Sisällysluettelo

Tämä dokumentti astuu voimaan hyväksymisen jälkeen ja on voimassa 1 vuosi tai siihen asti, kun uusi versio dokumentista hyväksytään.

VERSIOHISTORIA

Päivämäärä	Versio	Muutos	Tekijä
16.2.2021	1.0	1. version hyväksyntä Johdon katselmuksessa	Jenni Siermala

1. TIETOTILINPÄÄTÖKSEN TARKOITUS

Tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa sekä arvioi tietosuojan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja -toimenpiteitä.

Tietotilinpäätös on tarkoitettu DigiFinland Oy:n sisäiseen käyttöön johtamisen raportiksi sekä sidosryhmille tietojen käsittelyn kuvaukseksi. Se toimii myös suunnittelun ja toiminnan ohjauksen sekä raportoinnin ja johtamisen tukena. Tietotilinpäätös on myös keskeinen dokumentti EU:n yleisen tietosuoja-asetuksen mukaista osoitusvelvollisuutta. Osoitusvelvollisuus tarkoittaa lakien, hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan noudattamista.

DigiFinland Oy kunnioittaa tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita. Henkilötietojen käsittelyssä noudatetaan seuraavia vaatimuksia:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus

Tässä dokumentissa kuvataan, miten em. periaatteet toteutuivat DigiFinland Oy:n toiminnassa vuonna 2020.

2. TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

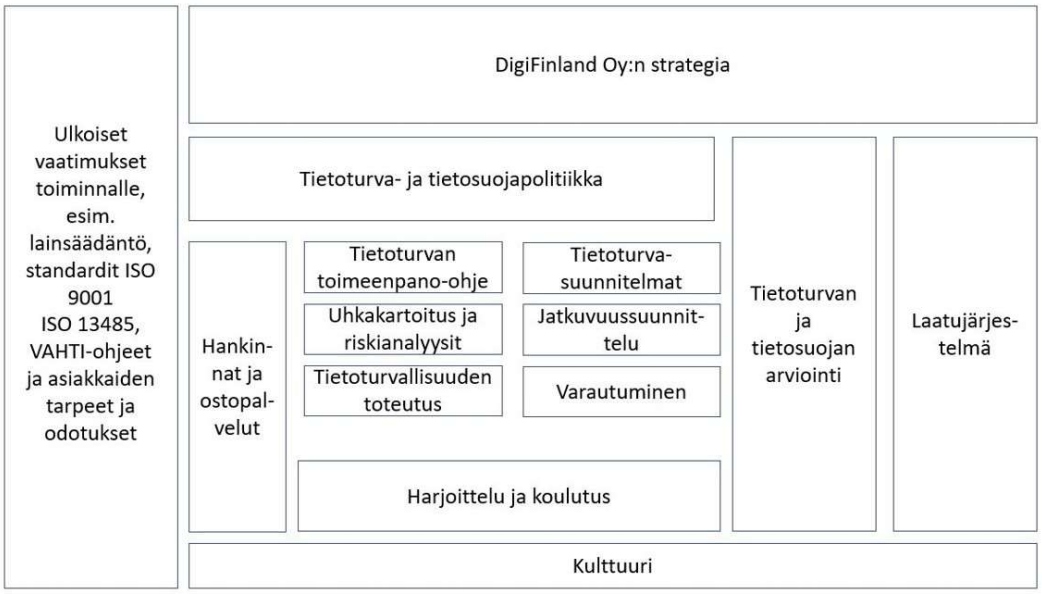
Tässä luvussa kuvataan, miten eheys ja luottamuksellisuus sekä tietosuojaperiaatteet toteutuvat DigiFinland Oy:n toiminnassa.

