TIEDONLUOKITUS: JULKINEN

VANTAAN JA KERAVAN HYVINVOINTIALUEEN

TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Tietoturvatoiminto

Vantaan ja Keravan hyvinvointialue

Sisällysluettelo

1. Tietoturva- ja tietosuojapolitiikan tarkoitus

Tietoturva- ja tietosuojapolitiikka sisältää tavoitteet, periaatteet, vastuut ja toimintatavat, jotka ohjaavat Vantaan ja Keravan hyvinvointialueen toimintaa hyvinvointialueen tietojen käsittelyssä ja suojaamisessa. Tietoturva- ja tietosuojapolitiikan tavoitteena on varmistaa yhdenmukaiset käytännöt tietoturvan ja tietosuojan toteuttamiseksi. Tietoturvasta ja tietosuojasta huolehtiminen on osa hyvinvointialueen riskienhallintaa. Kaikessa tietojen käsittelyssä noudatetaan lainsäädäntöä, viranomaismääräyksiä ja -ohjeita sekä hyvinvointialueen määräyksiä, ohjeita ja linjauksia. Keskeisiä säädöksiä tietosuojan ja tietoturvan toteuttamisessa ovat muun muassa Euroopan unionin yleinen tietosuoja-asetus (679/2016), tietosuojalaki (1050/2018), viranomaisten toiminnan julkisuudesta annettu laki eli julkisuuslaki (621/1999), julkisen hallinnon tiedonhallinnasta annettu laki eli tiedonhallintalaki (906/2019), laki sähköisen viestinnän palveluista (917/2014), laki yksityisyyden suojasta työelämässä (759/2004), potilaan asemasta ja oikeuksista annettu laki eli potilaslaki (785/1992), sosiaalihuollon asiakkaan asemasta ja oikeuksista annettu laki (812/2000), sosiaalihuollon asiakasasiakirjoista annettu laki (254/2015), sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki (784/2021) ja potilasasiakirjoista annettu sosiaali- ja terveysministeriön asetus (94/2022).

Tietoturva- ja tietosuojapolitiikka koskee hyvinvointialueen johtoa, luottamushenkilöitä, viranhaltijoita, henkilöstöä, konsultteja sekä muita hyvinvointialueen tietoja käsitteleviä henkilöitä. Se tulee huomioida myös hyvinvointialueen käyttämien palvelutuottajien ja sidosryhmien sekä hyvinvointialueen mahdollisten tytäryhtiöiden toiminnassa. Tietoturva- ja tietosuojapolitiikkaa täydentävät hyvinvointialueen yleiset ja tarkentavat tietoturvaohjeet.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi. Asiakirjan sisältöä tarkistetaan ja päivitetään säännöllisesti. Asiakirja on julkinen.

Tämä tietoturva- ja tietosuojapolitiikka on päivitetty: 20.4.2022

Tämä tietoturva -ja tietosuojapolitiikka on hyväksytty: **XX.4.2022**

Hyväksyjä: **Aluehallitus XX.4.2022**

2. Hyvinvointialueen tietoturvan ja tietosuojan tavoitteet

Tietoturva- ja tietosuojapolitiikka sisältää tavoitteet, periaatteet, vastuut ja toimintatavat, jotka ohjaavat Vantaan ja Keravan hyvinvointialueen toimintaa hyvinvointialueen tietojen käsittelyssä ja suojaamisessa.

Hyvinvointialueen tietoturva- ja tietosuojatyön tavoitteena on varmistaa ja turvata tiedon ja järjestelmien luottamuksellisuus, eheys, saatavuus ja kiistämättömyys.

Tietoturva- ja tietosuojapolitiikan tavoitteena on varmistaa yhdenmukaiset käytännöt tietoturvatyön tavoitteen saavuttamiseksi hyvinvointialueella.

2.1 Tietoturvatavoitteet

Hyvinvointialue huolehtii tietojen, asiakirjojen ja tietojärjestelmien saatavuudesta, käytettävyydestä, eheydestä ja suojaamisesta sekä muusta tiedon laatuun vaikuttavista tekijöistä. Samoin hyvinvointialue huolehtii riskiarvioon perustuvien tarpeellisten organisatoristen ja teknisten toimenpiteiden suorittamisesta tietojen suojaamiseksi, kuten asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta tai siirtämiseltä.

Tiedon suojaaminen on oleellinen osa hyvinvointialueen kokonaisturvaa ja päivittäistä toimintaa sekä tärkeä osa hyvinvointialueen toiminnan ja palveluiden laatua ja varmentamista. Hyvinvointialueen hallussa olevat tiedot ja tietojen käsittely sekä tietojärjestelmät ja -verkot suojataan lakien, asetusten ja vallitsevan riskiarvion edellyttämällä tavalla kaikissa olosuhteissa, jotta toiminnan laatu ja jatkuvuus pystytään varmistamaan.

Hyvinvointialueen tietoturvatavoitteet ovat:

- Tietoturvariskien ennakoiminen ja vaikutuksien järjestelmällinen hallitseminen jatkuvalla tietoturvariskien tunnistamisella, arvioimisella ja toimenpiteillä
- Tiedon ja tietolähteiden luotettavuuden, virheettömyyden ja laadun varmistaminen hyvinvointialueen johtamisessa, päätöksenteossa, toiminnassa ja viestinnässä
- Tiedon saatavuuden ja käytettävyyden varmistaminen
- Tiedon ja tietojärjestelmien valtuudettoman tai oikeudettoman käytön estäminen

- Tiedon tahattoman tai tahallisen tuhoutumisen tai vääristymisen estäminen
- Toiminnan keskeyttävien häiriöiden estäminen ja toipumiseen varautuminen
- Tietoturvaloukkauksien havaitseminen, jäljittäminen, tutkinta ja niistä toipuminen
- Sähköisen asioinnin saatavuuden, luotettavuuden ja kiistämättömyyden varmistaminen
- Hyvinvointialueen tietoturvapolitiikan ja -periaatteiden noudattamisen varmistaminen hyvinvointialueen käyttämissä tietopalveluissa ja tietojärjestelmissä
- Hyvinvointialueen tärkeiden palveluiden ja prosessien keskeytymättömän toiminnan suojaaminen ja häiriöihin varautuminen mukaan lukien tietojärjestelmät ja -verkot
- Tietoturva huomioidaan hyvinvointialueen ja eri osapuolten välisissä sopimuksissa
- Valtionhallinnon tietoturvaperiaatteiden perustietoturvatason ja kriittisissä toiminnoissa korotetun tietoturvatason (VAHTI) saavuttaminen ja toteuttaminen.

Tietoturvatavoitteiden saavuttaminen edellyttää hyvinvointialueen kaikkien toimialojen osalta sitoutunutta ja määrätietoista toteutusta.

2.2 Tietosuojatavoitteet

Hyvinvointialue noudattaa asiakkaiden, kuntalaisten ja hyvinvointialueen henkilöstön henkilötietojen keräämisessä ja käsittelyssä voimassa olevaa lainsäädäntöä ja seuraavia tietosuojatavoitteita.

Vantaan ja Keravan hyvinvointialueen tietosuojatavoitteet ovat:

- Lain ja hyvinvointialueen ohjeiden noudattaminen varmistetaan henkilötietojen käsittelyn suunnittelulla ja osoitetaan dokumentoinnilla.
- Tietosuojasta huolehditaan henkilötietojen käsittelyn koko elinkaaren ajan: Hallinnollisilla ja teknisillä toimenpiteillä varmistetaan, että käsittelyyn valitaan vain käyttötarkoituksen kannalta tarpeelliset henkilötiedot. Henkilötietoja kerätään ja käsitellään vain tiettyä etukäteen määriteltyä ja lain mukaisesti perusteltua tarkoitusta varten. Henkilötietoja ei käsitellä kauemmin kuin on tarpeen niiden käyttötarkoituksen vuoksi. Vain lain velvoittamat ja hyvinvointialueen ohjeiden mukaiset henkilötiedot arkistoidaan käsittelytarpeen päätyttyä. Henkilötiedot hävitetään lainmukaisen säilytysajan päätyttyä kaupungin ohjeistuksen mukaisesti.

