Tietoturva- ja tietosuojapolitiikka

Lapin ensi- ja turvakoti ry

Lapin ensi- ja turvakoti ry

Vastuuhenkilö: Merja Kuntsi

TIETOTURVAPOLITIIKKA

Hyväksytty hallituksessa 26.4.2018

Viimeksi päivitetty 19.12.2024

Sisällysluettelo:

1 Tietoturvapolitiikka

1.1 Yleistä

Tietoturvapolitiikka kattaa yhdistyksen kaikkeen toimintaan liittyvät tietojen käsittelyn tehtävät. Tietoturvapolitiikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita yhdistyksessä noudatetaan tietoturvan toteuttamisessa ja kehittämisessä.

Tietoturvapolitiikka on Lapin ensi- ja turvakoti ry:n hallituksen hyväksymä sisäinen toimintapolitiikkamääräys. Se on koko henkilöstön sekä yhdistyksen toimitiloja käyttävien muiden henkilöiden kuten vapaaehtoisten käytössä ja noudatettavissa. Tätä tietoturvapolitiikkaa täydentävät erilliset käyttö- ja ylläpito-ohjeet. Määritelty tietoturvapolitiikka tulee huomioida kaikessa yhdistyksen ohjeistuksessa.

Tietojärjestelmiin ja tietojen käsittelyyn liittyy riskejä, jotka pitää tunnistaa ja hallita. Lapin ensi- ja turvakoti ry:n ja kuntien välinen yhteistyö palvelujen tuottamiseen liittyen tapahtuu yhä enemmän yhteisten tietojärjestelmien ja viestintäkanavien kautta, mikä edellyttää vahvaa tietoturvaa yhdistyksen tietojärjestelmiltä ja tietoturvakäytännöiltä.

Yhdistyksen tietoaineistot sisältävät asiakkaisiin, työntekijöihin, vapaaehtoisiin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Yhdistyksessä käytössä oleva tietoaineisto voi olla julkista, perussuojaustasoa tai korkeaa suojaustasoa edellyttävää tietoa.

1.2 Tietoturvapolitiikan tavoite

Lapin ensi- ja turvakoti ry:n tietoturvallisuuden ensisijainen päämäärä yksityisyyden suojan toteutuminen tietosuoja-asioissa sekä yhdistyksen vastuulla olevien palveluiden jatkuvuuden turvaaminen kaikissa olosuhteissa. Tietoturvapolitiikka ohjeistaa ja tukee yhdistyksen toiminnalle ja sen tuottamille palveluille asetettuja vaatimuksia.

Tämä edellyttää yhdistyksen palveluihin liittyvien tietoteknisten ratkaisujen käytettävyyttä prosesseissa ja rekistereissä samoin kuin palveluissa käytettävien tietojen eheyttä ja luottamuksellisuutta kaikissa olosuhteissa. Henkilöstön tietoturva- ja tietosuojaohjeistus painottuu käytännön asiakastyön toteuttamiseen ja tukee yhdistyksen toiminnalle asetettuja vaatimuksia. Ohjeiden noudattamisella varmistetaan tietojen ja tietojärjestelmien huolellinen käsittely sekä asiakkaiden ja henkilöstön yksityisyyden suoja.

1.3 Tietoturvallisuuden merkitys

Tietoturvallisuus kattaa järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Se edellyttää tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä, toiminnallisilla ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Tietoturvallisuus on toimintatapa, jonka tavoitteena on tietojärjestelmien ja toiminnan jatkuvuutta uhkaavien riskien tunnistaminen, analysointi, ennakointi, ehkäisy ja hallinta. Tietoturvallisuus on edellytys Lapin ensi- ja turvakoti ry:n luotettavan asiakastyön hoitamiselle.

1.4 Määritelmät

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Sillä tarkoitetaan toimenpiteitä, joilla varmistetaan rekisteröidyn yksityisyyden suojaaminen sekä oikeuksien ja vapauksien turvaaminen.

Näitä ovat tiedon laadun ja eheyden koskemattomuuden (integriteetin) säilyttäminen sekä tiedon luottamuksellisuuden suojaaminen teknisin ja hallinnollisin keinoin. Tietoturvalla tarkoitetaan toisin sanoen niitä käytännön toimenpiteitä, joilla tietosuojaa toteutetaan.

