsuojeluasioissa Kainuun hyvinvointialueen työnantajan edustajana.

Tietojärjestelmien ja laitteistojen vastuuhenkilöt

Kaikille tietojärjestelmille ja laitteistoille, hyvinvointialueen omille ja ulkoistetuille palveluille, on määritelty vastuuhenkilöt/pääkäyttäjät. Vastuuhenkilöt/pääkäyttäjät määrittelevät ja vastaavat tietojärjestelmien/sovellusten/laitteistojen tietoturvasta, palvelutasosta, käyttöoikeuksista, varmistamisesta, kehittämisestä ja käytöstä tietoturvapolitiikan ja tietoturvakäytäntöjen mukaisesti tarvittaessa yhdessä toimittajien sekä tietohallinnon kanssa. Vastuuhenkilöt/pääkäyttäjät vastaavat tietoturvallisuudesta myös yksittäisen tietojärjestelmän toiminnan ja käytön osalta.

Jokainen työntekijä

Jokainen työntekijä vastaa omalta osaltaan tietoturvallisuuden toteutumisesta voimassa olevan lainsäädännön ja tietojen käsittelystä ja viestintävälineiden tietoturvallisesta käytöstä annettujen ohjeiden mukaisesti. Ohjeilla annetaan henkilöstölle perustiedot tietoaineiston ja tietojärjestelmien käytöstä sekä niihin liittyvästä tietoturvasta.

Jokaisen työntekijän tulee aina raportoida HaiPro-järjestelmään havaitsemistaan tahattomista tai tahallisista tietosuojarikkomuksista ja lisäksi asiasta tulee ilmoittaa esimiehelle ja Kainuun hyvinvointialueen tietoturvavastaavalle sekä tietosuojavastaavalle. Esimiehen tulee huolehtia, että vaadittavat tietosuoja ja -turva koulutukset on käyty.

3.3 Soveltaminen

Tämä Kainuun hyvinvointialueen aluehallituksen hyväksymä Tietoturvapolitiikka -asiakirja saatetaan tiedoksi jokaiselle Kainuun hyvinvointialueen työntekijälle ja tietojärjestelmien käyttäjälle. Tietoturvallisuuden toteutuminen varmennetaan vuosittain toimintakertomukseen tulevalla maininnalla suoritetuista toimenpiteistä, sisäisen valvonnan raportista ja HaiPro ilmoitusten käsittelystä.

Tietoturvallisuuteen liittyviä määrityksiä tarkistetaan ja arvioidaan hankintojen suunnitteluvaiheessa, tietojärjestelmien käyttöönotoissa, muutosten yhteydessä ja poikkeamailmoitusten ja sisäisen valvonnan raporttien perusteella.

Kainuun hyvinvointialueen tietoturvapolitiikka on saatavissa Kainuun hyvinvointialueen sisäisiltä verkkosivuilta.

3.4 Valvonta

Tietojärjestelmien käytöstä kertyy tietoa ja järjestelmien käyttöä seurataan. Hyvinvointialueella tehdään sisäistä valvontaa muun muassa potilas-/asiakastietojärjestelmien käytöstä ja henkilötietoja sisältävien järjestelmien käytöstä. Sisäisellä valvonnalla tarkoitetaan kaikkia niitä toimenpiteitä ja menetelmiä, joilla pyritään organisaation henkilötietojen asianmukaiseen ja luottamukselliseen käyttämiseen. Valvonta toteutetaan Kainuun hyvinvointialueen lokipolitiikan sekä käyttölokien seuranta- ja valvontasuunnitelman mukaisesti.

3.5 Rikkomukset ja seuraamukset

Jokainen hyvinvointialueen tietojärjestelmien käyttäjä ja organisaation työntekijä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla salassapito- käyttäjäsitoumuksen työsuhteen alkaessa. Esimies ja työntekijä käyvät läpi tietosuoja- ja käyttäjäsitoumuksen ja sen merkityksen organisaation toiminnassa.

Tietosuojasitoumuksen ja toimintaohjeiden sekä lainsäädännön vastainen toiminta käsitellään käyttölokien seuranta- ja valvontasuunnitelman mukaisesti.