- Varmistetaan henkilöstön ja sidosryhmien pääsy henkilötietoihin vain tehtävien edellyttämällä oikeudella ja tavalla.
- Henkilötietojen käsittelyssä huolehditaan tietojen virheettömyydestä.
- Henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen toteutetaan hyvinvointialueella hallinnollisilla ja teknisillä toimenpiteillä.
- Tietosuoja huomioidaan hyvinvointialueen ja eri osapuolten välisissä sopimuksissa.

3 Tietoturva- ja tietosuojariskeihin varautuminen

3.1 Tietoriskien arvioiminen

Tietoturva- ja tietosuojatoimenpiteitä suunniteltaessa ja kehitettäessä tulee arvioida ja analysoida toimintaan liittyvät tietoriskit ja tietosuojariskit. Riskien vaikuttavuuden perusteella voidaan määrittää optimaaliset hallinnolliset ja tekniset tietoturva- ja tietosuojavaatimukset toimintaa suojaaviksi toimenpiteiksi.

Hyvinvointialueen tiedon määrä on valtava. Tieto voi olla esimerkiksi yksittäisessä asiakirjassa, sähköposti-, pika- tai tekstiviestissä, anturissa, verkossa, pilvipalvelussa, tietokannassa, tietokoneen tai puhelimen muistissa, ääni- tai kuvatiedostossa, ihmisen muistissa tai paperilla.

Tietoriskejä tulee arvioida ja hallita hyvinvointialueen riskienhallinnan ohjauksen mukaisesti ja suurimmat tietoturvariskit tulee sisältyä organisaation tai palvelun riskienhallintasuunnitelmaan ja jatkuvaan riskien arviointiin.

Tietoon kohdistuu tyypillisesti seuraavia riskejä:

- Tietoon pääsy on hankalaa, hidasta tai estetty (saatavuus).
- Tieto vuotaa sivullisille (luottamuksellisuus).
- Tieto ei ole käyttökelpoista puutteen/virheen vuoksi tai tieto on hävinnyt (eheys).
- Tieto ei jalostu eikä ole käyttökelpoista toiminnan kehityksen tahdissa (ketteryys).
- Tieto ei ole kenenkään käytettävissä (saatavuus).

Tietoturvariskien arvioinnissa tulee huomioida tiedon saatavuuteen, luottamuksellisuuteen ja eheyteen liittyvät riskit toimialan toiminnan mukaisesti. Oikean ihmisen tulee päästä oikeaan tietoon silloin, kun tietoa tarvitaan. Tieto voi olla saavuttamattomissa tai sitä ei löydy, kun sitä tarvitaan. Tieto voi vuotaa asiattomille. Tieto voi puuttua kokonaan tai olla puutteellista tai virheellistä. Tieto voi olla vaikeasti kehitettävissä tai laajennettavissa kehittyvän toiminnan tukemiseksi. Laaja teknologian toimintahäiriö voi aiheuttaa sen, ettei kukaan pääse käsittelemään tietoa.

Hyvinvointialueen toiminta on enenevässä määrin riippuvainen toimintaa ja fyysistä maailmaa ohjaavasta verkostetusta automaatioteknologiasta, jopa siinä määrin, että henkilöiden turvallisuus voi vaarantua. On syytä huomioida, että tietoon ja teknologiaan kohdistuva riski voi aiheuttaa vaikutuksen ihmisen terveyteen tai henkeen, jos tietojärjestelmä ohjaa fyysisen maailman toimintaa, josta ihmiset ovat riippuvaisia.

Tietosuojariskeihin varautumisessa tulee arvioida, aiheuttaako henkilötietojen käsittely luonnolliselle henkilölle (palveluiden asiakkaille, henkilökunnalle tai sidosryhmien henkilöille) jonkin oikeuden tai vapauden menetyksen. Esimerkiksi arkaluonteisten tietojen vuotamisen tai virheellisten tietojen takia henkilö voi altistua syrjinnälle, menettää oikeuden palveluun tai saada virheellistä palvelua väärän päätöksen perusteella.

Tieto- ja tietosuojariskit voivat aiheutua tyypillisesti seuraavista syistä:

- Tietojen hallintatoimet ja käsittely on järjestetty puutteellisesti. Jos henkilötietojen käsittely on järjestetty puutteellisesti, henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen voi vaarantua.
- Tietoja ja tietojärjestelmiä voivat vaarantaa mm. laite-, ohjelma-, tietokanta- ja tietoliikenneviat sekä ympäristöriskit (esim. sähkökatko).
- Hyvinvointialueen henkilöstön tai ulkopuolisten henkilöiden tahattomat virheet tai tahallinen toiminta voi vaarantaa tiedon laadun tai tietojärjestelmien toimivuuden.
- Koska toimintaympäristöt ovat tyypillisesti verkotettuja, tietoturva ja tietosuoja voivat vaarantua tietojen siirrossa tai yhteyksien ja käyttöoikeuksien määrittelyssä (esim. henkilöstön tiedot jaetaan useisiin järjestelmiin)
- Tietoturva- ja tietosuojariskit ovat suurempia, kun tietoja käsitellään ja tietojärjestelmiä käytetään julkisten verkkojen kautta, työpaikan ulkopuolelta ja/tai muilla kuin hyvinvointialueen laitteilla. Silloin asiattomat voivat päästä helpommin tietoon käsiksi luvattomasti.

Tietoturvariskien arvioinnissa on olennaista, että erilaisten toimintaa ohjaavien tietojärjestelmien (esim. IT/OT/IoT-järjestelmien) häiriöiden tai poikkeamien kautta aiheutuvat fyysisen maailman vaikutukset otetaan huomioon. Anturit voivat tuottaa esimerkiksi sairaaloiden järjestelmiin erittäin suuria, jatkuvasti lisääntyviä tietomassoja, jotka voivat sisältää hyvinvointialueen kannalta kriittistä tietoa. Yhä useampia laitteita on kytketty toimintaympäristöissä toisiinsa ja mahdollisesti yhden laitteen saatavuuteen liittyvät ongelmat voivat vaikuttaa laitteen itsensä lisäksi systeemisesti muihin toimintaa ohjaaviin laitteisiin. Näiden lisäksi tietoturva voi vaarantua sensorien tuottaminen tietojen tahattomasta tai tahallisesta vääristymisestä johtuen. Muita digitalisoinnin tietoturvauhkia ovat mm. robotisoinnin virheet ja massatiedon hallinnan riskit. Lisäksi lainsäädännön muuttuminen voivat aiheuttaa tarvetta nopeille muutoksille monimutkaiseen toimintaympäristöön.

3.2 Riskienhallinnan toimenpiteet

Kun tietoturva- ja tietosuojavaatimukset on määritelty tietoturvariskien suuruuden mukaisesti, voidaan hallinnolliset ja tekniset suojaustoimenpiteet suunnitella ja toteuttaa optimaalisesti.

Hallinnollisia suojaustoimenpiteitä ovat mm.

