JULKINEN

Perusturvakuntayhtymä Akseli

TIETOSUOJA- JA TIETOTURVAPOLITIIKKA JA PERIAATTEET

Päivitetty: 4.5.2018 Marjut Kaarilahti
Tietosuojatyöryhmä 4.5.2018 käsitelty
Johtoryhmä 8.5.2018 hyväksytty
Yhtymähallitus 16.5.2018 § 82 hyväksytty

Sisällysluettelo

TIETOSUOJAPOLITIIKKA

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Perusturvakuntayhtymä Akselin (jäljempänä kuntayhtymä) tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa kuntayhtymä toimii rekisterinpitäjänä.

Kuntayhtymän palveluiden perustana ovat asiakkaiden / potilaiden tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn kuntayhtymän toimintaympäristössä. Palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta.

Kuntayhtymän toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Henkilötietojen käsittelyn suunnittelussa ja ohjaamisessa tulee varautua niin pieneen, keskisuureen, kuin suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin. Erityisesti huolellista ennakkovalmistelua edellyttävät tilanteet, joissa henkilötietojen käsittelyä ohjataan sopimuksilla.

Tietosuoja ja tietoturvallisuus on huomioitava kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. Kuntayhtymän johto tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet sekä tietoturvatoiminnan periaatteet. Politiikka toimii perustana kuntayhtymän tietosuojaa ja tietoturvaa koskeville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojapolitiikka koskee koko organisaatiota ja sen henkilöstöä sekä niitä kuntayhtymän sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kuntayhtymän omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kuntayhtymän omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta sen on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt virheelliset tai tarpeettomat tiedot muutetuiksi tai poistetuiksi.

Tietoturvallisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen turvaaminen siten, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen.

- Luottamuksellisuus: Tieto on vain siihen oikeutettujen saatavilla.
- Eheys: Tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- Saatavuus: Tieto on saatavilla aina sitä tarvittaessa.

Tietosuojan tavoitteet ja periaatteet

Kuntayhtymän lähtökohtana tietosuojassa on riskilähtöisyys. Kuntayhtymä rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa kuntayhtymän henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Kuntayhtymä toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä.

Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

Kuntayhtymän toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Kuntayhtymän tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

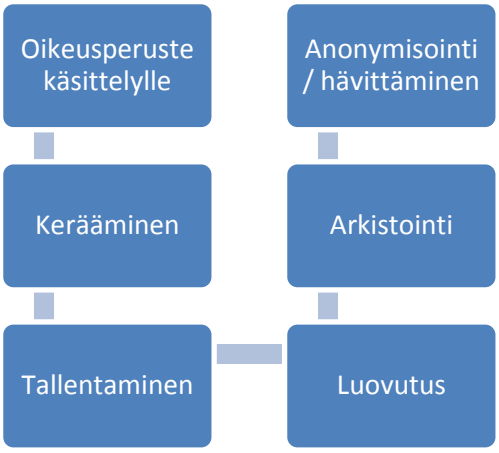
- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

Tietosuojan toteuttaminen

Kuntayhtymä haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia.
Näiden toimenpiteiden avulla varmistetaan, että:

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin

Tietosuojan toteuttamisessa kuntayhtymä haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.



Kuva : Henkilötietojen elinkaaren vaiheet

Kuntayhtymän järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan.

Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

Kuntayhtymä voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle / palvelun tuottajalle.

Kuntayhtymä valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Kuntayhtymän ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti.

Kuntayhtymä ohjeistaa ulkoistettua henkilötietojen käsittelijää kyseistä tarkoitusta varten tehdyllä ohjeistuksella. Samaa ohjeistusta sovelletaan myös kuntayhtymän oman henkilöstön kohdalla.

Kuntayhtymä rekisterinpitäjänä sisällyttää tietosuojan myös projektihallintamallinsa osaksi. Kuntayhtymässä on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

Kuntayhtymä huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja tiedottamisen kautta. Organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä tehtävissä, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

TIETOTURVAPOLITIIKKA

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

Arkistotoimella että tietohallinnolla on yhteisenä tavoitteena tietojen saatavuuden ja käytettävyyden turvaaminen. Tiedon käytettävyydellä ja saatavuudella tarkoitetaan, että tieto on tallennettu siten ja sellaisessa muodossa, että se on luettavissa, ymmärrettävissä, tulkittavissa oikein, kattava, ajantasainen, oikeellinen ja muuten käyttökelpoinen vaadittavalla tavalla ja helppokäyttöisesti ilman tulkinta- ja väärinkäyttömahdollisuutta.

