YLÄ-SAVON SOTE KUNTAYHTYMÄN TIETOTURVA- JA TIETOSUOJA-POLITIIKKA 9.6.2020

Kuntayhtymän hallitus 9.6.2020

Sisällys

KÄSITTEITÄ

TIETOTURVAPOLITIIKKA

Organisaation tasolla 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 yritysturvallisuutta.

TIETOSUOJA

Henkilötietoja käsiteltäessä 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. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.

KYBERTURVALLISUUS

Tietoturvallisuuden alalaji, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Sosiaali- ja terveydenhuollon kyberturvallisuuteen varautuminen tarkoittaa sitä, että keskeisten toimintojen osalta on tehty varautumis- ja riskienhallintasuunnitelma

HAKKEROINTI

Tässä dokumentissa ja asiayhteydessä hakkeroinnilla tarkoitetaan luvatonta tunkeutumista tietokoneeseen tai verkkoon, eli tietomurtoja. Hakkerointia suorittava henkilö tunnetaan termillä hakkeri. Hakkeroinnin tavoitteena on muuttaa järjestelmää tai suojausominaisuuksia päästäkseen käsiksi tietoon joka ei ole tarkoitettu ulkopuolisille. Hakkeroinnin eri muotoja ovat mm. salasanojen murtaminen, viruksien jakaminen, haavoittuvuusskannaukset, sekä tietojenkalasteluviesteihin perustuvat tietomurrot.

ICMT

Information, Communication and Medical Technology, tieto-, viestintä-, ja lääkintälaiteteknologia

1 JOHDANTO

Tietoturva- ja tietosuojapolitiikalla tarkoitetaan tässä dokumentissa Ylä-Savon SOTE kuntayhtymän johdon hyväksymää näkemystä tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Tietoturva- ja tietosuojapolitiikan avulla vaikutetaan omalta osaltaan siihen, että Ylä-Savon SOTE kuntayhtymän strategiassa määritelty visio, toiminta-ajatus, arvot ja palvelut toteutetaan laadukkaasti ja turvallisesti.

Tietojen turvaaminen on olennainen osa Ylä-Savon SOTE kuntayhtymän toiminnan turvallisuutta. Tietojärjestelmät tukevat merkittävässä määrin kuntayhtymän toimintaa sen tuottaessa toiminta-ajatuksensa mukaisia erikoissairaanhoidon, perusterveydenhuollon, sosiaalitoimen ja ympäristö- ja terveysvalvonnan palveluita. Ylä-Savon SOTE kuntayhtymän tietoturva- ja tietosuojapolitiikan tarkoituksena on yhdenmukaistaa tietoturva- ja tietosuojakäytäntöjä alueellisesti sekä vahvistaa tietojenkäsittelyn turvan perustaso, organisointi, vastuut ja seurantamenetelmät.

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

Ylä-Savon SOTE kuntayhtymälle on erityisen tärkeää, että potilas/asiakas voi luottaa siihen, että hänen tietonsa ovat turvassa, oikeita ja vain hoitoon/asiakassuhteeseen osallistuvien saatavissa ja että niitä käsitellään kaikissa vaiheissa asianmukaisesti. Tietojen käsittely perustuu hoito- tai asiakassuhteeseen tai muuhun asialliseen yhteyteen, jonka perusteena on virka- tai työtehtävien hoito. Luottamuksellisuus ja yksityisyyden suoja painottuvat myös henkilöstöasioiden käsittelyssä.

Kyberturvallisuuden varautumisen toimilla on tarkoitus varmistaa organisaatioiden sisäistä turvallisuutta sekä sitä, että esimerkiksi kuntayhtymän tietojärjestelmiä/ -verkkoja ei käytetä kyberiskujen ja/tai hakkerointien suunnittelussa. Tietoturvallisuuden näkökulmasta kyberturvallisuus noudattaa organisaatioiden varautumis- ja riskienhallintasuunnitelmia, eikä muuta sen toimivaltuuksia.

1.1 Tavoite

Tietoja käsitellään Ylä-Savon SOTE kuntayhtymässä yhdenmukaisten tietoturva- ja tietosuojaperiaatteiden mukaisesti. Tietoturva- ja tietosuojapolitiikka on kaikkia sitova ja sitä tarkennetaan erillisohjeilla ja määräyksillä. Tällä turvataan potilas- ja asiakastyön mahdollisimman sujuva ja häiriötön toiminta.

Ylä-Savon SOTE kuntayhtymän koko henkilökunnan, luottamushenkilöiden sekä yhteistyö- että sopimuskumppaneiden edellytetään noudattavan kuntayhtymän tietoturva- ja tietosuojamääräyksiä. Mikäli yhteistyön puitteissa käsitellään luottamuksellisia tietoja, tietoturvaan ja tietosuojaan liittyvät vastuut ja käytännöt on kirjattava yhteistyökumppanin kanssa tehtäviin sopimuksiin.