- operatiivisen käsikirjan täyttäminen projekteihin (järjestelmän kuvaus)
- Tietoturva- ja tietosuojavaatimusten tarkastelu osana hankintaprosessia
- Henkilöstön ja palveluntuottajien kouluttaminen ja ohjeistaminen
- riskienhallintatyö liittyen projekteihin, järjestelmiin ja palveluihin

Tietosuojatoimenpiteet tulee dokumentoida, jotta hyvinvointialue täyttää tietosuoja-asetuksen mukaisen osoitusvelvollisuuden.

Teknisiä toimenpiteitä ovat mm.

- Teknisten suojausmekanismien sisään rakentaminen osaksi toiminta- ja tietotekniikkaa (esim. pääsykontrollit)
- Tietoturvatekniikan hyödyntäminen tiedon suojaamisessa (esim. päätelaitetietoturva ja salausohjelmat).

Hallinnollisten ja teknisten suojausmekanismien tulee tukea sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita.

Tietoturva ja tietosuoja tulee sisään rakentaa osaksi hyvinvointialueen kaikkia prosesseja. Parhaimmillaan tietoturva- ja tietosuojatoimenpiteet suojaavat tarpeen mukaan tietoa, mutta eivät hankaloita, hidasta tai jäykistä toimintaa, prosesseja tai tekniikkaa. Lisäksi Tietoturvatoiminto tarjoaa hyvinvointialueelle tukea ja palvelua esim. häiriötilanteissa.

4 Tietoturvan ja tietosuojan vastuut ja organisointi

Tietoturvan ja tietosuojan vastuut on määritelty hyvinvointialueen hallintosäännössä. Tässä tietoturva- ja tietosuojapolitiikassa syvennetään hyvinvointialueen viranhaltijoiden ja organisaatioiden tietoturva- ja tietosuojavastuita.

4.1 Tietoturvan ja tietosuojan vastuut

Aluehallitus Kokonaisvastuu hyvinvointialueen tietoturvasta ja tietosuojasta
Hyvinvointialuejohtaja Vastaa hyvinvointialueen tietoturvan ja tietosuojan ohjauksesta
ICT-valmistelujohtaja Vastaa tietoturvan toimeenpanosta, ohjauksesta ja soveltamisohjeiden antamisesta
Valmistelujohtaja Vastaa valmistelualueensa tietosuojan ja tietoturvan järjestämisestä
Tietohallinto Kokonaisvastuu hyvinvointialueen tietoturvan ohjauksesta
Tietoturvatoiminto Vastuu valmistella tietoturvaan liittyviä ohjeita sekä antaa suosituksia, riskiarvioita ja kannanottoja
Esihenkilöt Vastuu alaisten toiminnasta tietoturva- ja tietosuojaohjeiden mukaisesti

Työntekijät ja viranhaltijat Velvollisuus noudattaa ja toimia tietoturva- ja tietosuojaohjeiden mukaisesti
Aluevaltuutetut Velvollisuus noudattaa ja toimia tietoturva- ja tietosuojaohjeiden mukaisesti

4.1.1 Aluehallitus ja hyvinvointialuejohtaja

Aluehallitus huolehtii hyvinvointialueen sisäisestä valvonnasta ja riskienhallinnan järjestämisestä, ja siten aluehallituksella on kokonaisvastuu hyvinvointialueen tietoturvasta ja tietosuojasta. Aluehallitus vastaa siitä, että hyvinvointialue täyttää tietoturvaan ja tietosuojaan liittyen lainsäädännön velvoitteet. Aluehallitus hyväksyy hyvinvointialueen tietoturva- ja tietosuojapolitiikan.

Hyvinvointialuejohtaja vastaa hyvinvointialueen tietoturvan ja tietosuojan ohjauksesta sekä vahvistaa niihin liittyvät hyvinvointialueen tasoiset päätökset.

Aluehallituksen ja hyvinvointialuejohtajan tulee sitoutua tietoturvan ja tietosuojan jatkuvaan kehittämiseen sekä huolehtia toiminnan riittävästä resursoinnista.

4.1.2 ICT-valmistelujohtaja ja valmistelujohtajat

ICT-valmistelujohtaja päättää tietoturvan toimeenpanosta, ohjauksesta ja soveltamisohjeiden antamisesta. Tässä työssä häntä auttaa Tietohallinto ja Tietoturvatoiminto.

Valmistelujohtajat vastaavat oman valmistelualueensa tietoturvan järjestämisestä. Valmistelujohtajien tulee huolehtia riittävästä tietoturvan resursoinnista, ohjeistamisesta, koulutuksesta ja asioiden säännöllisestä käsittelystä johtoryhmissä valmistelualueillaan. Valmistelujohtajat vahvistavat omia valmistelualueitansa koskevat tietoturvan erityisohjeet. Valmistelualuekohtaiset erityisohjeet voivat tarkentaa, täydentää ja tiukentaa hyvinvointialuetasoista ohjeistusta. Mikäli pakottavista syistä ilmenee tarve poiketa hyvinvointialuetasoisesta ohjeistuksesta valmistelualuekohtaisella erityisohjeistuksella, poikkeamia koskevat riskipäätökset tekee hyvinvointialuejohtaja.

4.1.3 Tietohallinto ja Tietoturvatoiminto

Tietohallinnolla on kokonaisvastuu hyvinvointialueen tietoturvan ohjauksesta. Tietohallinnon vastuulla on määrittää työasemaverkossa käytettävät laitteet, järjestelmät, sovellukset ja ohjelmistot.

Tietoturvatoiminnon vastuulla on valmistella tietoturvaan liittyviä ohjeita sekä antaa suosituksia, riskiarvioita ja kannanottoja tietoturvaan liittyen. Tietoturvatoiminto toimii hyvinvointialueella asiantuntijaorganisaationa ja tarjoaa mm. konsultointia ja neuvontaa tietoturvakontrolleihin ja ratkaisuihin liittyen.

4.1.4 Toimiala, palvelualue, tehtäväalue, toimintayksikkö, hanke tai projekti

Hyvinvointialueen toimiala, palvelualue, tehtäväalue, toimintayksikkö, hanke tai projekti, tai se, joka tuottaa tai suunnittelee hyvinvointialueen palveluita hyvinvointialueen henkilöstölle, toiminnoille tai asiakkaille, on kokonaisvastuussa palvelunsa tietoturvasta ja tietosuojasta riippumatta siitä, onko palvelun osana hankittu teknologiaa tai ulkoistettu palvelun osia palveluntoimittajille.

Hyvinvointialueen palveluissa tulee

- määritellä tietoturvaan liittyvät hallinnolliset ja tekniset vaatimukset
- ottaa vaatimukset huomioon palvelun kehittämisessä ja
- toteuttaa ne noudattaen hyvinvointialueen tietoturvavaatimuksia.

Hyvinvointialueen tietoturvapäälliköllä tai hänen edustajallaan on tarvittaessa oikeus varmistua tarkastamalla palvelun tietoturvan ja tietosuojan riittävästä tasosta mukaan lukien ostetut tai ulkoistetut palveluiden osat.

4.1.4 Tiedon omistajat

Hyvinvointialueen eri järjestelmien tietosisällöstä vastuullinen taho on järjestelmässä olevan tiedon omistaja.

Tiedon omistaja tulee tunnistaa ja omistajan vastuulla on määrittää tiedon luokitus, luokitella sekä luoda ehdot ja edellytykset tiedon käyttöön. Tiedon luokittelu tehdään hyvinvointialueen tiedonluokitteluohjeistuksen mukaisesti.

Tiedon omistaja on yksikkö, jonka toimintaan tiedot lähinnä liittyvät tai jonka toimintaa ne tukevat, ja joka käyttää niihin kuuluvaa määräysvaltaa.