Tiedon, tietojärjestelmän ja palvelun on oltava saatavilla ja hyödynnettävissä siihen oikeutetuille riittävän esteettömästi, vaivattomasti ja nopeasti vaaditulla tavalla ja vaadittuna aikana.

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista, jonka päämääränä on turvata kuntayhtymän toiminnalle tärkeiden tietojärjestelmien ja tietoverkko-

jen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoaminen tai vääristyminen sekä minimoida aiheutuvat ongelmat.

Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen. Suojautuminen kattaa sekä riskien toteutumista ehkäisevät toimenpiteet, toiminnan jatkuvuutta suojaavat toimet että poikkeustilanteita varten laadittujen valmiussuunnitelmien mukaiset toimet.

Tietoturvan tavoitteet ja periaatteet

Hallinnollinen turvallisuus

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

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

Hallinnollisen tietoturvallisuuden periaatteet:

- Kuntayhtymä noudattaa sitä sitovia lakeja ja asetuksia sekä kehittää toimintaansa vastaamaan voimaan tulevia toimialan viranomaissuosituksia, valtakunnallisten tietojärjestelmäpalveluiden asettamia tietoturvavaatimuksia ja tietoturvakäytäntöjä. Kuntayhtymässä on henkilöstön tietoturvaohjeet, jotka ohjeistavat tietoturva- ja tietosuojapolitiikan mukaisiin tietoturvakäytäntöihin.

- Tietoturvaan ja tietosuojaan liittyvillä tehtävillä on nimetyt vastuuhenkilöt, jotka ovat organisaatiossa työskentelevien ja sidosryhmien vastuuhenkilöiden tiedossa. Vastuuhenkilöillä on resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät.

- Tietoturvan eri osa-alueilla seurataan tietoturvatilannetta säännöllisesti raporteilla ja valvontajärjestelmillä sekä erikseen tehtävillä riskikartoituksilla. Havaintojen pohjalta tehdään tarvittaessa tietoturvan kehittämissuunnitelma.

- Keskeisistä tietoturvallisuusasioista annetaan ohjeet. Tietoturvallisuustietämyksen ajan tasalla pysymisestä huolehditaan säännöllisen koulutuksen, tiedotuksen, ohjeistuksen ja motivoinnin keinoin.

- Palveluiden hankinnoissa edellytetään, että tiedon käsittelyyn liittyvät suojaustoimet, vastuut ja tekniset tietoturvavastuut sisältyvät ostopalvelusopimuksiin. Palveluiden tuottajilta edellytetään sovittua palvelutasoa vastaavaa tietoturvatasoa. Palvelun tuottajalta edellytetään kuvausta palvelun tietoturvatasosta sekä tietoturvapoikkeamien valvonta-, havaitsemis-, ilmoittamis- ja käsittelykäytännöistä. Palvelun tuottajalta edellytetään, että se pitää organisaatiolle toimitetut dokumentit ajantasaisina, ja että se raportoi ostopalveluun liittyvistä tietoturvapoikkeamista. - Ohjelmistojen ja laitteiden tarjouspyynnöissä ja hankinnoissa edellytetään voimassa olevien standardien noudattamista ja ennen hankintapäätöksiä tehtyä tietoturvallisuusnäkökohtien arviointia.

Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstön toimista aiheutuvien ja heihin kohdistuvien tietoturvauhkien hallintaa. Henkilöstöturvallisuustyön tulos on luotettava ja tehtäviinsä soveltuva henkilöstö, joka tuntee itselleen asetetut tietoturvavaatimukset omaan toimenkuvaansa ja rooliinsa liittyen.
Oman ja ostopalveluita organisaatiolle tuottavan henkilöstön tulee tuntea tiedonsaantioikeutensa, käyttöoikeutensa, sijaisuus- tai muihin työtä koskeviin järjestelyihin liittyvät toimet, oma tietosuojansa sekä velvollisuutensa ja oikeutensa työsuhteen alkaessa ja päättyessä.