Tietoturva- ja tietosuojarikkomusten mahdollisiin seuraamuksiin sovelletaan organisaation määrittämien tietoturva- ja tietosuojarikkomusten seuraamustaulukon mukaisia toimia. Tietosuojarikkomukset raportoidaan hyvinvointialueen johdolle ja tietosuojavastaavalle.

3.6 Tietoturvapolitiikan poikkeamaluvat

Tietoturvapolitiikka ja sitä tarkentavat tietoturvakäytännöt ovat siis kaikkia hyvinvointialueen palveluksessa työskenteleviä velvoittavia, ja niitä tulee noudattaa lähtökohtaisesti kaikessa toiminnassa.

On kuitenkin mahdollista, että teknisistä tai toiminnallisista syistä, joissain toiminnoissa ei voida toimia tietoturvapolitiikan mukaisesti. Näissä tapauksissa tulee aina anoa tietoturvapolitiikan poikkeamalupaa tietoturva- ja tietosuojatyöryhmältä. Anomus tarvitaan, jotta poikkeaman tarve voidaan asianmukaisesti arvioida, toiminta ohjeistaa ja politiikan poikkeaman tarpeen tilannetta voidaan seurata.

4. Liite 1 Tietoturvallisuuden osa-alueet

1. HALLINNOLLINEN TURVALLISUUS

Hallinnollisella tietoturvallisuudella tarkoitetaan tietoturvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Sen tarkoituksena on luoda organisaatioon tietoturvastrategia ja tietoturvalliset toimintatavat luonnolliseksi osaksi kaikkea toimintaa. Toimintamallien pohjalta luodut henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä tietoturvallisuuden kehittämiseksi ja ylläpitämiseksi. Tietoturvan kehittäminen ja ylläpito ovat puolestaan osa organisaation yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Hallinnollisen turvallisuuden perustaso edellyttää, että

- organisaatiolla on kirjallinen hyvinvointialueen aluehallituksen hyväksymä tietoturvapolitiikka
- organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia
- organisaatiolla on suunnitelmat toiminnan jatkuvuudesta ja toipumisesta tärkeimpien omien järjestelmien häiriöiden osalta sekä tietoturvasta
- organisaation tietoturvatavoitteet on määritelty ja viety organisaation ohjaukseen
- tietoturvakoulutus on organisaatiossa jatkuvaa ja valvottua
- tietoturvavastuut ja -tehtävät on määritelty
- tietoturvatehtäviin on nimetty vastuuhenkilöt ja heille varamiehet

Hallinnollinen tietoturvallisuus on kaikkien muiden tietoturvallisuuden osa-alueiden toteutuksen ja määrittelyn perusta. Sen avulla määritellään tietoturvallisuuden suuntaviivat ja turvallisuutta parantavat toimenpiteet.

Hallinnollisessa tietoturvassa päämääränä on luoda organisaatioon toimintatapa, jolla pystytään välttämään tietoturvariskit.

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 tilaajalle toimitetut kuvaukset 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.

2. OHJELMISTOTURVALLISUUS

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistautumis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen määrittelyyn, suunnitteluun, kehittämiseen ja hankintaan sekä ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä (mm. versiointi, lisensointi ja muutoksenhallinta).

Ohjelmiston suunnittelijan, valmistajan ja myyjän vastuu ohjelmistotuotteista määräytyy hankinta- ja käyttöoikeussopimusten mukaan.

Hyvinvointialueen ohjelmistoturvallisuuden perustaso edellyttää, että

- tietojärjestelmien ylläpidosta huolehditaan ohjelmistotoimittajien kanssa tehtyjen ylläpitosopimusten mukaisesti
- ohjelmistotoimittajilta vaaditaan tuotteelleen tietoturva/-suojaselvitys, hyväksytty auditointi, tietoturvasuunnitelma/kuvaus
- järjestelmämuutoksia varten järjestelmän omistaja kartoittaa käyttäjien toiveet, vie tulevat muutokset muutoksenhallinta käsittelyyn sekä tekee testaussuunnitelman ja -aikataulun. Järjestelmän omistaja kuvaa testaussuunnitelmassa testaukseen valtuutetut (esim. pääkäyttäjät, ohjelmistotoimittajat, ICT -palveluntuottajat), testauksen tyypit ja vastuut (omistaja: toiminnallinen testaussuunnitelma, ohjelmistotoimittaja: tekninen testaussuunnitelma) sekä kriteerit joilla testaus katsotaan hyväksytyksi.
- tietoturvapäivityksien kriittisyys arvioidaan riskianalyysin mukaisesti ja päivitykset toteutetaan hätä-, standardi- tai normaalimuutoksena.
- kaikki etäyhteydet ovat suojattuja ja sanomaliikenne salattua. Etäyhteyden käyttö edellyttää luotettavaa tunnistautumista.