Tiedon omistajan tulee varmistaa tiedon koko elinkaaren ajan, että:

- kaikki tieto on luokiteltu (julkisuusarvon määrittely),
- tietoa käsitellään huolellisesti, ja
- tieto on asianmukaisesti suojattu (tietosuoja).

Tiedon omistaja päättää lakien ja hyvinvointialueen ohjeistuksen mukaisesta tiedon luokittelusta sekä sisäisen ja salassa pidettävän tiedon jakamisesta hyvinvointialueen sisällä ja luovuttamisesta ulkopuolisille.

Tiedon luokittelua, käsittelyä ja suojaamista on käsitelty tarkemmin hyvinvointialueen tiedon luokittelun ohjeistuksessa (*kts. kappale 5 Tietoturvaohjeistukset*).

4.1.5 Tietojärjestelmien omistajat

Hyvinvointialueen eri tietojärjestelmien tietoturvasta vastuullinen taho on järjestelmän omistaja. Tietojärjestelmällä tarkoitetaan hyvinvointialueen toimintaa varten toteutettua ohjelmistoa tai järjestelmää, jonka avulla tallennetaan, prosessoidaan ja ylläpidetään hyvinvointialueen tietoa tai asiakirjoja ja niissä olevia tietoja.

Tietojärjestelmän omistaja on taho, jonka toimintaan tietojärjestelmä lähinnä liittyy tai jonka toimintaa se tukee, ja joka käyttää siihen kuuluvaa määräysvaltaa.

Järjestelmänomistaja on nimetty henkilö, jolla on oikeudet ja valtuutus päättää järjestelmästä.

Omistaja nimeää tietojärjestelmälle vastuuhenkilön, jonka vastuulle asianomainen tietojärjestelmä kuuluu, ja joka käyttää siihen kuuluvaa määräysvaltaa. Tietojärjestelmän vastuuhenkilö varmistaa, että:

- Tietojärjestelmä on asianmukaisesti luokiteltu, hallittu ja suojattu tiedon luokittelun ja hyvinvointialueen ohjeiden mukaisesti ja resurssien rajoissa.
- Järjestelmän tietoturvasta, vaatimuksenmukaisuudesta ja riittävistä tietoturvakontrolleista on huolehdittu.
- Järjestelmän suojaustaso on määritetty sinne tallennetun tai siinä käsitellyn sensitiivisimmän tiedon mukaisesti.

Tietojärjestelmän vastuuhenkilön tulee ilmoittaa tarvittaessa tietoturvaan liittyvistä uhkista, riskeistä tai suojauksien puutteista esimiehelleen ja tietoturvapäällikölle.

4.1.6 Henkilörekisterin pitäjät

Henkilörekisterin pitäjällä tarkoitetaan organisaatiota, jonka käyttöä varten henkilörekisteri perustetaan, ja jolla on oikeus päättää henkilörekisterin käytöstä tai jonka tehtäväksi henkilörekisterin pito on lailla säädetty.

Hyvinvointialueella henkilötiedon rekisterinpitäjä on

- aluehallitus koko hyvinvointialuetta koskevan henkilörekisterin osalta ja
- toimialan lautakunta tai vastaava luottamuselin toimialakohtaisen henkilörekisterin osalta

Henkilörekisterin pitäjä vastaa henkilötietoon kohdistuvien uhkien riski- ja vaikutusarvioinneista sekä henkilötiedon suojaamisesta.

4.1.7 Esihenkilöt

Esihenkilöt ovat vastuussa tietoturvasta oman alueensa ja yksikkönsä osalta. Esihenkilöiden tulee järjestää riittävä resursointi tietoturvan ja tietosuojan toteutumiseksi omassa yksikössään.

Esihenkilöt ovat vastuussa palveluiden tuottamisesta siten, että palveluiden käyttäjät voivat toimia tietoturvallisesti ja käsitellä henkilötietoja lainmukaisesti.

Esihenkilöiden tulee huolehtia alaistensa ja ulkopuolisten konsulttien:

- sitouttamisesta hyvinvointialueen salassa pidettävän tiedon ja henkilötietojen asianmukaiseen suojaamiseen
- perehdyttämisestä tietoturva- ja tietosuojavastuisiin
- annettujen tietoturva- ja tietosuojamääräysten ja –ohjeiden noudattamisesta
- pääsystä tarpeelliseen tietoon työsuhteen tai yhteistyön alkaessa
- työtehtävien muuttuessa valtuuksien muutoksista ja
- työsuhteen tai yhteistyön päättyessä tietoon pääsyn ja valtuuksien poistamisesta sekä henkilöiden hallussa olevien hyvinvointialueen tietojen siirtämisestä hyvinvointialueelle

Kaikkien esihenkilöiden on saatettava havaitsemansa tai tietoonsa saamat tietoturva- ja tietosuojarikkomukset viipymättä hyvinvointialueen tietoturvapäällikön, toimialan tietosuojavastaavan ja/tai hyvinvointialueen tietosuojavastaavan ja hänen edustajansa tietoon.

4.1.8 Työntekijöiden ja muiden tietoja käsittelevien vastuu

Jokainen Vantaan ja Keravan hyvinvointialueen omistamia tai hallinnoimia tietoja käsittelevä (esim. viranhaltijat, työntekijät, luottamushenkilöt sekä sopimus- ja yhteistyötahojen edustajat) on vastuussa tietoturvan toteutumisesta omissa tehtävissään.

Jokaisen on noudatettava, lainsäädännön lisäksi, hyvinvointialueen

- tietoturva- ja tietosuojapolitiikkaa,
- tietoturva-, ja salassapitositoumuksia,
- tietoturvaperiaatteita ja -ohjeita,
- palvelu- ja tietojärjestelmäkohtaisia tietoturva- ja tietosuojakäyttöohjeita

Jokaisen vastuulla on tietoturvaan ja tietosuojaan liittyvien uhkien, riskien tai rikkomusten ilmoittaminen viipymättä:

- esihenkilölleen,
- palvelusta tai toiminnasta vastuulliselle taholle (esim. palvelun tukeen tai tietojärjestelmän pääkäyttäjälle)
- tietoturva- tai tietosuojapoikkeamien ilmoituskanavaan tai
- tietoturvatoiminnolle tai tietosuojavastaavalle.

4.1.9 Palveluntoimittajat

Hyvinvointialueen yksikkö, joka ostaa teknologiaa tai palveluja ulkopuoliselta palveluntoimittajalta/-tuottajalta, vastaa tietoturvasta ja tietosuojasta myös ostetun teknologian ja palveluiden osalta.

Palvelusopimuksessa tulee sopia tietoturvaan ja tietosuojaan liittyvistä vaatimuksista ja käytännön toteuttamistoimenpiteistä. Hyvinvointialueen palveluntoimittajien tai -tuottajien edellytetään noudattavan hyvinvointialueen tietoturva- ja tietosuojalinjauksia. Hyvinvointialueella tulee olla oikeus varmistua toimittajan tietoturvan ja tietosuojan riittävästä tasosta.

Mikäli palveluntoimittaja tai -tuottaja käsittelee hyvinvointialueen omistamia tai hallinnoimia henkilötietoja tai muita tietoja, sen on osapuolten välisessä sopimuksessa sitouduttava noudattamaan voimassa olevaa tietoturva- ja tietosuojalainsäädäntöä, hyvinvointialueen Tietoturva- ja tietosuojapolitiikkaa sekä soveltuvin osin tietoturvaan ja tietosuojaan liittyviä hyvinvointialueen ohjeita ja määräyksiä.