Henkilöstötietoturvallisuuden periaatteet:

- Uuden henkilöstön perehdytykseen kuuluu henkilöstön tietoturvaohjeiden läpikäyminen sekä tietoturvan ja tietosuojan verkkokoulutuksen suorittaminen. Nämä koulutukset suoritetaan Perusturva-kuntayhtymä Akselin tietoturva, tietosuoja ja tietojärjestelmien käyttöön liittyvän omavalvonta-suunnitelmassa määriteltyjen koulutusten mukaisesti. Ennen tietojärjestelmän käyttöoikeuksien myöntämistä allekirjoitetaan asiakirjojen, tietojen ja tietojärjestelmien vaitiolo- ja salassapitositoumus.
- Henkilöstön tehtäväkuvauksia ylläpidetään siten, että niistä on johdettavissa tehtävien edellyttämät henkilökohtaiset tietojärjestelmien käyttöoikeudet.

- Tietojärjestelmien käyttäjistä pidetään ajantasaista rekisteriä, josta ilmenee käyttäjän yksilöintitietojen lisäksi käyttäjärooli. Ostopalveluiden tuottajien henkilöistä tai muuten organisaation tietojärjestelmiä käsittelevistä (esim. harjoittelijat ja opiskelijat) edellytetään vastaavien tehtäväkuvauksien ylläpitoa käyttäjärekisteriä varten.

- Käyttöoikeuden saaminen alueelliseen tai valtakunnalliseen tietojärjestelmäpalveluun edellyttää työntekijän henkilöllisyyden luotettavaa varmistamista tai henkilökohtaisen varmennekortin myöntämistä.

- Organisaation toiminnan kannalta kriittisten tietojärjestelmien vastuuhenkilöillä on nimetyt varahenkilöt.

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

- Esimiehet vastaavat siitä, että henkilökunta on selvillä tietoturvavaatimuksista ja noudattaa annettuja tietoturvaohjeita ja käytäntöjä.

- Työntekijät saavat säännöllisesti tietoturvakoulutusta. Tietämystasoa ja osallistumista koulutukseen seurataan ja tulokset raportoidaan organisaation vastuuhenkilölle ja johdolle. Tietosuojavastaava huolehtii tietoturvan ja tietosuojan verkkokoulutuksen ylläpidosta, seurannasta ja raportoinnista.
- Tietoturvaohjeiden noudattamisen seuranta: Käyttö- ja luovutuslokivalvontana on suunnitelmallista ja säännöllistä / pistokoevalvontana. Tietosuojarikkomukset käsitellään seuranta ja valvontasuunnitelman mukaisesti. Väärinkäytösten varalle on laadittu seuraamusjärjestelmä.

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

Fyysinen turvallisuus

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

Fyysisen tietoturvallisuuden periaatteet:

- Asiaton pääsy toimintayksikön tai sen palveluntuottajan tiloihin, joissa on pääsy suojattuun tietojärjestelmäympäristöön, estetään valvonnalla ja pitämällä lukittuna tilat, joissa ei ole henkilökuntaa tai kameravalvontaa. Tilojen avaimet ovat henkilökohtaisia ja avainten haltijoista pidetään rekisteriä.
- Tietoteknisten laitteiden sijoittelussa on huomioitu vesi-, lämpö- ja tulivahinkojen riski. Palvelinten ja muiden järjestelmään kuuluvien laitteiden ja tiedonsiirtoverkon suojaus ja valvonta ulkoisilta uhkilta vastaa tietojärjestelmien kriittisyyttä palvelutoiminnan hoidossa. Varmuuskopiot on sijoitettu fyysisesti eri palotiloihin.

- Sähkönsyöttö ja varautuminen sähkönsyötön katkoksiin tietojärjestelmän laitteille ja tiedonsiirtoverkolle vastaa IT-yksikkönä ohjelmistojen kriittisyyttä palvelutoiminnan hoidossa.
- Tietojärjestelmille ja kriittisille työasemille on tehty jatkuvuus- ja toipumissuunnitelmat.
- Paikallisverkon käytönvalvonta on järjestetty.

Laitteistoturvallisuus

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

Laitteistotietoturvallisuuden periaatteet:

- Kaikki hankittavat laitteistot ovat kokonaisarkkitehtuurin mukaisia tai muuten yhteensopivia organisaation tietojärjestelmäympäristön sekä tiedonvälitysverkoston kanssa. Hankinnat, asennukset ja käytöstä poistot hoidetaan keskitetysti.