Hyvinvointialueella on määritelty ohjelmistojen käyttöön liittyvät velvollisuudet:

- ohjelmistoihin kuuluvat alkuperäiset dokumentit ja/tai käsikirjat on talletettu ja niiden sijainti on tiedossa
- ohjelmistojen kopioinnissa ja käytössä noudatetaan tekijänoikeuslakia sekä ohjelmistonvalmistajan lisenssiehtoja
- ohjelmistolisensseistä pidetään kirjaa
- tietojärjestelmien varmuuskopiointi on sovittu järjestelmäkohtaisesti
- säilytyksestä ja varmuuskopioiden palautuksen testaamisesta vastaa tietohallinto.

Ohjeet ohjelmistojen käytöstä päätelaitteilla:

- ohjelmistojen elinkaaren hallinta ja hankintojen koordinointi on keskitetty tietohallintoon.
- kaikki päätelaitteille asennettavat ohjelmistot on hyväksytettävä tietohallinnolla
- ohjelmistojen asennusmediat, samoin kuin niiden kopiot, säilytetään tietoturvaohjeiden mukaisesti
- päätelaitteiden käyttäjien tulee noudattaa tietojen käsittelyssä tietojen luonteelle ja sisällölle asetettuja vaatimuksia sekä organisaation omia ohjeistuksia niiden tallentamisesta ja varmuuskopioinnista.
- pilvipalveluiden käytöstä työhön liittyvien tiedostojen tallennuspaikkana päättää tietohallinto. Sallitut tallennuspaikat tiedotetaan käyttäjille ja kirjataan tietoturvaohjeisiin

- KanTa-palvelun kautta luovutetun potilas- ja asiakastiedon käsittely ohjelmistolla on mahdollista vain Väestörekisterikeskuksen toimikortilla tunnistetulle henkilölle, joka on nimenomaisesti saanut käyttöoikeuden katsoa luovutettua tietoa tai luovuttaa organisaation tietoja.

Tiedon luovutus organisaation ulkopuolelle perustuu lakeihin ja/tai valtuutukseen. Tavoitteena on varmistaa tietojärjestelmien jatkuva toiminta ja luotettavuus.

3. KÄYTTÖTURVALLISUUS

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojakopioinnista sekä häiriöraportoinnista.

Käyttöturvallisuuden perustaso edellyttää, että organisaatiossa:

- on hyväksytty erilliset ohjeet tietojenkäsittelyn toipumisen ja jatkuvuuden varalta
- on tietojärjestelmille nimetyt vastuuhenkilöt/pääkäyttäjät sekä päivittäin hoidettavien rutiinitehtävien ohjeistukset
- yksiköillä on varasuunnitelmat laadittu käyttökatkoksia varten
- noudatetaan turvallisuusohjeita ja käyttöoikeuskäytäntöjä
- tietojärjestelmiä käyttävät henkilöt tunnistetaan ja todennetaan
- on käytössä käyttäjätunnus- ja salasanamenettelyt
- on menettelytavat tietokonevirusten ja haittaohjelmien torjuntaan
- varmistetaan ja valvotaan suojausten riittävyys väärinkäytösten ennaltaehkäisemiseksi ja paljastamiseksi
- varmistetaan tiedostojen sisältöjen käyttökelpoisuus ja tietojen saatavuus
- varmistetaan ICT-ohjelmien huollon ja ylläpidon saatavuus
- varmistetaan kannettavien työasemien tietosisällön turvaaminen salausohjelmistolla
- seurataan verkon tietoturvallisuustasoa säännöllisesti
- suoritetaan tietoturvapäivitykset viivytyksettä
- seurataan verkon liikennettä, komponenttien tilaa ja verkkoon tunkeutumista ympärivuorokautisesti sekä toteutetaan poikkeuksellisen liikenteen vaatimat toimenpiteet viivytyksettä