Hyvinvointialueen palveluntoimittajilta tai -tuottajilta edellytetään sopimuksessa säännöllistä raportointia tietoturvaan ja tietosuojaan vaikuttavista seikoista. Hyvinvointialueella tai sen valtuuttamalla kolmannella osapuolella tulee olla tarkastusoikeus hyvinvointialueelle toimitettujen ratkaisujen ja palveluiden tietoturvan ja tietosuojan tasoon.

4.2 Tietoturvan ja tietosuojajärjestäminen hyvinvointialueella

Aluehallitus Kokonaisvastuu hyvinvointialueen tietoturvasta ja tietosuojasta	
Hyvinvointialuejohtaja Vastaa hyvinvointialueen tietoturvan ja tietosuojan ohjauksesta	
Hyvinvointialueen tietoturvan ja tietosuojan ohjausryhmä Vastaa valmistelualueensa tietosuojan ja tietoturvan järjestämisestä	
Tietoturva- ja tietosuojahallinta	

	Tietoturva- ja tietosuojapalvelu ja teknologia
Tietoturva- ja tietosuoja työryhmä Työryhmä vastaa tietoturva- ja tietosuojaohjeiden valmistelusta, kannanotoista ja suosituksista. Työryhmän jäsenet pitävät yhteyttä hyvinvointialueen toimialoihin.	**Toimialojen toiminnan teknologia** Toimialat vastaavat omassa toiminnassaan käytetyn teknologian tietosuojasta ja tietoturvallisuudesta.

4.2.1 Tietoturvapäällikkö (rekrytoidaan kesän/alkusyksyn 2022 aikana)

Tietoturvapäällikkö vastaa

- tietoturvan strategisesta ohjauksesta ja kehittämisestä
- tietoturvan kehittämishankkeiden valmistelusta ja ohjauksesta
- tietoturvaohjeistuksien valmistelusta ja jalkauttamisesta
- tietoturvatietouden edistämisestä
- tietoturvakoulutuksen tuottamisesta osaksi hyvinvointialueen koulutuksia
- tietoturvapalveluiden ohjauksesta
- tietoturvarikkomusten hallinnoinnista
- tietoturvan seurannasta, viestinnästä ja raportoinnista
- hyvinvointialuetta ohjaavan tietoturvasääntelyn seurannasta

Tietoturvapäällikkö raportoi säännöllisesti tietoturvasta hyvinvointialueen johdolle sekä tarvittaessa hyvinvointialueen eri toimielimille. Tietoturvapäällikön tukena toimii hyvinvointialueen tietoturva- ja tietosuojatyöryhmä.

4.2.2 Tietosuojavastaava

Tietosuojavastaava toimii hyvinvointialueentasoisena tietosuojavastaavana. Toimiala voi tarpeen mukaan nimetä toimialakohtaisen tietosuojavastaavan, jonka tulee raportoida tietosuojasta myös hyvinvointialueen tietosuojavastaavalle.

Tietosuojavastaava vastaa

- tietosuojan kehittämishankkeiden valmistelusta ja ohjauksesta
- tietosuojaohjeistuksien valmistelusta ja jalkauttamisesta
- tietosuojatietouden edistämisestä

- tietosuojakoulutuksen tuottamisesta osaksi hyvinvointialueen koulutuksia
- tietosuojapalveluiden ohjauksesta
- tietosuojarikkomusten hallinnoinnista
- henkilötietojen käsittelyn ohjauksesta ja seurannasta lainsäädännön, viranomaismääräysten sekä hyvinvointialueen ohjeistusten mukaisesti
- tietosuojan viestinnästä ja raportoinnista
- yhteydenpidosta ja yhteistyöstä rekisteröityjen ja valvontaviranomaisen kanssa
- hyvinvointialuetta ohjaavan tietosuojasääntelyn seurannasta

Tietosuojavastaava raportoi säännöllisesti tietosuojasta hyvinvointialueen johdolle sekä tarvittaessa hyvinvointialueen eri toimielimille. Tietosuojavastaavan tukena toimii hyvinvointialueen tietoturva- ja tietosuojatyöryhmä.

4.2.3 Tietoturvan ja tietosuojan ohjausryhmä

Tietoturvan ja tietosuojan ohjausryhmä vastaa valmistelualueensa tietosuojan ja tietoturvan järjestämisestä. Ohjausryhmän tehtävänä on;

- valmistella hyvinvointialuetta koskevia tietoturvaan ja tietosuojaan liittyviä ohjeita sekä antaa suosituksia ja kannanottoja edellä mainituista asioista

viedä hyvinvointialueen tietoturva- ja tietosuojaohjeistuksia omalle toimialalle jalkautettavaksi

4.2.3 Tietoturva- ja tietosuojatyöryhmä

Työryhmän jäsenet toimivat yhteyshenkilöinä tietoturva- ja tietosuoja-asioissa työryhmän ja oman toimialansa välillä. Toimialajohtajat vastaavat oman toimialansa osalta yhteyshenkilöiden tehtävän hoitamisen edellyttämästä koulutuksesta ja työajan resursoinnista. Tietoturvatoiminto kuuluu kokonaisuudessaan tähän työryhmään.

Työryhmän tehtävänä on

- tuoda työryhmän käsittelyyn toimialan ehdotuksia hyvinvointialueen tietoturvan ja tietosuojan parantamiseksi
- seurata hyvinvointialueen tietoturva- ja tietosuojaohjeistuksen toteutumista toimialallaan
- nostaa hyvinvointialuetta koskevia tietoturva- ja tietosuojapuutteita ohjausryhmän käsittelyyn

- tietoturvaloukkausten käsittely
- muut työryhmän operatiiviset tehtävät.

4.2.4 Toimialojen tietoturva- ja/tai tietosuojavastaavat

Toimialalla voi olla nimetty toimialakohtainen tietoturva- ja/tai tietosuojavastaava.

Vastaavan tehtävänä on omalla toimialallaan

- laatia ja esittää toimialakohtainen käytännön ohjeistus
- opastaa, neuvoa ja jalkauttaa käytäntöjä
- seurata määräysten ja ohjeiden noudattamista
- raportoida toimialan johdolle ja hyvinvointialueen tietoturvapäällikölle ja/tai tietosuojavastaavalle.

Toimialalla voi olla oma pysyvä tai tilapäinen toimialakohtainen operatiivinen tietoturva- ja tietosuojatyöryhmä asioiden juoksevaan käsittelyyn.

4.2.5 Tietohallinto

Tietohallinto vastaa ICT-valmistelujohtajan johdolla

- IT-ympäristön ja tietojärjestelmien tietoturvan ja tietosuojan teknisestä suunnittelusta, kehittämisestä ja toteuttamisesta sekä toteutumisen seuraamisesta
- tietojärjestelmäpalveluiden tuottamisesta siten, että palveluiden käyttäjät voivat toimia tietoturvallisesti ja käsitellä henkilötietoja lainmukaisesti
- hallinnollisten ja teknisten keinojen tuottamisesta IT-ympäristössä ja tietojärjestelmissä olevan tiedon ja sen käsittelyn suojaamiseksi
- IT-ympäristön ja tietojärjestelmien tietoturva- ja tietosuojaohjeistuksen tuottamisesta ja jalkauttamisesta
- IT-ympäristön tietoturvatietouden edistämisestä ja -koulutuksen tuottamisesta
- IT-ympäristöön ja tietojärjestelmiin kohdistuvien merkittävien uusien uhkatekijöiden raportoinnista tietoturvapäällikölle
- tietoturva- ja tietosuojarikkomuksien raportoinnista viipymättä tietoturvapäällikölle tai tietosuojavastaavalle.