- Laitteisto valitaan siten, että sen käyttöikä ja vastaavuus tietojärjestelmävaatimusten muutoksiin arvioidaan kohtuulliseksi. Laitteistoja hankittaessa otetaan huomioon varaosien, huollon ja vararatkaisujen saatavuus.
- Työasemista ja oheislaitteista, esim. tulostimista, on tunnistettu kriittiset laitteet palvelutoiminnan toteuttamisen jatkuvuuden sekä palvelutasovaatimusten kannalta. Kriittisille laitteille on järjestetty katkojen aikainen sähkönsyöttö ja riittävä palvelutaso ylläpidossa.

- Palvelimien, verkon ja muiden laitteiden kriittisyys johdetaan niissä ylläpidettävien ohjelmistojen ja työasemien kriittisyyden perusteella. Kriittisille laitteistoille taataan katkoton sähkön syöttö ja korkea palvelutaso ylläpidossa.

Ohjelmistoturvallisuus

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

Ohjelmistotietoturvallisuuden periaatteet:

- Ohjelmistohankinnat ja kehittäminen perustuu toiminnan lähtökohdista todettuihin tarpeisiin. Uuden ohjelman hankinnan edellytys on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja kokonaisarkkitehtuurin kanssa.
Hankinnat, ohjelmistojen asennukset ja käytöstä poistot hoidetaan keskitetysti.

- Ohjelma tai sen versio hyväksytään käyttöön vasta, kun se on testattu tulevassa ympäristössään ja todettu tilausta vastaavaksi teknisesti ja toiminnallisesti. Käyttöönotto perustuu hyväksyttyyn käyttöönottosuunnitelmaan, jossa kuvataan myös mahdollisten ongelmien luokittelu, korjausmenettelyt ja niiden vasteaika.

- Valtakunnallisten tietojärjestelmäpalveluiden kanssa asioiva ohjelmisto tulee olla testattu hyväksyttävästi valtakunnallisen palvelun järjestäjän edellyttämällä tavalla ja järjestelmä todettu kansallisten auditointivaatimusten mukaiseksi.

- Ohjelmistoille on määritelty selkeät käyttötarkoitukset siten, että käyttäjä tietää mitä ohjelmistoa hänen tulee käyttää eri tehtävissä ja tarkoituksissa. Ohjelmistojen yhteistoiminnallisuus on varmistettu ja tietoaineisto pysyy eheänä ilman erillisiä käyttäjän toimia tallennusvaiheessa tai tietoa haettaessa.

- Alueellisen tai valtakunnallisen tietojärjestelmäpalvelun kautta luovutetun tiedon käsittely ohjelmistolla on mahdollista vain henkilölle, joka on nimenomaisesti saanut käyttöoikeuden katsoa luovutettua tietoa tai luovuttaa organisaation tietoja.

- Ohjelmistojen toimivuuden valvonta ja ylläpidon palvelutaso vastaavat niiden määriteltyä kriittisyyttä palvelutoiminnalle.

- Salattuja tietoja sisältävistä ohjelmistoista on dokumentti, jossa kuvataan ohjelmiston suojaus haittaohjelmilta ja asiattomalta tunkeutumiselta sekä suojauksen valvonta.
- Ohjelmistossa käsiteltävien tietojen tietoturva vastaa tietoaineistojen kriittisyyttä ja määriteltyä elinkaarta. Ohjelmistoilla on jatkuvuus- ja toipumissuunnitelma.

- Ohjelmistojen ylläpitoa varten avatut etäyhteydet ovat suojattuja ja sanomaliikenne salattua. Etäyhteyden käyttö edellyttää luotettavaa tunnistautumista. Ohjelmiston ylläpitotoimien laajuus sekä niistä riippuvat hyväksymiskäytännöt ja ajoitus on sovittu ja dokumentoitu. Poikkeamista sovituista malleista seurataan ja siihen puututaan.

- Työasemien ja palvelinten käyttöjärjestelmien sekä ohjelmistojen turvapäivityksiä varten on toimintasuunnitelma. Päivitystarvetta seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan.

Tietoliikenneturvallisuus

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

Tietoliikenneturvallisuuden periaatteet:

- Organisaation tietojärjestelmäympäristö on suojattu palomuurilla, jota valvotaan. Palomuuri sallii vain määritellyn liikenteen järjestelmiin. Yhteydet ulkoisiin järjestelmiin ja portaaleihin ovat vahvasti salattuja.

- Arkaluonteisia ja salassa pidettäviä tietoja ei lähetetä organisaation sisällä eikä organisaatiosta ulos salaamattomina eikä suojaamatonta yhteyttä pitkin.
Tietosuojaa koskevat vaatimukset ja vastuut on määritetty viestinvälityspalvelua koskevissa sopimuksissa.
Etäyhteydet on toteutettu suojattuna ja vahvaa tunnistautumismenetelmää käyttäen.
- Tietoliikennelokia ja käyttöhäiriöitä seurataan säännöllisesti.