Tietosuoja tarkoittaa henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi. Tietosuojan tarkoituksena on turvata tiedon kohteen (data subject) yksityisyys sekä edut, oikeudet ja vapaudet sekä oikeusturva. Henkilöllä on oikeus tietojensa asianmukaiseen käsittelyyn.

Tietoturvalla ja tietoturvallisuudella tarkoitetaan järjestelyitä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa:

Luottamuksellisuus (kukaan sivullinen ei saa tietoa): tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkauksilta.
Eheys (tiedon yhtäpitävyys alkuperäisen tiedon kanssa): tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus sekä ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.
Käytettävyys (tiedot eivät tuhoudu ja ovat niihin oikeutettujen hyödynnettävissä haluttuna aikana): tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.
Todentaminen (autentikointi): varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta, alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.
Kiistämättömyys: tietoverkossa eri menetelmin saatava näyttö siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi.

1.5 Tietoturvallisuuteen kohdistuvat uhat

Tietoturvallisuusuhat aiheuttavat eriasteisia riskejä tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle. Uhkia aiheuttavat tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, tekniset ongelmat sekä yhdistykselle palveluita tuottavien ulkopuolisten palveluiden tarjoajien toimet.

Henkilöiden mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys aiheuttavat merkittävän uhan yhdistyksen tietoturvallisuudelle. Ulkopuolisia palveluja kuten siivousta, kiinteistöhuoltoa ja vartiointia tuottavien tahojen kanssa tehtävissä sopimuksissa tulee huomioida tietoturvaan liittyvät asiat sekä rikkomuksiin liittyvät sanktiot.

2 Tietoturvatoimintaa ohjaavat tekijät

Tietoturvatoimintaa ohjataan säädöksin, ohjein ja suosituksin. Keskeiset Lapin ensi- ja turvakoti ry:n toimintaa tietoturvallisuuden ja tietosuojan näkökulmasta ohjaavat säädökset ovat EU-tietosuoja-asetuksen ohella Suomen perustuslaki, henkilötietolaki (523/1999), lastensuojelulaki (471/2007), sosiaalihuoltolaki (1301/2014), hallintolaki (434/2003), laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000), laki sosiaalihuollon asiakasasiakirjoista (254/2015), laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), rikoslaki (39/1889), laki yksityisyyden suojasta työelämässä (759/2004) ja laki yksityisistä sosiaalipalveluista (922/2011).

Lainsäädännön lisäksi yhdistyksessä tulee noudattaa muita yhdistyksessä hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Nämä eivät saa olla ristiriidassa tietoturvapolitiikan tai muiden ylemmän tason määräysten kanssa siten, että tietosuoja tai tietoturva heikkenee.

3 Tietoturvallisuuden merkitys organisaatiolle

Lapin ensi- ja turvakoti ry:n toiminnassa on keskeistä salassa pidettävän asiakastiedon huolellinen käsittely, joka tapahtuu suurelta osin sähköistä asiakastietojärjestelmää hyödyntäen. Tästä syystä tietoriskien hallintaan tulee kiinnittää erityistä huomiota.

3.1 Toiminnan kannalta elintärkeät palvelutehtävät ja turvattavat kohteet

Yhdistyksen toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot riippumatta siitä, missä muodossa ne ovat yhdistyksen hallussa. Turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen verkon toiminnan turvaaminen sekä toiminnan ja palveluiden tuottamisen turvaaminen normaali- ja poikkeusoloissa.

3.2 Tietoturvaperiaatteet

Turvaamisperiaatteita ovat riskien ehkäisy, turvatoimien ajantasainen seuranta ja kehittäminen sekä tietojärjestelmien toiminnan ja käytön valvonta.

Lapin ensi- ja turvakoti ry:n tietojärjestelmien hankinta- ja toteutusvaiheissa on huomioitava mahdolliset järjestelmien käyttöön kohdistuvat riskit ja varauduttava niiden ehkäisyyn. Käytön aikana varmistetaan tarkoituksenmukaiset suojausmenettelyt, jolloin järjestelmien käyttäjillä eli työntekijöillä ja vapaaehtoisilla on tietotarpeisiin sopiva ja tietoturvallisuusvaateet täyttävä käyttöympäristö.

