



5.6.2025

julkinen

TIETOTURVA- JA TIETOSUOJAPOLITIikka

PURUVEDEN PALVELUTALO

Laatija: Anu Kastikainen

Hyväksyjä ja pvm: Tapani Hannonen 11.8.2025

Versiohallinta:

Versio	Päivämäärä	Käsittelijä	Toimenpide (muutos tms.)	Lisätietoja
0.01	5.6.2025	Anu Kastikainen	ensimmäinen versio	Tietoturvatimi käsitellyt



Kerimäen Vanhusten ja Vammaisten Tuki ry
TIETOTURVA- JA TIETOSUOJAPOLITIikka

2 (9)

5.6.2025

julkinen

SISÄLLYSLUETTELO:

1	JOHDANTO.....	3
2	TIETOTURVA- JA TIETOSUOJAPOLITIikan TARKOITUS JA TAVOITTEET	3
2.1	TIETOTURVA- JA TIETOSUOJAPOLITIikan TARKOITUS	3
2.2	TIETOTURVATAVOITTEET	4
2.3	TIETOSUOJAA KOSKEVAT PERIAATTEET	4
3	TIETOTURVAN JA TIETOSUOJAN HALLINTA.....	5
3.1	TIETOTURVALLISUUDEN TOTEUTUKSEN PERIAATTEET	5
3.2	TIETOSUOJAN TURVAAMINEN	5
3.3	TIETOTURVARISKIEN ARVIOINTI JA KÄSITTELY	6
3.4	TIETOJEN LUOKITTELU JA KÄSITTELY	6
3.5	HENKILÖTIETOJEN KÄSITTELY	7
3.6	TIETOTURVAVAATIMUKSET JA NIIHIN SITOUTUMINEN.....	7
3.7	TIETOTURVAKOULUTUS JA -TIE TOISUUS	7
3.8	TIETOTURVALLISUUDEN VALVONTA JA SEURANTA.....	7
3.9	TIETOTURVAPOIKKEAMIE N KÄSITTELY.....	8
3.10	MENETTELYTAVAT TIETOTURVARIKKOMUKSISSA	9
3.11	TIETOTURVAVASTUUT JA ORGANISOINTI	9
3.12	TIETOTURVALLISUUDEN JATKUVA PARANTAMINEN.....	9



5.6.2025

julkinen

1 JOHDANTO

Tietoturva on olennainen osa Kerimäen Vanhusten ja Vammaisten Tuki ry:n toimintaa, sillä se käsittelee laajasti erilaisia sosiaali- ja terveydenhuollon asiakastietoja, työntekijöiden henkilötietoja ja muita luottamuksellisia tietoja. Tämä tietoturvapolitiikka määrittelee periaatteet ja käytännöt, joilla varmistamme tietojen turvallisuuden ja noudatamme tietosuojasetusta (GDPR), tietosuojalakea, asiakastietolakea sekä muuta soveltuvaa lainsäädäntöä.

Tässä politiikassa kuvataan Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturva- ja tietosuojapolitiikan päämäärä ja periaatteet sekä tietoturva- ja tietosuojatoiminnan vastuut ja organisointi. Tietoturva- ja tietosuojapolitiikka toimii perustana tietoturvaa ja tietosuoja koskeville toimintatavoille ja -ohjeille, joiden avulla tarkennetaan politiikassa annettuja määräyksiä ja ohjataan niiden soveltamista organisaation arkeen.

2 Tietoturva- ja tietosuojapolitiikan tarkoitus ja tavoitteet

2.1 Tietoturva- ja tietosuojapolitiikan tarkoitus

Tietoturva- ja tietosuojapolitiikan tarkoituksena on kuvata Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturvallisuuden ja tietosuojan tavoitteet ja periaatteet sekä varmistaa, että kaikki henkilötietojen, kuten asiakastietojen käsittely tapahtuu Suomen lainsäädännön, kuten GDPR:n, asiakastietolain ja muiden säädösten mukaisesti. Tämä sisältää erityisesti arkaluontoisten asiakastietojen suojaamisen, tietoturvariskien hallinnan sekä henkilökunnan jatkuvan koulutuksen tietoturvaan liittyvissä asioissa. Käytännössä tämä tarkoittaa esimerkiksi asiakastietojen huolellista suojaamista, henkilökunnan kouluttamista tietoturvakäytännöistä ja järjestelmien asianmukaista valvontaa mahdollisten tietovuotojen ja muiden tietoturvapoikkeamien estämiseksi.