Käyttöturvallisuus

Käyttöturvallisuus kattaa turvallisen käytön toimintaolosuhteet, tekniikan toimivuuden valvonnan, käyttöoikeudet, käytön ja lokien valvonnan, ohjelmistotuen, ylläpidon ja huollon turvallisuustoimenpiteet, varmuus- ja suojakopioinnin sekä häiriöraportoinnin.

Käyttöturvallisuustyön tulos on hallittu tietoaineiston käsittely, jossa tietojen käyttäjä on suojattu tietämättömyyden, osaamattomuuden, tahattomien virheiden ja vahinkojen sekä tahallisten tekojen aiheuttamilta tilanteilta, joissa käyttäjä voisi syyllistyä tietojen asiattomaan tai oikeudettomaan käsittelyyn.

Käyttöturvallisuuden periaatteet:

- Tietojärjestelmien käyttökoulutus ja tehtävien mukaisen käytön opetus kuuluu jokaisen käyttäjän perehdytykseen. Käyttäjien osaamista seurataan ja tulokset huomioidaan henkilöstön koulutuksessa.
- Henkilöstön tietoturvaohjeisiin on koottu ohjeita ja neuvoja tietojen, tietojärjestelmien ja työvälineiden tietoturvalliseen käyttöön.

- Asiayhteys käyttäjän ja rekisteröidyn välillä on aina salassa pidettävien tietojen käytön edellytys. Tahaton käyttö ilman asiayhteyttä estetään informoinnin, teknisten järjestelmien ja tehtäväkuvien selventämisen avulla.

- Henkilötietoja sisältävän tietojärjestelmän käyttäjällä tulee olla henkilökohtainen ja yksilöivä käyttäjätunnus ja vain omassa tiedossa oleva salasana tai varmennekortti tai vastaava tunnistautumisväline.

- Käyttöoikeuksien myöntämisen periaatteet on dokumentoitu ja niiden noudattamista valvotaan. Käyttöoikeuksien haltijoista pidetään rekisteriä, jota säilytetään 12 vuotta.

- Käytöstä kerätään lokitiedot, joiden avulla käyttö voidaan jäljittää yksilötasolle. Säännöllisessä lokivalvonnassa syntyvät raportit säilytetään 5 vuotta. Käyttölokitietojen selvityspyynnöt ja niiden lokiseurantaraportit säilytetään 12 vuotta. Samoin 12 vuotta säilytetään toimenpiteisiin johtaneiden tapausten selvitykset ja raportit.

Tietoaineistoturvallisuus

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

Tietoaineistoturvallisuuden periaatteet:

- Henkilö- ja potilastietojen käsittelyn edellytys on käyttäjän tehtävistä johtuva asiayhteys asiakkaaseen tai potilaaseen tai häntä koskeviin tietoihin. Henkilökuntaa sitoo vaitiolo- ja salassapitovelvollisuus.

- Sähköisessä muodossa olevia ja valtakunnallisten tietojärjestelmäpalveluiden kautta saatavia tietoja saa käsitellä vain henkilökohtaisilla käyttäjätunnuksilla ja varmennekortilla tunnistautunut henkilö.
Tietoaineistojen käyttöä seurataan säännöllisesti ja seurannan periaatteet on käsitelty YT-menettelyn mukaisesti työntekijöiden kanssa.

- Henkilökunnan edellytetään tuntevan henkilötietojen käsittelyä ohjaavat ja rajoittavat normit sekä tietojen ja asiakirjojen luokittelu julkisuus- ja salassapitosäännösten mukaisesti.
Perehdytyksen, koulutuksen ja tietoturvaohjeistuksen avulla ylläpidetään ja kehitetään henkilökunnan valmiuksia.

- Henkilö- ja potilastietojen käsittelystä ja menettelytavoista on laadittu ohjeita, jotka esimerkiksi tarkentavat kansallisia suosituksia ja ohjeita sekä alueellisesti sovittuja toimintamalleja. Näiden ohjeiden annosta ja ylläpidosta vastaa kyseinen linjajohtaja.
- Asiakirjahallinnon / rekisterihallinnon ohjeeseen sisältyy ohjeistoa tietojen luokittelusta, säilyttämisestä ja hävittämisestä sekä tietojen luovuttamisesta.