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 sekä ymmärtää ja hyväksyä potilaan halu ja oikeudet kieltää tietojensa käsittely tietyissä tilanteissa.
- Organisaation koko henkilöstö sitoutuu toteuttamaan tietoturvaa ja tietosuojaa. Kaikki ymmärtävät tietoturvan ja tietosuojan merkityksen sekä tehtävänsä ja velvollisuutensa tietoturvallisuuden ja tietosuojan ylläpidossa.
- Tietoturva- ja tietosuojaperiaatteita toteutetaan kuntayhtymän 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

Ylä-Savon SOTE kuntayhtymässä tietojenkäsittelyn ja sen turvaamisen periaatteet noudattavat kansallisia ja kansainvälisiä tietoturvallisuutta koskevia säädöksiä, standardeja sekä auditointivaatimuksia ja suosituksia. Näistä keskeisimpiä ovat tiedonhallintalaki, julkisuuslaki, laki potilaan asemasta ja oikeuksista, laki asiakas- ja potilastietojen sähköisestä käsittelystä sekä Euroopan unionin tietosuojadirektiivi ja siitä johdettu suomalainen lainsäädäntö. Kaikessa toiminnassa noudatetaan hyvää tietojenkäsittelytapaa, velvoitteita ja sopimuksia. Tietoturva- ja tietosuojaratkaisujen tulee noudattaa myös taloudellisia realiteetteja, eivätkä ne saa vaikeuttaa merkittävästi tietojen ja tietojärjestelmien hyötykäyttöä ja asiakaspalvelua.

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

Sähköisten hallinnollisten dokumenttien ja niiden tuottamisen ja hallinnan prosessien osalta noudatetaan voimassa olevaa normia siinä vaiheessa, kun se on tietojärjestelmien puolesta toteutettavissa.

1.3 Tarkoitus

Tietoturva- ja tietosuojatoimilla estetään tietojen luvaton käyttö ja haltuunotto. Suuri osa kuntayhtymässä käsiteltävästä tiedosta on luottamuksellista, arkaluonteista sekä salassa pidettävää, ja voi paljastuttuaan rikkoa yksityisyyden suojaa. Tietoturva- ja tietosuojatoiminnan tavoitteena on vastata siitä, että tieto on oikeaan aikaan oikeassa paikassa ja oikean muotoisena 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, luotettavaa, ajantasaista, oikeellista ja helposti käytettävissä ilman tulkinta- ja väärinymmärrysmahdollisuutta.

Tietoturva- ja tietosuojatoimilla vähennetään ja ennaltaehkäistään tietoturvariskien syntyminen, varmistetaan tietojen saatavuus, toiminnan jatkuvuus, asiakkaiden ja potilaiden oikeusturva ja yksityisyyden suoja lainsäädännön ja muiden määräysten edellyttämällä tavalla - myös poikkeuksellisissa olosuhteissa. Lisäksi varmistetaan, että henkilöstö ja sopimussuhteiset palveluntuottajat ovat tiedostaneet tietoturvan ja tietosuojan merkityksen.

1.4 Suojattavat kohteet

Turvattavia tietoja ovat sekä analogisessa että digitaalisessa (sähköisessä) muodossa olevat tiedot. Tietoturva- ja tietosuojapolitiikka kattaa myös vaitiolovelvollisuuden piiriin kuuluvan 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. Ne kuvataan käyttöympäristöille ja tarvittaessa yksiköille laadituissa tietoturvallisuuden kehittämissuunnitelmissa. Käyttäjien toimintaa ohjataan toimintaohjeilla sekä tietoturvakoulutuksella.

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.

Ylä-Savon SOTE kuntayhtymän 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

Ylä-Savon SOTE kuntayhtymän 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 ja jatkuvuudenhallintaan.

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

Tietoturvariskejä hallitaan riskienhallintaprosessin avulla. Hyväksyttävän riskitason määrittelee johtoryhmä riskianalyysin tulosten perusteella ja yhteisesti valmisteltujen kriteerien ja mittarien avulla.

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

2.1.4 Tietoturvallisuusasioiden tiedottaminen

Tietoturvallisuutta koskevista asioista tiedottaminen kuuluu kuntayhtymän toiminnasta vastuussa oleville tahoille, kuntayhtymän johtajalle ja yhtymän vastuualueiden johtajille kuntayhtymän viestintäsuunnitelman mukaisesti. Tietosuoja-asioihin liittyvässä tiedottamisessa tietosuojavastaava on ensisijaisesti yhteydessä rekisterinpitäjään.

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 ja verkkoliikenteen sisällön turvallisuuden 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 tunnistamisesta, henkilötietojen hallinnasta, käyttöoikeuksien ja pääsynhallinnasta, 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.