Potilaan / asiakkaan tunnistaminen

Kainuun hyvinvointialueella tapahtuvan asioinnin yhteydessä potilas/asiakas tunnistetaan luotettavasti viranomaisen myöntämällä kuvallisella henkilöasiakirjalla tai vastaavalla. Lisäksi sähköisessä asioinnissa luotettavaksi tunnistamiseksi hyväksytään mm. sähköisellä henkilökortilla tapahtunut tunnistautuminen, johon liittyy Väestörekisterikeskuksen varmenne. Hyväksyttävä menetelmä on myös vastaava vähintään Väestörekisterikeskuksen varmenteen tasoinen mobiili-tunnistaminen ja varmentaminen sekä verkkopankkipalvelun avulla tapahtuva tunnistaminen.

Potilaan/asiakkaan tunnistaminen erityistilanteissa esimerkiksi, kun otetaan kantaa hoitoon puhelimessa tai ensihoidossa (henkilöllä ei mukana henkilöllisyystodistuksia), tapahtuu

tunnistaminen ensisijaisesti henkilötunnuksella ja tarvittaessa esittämällä henkilölle henkilöllisyyttä tarkentavia kysymyksiä, joiden pohjalta voidaan henkilöllisyys varmentaa. Mikäli kyseessä on tunnettu potilas/asiakas, jolloin ei ole syytä epäillä henkilöllisyyttä, erillistä tunnistamista ei tarvita. Kainuun hyvinvointialueella on hallinnollinen ohje potilaan tunnistamisesta, joka löytyy hyvinvointialueen sisäisiltä verkkosivuilta.

Työntekijän tunnistaminen

Organisaation tietojärjestelmiä käytettäessä käyttäjä tunnistetaan joko henkilökohtaisella käyttäjätunnus/salasana -parilla tai ammatti- /henkilökortilla.

Työntekijän tunnistaminen erityistilanteissa esimerkiksi puhelimessa tapahtuu ensisijaisesti henkilötunnuksella ja tarvittaessa esittämällä henkilölle henkilöllisyyttä tarkentavia kysymyksiä tai tietojärjestelmien hallinnollisia tietoja, joiden pohjalta voidaan henkilöllisyys varmentaa.

Kanta-palveluja käytettäessä ja sähköistä lääkemääräystä käsiteltäessä ammattihenkilö tunnistetaan kansallisen varmennekortin avulla. Ammattihenkilö saa käyttöönsä ammattikortin, jossa on Sosiaali- ja terveydenhuollon lupa- ja valvontaviraston (Valvira) ammattivarmenne, sekä siihen liittyvän PIN -koodin. Muut kuin sosiaali- ja terveydenhuollon ammattihenkilöt saavat käyttöönsä henkilöstökortin, jossa on varmenne, sekä siihen liittyvän PIN -koodin.

4. LAITTEISTOTURVALLISUUS

Laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja valvonta sekä niiden kapasiteettien suunnittelu. Laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon myös kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Laitteistoturvallisuuden perustasossa edellytetään, että

- toiminnan jatkuvuus kriittisten laitteistojen osalta varmistetaan ylläpitosopimuksilla ja varajärjestelyillä
- laitteistojen fyysisen kunnon varmistamiseksi laadittuja ohjeita noudatetaan
- huolto- ja ylläpitosopimukset ovat ajan tasalla ja vastaavat käytettävyysvaatimuksia
- laitteen käyttäjä vastaa laitteen huolellisesta käytöstä ja säilytyksestä
- laitteista on laiterekisteri
- tietojenkäsittelykapasiteettia seurataan, suunnitellaan ja ennakoidaan
- laitteistojen poistot tehdään suunnitelmallisesti
- laitteistoilla on ajantasainen suojaus haittaohjelmia varten
- laitteiden tietoturvapäivityksille on olemassa määritelty prosessi

5. FYYSINEN TURVALLISUUS

Fyysisin turvallisuustoimenpitein luodaan ja ylläpidetään tiedonkäsittelyn vaatiman käyttöympäristön toimintaolosuhteet, suojataan ja valvotaan fyysiset tilat sekä varmistetaan teknisten järjestelmien toiminta normaali- ja häiriötilanteissa. Fyysinen turvallisuus käsittää kiinteistöjen rakenteellisen turvallisuuden, valvontatekniikan kuten kulunvalvonta-, rikosilmoitus- ja videovalvontajärjestelmät sekä valvonnan ja vartioinnin.