2.1 Tietoturvan organisointi

Tietosuojasta ja tietoturvallisuudesta DigiFinland Oy:ssä vastaa toimitusjohtaja. Tietosuoja- ja tietoturva-asioista raportoidaan johtoryhmälle. DigiFinland Oy:ssä on tietoturvapäällikkö, jonka tehtäviin kuuluvat myös tietosuojavastaavan tehtävät. Tietosuojavastaava on suorittanut Itä-Suomen yliopiston järjestämän Osaava tietosuojavastaavakoulutuksen, joka luo pätevyyden toimia tietosuoja-asetuksessa säädettyjen tehtävien hoitamiseen.

DigiFinland Oy on laatinut tietosuoja- ja tietoturvapolitiikan. Yleiset tietoturvavastuut ja tiettyihin tehtäviin liittyvät tietoturvavastuut on kuvattu DigiFinland Oy:n tietoturva- ja tietosuojapolitiikoiden liittyvässä tietoturva ja tietosuojavastuut -dokumentissa.

DigiFinland Oy:ssä on tietoturvanhallintamalli ja palvelutuotannon tietoturva, tietosuoja sekä jatkuvuudenhallintamenetelmä. Alla kuva SoteDigin tietoturvanhallintamallista.



Kuva 1. Tietoturvan hallintamalli

Vuonna 2020 perustettiin tietoturva- ja tietosuojaryhmä. Ryhmän tarkoituksena on olla operatiivinen toimija tietoturvan, tietosuojan ja jatkuvuudenhallinnassa. Jokainen ryhmän jäsen toimii linkkinä oman tiiminsä ja tietoturva- ja tietosuojaryhmän välillä.

Tietoturvaryhmän tehtävät

- sovittaa yhteen vaadittu turvallisuustaso ja turvallisuustoimenpiteet omassa tiimissä
- tehdä ehdotuksia tietoturvallisuuden parantamiseksi
- osallistua DigiFinlandin tietoturvasuunnitelman ja jatkuvuussuunnitelman valmisteluun
- tukea tietoturvallisuuden kehittämistä ja tietoturvallisuuden seuranta
- tehdä esityksiä henkilöstön tietoturvallisuustietoisuuden lisäämisestä ja tietoturvakoulutuksesta
- toimia tietosuojatyökalun käyttäjänä

Vuonna 2020 tietoturva- ja tietosuoja ryhmä kokoontui neljä kertaa: 8.5., 10.6., 17.10. ja 15.12. tietoturvan- ja tietosuojan toimintasuunnitelman mukaisesti.

2.2 Tietosuojan ja tietoturvan koulutus ja ohjeistus

Vuonna 2020 DigiFinlandissa päivitettiin tietoturva- ja tietosuojapolitiikka vastaamaan SoteDigin ja Vimanan yhdistymisen myötä monialaista toimialaa. Päivitetty tietoturva- ja tietosuojapolitiikka hyväksyttiin 16.3.2020. Tietosuoja- ja tietoturvapolitiikkoja täydentävät tietoturvasäännöt, henkilöstön tietoturvaohjeet, tietosuojan lomakkeet, tietosuoja- ja tietoturvaohjeet, koulutusaineistot.

Kuva 2, Tietoturva- ja tietosuojapolitiikka sekä ohjeistukset.

Näiden päivitykset jatkuvat osana yhtiön toiminnan kehittymistä. Henkilökunta sitoutuu salassapitoon työsopimuksessaan. Henkilöstö suoritti tietoturva- ja tietosuojakoulutuksen vuonna 2020.

2.3 Henkilötietojen tekniset ja organisatoriset suojaustoimet

Henkilötietojen käsittelyssä käytettävien tietojärjestelmien hallinnassa noudatetaan DigiFinlandin tietoturvasäännöstöä ja -ohjeita. Teknisesti tietojärjestelmät ja niiden käyttöliittymät ovat suojattu mm. palomuurilla ja työasemilla on virustorjuntaohjelmistot. DigiFinland vastaa työaseman käyttöoikeuksien teknisestä toteuttamisesta. Ulkoinen kumppani avustaa myös teknisessä tietoturvassa sekä sen valvonnan.