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

Ylä-Savon SOTE kuntayhtymä suorittaa potilas- ja asiakastietojen käytön valvontaa lokivalvonnalla ja muilla tarvittavilla menetelmillä. Toimitiloissa suoritetaan analogisessa muodossa olevien asiakirjojen ja aineistojen käsittelyn valvontaa sekä tietokoneiden käytön valvontaa katselmuksin.

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

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 kuvauksissa.

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

Tietoturvallisuusmääritykset tarkistetaan ja arvioidaan vuosittain tai merkittävien muutosten yhteydessä. Tietoturvallisuuden hallintajärjestelmän toimivuus käsitellään johdon katselmoinnissa ja johto päättää tarvittavista laajavaikutteisista muutoksista. Tietoturvallisuuskuvausten teknisen ylläpidon tietosuojasta vastaa digi- ja tietohallintojohtaja.

3 TIETOTURVA- JA TIETOSUOJATYÖN ORGANISOINTI JA TEHTÄVÄT

Tietojen turvaaminen ja tietosuojan toteuttaminen ovat osa johtamistoimintaa. Käytännön tietoturvatoimia hallinnoi ja hoitaa nimetty kuntayhtymän 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 Kuntayhtymän tietoturva- ja tietosuojaorganisaatio

Kuntayhtymän hallitus hyväksyy tietoturva- ja tietosuojapolitiikan. Kuntayhtymän toimitusjohtaja vastaa tietoturvallisuuden yleisestä järjestämisestä. Vastuualueiden johtajat, tehtäväalueiden päälliköt sekä yksiköiden esimiehet vastaavat tietoturvan toteuttamisesta osaltaan (Liite 1, hallinnollinen turvallisuus). Henkilörekisterilain mukaisesta rekisterihallinnosta on annettu ohje. Rekisterinpitäjän edustajat (tietojärjestelmien omistajat rekistereineen) vastaavat tietoturvan ja tietosuojan toteutumisesta jokaisen rekisterin osalta (Liite 1, tietoaineistoturvallisuus). Digi- ja tietohallintojohtaja vastaa kuntayhtymän tietoturvallisuuden johtamisesta ja koordinoinnista sekä tietojärjestelmien operatiivisesta toiminnasta tietoturvallisella tavalla. Toimitusjohtaja vastaa tietosuojan järjestämisestä ja kehittämisestä.

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.

Tietoturvavastaavan tehtävänä on osaltaan ohjata ja valvoa kuntayhtymän tietoturva- ja tietosuojapolitiikan toteutumista.

Tietohallinto koordinoi kuntayhtymän johdon toimeksiannosta tietojärjestelmien ja niiden käytön tietoturvan ja teknisen toteutuksen suunnittelua, toteutumista ja raportointia (Liite 1, laitteistoturvallisuus). Tietohallinto yhdessä palveluntuottajien kanssa toimii teknisenä asiantuntijana tietoturvaa koskevissa kysymyksissä (Liite 1, käyttöturvallisuus).

Tietoturva- ja tietosuojatyöryhmän päätehtävänä on ohjata ja koordinoida tietoturvallisuuteen ja tietosuojaan liittyvien asioiden seurantaa ja kehittämistä. Keskeisenä näkökulmana on henkilöstön opastaminen ja ohjaaminen kohti tietoturvallisempia toimintatapoja (Liite 1, henkilöstöturvallisuus).

Palveluina ostettavien järjestelmien, tietoliikenteen ja ICMT-palvelujen osalta tietoturvallisesta toiminnasta vastaavat palveluja toimittavien yritysten ja yhteisöjen johtajat (Liite 1, tietoliikenneturvallisuus, ohjelmistoturvallisuus).

Kiinteistöhuoltoyksikkö vastaa omien kiinteistöjen fyysisten turvallisuustoimenpiteiden toteutumisesta. Tilapalvelukoordinaattori vastaa vuokralaisen osalta

vuokrakiinteistöjen fyysisen turvallisuuden määrittelystä. Digi- ja tietohallintojohtaja vastaa tietoliikenteen ja muun tekniikan järjestämisestä tietoturvallisella tasolla (Liite 1, fyysinen turvallisuus).

Tietoturvapoikkeamat käsitellään osana kuntayhtymän riskienhallintaprosessia ja –organisaatiota.

3.2 Tietoturvatehtävät ja organisointi

Tietoturva- ja tietosuojaorganisaatio sekä tietohallinto huolehtivat, ylläpitävät ja valvovat koko organisaation tietoaineiston tietoturvaa omien vastuualueidensa mukaisesti.

