25.1.2024 Julkinen

TIETOTURVA JA TIETOSUOJAPOLITIIKKA

1. Johdanto

DigiFinland Oy:n toiminta ja palvelut ovat riippuvaisia tietojärjestelmäpalveluiden keskeytyksettömästä saatavuudesta ja niiden turvallisesta toiminnasta. Tietojärjestelmäpalveluiden hyödyntäminen ja tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan toimintakykyyn. Myös lainsäädäntö, standardit ja sopimukset asettavat velvoitteita tietoturvallisuudesta ja tietosuojasta huolehtimiselle. Tietoturvapolitiikka on velvoittava kaikessa yhtiön toiminnassa ja se katselmoidaan säännöllisesti.

Tiedon turvaaminen ja tietosuojasta huolehtiminen ovat osa toiminnan ja palveluiden laatua, kokonaisturvallisuutta sekä päivittäistä tietojen käsittelyä. Tietoturvan ja tietosuojan hyvä hallinta edellyttävät kaiken toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua, varautumista uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö niin henkilöstön kuin sen sidosryhmienkin tietojen käsittelyn osalta.

2. Tavoitteet

2.1 Tietoturvan tavoitteet

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen. Tietojen turvallisuudesta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä eli tiedon kaikissa muodoissa sen koko sen elinkaaren ajan. Tietojen turvaamisesta on huolehdittava kaikissa DigiFinland Oy:n toiminnoissa.

Tietoturvallisuustyö on tietojen turvaamiseksi tehtävää jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa. Sillä pyritään ennaltaehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne riskienhallinnan avulla hyväksyttävälle tasolle. Tietoturvallisuudesta huolehditaan asiakkaiden vaatimusten sekä kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti noudattaen tietoturvallisuuden parhaita käytäntöjä ja suosituksia.

Tietoturvan tavoitteet asetetaan osana yhtiön toiminnan suunnittelua ja johtamista (LJ_24, Toiminnan suunnittelu ja johtaminen) ja niitä seurataan seuranta- ja arviointijärjestelmän (LJ_27, Seuranta- ja arviointijärjestelmän) mukaisesti

2.2 Tietosuojan tavoitteet

DigiFinland noudattaa tietosuojalainsäädäntöä kaikessa toiminnassaan. Rekisterinpitäjänä ja henkilötietojen käsittelijänä DigiFinland Oy huolehtii, että EU:n yleisessä tietosuoja asetuksessa määriteltyjä tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa.

DigiFinlandissa henkilötietojen käsittely rajoitetaan vain niihin tarkoituksiin, joita varten tiedot on kerätty tai jotka ovat yhteensopivia alkuperäisen käyttötarkoituksen kanssa. Henkilötietoja ei saa käsitellä, kuten säilyttää tai kerätä, enempää kuin mitä on tarpeen käyttötarkoituksen kannalta. Henkilötiedot pidetään ajan tasalla eli epätarkat ja virheelliset tiedot poistetaan tai oikaistaan viipymättä. Tietosuojasta huolehditaan tiedon kaikissa muodoissa sen koko sen elinkaaren ajan. Lisäksi henkilötietoja käsitellään luottamuksellisesti ja turvallisesti ja ne suojataan oikeudettomalta tai henkilöä vahingoittavalta käsittelyltä

3. Tietoturvan organisointi ja vastuut

Kokonaisuutena DigiFinland Oy:n toiminnasta ja sen turvallisuudesta vastaa yhtiön toimitusjohtaja.

Kunkin palvelun ja prosessin omistaja on vastuussa tietosuojan lisäksi myös tietoturvasta. Tarvittaessa palveluille ja prosesseille voidaan nimetä erilliset tietoturvan vastuuhenkilöt. Jokaisen prosessiin ja toimintoon kuuluvan ja muuten palvelun tuottamiseen osallistuvan henkilön edellytetään toimivan vastuullisesti sekä huolehtivan omalta osaltaan vastuu- ja tehtäväalueensa turvallisuudesta.

Jokainen DigiFinland Oy:lle työskentelevä on velvollinen noudattamaan sääntöjä ja ohjeita. Jokaisen velvollisuutena on ilmoittaa havaitsemistaan turvallisuuspuutteista ja -heikkouksista sekä tapahtuneista häiriöistä ja vahingoista tai niiden epäilyistä sekä läheltä piti -tilanteista joko esimiehelleen tai tietoturvapäällikölle.

Keskeisimmät tietoturvallisuuteen ja tietosuojaan liittyvät toimijat, roolit, vastuut ja velvollisuudet on kuvattu Tietoturva- ja tietosuojavastuut -dokumentissa.