Työasemien kovalevyt on salattu ja käytössä olevat muistitikut salataan myös työasemassa olevan salaustyökalun avulla. Lisäksi jokainen on vastuussa muistitikkujen viruksettomuudesta. DigiFinland vastaa perustietotekniikasta yhdessä kumppanin kanssa, johon sisältyy työasemien ja verkkolaitteiden hankinta, käyttöönotto ja ylläpito. Työasemien asennuspalvelu on ulkoistettu kumppanille. Sovellusten hankinnat ja asennukset sovitaan yhteistyössä ulkopuolisen kumppaninen kanssa. Työasemientukitehtävissä käytettävät etäyhteydet toteutetaan salatusti. Työasemien tietoliikenne turvataan VPN yhteyden avulla.

DigiFinlandissa on vähimpien käyttöoikeuksien periaate, jonka mukaisesti esimies valtuuttaa henkilöstölle riittävät käyttöoikeudet, siten että henkilöstöllä on työtehtäviensä laajuuden mukaiset käyttöoikeudet. DigiFinlandissa on tietoturvan- ja tietosuojan omavalvontasuunnitelma, jonka mukaisesti tietoturvan ja tietosuojan toteutumista arvioidaan. Lisäksi palvelutuotannon tietoturva, tietosuoja ja jatkuvuudenhallintaohje turvaa palvelun elinkaarenhallinnan.

Vuonna 2020 käynnistettiin perustietotekniikan kilpailutus, jonka tarkoituksena on parantaa teknisiä suojaustoimia ja lisätä havannointikykyä.

2.4 Pseudonymisointi, anonymisointi

Pseudonymisointi tarkoittaa henkilötietojen käsittelyä siten, että niitä ei voida enää yhdistää tiettyyn henkilöön ilman erillään säilytettäviä lisätietoja. Henkilötiedot pseudonymisoidaan aina, kun henkilön suora tunnistaminen ei ole välttämätöntä. Henkilötiedon anonymisointi tarkoittaa henkilötiedon poistamista siten, että henkilön tunnistaminen uusia tietoja yhdistämällä on mahdotonta.

DigiFinlandissa on ohje tunnisteellisen tiedon ja anonymisoinnin osalta. Kaikissa hankkeissa on tärkeää arvioida tilanteet, joissa suorat ja epäsuorat henkilötiedot on tarpeen poistaa. Lisäksi Omaolon analytiikkaa toteutettaessa on huomioitava henkilötietojen poistaminen pseudonymisoinnin ja anonymisoinnin avulla.

2.5 Riskienhallinta ja tietoturvapoikkeamien käsittely

Vuosittain käydään läpi tietoturva- ja tietosuojariskiarviointi organisaation tasolla. Lisäksi Vaikutustenarviointi tehdään aina otettaessa käyttöön uutta teknologiaa, käsiteltäessä laajamittaisesti erityisiä henkilötietoryhmiä (EU:n yleinen tietosuoja-asetus, artiklat 9 ja 10) koskevia henkilötietoja.

Organisaation riskit käsitellään vuosittain ja toimitusjohtaja hyväksyy riskit. Vaikutuksenarvioinnin tarpeellisuusvaatimus arvioidaan omassa toiminnassa ja se toteutetaan tarvittaessa. Palvelutuotannossa toteutetaan tietoturva- ja tietosuojariskien arviointia riskisuunnitelman mukaisesti. Lisäksi palvelutuotannossa avustetaan rekisterinpitäjiä ja toteutetaan vaikutuksenarviointi.

Kaikki tietoturvapoikkeamat käsitellään capa-prosessin tai MIM-prosessin mukaisesti riippuen poikkeaman laajavaikutteisuudesta. Capa prosessia on täydennetty tietoturva- ja tietosuojapoikkeamaprosessilla.