Kainuun hyvinvointialue toimii omissa sekä vuokrakiinteistöissä. Turvallisuustasot sekä turvallisuusvastuut ovat erilaisista yksiköistä ja toiminnoista johtuen eritasoisia. Kiinteistöjen fyysinen turvallisuus noudattaa toiminnan luonteen ja määräysten vaatimaa turvallisuustasoa. Kriittisimmissä yksiköissä turvallisuusyhteistyötä tehdään myös muiden viranomaisten kanssa.

Kiinteistöjen fyysistä turvallisuutta ylläpidetään ja kehitetään jatkuvasti yhdessä toiminnan harjoittajan, kiinteistön omistajan, tekniikan, viranomaisten sekä turvallisuuspäällikön toimesta.

Turvaluokiteltujen ja henkilötietoja sisältävien paperisten asiakirjojen kuljettaminen työpisteeltä toiselle ja kotiin on pyrittävä pitämään mahdollisimman vähäisenä. Jos kuitenkin joudutaan em. asiakirjoja kuljettamaan, niin käytetään siihen tarkoitettua turvapussia suojaamaan tiedon eheyttä ja luottamuksellisuutta. Turvaluokiteltuja ja henkilötietoja sisältäviä asiakirjoja säilytetään vaatimusten mukaisesti joko kassakaapissa tai lukitussa kaapissa. Toimistotiloissa noudatetaan ns. ”puhtaan pöydän” -politiikkaa.

6. TIETOLIIKENNETURVALLISUUS

Tietoliikenneturvallisuus käsittää tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyvät turvallisuustoimenpiteet. Tietoliikenneturvallisuus voidaan jakaa kolmeen osa-alueeseen joita ovat; järjestelmänhallinta, verkonhallinta sekä siirtoteiden hallinta. Tavoitteena on estää luvaton tunkeutuminen järjestelmiin tietoverkon kautta, paljastaa tunkeutumisyritykset, estää siirrettävän tiedon joutuminen sivullisten haltuun ja tarvittaessa estää sen käyttö sekä estää väärän tiedon syöttö tietojärjestelmiin.

Tietoliikenneturvallisuuden perustaso edellyttää, että

- tietoverkot on dokumentoitu ja niiden muutokset tapahtuvat muutoksenhallintamenettelyn mukaisesti
- tietoihin ja tietojärjestelmiin pääsy on tarkoin määritelty
- käyttöoikeudet tarkistetaan säännöllisesti ja käyttöoikeustasot on määritelty
- luvaton käyttö on estetty teknisesti
- tietoliikennelokia ja käyttöhäiriöitä seurataan säännöllisesti
- noudatetaan työasemiin asennettavien varus-, sovellus- ja tietoliikenneohjelmien osalta annettuja ohjeita
- varmistetaan tietoliikenneohjelmien ja -laitteiden turvallisuus ja tietoliikenneviestien sisällön muuttumattomuus

- luottamuksellisten viestien lähettäjä ja vastaanottaja todennetaan
- tietosuoja- ja vastuukysymykset omassa verkossa sekä eri tietoliikenneoperaattoreiden ja huollon välillä on sovittu kirjallisesti
- langaton (WLAN) -tietoverkko suojataan käyttäen riittävän vahvaa salausta ja tukiasemien välistä salausta
- verkon komponenttien tietoturvapäivitykset suoritetaan viivytyksettä
- eri turvatasojen verkot on tunnistettu ja verkot eriytetty
- kiinteistönvalvontaverkko on eriytetty muista tietoverkoista
- verkon aktiivilaitteet on suojattu ja konfiguroitu suojaustason mukaisesti.
- kriittiset tietoliikenneyhteydet on kahdennettu
- tietoverkoissa on mekanismi tunkeutumisen estoa ja havainnointia varten etäkäyttöyhteyksien tietoturvan taso pitää olla käytettyjen järjestelmien luokituksen mukainen (esim. sähköpostiin ei tarvita vahvaa tunnistautumista, potilastietojärjestelmiin tarvitaan).
- käyttöoikeuksien valtuuttamiseen, muutoksiin ja poistamisiin on dokumentoitu prosessi