1. Lapin ensi- ja turvakoti ry:n tietoturvapolitiikka on Suomen lainsäädännön mukaista ja se koskee koko yhdistyksen toimintaa ja henkilöstöä.
2. Jokainen yhdistyksen työntekijä huolehtii siitä, että riittävän hyvä tietoturvallisuus toteutuu yhdistyksen toiminnassa ja yhteistyössä sidosryhmien kanssa.
3. Yhdistyksen tietojärjestelmien tietojen käyttö on sallittua vain työtehtävien hoitamiseen.
4. Tietoturva-asiat huomioidaan kaikessa toiminnassa, sillä ne eivät liity vain tietotekniikkaan.
5. Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot suojataan asianmukaisesti kaikissa oloissa.
6. Varmistetaan, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
7. Lähiesimies huolehtii siitä, että henkilöstö perehdytetään tietoturvamääräyksiin ja –ohjeisiin.
8. Yhdistyksessä organisoidaan tietoturvaan liittyvä ohjaus, valvonta ja seuranta.
9. Tietoturvan toteutumista seurataan ja kehitetään.

3.3 Tietoturvallisuuden toteutumista tukevia käytäntöjä

Toiminnan jatkuvuus turvataan toipumissuunnittelulla, joka sisältää häiriöiden ennalta estämisen ja mahdollistaa niistä nopean toipumisen.

Tietojärjestelmien turvasuunnitelmissa, -järjestelyissä ja -ohjeissa varaudutaan tietoturvallisuutta koskevien laiminlyöntien, vahinkojen tai virheiden jälkikäteen selvittämiseen periaatteena kustannusten kohtuullisuus saatuun hyötyyn nähden.

Uusien tietojärjestelmien ja tilojen tietoturvallisuus huomioidaan ja testataan ennen niiden käyttöönottoa. Tietojärjestelmien toimintaa ja käyttöä ylläpidetään ja valvotaan aktiivisesti. Tietoturvan toteuttamisessa käytetään tarvittaessa ulkopuolisten asiantuntijoiden apua.

4 Turvatoimien priorisointi

Lapin ensi- ja turvakoti ry:n turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia:

- asiakkaiden, työntekijöiden ja muiden mahdollisten osallisten hengen tai terveyden turvaaminen
- arkaluonteisen tai muuten erittäin merkittävän tiedon luottamuksellisuuden turvaaminen
- tietojärjestelmien ja rekistereiden eheyden turvaaminen
- käyttö- ja toimintaympäristön käytettävyyden turvaaminen

5 Tietoturvallisuuden hallintajärjestelmä

Hallintajärjestelmä kattaa Lapin ensi- ja turvakoti ry:n tietoturvallisuuden politiikan, organisoinnin, suunnittelun, vastuut, menettelytavat, prosessit ja tarvittavat resurssit. Sen avulla seurataan ja arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen parantaa valmiuksia hallita tietoturvallisuutta systemaattisesti. Tietoturvallisuuden hallintajärjestelmä on luonteeltaan viitekehys, joka koostuu mm. seuraavista toimintamalleista ja dokumenteista:

- tietoturvapolitiikka,
- tietoturvakäytännöt ja -periaatteet,
- tietoturvallisuuden ohjeistus ja koulutus,
- tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus,
- tietoturvapoikkeamien käsittely,
- tietoturvaraportointi johdolle,
- toipumis-, jatkuvuus- ja valmiussuunnitelmat sekä
- toimintaan liittyvät tietoturvaprosessit
- tietoturvan arviointi

6 Tietoturvavastuut

6.1 Organisaation tietoturvavastuut

Tietoturvallisuuden ja tietosuojan kehittäminen on jatkuvaa laaja-alaista toimintaa, jossa nimetyillä vastuuhenkilöillä on omat tehtävänsä. Tietoturvatoiminnan ja tietoturvallisuuden hallintajärjestelmän kehittämisestä vastaa Lapin ensi- ja turvakoti ry:n hallitus yhdessä johtoryhmän kanssa. Tietosuoja- ja tietoturva on tärkeä osa yhdistyksen toimintastrategiaa.