Tämä tietoturva- ja tietosuojapolitiikka määrittelee organisaation vastuut ja periaatteet tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaamiseksi sekä henkilötietojen lainmukaisen käsittelyn ja tietosuojan korkean tason varmistamiseksi. Lisäksi se ohjaa organisaation toimintaa niin, että tietoturvaan ja tietosuojaan liittyvät periaatteet sisältyvät päivittäiseen toimintaan tietosuoja-asetuksen sisäänrakennetun ja oletusarvoisen tietosuojan periaatteen mukaisesti.



5.6.2025

julkinen

2.2 Tietoturvatavoitteet

Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturvallisuuden tavoitteina on:

1. Suojata asiakkaiden ja henkilöstön luottamuksellisia tietoja väärinkäytöksiltä, tietovuodoilta ja luvattomalta pääsylvä.
2. Taata tietojen eheys ja oikeellisuus, jotta kaikki käsitellyt tiedot ovat ajantasaisia ja virheettömiä.
3. Varmittaa tietojen saatavuus niiden käsittelyyn valtuutetuille henkilöille tarpeen mukaan.
4. Noudattaa systemaattisesti lainsäädäntöä ja viranomaisohjeita.

Tavoitteiden toteutumista seurataan mittaamalla tietoturvapoikkeamien määrää, henkilöstön koulutusten kattavuutta sekä säännöllisesti suoritettujen riskianalyyysien tuloksia. Organisaatio pyrkii myös parantamaan asiakastytyväsyyttä varmistamalla, että tietoturvaan liittyvät käytännöt tukevat asiakkaiden luottamusta ja asioinnin sujuvuutta.

2.3 Tietosuoja koskevat periaatteet

Oikeus henkilötietojen suojaan on jokaiselle ihmiselle kuuluva perusoikeus, joka pohjautuu Suomen perustuslakiin. Kerimäen Vanhusten ja Vammaisten Tuki ry suunnittelee henkilötietojen käsittelyyn liittyvän toiminnan etukäteen. Käsittely on lainmukaista, kohtuullista ja läpinäkyvää ja se tapahtuu aina tiettyä, nimettyä tarkoitusta varten laissa säädetyn oikeusperusteen nojalla. Kerimäen Vanhusten ja Vammaisten Tuki ry käsittelee henkilötietoja vain siinä laajuudessa ja niin kauan, kuin se on kunkin käyttötarkoituksen kannalta tarpeellista.

Kerimäen Vanhusten ja Vammaisten Tuki ry pyrkii varmistamaan käsiteltävien henkilötietojen oikeellisuuden ja tietoja päivitetään tarpeen mukaan henkilöltä itseltään tai muista luotettavista lähteistä. Kun henkilötiedot eivät enää ole tarpeen, tiedot tuhotaan asianmukaisesti.

Tietosuoja tarkoittaa myös jokaiselle taattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada itseään koskevat virheelliset tiedot oikaistuiksi ja tarpeettomat tiedot poistetuiksi.



5.6.2025

julkinen

3 Tietoturvan ja tietosuojan hallinta

3.1 Tietoturvallisuuden toteutuksen periaatteet

Tietoturvan toteutuksessa noudatetaan seuraavia periaatteita:

- **Luottamuksellisuus:** Pääsy tietoihin myönnetään vain niille, joilla on siihen oikeus tehtävänsä mukaisesti.
- **Eheys:** Tietojen muuttumattomuus varmistetaan asianmukaisilla teknisillä ja organisatorisilla ratkaisuilla.
- **Saatavuus:** Tiedot ja järjestelmät ovat käytettävissä niiden tarpeen mukaisesti.
- **Lainmukaisuus:** Kaikessa toiminnassa noudatetaan soveltuvaa lainsäädäntöä ja viranomaismääräyksiä.
- **Ennaltaehkäisy:** Tietoturvahkien tunnistaminen ja niihin varautuminen ovat keskeisiä osia tietoturvaprosessia.

3.2 Tietosuojan turvaaminen

Riskilähtöisyys on perusta tietosuojan turvaamiselle. Tietosuojariskien hallinta on osa Kerimäen Vanhusten ja Vammaisten Tuki ry:n riskienhallintaprosessia. Tietosuojariskien arviointia toteutetaan henkilötietojen käsittelyn suunnitteluvaiheessa sekä osana vuosittaista riskiarviointia. Lisäksi tietosuojaa koskeva vaikutustenarviointi (DPIA) tehdään aina laissa ja viranomaisohjeistuksessa erikseen määritellyissä tilanteissa tai jos käsittelystä voi koitua korkeita riskejä rekisteröidyille. Vaikutustenarviointien tuloksia käytetään määrittäessä niitä teknisiä ja organisatorisia keinoja, joilla pyritään pienentämään henkilötietojen käsittelyn riskejä koko tietojen elinkaaren ajan. Samalla varmistetaan tietosuojalainsäädännön vaatimusten toteutuminen.