7. HENKILÖSTÖTURVALLISUUS

Henkilöstöön liittyvien riskien hallintaa kutsutaan henkilöstöturvallisuudeksi. Sen tavoitteena on ehkäistä henkilökuntaan suuntautuvia ja henkilökunnasta tulevia uhkia. Näitä riskejä voidaan torjua turvakartoituksilla, vastuun ja velvollisuuden selkeällä määrittämisellä, selkeillä ohjeilla toimenpiteistä, kun työsuhde päättyy ja sitouttamalla henkilö tietoturvalliseen toimintaan.

Työnantajan ja henkilöstön välistä yhteistoimintaa kunnissa koskevan lain (2007/449) tavoitteena on edistää työnantajan ja sen henkilöstön välistä vuorovaikutusta. Yhteistyötoimikunta muodostuu työntekijöiden ja työnantajan edustajista. Tietoturvaan liittyvät ohjeet, sopimukset ja sanktiot viedään yhteistyötoimikunnan tiedoksi ja hyväksyttäväksi.

Tietojärjestelmien käyttäjistä pidetään ajantasaista rekisteriä, josta ilmenee käyttäjän yksilöintitietojen lisäksi käyttäjärooli. Ostopalveluiden tuottajilta tai muuten hvyinvointialueen tietojärjestelmiä käsitteleviltä henkilöiltä edellytetään vastaavien tehtäväkuvauksien ylläpitoa käyttäjärekisteriä varten.

Uuden henkilöstön perehdytykseen kuuluu terveydenhuollon ja sosiaalitoimen salassapitosäännösten läpikäynti ja ennen tietojärjestelmäoikeuksien myöntämistä tietosuoja- ja käyttäjäsitoumuksen allekirjoittaminen. Työnantaja järjestää säännöllisesti tietoturva- ja tietosuojakoulutusta.

Työntekijältä, jonka tehtävät edellyttävät alueellisten tai valtakunnallisten potilastietojärjestelmäpalveluiden käyttöä, edellytetään virallisen henkilötodistuksen esittämistä ennen käyttöoikeuksien myöntämistä. Valtakunnallisten tietojärjestelmäpalveluiden käyttö edellyttää henkilökohtaista Väestörekisterikeskuksen myöntämää varmennekorttia. Käyttäjätunnuksen ja salasanan saaminen myös muihin potilastietoja sisältäviin järjestelmiin edellyttää työntekijän henkilöllisyyden varmistamista luotettavalla tavalla.

Työtehtävien loppumiseen liittyvät järjestelyt on ohjeistettu siten, että tietojärjestelmien käyttöoikeudet ja valvomaton pääsy tiloihin, joissa on yhteys suojattuun tietojärjestelmäympäristöön, päättyvät tehtävien loppuessa. Käyttöoikeuksien päättäminen on esimiehen vastuulla.

Työntekijät saavat säännöllisesti tietoturva-/tietosuojakoulutusta. Tietämystasoa ja osallistumista koulutukseen seurataan ja tulokset raportoidaan hyvinvointialueen esimiehille.

Kainuun hyvinvointialueen toiminnan kannalta kriittisten tietojärjestelmien kriittisten tehtävien vastuuhenkilöllä/pääkäyttäjällä on sovittu varahenkilö.

Henkilöstöturvallisuustyön tulos on luotettava ja tehtäviinsä soveltuva henkilöstö, joka tuntee itselleen asetetut tietoturva-/tietosuojavaatimukset omaan toimenkuvaansa ja rooliinsa liittyen.