- Tietoaineiston säilytys tapahtuu arkistonmuodostussuunnitelman mukaisesti, joka on laadittu arkistosäädöksiä ja kansallisia tehtäväluokituksia noudattaen.
Tietoaineiston säilyminen luottamuksellisena, eheänä ja muuttumattomana on huomioitu tiedon koko elinkaaren aikana aineiston lopulliseen hävittämiseen asti.

- Henkilörekisterin perustaminen ja henkilötietojen käsittely tulee olla asiallisesti perusteltua rekisterinpitäjän tehtävän ja toiminnan kannalta. Rekisteristä laaditaan tietosuojaseloste ja / tai seloste rekisterinpitäjän henkilötietojen käsittelystä.

- Tietoaineiston lakisääteisen tiedonsaantioikeuden käytön, tarkastusoikeuden ja tiedon korjaamisvaatimuksen toteuttamista varten on sovittu palvelusta vastaavat henkilöt ja kuvattu prosessin toteuttamistapa.

- Tietoaineiston käyttämisestä tai luovuttamisesta laskutus, tilastointi-, raportointi-, kehittämis- ja tutkimustarkoituksiin on annettu ohjeet.

Tietosuojan- ja tietoturvan organisointi ja vastuut

Kuntayhtymän tietosuojaa johtaa ja valvoo yhtymähallitus. Yhtymähallitus nimeää tietosuojavastaavan. Kuntayhtymän johtaja päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet ja nimeää tietosuojatyöryhmän ja tietoturvavastaavat.

Kuntayhtymän tietosuojavastaava toimii tietosuojan erityisasiantuntijana, joka valvoo tietosuojalainsäädännön noudattamista organisaatiossa sekä vastaa neuvonnasta ja kouluttamisesta tietosuojaasioissa. Tietosuojavastaava raportoi organisaation johdolle tietosuojan toteutumisesta. Tietosuojavastaavan asema organisaatiossa on riippumaton.

Kuntayhtymässä toimii tietosuojatyöryhmä tietosuojan kehittämisen suunnittelua ja toimeenpanon valmistelua varten. Tietosuojaryhmä ylläpitää tietosuoja ja valmistelee tietosuojaan liittyvää ohjeistusta, tiedottaa tietosuojatyöhön liittyvistä hankkeista ja muutoksista sekä vie tietosuojatyön osaksi organisaation operatiivista toimintaa.

Kunkin henkilörekisterin vastuuhenkilön on huolehdittava siitä, että tietosuojalainsäädännön edellyttämät velvoitteet ko. rekisterinpidon osalta tulevat hoidettua.

Henkilöstöhallinnolliset esimiehet vastaavat alaistensa toimintatavan tietosuojalainsäädännön mukaisuudesta organisaatiossa annettujen ohjeiden mukaisesti. Jokainen kuntayhtymän tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä on vastuussa tietosuojan toteuttamisesta omalta osaltaan.

Kuntayhtymän rekisterihallinnon vastuut ja menettelytavat määritellään tarkemmin kuntayhtymän rekisterihallinnosta annetussa ohjeessa.

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Kuntayhtymässä on määritetty toimintaprosessi ja ohje liittyen toimintaan henkilötietoihin kohdistuvien tietoturvaloukkausten tapahtuessa. Prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa.

Henkilötietojen tietoturva- / tietosuojapoikkeaman sattuessa kuntayhtymällä on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturva- / tietosuojapoikkeama on tullut ilmi, paitsi jos henkilötietojen ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Kun henkilötietojen tietoturva- / tietosuojaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, ilmoitetaan rekisteröidylle loukkauksesta ilman aiheetonta viivytystä.

Rikkomukset ja seuraamukset

Jokainen kuntayhtymän tietojärjestelmien käyttäjä on sitoutunut noudattamaan organisaation tietosuoja- ja tietoturvaperiaatteita allekirjoittamalla käyttöoikeus- ja salassapitositoumuksen. Käyttöoikeus- ja salassapitositoumuksen ja toimintaohjeiden sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti. Tietosuojarikkomusten mahdollisiin seuraamuksiin sovelletaan Yhteistoimintamenettelyssä hyväksyttyä toimintaohjetta, jossa kuvataan tietosuojarikkomusten seuraamukset. Tietosuojarikkomukset raportoidaan organisaation johdolle ja tietosuojavastaavalle.