Tietohallinto vastaa tietohallinnon hankinnoista kohdassa 4.2.7 määritellyn mukaisesti (vastaavasti kuin hankintapalvelut muista hankinnoista).

4.2.6 HR

HR:n tulee varmistaa henkilöstön tietojen ajantasaisuus ja oikeellisuus sekä mahdollistaa hyvinvointialueen henkilöstön lainmukainen ja hyvinvointialueen tietosuojaohjeistuksen mukainen henkilötietojen käsittely.

4.2.7 Hankintapalvelut ja hankinnoista vastaavat

Hankintapalvelut vastaa hankinnan kohteen tietoturvan ja tietosuojan tavoitteiden ja vaatimuksien sisällyttämisestä osaksi hankintaprosessia.

Hankintapalvelut vastaa siitä, että kilpailuttamisprosessissa toteutetaan hankinnan kohteeseen liittyvien tietoriskin arviointi ja niihin liittyvien suojaamisvaatimusten määrittely. Suojaamisvaatimusten määrittelyn sisältö tulee toteuttaa yhteistyössä hankintapalveluiden ja tietohallinnon kanssa. Hankintapalvelut vastaa siitä, että tietoiskien seurantaa koskeva toimintamalli sisällytetään hankintasopimuksiin, mutta seurannasta vastaa tietojärjestelmän tai tiedon omistaja.

Toimialojen hankinnoista vastaavien tulee ottaa huomioon tietoriskien mukaisesti tietoturva- ja tietosuojatavoitteet ja vaatimukset hankinnoissa, sopimuksissa ja toimittajien hallinnassa.

5 Tietoturva- ja tietosuojaohjeistukset ja -koulutus

Tietoturva- ja tietosuojapolitiikan lisäksi hyvinvointialueen tietoturva- ja tietosuojatyössä tärkeitä asiakirjoja ovat tietoturva- ja tietosuojaohjeistukset. Siinä missä tietoturva- ja tietosuojapolitiikka määrittää hyvinvointialueen tietoturvan ja tietosuojan vastuita, organisointia ja tietoturva- ja tietosuojatyön järjestäytymistä, tietoturva- ja tietosuojaohjeistukset määrittävät käytännössä, kuinka esim. hyvinvointialueen tarjoamia työkaluja (esim. kannettava tietokone tai älypuhelin) käytetään tietoturvallisesti ja tietosuojan turvaavalla tavalla, mitkä ovat hyvinvointialueen käytännöt sähköpostin käyttöön taikka miten tiedon luokittelua tehdään hyvinvointialueella.

Tietoturva- ja tietosuojaohjeistuksia päivitetään sen mukaan, kun uusia teknologioita ja työprosesseja otetaan hyvinvointialueella käyttöön. Ohjeistusten luonnista vastaavat Tietoturvatoiminto ja Tietohallinto ja ne hyväksytetään hyvinvointialueen johdolla.

Hyvinvointialueen ajantasaista tietoturvaohjeistusta säilytetään tässä sijainnissa: *Linkki Sharepointtiin / Teamsiin josta kaikki hyvinvointialuelaiset pääsevät käsiksi tietoturvaohjeistukseen.*

Tietoturvasta ja tietosuojasta järjestetään myös hyvinvointialueen henkilökunnalle koulutuksia. Koulutukset voivat olla kouluttajavetoisia, taikka verkkokoulutuksia. Aiheet voivat olla yleisiä esim. Tietoturva- tai tietosuojatietouteen liittyviä aiheita taikka hyvinvointialueen sisäisten tietoturvakäytäntöjen koulutuksia.

6 Tietoturvan ja tietosuojan käsitteet

Käsitteiden määrittelyssä on käytetty lähteinä valtionhallinnon tietoturvaohjeistusta (VAHTI) ja EU:n tietosuoja-asetusta.

Asenne
Tietoturvan ja tietosuojan tarpeen ja merkityksen ymmärtäminen sekä, motivoituminen ja sitoutuminen noudattamaan tietoturva- ja tietosuojaohjeita ja -määräyksiä.

Eheys
Eheys tarkoittaa tiedon ja tietojärjestelmän luotettavuutta sisäisen ristiriidattomuuden, kattavuuden, täydellisyyden, ajantasaisuuden, oikeellisuuden ja käyttökelpoisuuden kautta.
Eheys edellyttää tiedon ja tietojärjestelmän muutoksien todentamista kirjausketjusta (lokittamista) ja valtuudettomien muutoksien estämistä.

Fyysinen turvallisuus
Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä kuriirien toimittamien tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen turvallisuus

Tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilörekisteri

Henkilörekisteri on sähköinen tai paperimuotoinen rekisteri tai luettelo, johon on koottu samaa käyttötarkoitusta varten henkilötietoja.

Henkilöstöturvallisuus

Henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen sekä työyhdistelmien järjestelyihin liittyvien turvatekijöiden hoitamista.

Henkilötietojen tietoturvaloukkaus

Personal Data Breach: Tietoturva-loukkaus, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. vrt. Tietoturvaloukkaus

Jatkuvuussuunnittelu

Jatkuvuussuunnittelu tarkoittaa niitä toimia, joiden avulla pyritään pienentämään ja lyhentämään toimintaa haittaavien tapahtumien vaikutusta ja kestoa. Se sisältää varajärjestelyitä sekä toimenpiteitä, jotka parantavat toimintaa häiriötilanteissa tai toipumista ongelmien jälkeen. Jatkuvuussuunnittelu sisältää myös suunnitelmat, joissa kuvataan johtaminen, vastuut ja toimenpiteet, joiden mukaan toimintoja voidaan jatkaa erilaisissa häiriötilanteissa.

Jäljitettävyys

Tarpeen tullen on selvitettävissä, mitä tiedolle tai tietojärjestelmälle on tehty, kuka toimenpiteen on tehnyt ja milloin se on tehty.

Kiistämättömyys

Kiistämättömyyttä tarvitaan tiedon alkuperän, luovutuksen ja käsittelytapahtumien sekä tietojärjestelmämuutoksien luotettavuuden varmentamiseen. Luotettava näyttö saavutetaan tietoteknisin menetelmin, että tietty henkilö on tehnyt tietyn tietotapahtuman tai järjestelmämuutoksen. Tietotapahtumiin (lähetys, vastaanotto, lukeminen, käsittely) ja tietojärjestelmämuutoksiin liitetään aikaleima, joka todistaa tapahtuman ajankohdan.

Käytettävyys

Tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla, helposti hyödynnettävissä, käytettävissä haluttuna aikana ja vaaditulla tavalla sekä ilman ylimääräistä vaivaa.

Kyberriski

Tarkoittaa toimintateknologian ja sähköisten palveluiden kautta epävarmuuden vaikutusta fyysiseen toimintaan, poikkeamaa toiminnassa. Vaikutus voi olla asiakaspalvelun saatavuuteen, tarkkuuteen, joustavuuteen tai jatkuvuuteen, joka aiheuttaa palvelua saavien ihmisten toiminnan keskeytymisen tai virheellisyyteen. Pahimmassa tapauksessa ihmiselle voi aiheutua pysyvä vamma tai hengen menetys esim. teknologiasabotaasin johdosta. Kts. Kyberturva.