Kuntayhtymässä tulee olla **tietoturvasta vastaava henkilö**, joka

- valmistelee tietoturvallisuuteen liittyviä kehittämishankkeita yhdessä muiden tietoturvaorganisaatioon kuuluvien henkilöiden kanssa,
- ohjeistaa tietoturvallisuusasiat ja huolehtii, että niistä tiedotetaan ja koulutetaan,
- vastaa tietoturvaohjeiden olemassaolosta ja noudattamisesta sekä huolehtii niiden ajan tasalle saattamisesta ja hyväksyttämisestä,
- vastaa tietoturvapoikkeamien seurannasta ja tilastoinnista,
- tiedottaa tietoturvallisuusasioista ja – ongelmista,
- valmistelee tietoturvaan liittyvä kommunikoinnin koko organisaation, sidosryhmien ja erityisesti esimiesten kanssa,
- vastaa tietoturvatietoisuuden ja osaamistason seurannan toteuttamisesta,
- osallistuu kuntayhtymän turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tarvittaessa turvallisuusasioita käsittelevän ryhmän jäsenenä,
- raportoi tietoturvallisuudesta tietoturvatyöryhmälle,
- osallistuu tietoturvapoikkeamien vakavuusasteiden määrittelytyöhön,
- toimii tietoturvallisuuden asiantuntijana kuntayhtymän toiminta-alueella, tarvittaessa esittää asiantuntijapalveluiden hankkimisesta ja
- valvoo, että tietoturvallisuusasiat on organisoitu kuntayhtymän toimipaikoissa ja yksiköissä.

Tietosuojavastaava

- Vastaa tietosuojaohjeiden olemassaolosta ja noudattamisesta sekä huolehtii niiden ajan tasalle saattamisesta ja hyväksyttämisestä
- Toimii tietosuojan itsenäisenä ja riippumattomana erityisasiantuntijana kuntayhtymän toiminta-alueella.
- Tukee, ohjaa ja opastaa henkilökuntaa ja rekisteröityjä tietosuoja-asioissa.
- Kehittää ja edistää tietoturvallisuutta organisaatiossa
- Ohjeistaa tietoturvallisuusasiat ja huolehtii, että niistä tiedotetaan ja koulutetaan.
- Osallistuu kuntayhtymän turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tarvittaessa turvallisuusasioita käsittelevän ryhmän jäsenenä.
- Seuraa ja valvoo henkilö- ja potilastietojen käsittelyä ja suojaamista ja suojausmenetelmiä sekä raportoi niihin liittyvistä epäkohdista tietoturvaorganisaatiolle/turvallisuustyöryhmälle.

- Suunnitellee ja toteuttaa tietojärjestelmien lokiseurantaa eli käytönvalvontaa.
- Osallistuu organisaation henkilötietojen käsittelyä koskevaan suunnittelutoimintaan.
- Osallistuu henkilöstölle annettavan tietosuojakoulutuksen toteuttamiseen.
- Ohjaa ja neuvoo tietosuoja-asioissa (henkilökunta, asiakkaat).
- Toimii yhdyssiteenä valvontaviranomaisiin.
- Raportoi organisaation johdolle ja turvallisuustyöryhmälle tietosuojan tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta) sekä tietosuojavastaavan toiminnasta.
- Toteuttaa organisaation ja tietoturvaorganisaation johdon osoittamia muita tietosuojaa tukevia tehtäviä.
- Seuraa ja valvoo tietosuojan toimivuutta ja rekisteriselosteiden (HetiL § 10) laatimis- ja ylläpitovelvollisuuden toteutumista.

Tietosuoja- ja tietoturvatyöryhmä

Kuntayhtymän tietosuoja- ja tietoturvatyöryhmään kuuluvat tietosuojavastaava, asianhallintapäällikkö, digi- ja tietohallintojohtaja sekä tietoturvavastaava. Työryhmä voi kutsua tarvittaessa asiantuntijoita. Tietoturvatyöryhmä koordinoi tietoturvapolitiikan, tietoturvakäytäntöjen ja –periaatteiden sekä -ohjeiden laatimista, toteuttamista ja ajan tasalla pitämistä.

- Koordinoi kuntayhtymän tietosuoja- ja tietoturva-asioiden kokonaisuutta.
- Ohjaa ja valvoo tietosuoja- ja tietoturva-asioiden toteuttamista.
- Valvoo kuntayhtymän tietosuoja- ja tietoturvapolitiikan, -käytäntöjen, -periaatteiden sekä -suunnitelman ja -ohjeiden laatimista, toteuttamista ja ajan tasalla pitämistä.
- Määrittää säännölliset tietoturvatoimenpiteet.
- Vastaa tietosuoja- ja tietoturvakontrollien valinnasta ja toteutuksen ohjaamisesta yhteistyössä organisaation eri osien kanssa.
- Seuraa tietosuoja- ja tietoturvallisuustilannetta, -osaamistasoa ja reagoi tarvittaessa havaittuihin ongelmiin ja uhkiin.
- Valvoo, että tietohallinto on järjestänyt jatkuvuussuunnitelman infrastruktuurin ja keskeisten järjestelmien osalta poikkeustilanteita varten.
- Huolehtii säännöllisestä riski-/uhka-analysoinnin tekemisestä.
- Vastaa auditoinnin toteuttamisen järjestämisestä.
- Vastaa tietosuoja- ja tietoturvapolitiikan päivityksestä.
- Määrittelee ja suunnittelee sisäisen valvonnan kohteita.