Vuonna 2020 oli yksi henkilötietojentietoturvaloukkaus. Näiden korjaavat ja ehkäisevät toimenpiteet on toteutettu sekä juurisyy selvitetty. DigiFinlandin tieturvariskit on tunnistettu ja niille on suunniteltu mitigaatiot. Riskitasot hyväksytään johdon katselmoinnissa.

3. TIETOVIRRAT

Tässä luvussa kuvataan, miten tietojen minimointi, käyttötarkoitussidonnaisuus ja säilytyksen rajoittaminen tietosuojaperiaatteina toteutuvat DigiFinlandin toiminnassa.

DigiFinlandissa on käytössä tiedon luokittelu ja tiedonluokittelun mukainen käsittely. DigiFinlandin toimintaan velvoittavaa lainsäädäntöä ei ole tältä osin, joten tiedon luokittelu on toteutettu yhtiö tarpeiden mukaan riskiperusteisesti. Luokittelu on julkinen, sisäinen ja salainen. Tämän avulla voidaan kohdentaa kuhunkin tietoryhmään vaadittava käsittely ja tietoturvataso. Lisäksi tiedon säilytysajat on määritelty, jonka avulla varmistutaan siitä, että tiedon elinkaarenhallinta täyttää sille määritellyt säilytysajat.

Tietojärjestelmät on kartoitettu ja ne on määritelty tietojärjestelmä listaan. Lisäksi tietojärjestelmä kohtaisesti on määritelty:

- käyttötarkoitus
- mihin toimintoon järjestelmä liittyy
- palvelutuotteen elinkaarenhallintaan liittyvä tärkeysluokka
- tietoturvataso (VAHTI perustaso, korotettu tai pilvipalveluturvallisuus)
- tiedon luokittelu (julkinen, sisäinen salainen)
- kelpuutus (kyllä, ei)
- vastuut: omistaja ja pääkäyttäjä
- sijainti

Palvelutuotannon osalta on kuvattu tietovirrat, lokitiedot, henkilötietojen suojausvelvoite, jäljitettävyys ja läpinäkyvyys. Nämä on kuvattu kunkin palvelutuotteen tietoturva, tietosuoja ja jatkuvuudenhallinta -dokumentissa.

Vuonna 2020 Tietoturvaryhmä toteutti DigiFinlandissa henkilörekisteri inventoinnin ja rekisterien vastuuhenkilöt nimettiin tiimeissä. Lisäksi tunnistettiin henkilötietoasisältävät tietojärjestelmät ja päivitettiin tietosuojaselosteet. Tietosuojan vaatimusten mukaisuuden mukaisiin tehtäviin otettiin käyttöön Tietosuoja.fi -työkalu.

Vuonna 2020 käynnistettiin työkalujen kartoitusprojekti, jonka tarkoituksena on selvittää yhtiössä ja hankkeissa olevat työkalut sekä luoda prosessi työkalujen käyttöönotolle. Näin vältetään päällekkäisten työkalujen käyttö yhtiön toiminnassa.

4. REKISTERÖIDYN OIKEUDET JA NIIDEN TOTEUTTAMINEN

Tässä luvussa kuvataan, miten rekisteröityjen oikeudet toteutuvat DigiFinland Oy:n toiminnassa kohtuullisuus ja läpinäkyvyys tietosuojaperiaatteina.

Palvelutuotannon tietoturva, tietosuoja ja jatkuvuudenhallintaohjeessa varmistutaan rekisteröidyn oikeuksien toteutumisesta hankkeissa ja ollessa henkilötietojen käsittelijän roolissa.

Vuonna 2020 toteutettiin DigiFinlandin tietosuojahallintamalli, jonka mukaisesti varmistutaan osoitusvelvollisuuden mukaisesta toiminnasta.

Vuonna 2020 toteutettiin Rekisterinpitäjille ohjeet: Rekisterinpitäjän ohje sekä liitteet suostumuksen edellytykset ja Rekisteröidyn oikeudet. Henkilöstön tietoturva ja tietosuojaohjeessa kuvataan henkilöstölle, mitä tarkoittaa rekisteröityjen oikeuksien toteuttaminen.