Oman ja ostopalveluita Kainuun hyvinvointialueelle tuottavan henkilöstön tulee tuntea tiedonsaantioikeutensa, käyttöoikeutensa, sijaisuus- tai muihin työtä koskeviin järjestelyihin liittyvät toimet sekä velvollisuutensa ja oikeutensa työsuhteen alkaessa ja päättyessä.

8. TIETOAINEISTOTURVALLISUUS

Tietoaineistoturvallisuudella tarkoitetaan eri tallennusmuodoissa olevien tietojen suojaamista. Se koskee sekä paperiasiakirjoja että digitaalisessa muodossa olevia tallenteita, optisia ja magneettisia muistivälineitä, mikrofilmiä, äänitteitä tai muita vastaavia teknisiä laitteita. Tietoaineistoturvallisuudella varmistetaan asiakirja- ja tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito elinkaaren kaikissa vaiheissa.

Tietoaineistoturvallisuuteen kuuluvat ne ulkoiset normit, jotka rajoittavat tai ohjaavat tietosisällön perusteella tehtävää tietojenkäsittelyä, kuten yleiset ja/tai erityisalan lait, asetukset, viranomaismääräykset ja Kansallisarkiston ohjeet. Lisäksi tietoaineiston käsittelystä tarvitaan organisaatiokohtaiset ohjeet, johon kuuluvat tietojärjestelmien käsittelysäännöt sekä tietojen ja asiakirjojen luokittelu julkisuus- ja salassapitosäännösten mukaisesti.

Organisaatiolla on ajantasainen, tietoaineistot kattava tiedonhallintasuunnitelma, josta ilmenee tietoaineiston säilytysajat, julkisuusluokka ja salassa pidettävän aineiston osalta salassapidon perusteet.

Arkisto- ja tietosuojapalvelut -yksikkö vastaa henkilöstön perehdyttämisestä tietoaineistojen käsittelyohjeisiin ja tekee toimintokohtaisia käsittelyohjeita sekä kouluttaa organisaation arkistovastuuhenkilöitä. Tietoaineistojen tietoturvallisuuden varmistaminen koskee koko henkilöstöä ja tietoaineiston koko elinkaarta. Organisaation tietoaineistoturvallisuuden perustason edellytyksenä on, että henkilöstö tuntee ja noudattaa toiminnassaan

- henkilötietojen käsittelyä koskevia yleisiä periaatteita
- yksikkönsä toimintaa ohjaavia ja/tai rajoittavia normeja
- tietojärjestelmän sisältämän tietoaineiston käsittelyä koskevia turvasääntöjä
- tietojen ja asiakirjojen salassapito- ja käsittelysääntöjä.

Työntekijöitä koskee vaitiolovelvollisuus ja salassapitosäännökset. Luottamuksellisia tietoja voivat käsitellä vain henkilöt, jotka tarvitsevat niitä työssään. Potilas- ja asiakastietojen käsittelyn edellytys on käyttäjän tehtävistä johtuva asiayhteys asiakkaaseen tai häntä koskeviin tietoihin. Sähköisessä muodossa olevia potilas-/asiakastietoja saa käsitellä vain yksilöitävissä oleva henkilö, ja valtakunnallisten tietojärjestelmäpalveluiden kautta saatavien tietojen osalta, vain Väestörekisterikeskuksen myöntämällä varmennekortilla tunnistautunut henkilö. Tietoaineistojen

käyttöä seurataan säännöllisesti ja seurannan periaatteet on käsitelty yt-menettelyn mukaisesti hyvinvointialueen työntekijöiden kanssa. Potilas- ja asiakastietojen käsittelystä on laadittu henkilökunnalle ohjeet, joiden ylläpidosta vastaava henkilö on nimetty.

Tietoja säilytetään ja vanhentuneet tiedot hävitetään tiedonhallintasuunnitelman mukaisesti.

Huoltoon vietävästä, poistettavasta tai myyntiin luovutettavasta työasemasta poistetaan tai puhdistetaan kiintolevy aina ohjeen mukaisesti. Kokeilukäytössä olleen tutkimus- tai hoitolaitteen palautuksen yhteydessä huolehditaan tietojen poistamisesta laitteelta ohjeen mukaisesti.