Asianhallintapäällikkö

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

- Vastaa asiakirjojen käytettävyydestä ja lainmukaisesta säilyttämisestä.
- Asiakirja- ja tiedonhallinnan suunnittelu ja toteutus yhdessä tietohallinnon kanssa.

- Osallistuu organisaation tietoturvaan ja -suojaan liittyvien asioiden suunnitteluun ja kehittämiseen sekä ohjeiden laatimiseen ja ylläpitoon.
- Osallistuu kuntayhtymän turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tietoturvatyöryhmän jäsenenä.
- On tarvittaessa yhteydessä valvontaviranomaisiin.
- Tietosuoja-asioiden ohjaus ja neuvonta (henkilökunta, asiakkaat).
- Tiedonhallinnan vastuunjako löytyy yhtymähallituksen hyväksymästä tiedonhallinnan toimintaohjeesta.

Organisaation johto (kuntayhtymän johtoryhmä, yhtymähallitus)

Kuntayhtymän johtoryhmän jäsenet ja yhtymähallitus vastaavat kukin omalta osaltaan tietoturva- ja tietosuojapolitiikan noudattamisesta omassa toiminnassaan. Johdon tulee osoittaa sitoutumisensa tietoturva- ja tietosuojapolitiikkaan.

Yhtymähallitus

Hyväksyy tietoturva- ja tietosuojapolitiikan.

Vastuualueiden johtajat, tehtäväaluepäälliköt ja tulosyksiköiden esimiehet

- Vastaavat yksiköidensä tietoturvallisuudesta ja tietosuojasta ja siitä, että henkilöstö tuntee niiden perusasiat ja ovat käyneet vaadittavat koulutukset.
- Tukevat tietoturvan ja tietosuojan jatkuvaa ylläpitämistä ja kehittämistä.
- Toteuttavat, budjetoivat ja organisoivat yksikkönsä tietoturvallisuus- ja tietosuojatoimenpiteet yksiköissään.
- Huolehtivat, että vaadittavat tietoturva- ja tietosuojakoulutukset on käyty.
- Tietohallinnon kanssa nimeävät keskeisille järjestelmille vastuuhenkilöt.
- Raportoivat tietoturvallisuusongelmista ja tietosuojarikkomuksista sekä yksikkönsä johdolle että tietosuojavastaavalle.
- Tekevät HaiPro-ilmoitukset tietosuojaan ja tietoturvaan liittyvistä riskeistä ja ongelmista.

Jokainen työntekijä

Jokainen työntekijä vastaa omalta osaltaan tietoturvallisuuden ja tietosuojan toteutumisesta voimassaolevan 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 heti ja aina raportoida HaiPro-järjestelmään havaitsemistaan tahattomista tai tahallisista tietoturva- ja tietosuojarikkomuksista ja lisäksi voi ilmoittaa asiasta linjavastuussa olevalle esimiehelle tai Ylä-Savon SOTE kuntayhtymän tietosuojavastaavalle. Esimiehen tulee huolehtia, että vaadittavat tietosuoja- ja turvakoulutukset on käyty.

Tietojärjestelmien ja laitteistojen omistajat sekä vastuuhenkilöt

Kaikille tietojärjestelmille ja laitteistoille, kuntayhtymän omille ja ulkoistetuille palveluille, on määritelty omistajat/vastuuhenkilöt, jotka määrittelevät ja vastaa-

vat tietojärjestelmien/ sovellusten/laitteistojen palvelutasosta, käyttöoikeuksista, varmistamisesta, kehittämisestä ja hyväksikäytöstä. Tietojärjestelmän omistaja vastaa tietojärjestelmän tietoturvasta mm. tietojärjestelmään sisältyvien rekisterien oikeellisuudesta ja lainmukaisuudesta, kuten henkilörekisterilaissa mainitun rekisterinpitäjän velvollisuuksista.

Omistaja vastaa tietoturvallisuudesta myös yksittäisen tietojärjestelmän toiminnan ja käytön osalta. Ylä-Savon SOTE kuntayhtymään on laadittu valmiussuunnitelma, toiminnan jatkuvuuden turvaamiseksi normaaliolosuhteiden poikkeustilanteiden sekä eriasteisten poikkeusolojen varalle.

Tietohallintolain mukaiset tietohallintoyksikön tehtävät

Digi- ja tietohallintojohtajan johdolla toimivalle yksikölle on keskitetty 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).
- Vastaa organisaation tietoteknisten toimenpiteiden toteutuksesta.

