INVALIDISÄÄTIÖ

6.7.2018

Invalidisäätiö sr

Tietoturvapolitiikka

*****

21.5.2018

Dokumentin tila: hyväksytty
Hyväksyjä: Johtoryhmä
Hyväksymispäivämäärä: 21.05.2018

INVALIDISÄÄTIÖ

6.7.2018

Muutos- ja katselmointihistoria

PVM	Muutokset	Henkilö/Hyväksyjä

INVALIDISÄÄTIÖ

6.7.2018

Sisällysluettelo

6.7.2018

INVALIDISÄÄTIÖ

1 Johdanto

Tämä tietoturvapolitiikka kuvaa Invalidisäätiön tietoturvan hallintamallin, vastuut ja organisoitumisen sekä tietoturvatavoitteet. Tietoturvapolitiikassa Invalidisäätiön johto ilmaisee ne linjaukset ja painopisteet, joiden perusteella Invalidisäätiön tietoturvaa ohjataan.

Tietoturvapolitiikan hyväksyy Invalidisäätiön johtoryhmä. Sen sisältöä täydennetään ohjeistuksilla, jotka käsittelee ja hyväksyy tietohallinnosta vastaava johtaja. Tietoturvapolitiikka ja siihen liittyvät ohjeistukset päivitetään vuosittain tai tarpeen vaatiessa.

Tietoturvapolitiikka koskee kaikkia Invalidisäätiössä työskenteleviä ja se kattaa soveltuvin osin myös toimittajat ja muut sidosryhmät, jotka työnsä tai toimeksiantonsa puitteissa käsittelevät Invalidisäätiön omistamaa tai hallitsemaa tietoa.

1.1 Tausta

Invalidisäätiön tietoturvatyön taustalla on seuraavat motiivit:

- Tietoturvallisuuden ensisijainen päämäärä on Invalidisäätiön vastuulla olevien palveluiden sekä toiminnan jatkuvuuden turvaaminen
- Lainsäädännön ja muiden normien noudattaminen
- Keskeisten toimintojen turvaaminen poikkeustilanteissa
- Tietoturvallisen ympäristön luominen sekä Invalidisäätiön ydintoimintojen, että sidostyhmien tarpeisiin
- Invalidisäätiön maineesta ja luottamuksesta huolehtiminen

1.2 Määritelmät

Invalidisäätiössä tietoturvalla tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan Invalidisäätiön omistamaa tai hallinnoimaa tietoa normaalioloissa, häiriötilanteissa ja poikkeusoloissa. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietoturvaan liittyviä keskeisiä käsitteitä ovat:
Luottamuksellisuus: tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkauksilta.
Eheys: tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus sekä ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu,
Saatavuus: ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

2 Tietoturvallisuuden toteuttaminen ja tietoturvaperiaatteet

Tietojenkäsittelyn turvaamisperiaatteita ovat ennaltaehkäisy, turvatoimien ajantasainen seuranta ja kehittäminen sekä tietojärjestelmien toiminnan ja käytön valvonta.

Tietojärjestelmien määrittely-, suunnittelu- ja toteutusvaiheissa on huomioitava mahdolliset järjestelmien käyttöön kohdistuvat riskit ja varauduttava niiden ennaltaehkäisyyn. Toteutusvaiheessa varmistetaan tarkoituksenmukaiset suojausmenettelyt, jolloin järjestelmien käyttäjillä on tietotarpeita vastaava käyttöympäristö.

2.1 Tiedon elinkaari

Tietoturvapolitiikkaa sovelletaan kaikkeen Invalidisäätiössä tapahtuvaan tiedon käsittelyyn tiedon koko elinkaaren ajan riippumatta siitä, missä muodossa tai millä välineillä tietoa käsitellään. Tietoturvaperiaatteet koskevat jokaista Invalidisäätiöllä työskentelevää ja opiskelevaa.

Erilaisilla toimenpiteillä, vastuutuksilla ja ohjeistuksilla pyritään varmistamaan tiedon eheys, saatavuus, luottamuksellisuus ja tietoturvallisuus koko elinkaaren ajan.

Teknisiä tietoturvatoimenpiteitä ovat mm. tietoliikenteen salaaminen, tietoverkkojen suojaus palomuureilla ja tietojärjestelmien päivittäminen ja varmistaminen säännöllisesti.

Hallinnollisia toimenpiteitä ovat mm. salasanapolitiikka, tiedon luokittelu, henkilöstölle suunnattu tietoturvakoulutus ja ohjeistukset.

2.2 Riskienhallinta

Tietoturvallisuus arvioidaan vuosittain osana Invalidisäätiön tietosuojan riskienhallintaa. Riskienhallinnan tavoitteena on hallita haitallisia riskejä tavoitteiden saavuttamisen ja toiminnan jatkuvuuden mahdollistamiseksi.

