Live-säätiö sr

Tietoturvapolitiikka

*****

6.6.2022

Dokumentin tila: hyväksytty
Hyväksyjä: Johtoryhmä
Hyväksymispäivämäärä: 6.6.2022

Muutos- ja katselmointihistoria

PVM	Muutokset	Henkilö/Hyväksyjä
7.2.2022	Dokumentin päivitys	Jouni, Aki ja Jussi
28.2.2022	Siirto Live-pohjalle	Jouni
6.6.2022	Joryn hyväksyntä	Jory

Sisällysluettelo

1 Johdanto

Tämä tietoturvapolitiikka kuvaa Live-säätiö sr (jatkossa säätiö) tietoturvan hallintamallin, vastuut ja organisoitumisen sekä tietoturvatavoitteet. Tietoturvapolitiikassa säätiön johto ilmaisee ne linjaukset ja painopisteet, joiden perusteella säätiön tietoturvaa ohjataan.

Tietoturvapolitiikan hyväksyy säätiön 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 säätiössä työskenteleviä ja se kattaa soveltuvin osin myös toimittajat ja muut sidosryhmät, jotka työnsä tai toimeksiantonsa puitteissa käsittelevät säätiön omistamaa tai hallitsemaa tietoa.

1.1 Tausta

Tietoturva on yksi tietosuojan toteuttamisen keno. Säätiön tietoturvatyön taustalla on seuraavat motiivit:

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

1.2 Määritelmät

Säätiössä tietoturvalla tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan säätiön 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

2.1 Tietoturvan periaatteet

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.

Tietoturvapolitiikkaa sovelletaan kaikkeen säätiössä tapahtuvaan tiedon käsittelyyn tiedon koko elinkaaren ajan riippumatta siitä, missä muodossa tai millä välineillä tietoa käsitellään. Tietoturvaperiaatteet koskevat jokaista säätiöllä työskentelevää ja sidosryhmään kuuluvaa.

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

Tietohallinnon tehtävänä on seurata ja valvoa tietojärjestelmien toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

2.2 Riskienhallinta

Tietoturvallisuus arvioidaan vuosittain osana säätiön tietosuojan riskienhallintaa. Riskienhallinnan tavoitteena on hallita riskejä tavoitteiden saavuttamisen ja toiminnan jatkuvuuden varmistamiseksi.

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.

2.3 Tietoturvallisuustyön tavoitteet

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

3 Organisointi

3.1 Johtaminen

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

3.2 Vastuut

IT-päällikkö ohjaa ja kehittää säätiön 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 lähiesihenkilöiden ohjeistaminen, jotta heillä on riittävät valmiudet perehdyttää henkilöstöään tietoturva-asioihin.

Jokaiselle tietojärjestelmälle on määritelty omistaja, pääkäyttäjä/vastuuhenkilö, sekä tietohallinnon vastuuhenkilö. Sama henkilö voi toimia useassa roolissa.

- **Omistaja** vastaa tiedon luokittelusta (mm. salassapidon määrittely), eheyden varmistamisesta, riskienhallinnasta ja riskeihin varautumisesta. Käyttöoikeudet järjestelmään hyväksyy omistaja tai hänen valtuuttamansa taho.

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

- **Tietohallinnon vastuuhenkilö**n velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten määrittely ja valvonta.

3.3 Raportointi

IT-päällikkö raportoi säännöllisesti tietohallinnosta vastaavaa johtajaa sekä johtoryhmää tietoturvan tilasta. Tietoturvan poikkeamatilanteista raportoidaan tietoturvapoikkeamien hallintamallin mukaisesti.

3.4 Viestintä

Säätiön sisäisestä tietoturvaviestinnästä ja sen kehittämisestä vastaa IT-päällikkö. Toimintojen sisäisestä tietoturvaviestinnästä vastaa yksikön esihenkilö.

Kriisitilanteissa tietoturvaviestinnän vastuut jakautuvat kriisiviestintäsuunnitelman mukaisesti.

4 Tietoturvapoikkeamista ilmoittaminen

Säätiön työntekijä on omalta osaltaan vastuussa tietoturvan toteutumisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen käyttäjä ja ylläpitäjä on velvollinen ilmoittamaan havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvistä väärinkäytöksistä tai epäilemästään tietoturvarikkomuksesta esihenkilölleen tai tietohallintoon.

Tietoturvapoikkeamien hallintamallissa kuvataan poikkeamatilanteiden toimet ja käytänteet. Hallintamallia täydennetään ohjeistuksilla.