3.3 Soveltaminen

Ylä-Savon SOTE kuntayhtymän hallituksen hyväksymä kirjallinen tietoturva- ja tietosuojapolitiikka (tämä asiakirja) saatetaan tiedoksi jokaiselle Ylä-Savon SOTE kuntayhtymän työntekijälle ja tietojärjestelmien käyttäjälle. Tietoturvallisuuden toteutuminen varmennetaan vuosittain toimintakertomukseen tulevalla maininnalla suoritetuista toimenpiteistä, sisäisen valvonnan raportista ja HaiPro-ilmoitusten käsittelystä.

Tietoturva- ja tietosuojapolitiikkaa, tietoturvallisuuskäytäntöjä ja -periaatteita sekä näihin liittyviä ohjeita noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia Ylä-Savon SOTE kuntayhtymän palveluksessa olevia henkilöitä ja luottamushenkilöstöä. Niitä noudatetaan myös kaikessa toiminnassa kuntayhtymän ulkopuolisten yhteistyökumppaneiden kanssa. Tietoturvallisuuteen liittyviä määrityksiä tarkistetaan ja arvioidaan muutosten yhteydessä ja poikkeamailmoitusten ja sisäisen valvonnan raporttien perusteella.

Ylä-Savon SOTE kuntayhtymän tietoturva- ja tietosuojapolitiikan julkaisusta vastaa viestintä. Dokumentti on saatavissa kuntayhtymän verkkosivuilta osoitteessa http://www.ylasavonsote.fi.

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

- tietoturva- ja tietoperiaatteet on hyväksytty,
- tietoturva-, jatkuvuus- ja toipumissuunnitelmat on laadittu,
- tietoturvakoulutus on organisaatiossa jatkuvaa ja valvottua,
- tietoturvavastuut ja -tehtävät on määritelty ja
- 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 tietoturvallisuudessa päämääränä on luoda organisaatioon toimintatapa, jolla pystytään välttämään tietoturvariskit. Riskejä hallitaan erikseen määriteltävän ja kuvattavan riskienhallintaprosessin avulla. Hyväksyttävän riskitason määrittelee johto riskianalyysin perusteella ja yhteisesti valmisteltujen kriteeristöjen ja mittarien avulla.

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.

Kuntayhtymän ohjelmistoturvallisuuden perustaso edellyttää, että

- tietojärjestelmien ylläpidosta huolehditaan ohjelmistotoimittajien kanssa tehtyjen ylläpitosopimusten mukaisesti,
- ohjelmistotoimittajilta vaaditaan tuotteelleen tietoturva/-suojaselvitys, hyväksytty auditointi, tietoturvasuunnitelma/kuvaus sekä ICT -valmiussuunnitelma (toiminta poikkeusoloissa/sopimukset),
- 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 ja
- ohjelmistojen ylläpitoa varten avatut etäyhteydet ovat suojattuja ja sanomaliikenne salattua. Etäyhteyden käyttö edellyttää luotettavaa tunnistautumista.

Kuntayhtymässä on määritelty ohjelmistojen käyttöön liittyvät velvollisuudet:

- Ohjelmiin kuuluvat alkuperäiset dokumentit ja/tai käsikirjat on talletettu huolellisesti ja niiden sijainti on tiedossa.
- Kaikki ohjelmamuutokset/päivitykset käsitellään organisaation muutostenhallintaprosessin mukaisesti ja tiedotetaan viestintäsuunnitelmassa kuvatulla tavalla.
- Ohjelmien kopioinnissa noudatetaan tekijänoikeuslakia ja lisensseistä pidetään kirjaa.
- Keskuskoneilla varmuuskopiointi on sovittu järjestelmäkohtaisesti ja kopioinnista.
- Säilytyksestä ja varmuuskopioiden palautuksen testaamisesta vastaa palvelun suorittava operaattori.

Ohjeet ohjelmistojen käytöstä työasemilla:

- Ohjelmistojen elinkaaren hallinta ja hankintojen koordinointi on keskitetty tietohallintoon.
- Tietohallinto hyväksyy kaikki työasemille asennettavat ohjelmat.
- Ohjelmien asennusmediat, samoin kuin niiden kopiot, säilytetään tietoturvaohjeiden mukaisesti.

- Työasemien 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 ict- ja 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 tietojenkäsittelyn toipumis- ja valmiussuunnitelmat,
- on tietojärjestelmille nimetyt vastuu- ja varahenkilöt päivittäin hoidettavien rutiinitehtävien ohjeistukset,
- on varasuunnitelmat käyttökatkoksia varten,
- noudatetaan turvallisuusohjeita ja käyttöoikeuskäytäntöjä,
- tietojärjestelmiä käyttävät henkilöt tunnistetaan ja todennetaan,
- on käytössä käyttäjätunnus-, salasana-, toimikortti- ja PIN-koodi –menettelyt,
- on ohjeistus 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 ja
- seurataan verkon liikennettä, komponenttien tilaa ja verkkoon tunkeutumista ympärivuorokautisesti sekä toteutetaan poikkeuksellisen liikenteen vaatimat toimenpiteet viivytyksettä.