Kyberturva

Kyberturvalla hyvinvointialue pyrkii suojaamaan ihmisten tuottaman tiedon tai automaattisesti toimivien älykkäiden järjestelmien vaikutukset päätöksiin, toimintaan ja fyysiseen maailmaan kuten esimerkiksi taloushallinnon ja liikenteenohjauksen järjestelmät. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten palveluiden ja verkotettujen järjestelmien poikkeamien vaikutuksiin hyvinvointialueen toiminnoissa. Kyberturvassa yhdistyy tietoturvan, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelu. Useat hyvinvointialueen kriittiset toiminnot ovat riippuvaisia toimintoja automatisoitujen tietojärjestelmien ja -verkkojenluotettavuudesta ja toimivuudesta. Hyvinvointialueen toimintoja tukeviin järjestelmiin ja verkkoihin kohdistuvat häiriöt muodostavat kyberuhan hyvinvointialueen asiakaspalveluille. Häiriöt voivat olla tahallisia verkkohyökkäyksiä tai tahattomia laitteistojen ja ohjelmistojen vikaantumisia.

Käyttöturvallisuus

Toimenpiteitä, joilla luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat olosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käytön valvonnasta, ohjelmistotuesta ja varmistuksista.

Laitteistoturvallisuus

Laitteistojen käytettävyyden, toiminnan, ylläpidon sekä laitteiden ja tarvikkeiden saatavuuden turvaavat toimenpiteet. Laitteiston elinkaarta turvataan laitteistoturvallisuudella, johon kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Ohjelmistoturvallisuus

Käyttöjärjestelmiin, varus- ja työkaluohjelmistoihin sekä muihin ohjelmistoihin kohdistuvat turvatoimet. Näitä ovat esim. ohjelmistojen tunnistamis-, eheys-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus.

Operatiivinen käsikirja

Operatiivinen käsikirja on dokumentti, jolla varmistetaan ICT-järjestelmän tai -palvelun dokumentointi kokonaisuudessaan. Se kattaa mm. vastuut ja omistajat, konfiguraation, sovellukset, tiedon ja palvelimien sijainnin ja järjestelmään liittyvät tietoturvakontrollit.

Luottamuksellisuus

Tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus. Tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn, tietojärjestelmiin ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Palveluntoimittaja

Hyvinvointialueen julkisen tai sisäisen palvelu kokonaan tai osittain on sopimuksella ulkoistettu palveluntoimittajalle, jonka vastuulla on toimittaa palvelua tai sen osaa sopimuksella määrätyllä tavalla ja laadulla yhdessä hyvinvointialueen kanssa sovittujen hallintatoimien sekä jatkuvuuteen, tietoturvaan ja tietosuojaan liittyvien vaatimusten mukaisesti.

Palveluntuottaja

Hyvinvointialueen organisaation yksikkö tai sen johtaja, jonka vastuulla on hyvinvointialueen ulkoinen palvelu asiakkaille tai sisäinen tukipalvelu henkilöstölle. Tyypillisesti palvelu on asianomaisen yksikön tai sen johtajan päätäntävallassa sekä kulut ja tuotot lasketaan yksikön talouteen.

Pääsynvalvonta

Tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palveluelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille

Riski

Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.

Saatavuus

Palvelu, tieto tai tietojärjestelmä on saatavilla ja käytettävissä, kun sitä tarvitaan. Helppokäyttöisyys, nopeus, joustavuus ja luotettavuus ovat saatavuuden eri näkökulmia.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet

Henkilötietojen käsittelijöillä on velvollisuus antaa rekisterinpitäjälle riittävät takeet siitä, että niiden puolesta suoritettava henkilötietojen käsittely on tietosuoja-asetuksen vaatimusten mukaista ja rekisteröityjen oikeuksien suojaaminen on varmistettu. Tämä merkitsee erityisesti sitä, että

- tietosuojaperiaatteet sisäänrakennetaan rekisterinpitäjille tarjottaviin työkaluihin, tuotteisiin, sovelluksiin tai palveluihin
- työkalut, tuotteet, sovellukset tai palvelut takaavat oletusarvoisesti, että käsittely rajoittuu vain käsittelyn tarkoituksen kannalta tarpeellisiin henkilötietoihin. Käsittelyn rajaamisessa on huomioitava tiedon määrä, käsittelyn laajuus, tietojen säilytysaika ja tietojen käyttöön oikeutettujen henkilöiden lukumäärä.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita voidaan toteuttaa esimerkiksi seuraavilla tavoilla:

- Rekisterinpitäjälle annetaan mahdollisuus määritellä kerättävät tiedot siten, että vapaaehtoisesti annettavien tietojen kerääminen ei ole teknisistä syistä pakollista (esim. kenttien täyttäminen sähköisellä lomakkeella).
- Tiedot minimoidaan: vain käsittelyn kannalta tarpeelliset tiedot kerätään.
- Tietoja poistetaan käytöstä automaattisesti ja valikoivasti tietyin väliajoin.
- Tietojen käyttöoikeudet ja tietojen poistot määritellään tietokohtaisesti tai rekisteröityjen pyynnöstä (esimerkiksi sosiaalisen median palveluissa).

(*lähde: Tietosuojavaltuutetun internet-sivut*)

Tiedon laatu

Tarkoittaa tiedon ominaisuuksia kuten tiedon täydellisuus (completeness), soveltuvuus (validity), johdonmukaisuus (consistency), ajanmukaisuus (timeliness) ja tarkkuus (accuracy), jotka yhdessä mahdollistavat tiedon käyttämisen tiettyä tarkoitusta varten. Kaikki edellämainitut tiedon laadun kriteerit yhdessä ovat ISO 9000:2015 standardin mukaan yleisesti pakollisia tiedon laadun varmistamisessa osana toiminnan laatua.

Tietoaineistoturvallisuus

Toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen saatavuuden, käytettävyyden, eheyden, jäljitettävyyden ja luottamuksellisuuden ylläpitämiseksi, keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietojärjestelmä

Ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt

Tietojärjestelmän omistaja

Vastaa mm. henkilötietolaissa mainitun rekisterinpitäjän velvollisuuksista sekä oman tietojärjestelmänsä tietoturvallisuudesta dokumentoinnin, turvaluokittelun, käyttäjäoikeusrekisterin ylläpidon, käyttöoikeuksien, käytön, varmistusten, tuen, koulutuksen, ylläpidon, kehittämisen ja jatkuvuussuunnittelun osalta.

Tietojärjestelmän pääkäyttäjä

Pääkäyttäjällä on laajat oikeudet hallinnoida tietyssä tietojärjestelmässä muiden käyttäjien käyttäjätunnuksia, laiteresursseja, tiedostoja ja järjestelmän suojauksia.

Tietojärjestelmäriski

Tarkoittaa epävarmuuden vaikutusta tietojärjestelmään, poikkeamaa odotetusta. Vaikutusvoi olla myönteinen tai kielteinen odotettuun verrattuna. Tyypillisiä vaikutuksia on tietojärjestelmän toimintavirhe tai -häiriö, joka aiheuttaa tietojärjestelmän käyttökatkoksen tai sen tuotoksien käyttökelvottomuuden tai virheellisyyden ja tietojärjestelmää käyttävien organisaatioiden toiminnan keskeytymisen tai virheellisyyden.

Tietojärjestelmien ja IT-ympäristön turvallisuus

Hallinnolliset toimet kuten ohjeistus, kehitys ja seuranta, joilla pyritään aikaansaamaan tietojärjestelmien ja IT-ympäristön turvallisuus. Tietojärjestelmien hallinnolliset ja tekniset suojaamisen ja turvaamisen toimenpiteet.

Tietojärjestelmien käytettävyyden, virheettömyyden ja luottamuksellisuuden hallinnollinen ja tekninen varmistaminen. Tietojärjestelmien käyttöjärjestelmien ja ohjelmistojen tunnistaminen, valtuuttaminen ja eheyden varmistaminen ja tiedon tekninen suojaaminen. Tietojärjestelmien käyttäjien todentamisen ja valtuutuksien tekninen toteutus. Tietojärjestelmien jatkuvuuden varmistamisen toimenpiteet.