Kerimäen Vanhusten ja Vammaisten Tuki ry huolehtii GDPR:n mukaisista rekisteröityjen oikeuksista informoimalla rekisteröityjä henkilötietojen käsittelystä sekä määrittämällä toimintamallit ja ohjeet niihin tilanteisiin, joissa rekisteröidyt haluavat käyttää oikeuksiaan.

Kerimäen Vanhusten ja Vammaisten Tuki ry varmistaa tietosuojan toteutumisen dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyyn liittyvät käytännöt ja prosessit. Henkilöstön riittävästä tietosuojasaamisesta huolehditaan koulutusten ja



5.6.2025

julkinen

tietoisuuden lisäämisen avulla erillisen suunnitelman mukaisesti. Uudet työntekijät perehdytetään tietosuoja-asioihin työsuhteen alkaessa. Erityisesti tämä korostuu niissä tehtävissä, joissa käsitellään arkaluonteisia henkilötietoja ja suoritetaan rekisteröityjen oikeuksien liittyviä prosesseja.

Kerimäen Vanhusten ja Vammaisten Tuki ry voi rekisterinpitäjänä ulkoistaa henkilötietojen käsittelyn toimeksisaajalle, henkilötietojen käsittelijälle. Kerimäen Vanhusten ja Vammaisten Tuki ry voi myös itse toimia henkilötietojen käsittelijänä asiakkaidensa lukuun, esimerkiksi hyvinvointialueiden asiakkaiden tietojen käsittely. Kerimäen Vanhusten ja Vammaisten Tuki ry 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. Kerimäen Vanhusten ja Vammaisten Tuki ry laatii henkilötietojen käsittelijän kanssa lainsäädännön edellyttämän kirjallisen sopimuksen henkilötietojen käsittelystä.

3.3 Tietoturvariskien arviointi ja käsittely

Tietoturvariskejä arvioidaan säännöllisesti, vähintään kerran vuodessa, sekä aina merkittävien toiminnan tai järjestelmien muutosten tai hankinnan yhteydessä. Merkittävät muutokset määritellään esimerkiksi laajojen järjestelmäpäivitysten tai uusien toimintatapojen käyttöönoton yhteydessä, ja niiden arvioinnista päättää organisaation johto yhteistyössä tietosuojavastaavan kanssa.

Riskienhallinnassa hyödynnetään seuraavia toimenpiteitä:

- Riskianalyysit ja organisaatiossa toteutetut auditoinnit.
- Korjaavat toimenpiteet havaittujen heikkouksien poistamiseksi.
- Viranomaislähteistä ja mediasta saadut ajantasaiset uhatiedot

3.4 Tietojen luokittelu ja käsittely

Organisaatiolla on käytössä tietojen luokittelumenetelmä, jossa ohjeistetaan, miten tiedot tulee luokitella ja määritellään tarvittavat turvallisuuskäytännöt ja ohjeistukset eri luokkiin kuuluvan tiedon käsittelylle ja säilytykselle.



5.6.2025

julkinen

3.5 Henkilötietojen käsittely

Kerimäen Vanhusten ja Vammaisten Tuki ry henkilötietojen käsittelyä suunniteltaessa ja kehitettäessä analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja niiden käyttötarkoituksen mukaan. Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot ja tietoturvakäytännöt riskitason pienentämiseksi riittävälle tasolle sekä vaatimustenmukaisuuden saavuttamiseksi.

3.6 Tietoturvavaatimukset ja niihin sitoutuminen

Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturvavaatimukset määrittävät niin organisaation omalta toiminnalta kuin sopimuskumppaneilta vaadittavan minimitason tietoturvan osalta. Kaikki [organisaation nimi] työntekijät ja yhteistyökumppanit sitoutuvat noudattamaan organisaation toimintaan kohdistuvia tietoturvavaatimuksia. Yhteistyökumppaneiden osalta tietoturvan toteutumista valvotaan tarkastamalla sopimusten noudattamista säännöllisten auditointien avulla sekä seuraamalla mahdollisten poikkeamien raportointia.

Työsopimuksissa ja palvelusopimuksissa edellytetään salassapitoa ja tietoturvavaatimusten noudattamista. Vaatimustenmukainen tietoturvan taso voidaan tarvittaessa todentaa auditoinnin.

3.7 Tietoturvakoulutus ja -tietoisuus

Kaikille työntekijöille järjestetään:

- Perehdytys tietoturva- ja tietosuojakäytäntöihin uuden työntekijän aloittaessa.
- Vuosittainen tietoturvakoulutus, jossa käsitellään ajankohtaisia uhkia ja toimintatapoja.
- Ohjeistusta tietoturvapoikkeamien ja -havaintojen raportoinnille.

Tietoturvakoulutuksissa hyödynnetään Skhopen verkkokoulutusympäristöä sekä vuonna 2025 vielä osittain Navisec verkkokoulutusympäristöä.