4 Henkilön tunnistaminen ja sähköinen allekirjoitus

4.1 Asiakkaan tai potilaan tunnistaminen

Ylä-Savon SOTE Kuntayhtymässä 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 tunnistamisen erityistilanteissa esim., kun otetaan kantaa hoitoon puhelimessa tai ensihoidossa (henkilöllä ei mukana henkilöllisyys todistuksia), tapahtuu tunnistaminen ensisijaisesti henkilötunnuksella ja tarvittaessa esittämällä henkilölle henkilöllisyyttä tarkentavia kysymyksiä tai potilastietojärjestelmän hallinnollisia tietoja, joiden pohjalta voidaan henkilöllisyys varmentaa. Mikäli kyseessä tunnettu potilas/asiakas, jolloin ei ole syytä epäillä henkilöllisyyttä, erillistä tunnistamista ei tarvita.

4.2 Työntekijän tunnistaminen

Organisaation tietojärjestelmiä ja 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.

4.3 Työntekijän sähköinen allekirjoitus

Sähköisessä muodossa olevissa lausunnoissa ja todistuksissa sekä vastaavissa asiakirjoissa tulee olla asiakirjan laatijan allekirjoitus, joka vastaa Laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159 sekä sitä tarkentavassa asetuksessa annettuja määräyksiä. Muissa kuin lääkintälaillisissa asiakirjoissa käytetään vaatimustenmukaista sähköistä allekirjoitusta. Sähköisten lääkemääräysten laatijan tulee allekirjoittaa resepti noudattaen lakia sähköisistä lääkemääräyksistä.

Kaikki sähköiset asiakirjat tulee allekirjoittaa organisaation tai tietoteknisen laitteen tekemällä vaatimustenmukaista sähköistä allekirjoitusta vastaavalla allekirjoituksella.

4.4 Asiakkaan tai potilaan sähköinen allekirjoitus

Kirjallinen suostumus ja hakutietojen näkymisen kieltoasiakirja tulee olla allekirjoitettu joko omakätisesti Omakanta palvelussa tai paikan päällä suoraan potilastietojärjestelmään ammattihenkilön toimesta. Suostumus tai kielto tulostetaan ja ao. potilas allekirjoittaa suostumuksen/kiellon manuaalisesti. Allekirjoitettu kappale toimitetaan potilastietoarkistoon. Sosiaalihuollossa suostumukset ja kiellot tehdään toistaiseksi paperimuotoisena ja liitetään asiakasaktiin. Kiellosta ja/tai suostumuksesta tehdään merkintä asiakasreksiteriin.

4.5 Sähköinen allekirjoitus toimintayksikkö, organisaatio tai tietotekninen laite

Tekninen sähköinen allekirjoitus toteutetaan laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159 annettujen määräysten mukaisesti.

5 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja valvonta sekä niiden kapasiteettien suunnittelu. Ylipäätään 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

- tietoverkot, ICT- ja tutkimuslaitteistot on dokumentoitu ja niistä on laadittu toipumissuunnitelmat riskianalyysin pohjalta,
- varajärjestelmien käytettävyys poikkeusoloissa on varmistettu,
- laitteistojen fyysisen kunnon varmistamiseksi laadittuja ohjeita noudatetaan,
- huolto- ja ylläpitosopimukset ovat ajan tasalla ja vastaavat käytettävyysvaatimuksia,
- jokaisella laitteella on omistaja, joka vastaa laitteesta,
- laitteista on laiterekisteri,
- tietojenkäsittelykapasiteettia seurataan, suunnitellaan ja ennakoidaan,
- laitteistojen poistamisesta on kirjalliset ohjeet,
- laitteistoilla on ajantasainen suojaus haittaohjelmia varten ja
- laitteiden tietoturvapäivityksille on olemassa dokumentoitu prosessi.

6 Fyysinen turvallisuus

Fyysisin turvallisuustoimenpitein luodaan ja ylläpidetään tietotekniikan vaatiman käyttöympäristön toimintaolosuhteet ja suojataan ja valvotaan kiinteistö, sekä varmistetaan teknisten järjestelmien toiminta. Fyysinen turvallisuus käsittää kiinteistöjen rakenteellisen turvallisuuden, valvontatekniikan kuten kulunvalvonta-, rikosilmoitus- ja videovalvontajärjestelmät sekä valvonnan ja vartioinnin. Fyysisen turvallisuuden lähtökohta on organisaation laatima riskianalyysi.