Tietoturvan riskienhallinta on jatkuva prosessi ja riskien kokonaisarviointi tehdään vuosittain. Riskienhallinnassa varaudutaan tietojen käsittelyyn ja tietoturvaan liittyviin poikkeustilanteisiin. Poikkeustilanteiden aiheuttamia ongelmia ennakoidaan ja vahinkoja minimoidaan erilaisin toimenpitein.

IT-päällikkö vastaa tietoturvaan liittyvien riskien tunnistamisesta, riskienhallinnasta ja siihen liittyvästä tiedotuksesta ja ohjeistuksista. Tietoturvan tilasta raportoidaan johtoryhmälle ja vuosittain hallitukselle tietotilinpäätöksellä.

2.3 Tietoturvallisuustyön tavoitteet

Invalidisäätiön tietoturvallisuuden tavoitteena on rakentaa ja varmistaa toimintaympäristö siten, että häiriön (kuten inhimillinen erehdys, tekninen vika tai tahallinen haitanteko) vaikutukset saadaan rajoitettua ja toiminnon palautettua mahdollisimman nopeasti normaalitilanteeseen. Näin varmistetaan Invalidisäätiön asiakkaille tarjottavien palveluiden ja Invalidisäätiön sisäisten toimintojen korkea laatu.

3 Organisointi

3.1 Johtaminen

Invalidisäätiön tietoturvallisuuden johtamisesta ja tietoturvallisuuden päälinjauksista vastaa tietohallinnosta vastaava johtaja. Tietohallinnon operatiivisesta toiminnasta vastaa IT-päällikkö, joka vastaa organisoinnista, tehtävistä, resursseista ja vastuista. Tarvittaessa kootaan asiantuntijoista koostuva tietoturvaryhmä, joka käsittelee tietoturvan prosesseja, linjauksia ja ohjeistuksia yhdessä tietohallinnosta vastaavan johtajan ja IT-päällikön kanssa. Strategiset linjaukset hyväksytään Invalidisäätiön johtoryhmässä.

3.2 Vastuut

IT-päällikkö ohjaa ja kehittää Invalidisäätiön tietoturvatoimintaa. Hän vastaa tietoturvallisuustason määrittelystä, arvioinnista, raportoinnista sekä seurannasta. Hän vastaa myös tietoturvallisuutta koskevasta ulkoisesta yhteistyöstä yhdessä tietohallinnosta vastaavan johtajan kanssa sekä suunnittelee tietoturvallisuuden kehittämistoimenpiteitä. Vastuualueeseen kuuluu myös lähiesimiesten ohjeistaminen, jotta heillä on riittävät valmiudet perehdyttää henkilöstöään tietoturva-asioihin.

INVALIDISÄÄTIÖ

6.7.2018

Invalidisäätiön tietohallinto vastaa IT-päällikön johdolla tietoturvaan liittyvien ohjeistusten ja toimintojen kehittämisestä.

Jokaiselle tietojärjestelmälle on määritelty omistaja, pääkäyttäjä/vastuuhenkilö sekä tietohallinnon vastuuhenkilö. Omistaja vastaa tiedon luokittelusta (mm. salassapidon määrittely), eheyden varmistamisesta, riskienhallinnasta ja riskeihin varautumisesta. Käyttöoikeudet järjestelmään hyväksyy omistaja tai hänen valtuuttamansa taho. Ks. alla.

Pääkäyttäjä/vastuuhenkilö vastaa omistajan valtuuttamana tietojärjestelmän toiminnasta, hallinnasta ja käyttöoikeuksista.

Tietohallinnon vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten määrittely ja valvonta.

Sama henkilö voi toimia useassa roolissa (omistaja, pääkäyttäjä/vastuuhenkilö, tietohallinnon vastuuhenkilö).

3.3 Raportointi

Tietoturvallisuuden hallintaa seurataan ja parannetaan jatkuvasti. Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvistä väärinkäytöksistä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietohallintoon. Tietohallinnon tehtävänä on seurata ja valvoa tietojärjestelmien toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi. IT-päällikkö raportoi säännöllisesti tietohallinnosta vastaavaa johtajaa tietoturvan tilasta.

Tietoturvan poikkeamatilanteissa raportoidaan poikkeamaraportointimallin mukaisesti.

3.4 Viestintä

Invalidisäätiön tietoturvaviestinnästä ja sen kehittämisestä vastaa asiakkuusjohtaja yhdessä IT-päällikön kanssa. Toimintojen sisäisestä tietoturvaviestinnästä vastaa yksikön esimies.

Kriisitilanteissa tietoturvaviestinnän vastuut jakautuvat kriisiviestintäsuunnitelman mukaisesti.

4 Tietoturvapoikkeamista ilmoittaminen

Invalidisäätiön työntekijä on omalta osaltaan vastuussa tietoturvan toteutumisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietohallintoon.

Tietoturvapoikkeamien hallintamalli kuvaa poikkeamatilanteiden toimet ja käytänteet. Hallintamallia täydennetään ohjeistuksilla.