Yhdistys tuottaa sekä sosiaalihuollon että lastensuojelun palveluita ja siellä käsitellään siten arkaluonteisia asiakastietoja. Tämä velvoittaa nimeämään tietosuojavastaavan yhdistykseen. Yhdistyksen tietosuojavastaavana toimii taloussihteeri Merja Kuntsi. Yhdessä johtoryhmän kanssa hän vastaa tietoturva-asioista. Tietosuojavastaavalla on oikeus suorittaa käytönvalvontaa sekä tarkastaa toimintatapoja liittyen yhdistyksen tietoturvan sääntöjen ja ohjeiden noudattamiseen.

Henkilöstön tulee noudattaa johdon ja lähiesimiehen antamia ohjeita ja osallistua työnantajan osoittamiin koulutuksiin. Jokainen yhdistyksen henkilökuntaan kuuluva on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä lähiesimiehelle tai tietosuojavastaavalle.

Hallitus yhdessä johtoryhmän kanssa vastaa yleisestä tietoturvan hallinnan kehittämisestä ja organisoimisesta. Siitä huolimatta vastuu tietoturvan toteutumisesta sekä tietoturvapolitiikan noudattamisesta on jokaisella työntekijällä. Tietoturvaan liittyvissä asioissa jokainen henkilö on vastuussa riskeistä ja niiden ehkäisystä, jotka liittyvät hänen omaan toimintaansa työtehtävissä.

Tietoturvapolitiikka päivitetään tarvittaessa. Päivitystarvetta seuraa johtoryhmä.

6.2 Organisaation yhteistyökumppaneiden vastuut

Lapin ensi- ja turvakoti ry:lle palveluita tuottavat yritykset tulee velvoittaa nimeämään yritykseen tietoturvayhteyshenkilö, joka vastaa yhdistyksen ohjeistaman tietoturvatason noudattamisesta yrityksessä. Kumppaneille asetettavat tietoturvavaatimukset kuvataan kussakin sopimuksessa.

Yhteistyökumppaneiden tulee noudattaa yhdistyksen tietoturva- ja tietosuojaohjeistusta.

7 Tietoturvakoulutus ja –ohjeet

Tietoturvallisuus on sisällytetty Lapin ensi- ja turvakoti ry:n perehdytysprosessiin. Jokainen työntekijä suorittaa tietoturvakoulutuksen periaatteet -verkkokoulutuksen. Koulutusta järjestetään kaikille työntekijöille määräajoin ja tarpeen mukaan.

Tietoturvaohjeistuksen sisällöstä ja ajantasaisuudesta vastaa tietosuojavastaava *yhdessä* yhdistyksen johtoryhmän kanssa. Lähiesimiehet varmistavat, että henkilöstö hallitsee tietoturvan perusteet. Varmistaminen toteutetaan määräajoin tehtävällä tietoturvatestillä.

8 Tietoturvallisuudesta tiedottaminen

Tietoturva-asioista tiedotetaan tarpeen mukaan. Tietoturva-asioiden sisäisestä tiedottamisesta vastaa tietosuojavastaava yhdessä johtoryhmän kanssa.

Tietoturva-asioista ei aktiivisesti tiedoteta Lapin ensi- ja turvakoti ry:n ulkopuolelle, mutta jos tiedottamistarvetta ilmenee, se hoidetaan kuten muukin ulkoinen tiedottaminen.

Kriisiviestinnässä noudatetaan yhdistyksen omia sekä Ensi- ja turvakotien liiton laatimia kriisiviestintäohjeita.

9 Tietoturvallisuuden toteutumisen valvonta

Jokainen Lapin ensi- ja turvakoti ry:n henkilökuntaan kuuluva on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä lähiesimiehelle tai tietosuojavastaavalle.

Tietoturvallisuudesta annettujen ohjeiden toteutumisesta vastaa kukin toimintayksikkö ja yhdistykselle palveluja tuottava yritys omalla vastuualueellaan. Lähiesimiesten tulee valvoa, että henkilöstö noudattaa tietoturvasta annettuja määräyksiä ja ohjeita.

10 Toiminta poikkeustilanteissa ja –oloissa

Poikkeusoloissa toimitaan Lapin ensi- ja turvakoti ry:n valmiussuunnitelman menettelytapojen mukaisesti. Valmiussuunnitelmien sisältö tulee olla yhteismitallinen jatkuvuus- ja toipumissuunnitelmien kanssa.

Poikkeusolojen toiminnan suunnittelusta vastaa yhdistyksen hallitus yhdessä johtoryhmän kanssa.