Fyysisen turvallisuuden perustaso edellyttää, että

- kiinteistön toimitilat on luokiteltu kulku- ja pääsyvyöhykkeisiin,
- fyysisten tilojen suunnittelussa ja laitteiden sijoittelussa otetaan huomioon tietosuoja-, tietoturva- ja työturvallisuusnäkökohdat,
- tietoturvan ja tietosuojan kannalta oleelliset tilat pidetään lukittuna,
- toimitilojen turvallisuus on hoidettu vartioinnilla, teknisillä hälytysjärjestelmillä tai vastaavilla toimenpiteillä,
- korotetun suojaustason tiloissa tulee olla kulunvalvonta ja kulkuoikeudettomilla henkilöillä saattaja,
- palvelinlaitteistot on keskitetty erityisiin atk-tiloihin, joiden rakentamisessa on noudatettu em. tiloja koskevia ohjeita,
- tutkimuslaitteistot, verkon komponentit, kytkentätilat, työasemat ja muut automaattista tietojenkäsittelyä suorittavat laitteet on sijoitettu ja suojattu luokituksensa mukaisesti,
- kriittiset laitteistot on merkitty yksilöidysti,
- kriittisille laitteistoille on tehty toipumissuunnitelma ja toipumissuunnitelma on koestettu,
- varmuuskopiot on sijoitettu fyysisesti eri palotiloihin,

- kaapeloinnit suoritetaan voimassa olevan yleiskaapelointiohjeen mukaisesti,

- paikallisverkon käytönvalvonta on järjestetty ja
- paikallisverkolle on tehty valmius- ja toipumissuunnitelmat.

7 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) ja
- käyttöoikeuksien valtuuttamiseen, muutoksiin ja poistamisiin on dokumentoitu prosessi.

8 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.

Lain yhteistoimintamenettelystä yrityksissä (334/2007) tavoitteena on edistää yrityksen ja sen henkilöstön välistä vuorovaikutusta. Yhteistyötoimikunta muodostuu työntekijöiden ja työnantajan edustajista. Tietoturvaan liittyvät ohjeet, sopimukset ja sanktiosäännökset on hyvä saattaa yhteistyötoimikunnan tiedoksi ja myös tarvittavin osin hyväksyttää siellä.

Henkilöstön tehtäväkuvauksia ylläpidetään siten, että tehtävistä on johdettavissa tehtävien edellyttämät henkilökohtaiset tietojärjestelmien käyttöoikeudet. Tietojärjestelmien käyttäjistä pidetään ajantasaista rekisteriä, josta ilmenee käyttäjän yksilöintitietojen lisäksi käyttäjärooli. Ostopalveluiden tuottajilta tai muuten kuntayhtymän tietojärjestelmiä käsitteleviltä henkilöiltä edellytetään vastaavien tehtäväkuvauksien ylläpitoa käyttäjärekisteriä varten.

Uuden henkilöstön perehdytykseen kuuluu terveydenhuollon salassapitosäännösten läpikäynnin lisäksi tietoturvakoulutus ja ennen tietojärjestelmäoikeuksien myöntämistä tietoturvasitoumuksen allekirjoittaminen.

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.

Työntekijät saavat säännöllisesti tietoturvakoulutusta. Tietämystasoa ja osallistumista koulutukseen seurataan ja tulokset raportoidaan kuntayhtymän vastuuhenkilölle.

Ylä-Savon SOTE kuntayhtymän toiminnan kannalta kriittisten tietojärjestelmien kriittisten tehtävien vastuuhenkilöllä on sovittu varahenkilö.

Työnkuvissa on huolehdittu, ettei synny tilanteita tai käyttöoikeuksia, jotka mahdollistavat tietojen käsittelyn ilman toisen työntekijän mahdollisuutta kontrolloida käsittelyä (niin sanotut vaaralliset yhdistelmät).

Henkilöstöturvallisuustyön tulos on luotettava ja tehtäviinsä soveltuva henkilöstö, joka tuntee itselleen asetetut tietoturvavaatimukset omaan toimenkuvaansa ja rooliinsa liittyen. Oman ja ostopalveluita Ylä-Savon SOTE kuntayhtymälle tuottavan henkilöstön tulee tuntea tiedonsaantioikeutensa, käyttöoikeutensa, sijaisuus- tai muihin työtä koskeviin järjestelyihin liittyvät toimet, oma tietosuojansa sekä velvollisuutensa ja oikeutensa työsuhteen alkaessa ja päättyessä.

9 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 tulee olla ajantasainen, kaikki tietoaineistot kattava tiedonohjaussuunnitelma, josta ilmenee tietoaineiston käsittelysäännöt tietojen synnystä niiden tuhoamiseen tai pysyvään säilytykseen asti, määritellään julkisuusarvo sekä eheyden ja käytettävyyden varmistetaan aineiston elinkaaren kaikissa vaiheissa.

Organisaation johto vastaa henkilöstön perehdyttämisestä tietoaineistojen käsittelyohjeisiin. 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 ja
- tietojen ja asiakirjojen luokittelusääntöjä.

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 kuntayhtymän työntekijöiden kanssa. Potilas- ja asiakastietojen käsittelystä on laadittu henkilökunnalle ohjeet, joiden ylläpidosta vastaava henkilö on nimetty.

Tietoja säilytetään ja vanhentuneet tiedot hävitetään arkistonmuodostussuunnitelman 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.