4. Toteutuskeinot

Tietoturvan ja tietosuojan ylläpito ja kehittäminen ovat osa jatkuvaa parantamista, jota johdetaan suunnitelmallisesti. Turvallisuuden kehittämisen toimenpiteet suunnitellaan, resursoidaan, aikataulutetaan ja dokumentoidaan. Lisäksi varmistetaan kyky reagoida muutoksiin ja suunnata toimenpiteitä kulloinkin tärkeimpiin kohteisiin. Tietoturvallisuuteen ja tietosuojaan kohdistuvat riskit arvioidaan ja käsitellään Riskienhallintaprosessin (LJ_19) mukaisesti.

Henkilöstön turvallista toimintaa johdetaan käyttösäännöillä ja toimintaohjeilla sekä tietojen turvallisen käsittelyn perehdytyksillä, koulutuksilla, viestinnällä ja hyvällä esihenkilötyöllä. Henkilöstön turvallisuus- ja tietosuojaosaaminen ja toiminnan turvallisuus varmistetaan koulutuksien ja niiden suoritusseurannan avulla. Tietoturvapäällikkö, tietosuojavastaava tukevat esihenkilöä tässä työssä.

Järjestelmien, teknisten toimintaympäristöjen, käsittelyprosessien ja ulkoisten palveluiden tietoturvallisuus ja tietosuoja varmistetaan yhteistyössä tietoturvapäällikön, tietosuojavastaavan kanssa. Tietoturvallisuus varmistetaan määrittelemällä turvallisuusvaatimukset, varmistamalla asetettujen vaatimusten täyttyminen, huolehtimalla käyttöönottojen turvallisuudesta, ottamalla turvallisuusvaatimukset huomioon sopimuksissa sekä ylläpitämällä turvallisuusominaisuuksia koko elinkaaren ajan.

Tietoturvapoikkeamat käsitellään poikkeamien hallinta- prosessin (LJ_30) mukaisesti. Palveluiden jatkuvuuden varmistamiseksi ylläpidetään palvelukohtaisia jatkuvuussuunnitelmia, joiden mukaisesti toimitaan poikkeustilanteissa. Suunnitelmien toimivuus varmistetaan riittävällä testaamisella ja poikkeustilanteiden harjoittelulla.

Tietoturvallisuus ja tietosuoja osoitetaan dokumentoiduilla tietoturvallisuuden hallinnan työohjeilla ja niiden toteuttamisen ja seurannan yhteydessä syntyvällä dokumentaatiolla.

Henkilötietojenkäsittelyn tietosuoja varmistetaan lisäksi noudattamalla tietosuojaperiaatteita, kuten lainmukaisuus, läpinäkyvyys ja käyttötarkoitussidonnaisuus. Nimetty tietosuojavastaava seuraa ja antaa neuvoja tietosuojan huomioon ottamisesta henkilötietojen käsittelyprosesseissa.

5. Tietoturvan ja tietosuojan ongelmatilanteiden käsittely

Tietoturvapäällikön ja tietosuojavastaavan tehtävänä on tehdä tietojenkäsittelyn turvallisuuteen ja tietosuojaan liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi. Vastuullisilla henkilöillä on häiriötilanteissa oikeus ryhtyä välittömiin toimenpiteisiin organisaatioon tai sen tietoihin kohdistuvan riskin minimoimiseksi.

Tietoturvallisuuden ja tietosuojan ylläpito edellyttää jatkuvaa seurantaa ja raportointia. Tietoturvapäällikkö koordinoi tietoturvallisuuden seurantaa ja raportoi säännöllisesti tietoturvallisuudesta johdolle.

Tämä dokumentti astuu voimaan hyväksymisen jälkeen ja on voimassa kolme vuotta tai siihen asti, kun uusi versio dokumentista hyväksytään.

VERSIOHISTORIA

Päivämäärä	Versio	Muutos, tekijä	Hyväksyjä
16.3.2020	1.0	1. version hyväksyntä Yhdistetty SoteDigi Oy:n ja Vimana Oy:n politiikat ja vastuut Hyväksytty SoteDigi Oy:n johtoryhmässä	Jenni Siermala
29.10.2020	2.0	2. version hyväksyntä Muutettu organisaatio nimi DigiFinland Oy Toimitusjohtajan hyväksymä	Jenni Siermala
20.2.2023	2.1	Dokumentti päivitetty vastaamaan nykyistä organisaatiota ja dokumentointia, Vesa Niiranen, Anssi Virtanen, Susanna Halmela. Dokumentista luotu tiivistelmä, jonka versio 1.0	Mirva Antila

		Dokumentin versiohallinta päivitetty vastaamaan auditointihavaintoja: muutos → muutos, tekijä sekä tekijä → hyväksyjä Katselmoinut laatu- ja riskienhallintapäällikkö Raisa Karjalainen	
25.1.2024	2.2	Tiivistetty dokumentin sisältöä, poistettu duplikaatteja. Korjattu viitattujen dokumenttien nimikkeet ja lisätty LJ-tunnukset. Tarkennettu tietoturvatavoitteiden asetanta ISO27001- sisäisen auditoinnin havaintojen perusteella. /Vesa Niiranen, Raisa Karjalainen	Hallitus