3.8 Tietoturvallisuuden valvonta ja seuranta



5.6.2025

julkinen

Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturvan toteutumista valvotaan jatkuvasti seuraavilla menetelmillä:

- Työntekijöiden käyttöoikeuksien säännölliset tarkastukset.
- Tietojärjestelmien lokitietojen seuranta.
- Sisäiset ja ulkoiset auditoinnit.
- Tietoturva-/tietosuojatiimin kokoukset, joissa käsitellään ajankohtaisia tietoturva-asioita.

3.9 Tietoturvapoikkeamien käsittely

Kerimäen Vanhusten ja Vammaisten Tuki ry pyrkii turvaamaan henkilötietoja tietoturvaloukkauksilta, eli vahingossa tapahtuvalta tai lainvastaiselta tuhoamiselta, hävittämiseltä, muuttamiselta, luvottomalta luovuttamiselta tai pääsylvä tietoihin. Jokainen organisaation työntekijä on velvollinen viipymättä ilmoittamaan epäilemistään tai havaitsemistaan tietoturvaloukkauksista erillisen ohjeistuksen mukaisesti.

Mikäli tietosuojan epäillään vaarantuneen, tutkitaan asia viipymättä. Tutkintaan osallistuvat aina tarpeen mukaan johto, asiantuntijat sekä tietosuojavastaava. Kaikki tietoturvaloukkaukset dokumentoidaan lainsäädännön vaatimusten mukaisesti ja niistä tehdään ilmoitus tietosuojaviranomaiselle ilmoituskynnyksen ylittyessä. [Organisaation nimi] ilmoittaa tietoturvaloukkauksesta viipymättä myös henkilölle, jonka tietosuoja on vaarantunut, jos loukkauksesta seuraa korkea riski henkilölle.

Kaikki tietoturvapoikkeamat käsitellään viipymättä seuraavasti:

- Poikkeaman tunnistaminen ja kirjaaminen.
- Poikkeaman vaikutusten arviointi ja korjaavien toimenpiteiden toteuttaminen.
- Ilmoitus tietosuojavastaavalle ja tarvittaessa viranomaisille (esim. Tietosuojavaltuutetun toimisto, toimialan valvova virasto).
- Poikkeamasta oppiminen ja toimintatapojen päivittäminen vastaavien tapausten estämiseksi tulevaisuudessa.

Korjaavien toimenpiteiden toteutuksessa noudatetaan seuraavia menettelyjä:

- Nopeiden korjaustoimien käynnistäminen vahinkojen minimoimiseksi.
- Tapauksen juurisyyn selvittäminen ja analysointi.
- Prosessien, ohjeiden ja teknisten ratkaisujen päivittäminen vastaavien poikkeamien ennaltaehkäisemiseksi.
- Henkilöstön lisäkoulutus havaitun ongelman perusteella.



5.6.2025

julkinen

3.10 Menettelytavat tietoturvarikkomuksissa

Työntekijän aiheuttamiksi tietoturvarikkomukseksi lasketaan tietoturvapolitiikan ja -ohjeiden vastainen toiminta. Kerimäen Vanhusten ja Vammaisten Tuki ry on määritellyt menettelytavat rikkomustilanteille, kuten huomautus- ja varoitusmenettelyt.

3.11 Tietoturvavastuut ja organisointi

Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturvavastuut on määritelty seuraavasti:

- **Toimitusjohtaja:** Varmistaa tietoturvapolitiikan toteutuksen.
- **Tietosuojaavastaava:** Valvoo tietosuojalainsäädännön noudattamista, vastaa tietosuojaan ja tietoturvan kehittämisestä sekä auttaa muuta henkilöstöä tietosuojaan liittyvissä kysymyksissä.
- **Henkilöstö:** Sitoutuu tietoturvakäytäntöjen noudattamiseen ja ilmoittaa havaitsemistaan poikkeamista määriteltyjen raportointikäytäntöjen mukaisesti.
- **Tietoturva-/tietosuojiimi:** Seuraa tietoturvan ja tietosuojaan kehitystä ja koordinoi mm. riskienhallintatoimia ja poikkeamien hallintaa.

3.12 Tietoturvallisuuden jatkuva parantaminen

Kerimäen Vanhusten ja Vammaisten Tuki ry:n tietoturvapolitiikkaa päivitetään vähintään kerran vuodessa tai aina, kun lainsäädännössä, teknologiassa tai toiminnassa tapahtuu merkittäviä muutoksia. Organisaatio sitoutuu tietosuojaan ja tietoturvan jatkuvaan parantamiseen riskienhallinnan, henkilöstön koulutuksen ja ajan tasalla olevien teknologisten ratkaisujen avulla.