Tietoliikenneturvallisuus

Hallinnolliset toimet kuten ohjeistus, kehitys ja seuranta, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus. Tiedonsiirtoyhteyksien suojaamisen ja turvaamisen toimenpiteet.

Tietoliikenneyhteyksien käytettävyyden, virheettömyyden ja luottamuksellisuuden tekninen varmistaminen. Laitteiden verkkoon kytkettyjen laitteiden tunnistamisen ja valtuutuksien toimenpiteet. Verkon jatkuvuuden varmistamisen toimenpiteet.

Tietoriski

Tarkoittaa epävarmuuden vaikutusta tietoon, poikkeamaa tiedossa. Vaikutus voi olla tiedon saatavuuteen, käyttökelpoisuuteen, oikeellisuuteen, eheyteen, joustavuuteen tai jatkuvuuteen, joka aiheuttaa tietoa käyttävien organisaatioiden toiminnan keskeytymisen tai virheellisyyden.

Tietosuoja

Tietosuojalla tarkoitetaan henkilötietojen ja erityisesti arkaluonteisten tietojen suojaamista asiattomalta käsittelyltä. Henkilötiedolla tarkoitetaan kaikkia henkilöön liittyviä tietoja, joista tämä on tunnistettavissa. Henkilötietoja ovat mm. nimi, henkilötunnus, henkilöä esittävä valokuva, puhelinnumero, sähköpostiosoite, sijainti tai verkkotunniste (esim. IP-osoite). Arkaluonteisia henkilötietoja ovat mm. henkilön terveydentilaa, sairautta tai hoitotoimenpiteitä koskevat tiedot sekä tiedot henkilön saamista sosiaalihuollon palveluista ja etuuksista.

Tietosuojariski

Tarkoittaa epävarmuuden vaikutusta henkilötietoon, poikkeamaa henkilötiedossa. Vaikutus voi olla henkilötiedon saatavuuteen, käyttökelpoisuuteen, oikeellisuuteen, eheyteen, joustavuuteen tai jatkuvuuteen, joka vaikuttaa luonnolliselle henkilöille (palveluidemme asiakkaille, henkilökunnalle ja sidosryhmien henkilöille) oikeuden tai vapauden menetyksen. Esimerkiksi arkaluonteisten henkilötietojen vuotaminen tai virheellisten henkilötietojen takia henkilö voi altistua syrjinnälle tai menettää oikeuden palveluun tai saada virheellistä palvelua. Lisäksi henkilötietojen käsittely voi olla järjestetty puutteellisesti, siten että henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen vaarantuu.

Tietoturva

Tietoturvalla tarkoitetaan hallinnollisia, teknisiä ja muita mahdollisia keinoja, joilla suojataan ja varmennetaan hyvinvointialueen omistamaa tai hallinnoimaa tietoa ja sen käsittelyä kaikissa olosuhteissa. Tietoturvalla tavoitellaan asianmukaista tiedon suojaamista. Tietoturva koskee digitaalisessa, suullisessa ja kirjallisessa muodossa olevan tiedon käsittelyä, säilyttämistä, arkistointia, luovuttamista, siirtämistä ja hävittämistä. Tietoturva muodostuu tiedon saatavuudesta, käytettävyydestä, eheydestä, luottamuksellisuudesta, kiistämättömyydestä, jäljitettävyydestä ja pääsynvalvonnasta sekä henkilöstön osaamisesta, resursseista,

toimintatavoista ja asenteesta. Tiedon käyttö- ja käsittelyoikeudet määrittyvät henkilön työtehtävän ja roolin mukaisesti. Tiedon asianmukainen suojaaminen tulee toteutua koko tiedon elinkaaren ajan, jota on kuvattu tarkemmin hyvinvointialueen tiedon luokittelun ohjeessa. Tietoturva koostuu hallinnollisesta turvallisuudesta, henkilöstöturvallisuudesta, fyysisestä turvallisuudesta, tietoliikenneturvallisuudesta, käyttöturvallisuudesta, tietoaineistoturvallisuudesta sekä laitteisto- ja ohjelmistoturvallisuudesta.

Tietoturvallisuus

Järjestelyt, joilla pyritään varmistamaan tiedon turvallisuus. Katso tietoturva.

Tietoturvajaloukkaus

Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Tietoturvapoikkeama

tietoturvahäiriö, Information Security Incident: yksi tai useampi tietoturvatapahtuma, vaarantaen tietoturvan ja vaikuttaen organisaation toimintaan

Tietoturvatapahtuma

Information Security Event, Anomaly: yksittäinen tapahtuma, joka saattaa vaikuttaa tietoturvaan

Tietoturvarikkomus

Lievät tietoturvarikkomukset ovat väärinkäytöksiä kuten esimerkiksi henkilökohtaisen tietoturvan laiminlyönti, epäasiallinen käytös, haitan aiheuttaminen, resurssien tuhlaus, haittaohjelmien torjunnan tai tietoturvapäivityksien laiminlyönti, luvaton kaupallinen tai poliittinen toiminta tai kulunvalvontasääntöjen rikkominen. Tietoturvarikkomukset ovat vakavampia väärinkäytöksiä tai turvallisuuden vaarantamisia kuten esimerkiksi ohjelmien ja pelien luvaton kopiointi, luvattomien ohjelmien asentaminen, ylläpitäjän työkalujen luvaton hallussapito, palvelun luvaton pystytys, tunnuksen luovuttaminen tai tiedon suojaamisen vaarantaminen. Vakavat tietoturvarikkomukset ovat lain mukaan rikkomuksena tai rikoksena tuomittavia tekoja kuten esimerkiksi luvaton hakkerointi ja tunkeutuminen, rikoslain alaisen materiaalin oikeudeton käsittely, tekijänoikeuslain alaisen materiaalin laiton levittäminen, tarkoituksellinen luvaton porttiskannaus, haittaohjelmien tahallinen levittäminen ja palvelunestohyökkäys.

Toipumissuunnittelu

Toipumissuunnittelu liittyy yleensä tietojärjestelmiin ja niiden toipumiseen häiriötilanteissa, ja se on tärkeä osa jatkuvuussuunnittelua. Yksittäinen toipumissuunnitelma määrittelee ja dokumentoi suunnitelman piirissä oleviin toimintoihin liittyville tietojärjestelmille käytännön toimenpiteet, roolit ja vastuut normaalitilaan palaamiseksi. Lisäksi toipumissuunnitelmassa kuvataan teknisesti korkean käytettävyyden vaatimat toteutustavat sekä miten häiriötilanteessa viestitään toipumista ohjaavalle taholle. Toipumissuunnitelmat kuvaavat operatiivisella tasolla ja konkreettisesti järjestelmien palauttamisen häiriötilanteista. Ne sisältävät ohjeet vakavasta häiriöstä toipumiseen, normaaliin toimintaan paluusta ja toiminnan jatkamisesta. Jatkuvuussuunnitelma ohjaa toipumissuunnitelmien toteutusta.

Varautuminen

Varautumisella tarkoitetaan toimintaa, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen kaikissa tilanteissa. Varautumistoimenpiteitä ovat esimerkiksi riskien arviointi, jatkuvuus- ja valmiussuunnittelu, tekniset ja rakenteelliset etukäteisvalmistelut, koulutus, harjoitukset sekä tilojen ja kriittisten resurssien varaukset. Varautuminen jakaantuu suunnitteluun, sen edellyttämiin käytännön valmistelutoimenpiteisiin, näiden toteuttamiseen ja kehittämiseen sekä harjoitteluun.