Vuonna 2020 toteutettiin yhtiön internetsivut: https://digifinland.fi/tietosuoja/. Sivuilta löytyy:

- yhtiön tietoturva- ja tietosuojakäytänteet
- rekisterinpitäjän ja tietosuojavastaavan yhteystiedot
- tietosuojaselosteet

Rekisteröityjä informoidaan henkilötietojen käsittelystä DigiFinlandin internet sivuilla olevilla tietosuojaselosteilla. Rekisteröity voi käyttää oikeuksiaan toimittamalla pyynnön rekisterinpitäjälle osoitteeseen digifinland@digifinland.fi

4.1 Mistä henkilötiedot saadaan ja mihin niitä siirretään?

Henkilöstön ja eri sidosryhmiin kuuluvien henkilötiedot saadaan pääsääntöisesti rekisteröidyiltä itseltään. Henkilötietoja voidaan siirtää sisäisiin palveluihin esim. työsuhteen hoitamiseksi käsiteltäviä henkilötietoja. Henkilökunnan tietoja luovutetaan toiselle rekisterinpitäjälle ainoastaan asianomaisen suostumuksella tai lainsäädännön perusteella.

DigiFinland ei siirrä henkilötietoja EU tai ETA maiden ulkopuolelle.

4.2 Tietosuojaan liittyvät sopimusmallit

DigiFinland on tunnistanut tilanteet, joissa se on rekisterinpitäjä tai henkilötietojen käsittelijä. DigiFinland tekee tietosuojasopimukset henkilötietojen käsittelijöiden kanssa ja on laatinut hankintoihin tietosuojasopimukset ja turvallisuussopimukset.

Tiedon laatu ja käytettävyys toteutuvat Digifinlandin toiminnassa mm. siten, että

- käsitellään vain käyttötarkoituksen mukaisia ajan tasaisia henkilötietoja
- käyttöoikeudet on määritelty käyttäjäroolien mukaisesti
- tietosuoja ja tietoturva huomioidaan henkilötietojen käsittelyssä
- ja sitä valvotaan organisatorisin menetelmin
- tietojen elinkaari on hallinnassa ja säilytysajat sekä hävittäminen

Vuonna 2020 aloitettiin Omaolon asiakasorganisaatioden tietosuojavastaavien kanssa Omaolon tietosuoja ja tietoturvan yhteistyö. Pidettiin kaksi saman sisältöistä palaveria. Palavereissa käytiin läpi Omaolon rekisterit ja todettiin, että rekisterinpitäjien ja henkilötietojenkäsittelijän sopimus on uusittava, jotta se on vaatimuksien mukainen. Lisäksi DigiFinland sai rekisterinpitäjien kommentit Omaolon vaikutuksenarvioon. Henkilötietojen käsittelysopimus uusittiin ja toimitettiin allekirjoitettavasi rekisterinpitäjille. Omaolon vaikutuksenarvio on päivitetty.

5. TIETOJENKÄSITTELYYN VAIKUTTAVA LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Tietosuoja-asetus ei edellytä rekisterikohtaisia selosteita, vaan tietosuojaselosteita rekisterinpitäjän käsittelytoimista sekä läpinäkyvää informointia henkilötietojen käsittelystä. DigiFinlandissa on tietosuoja-asetuksen artiklan 30 mukainen tietosuojaselostepohja, jota hyödynnetään eri käyttötarkoituksiin.

Lainsäädäntö:
EU:n yleinen tietosuoja-asetus EU 679/2016
Tietosuojalaki 5.12.2018/1050
Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivi
Laki yksityisyyden suojasta työelämässä (759/2004)
Laki sähköisen viestinnän palveluista (68/2018)
Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
Valmiuslaki 29.12.2011/1552

Tietoaineistojen käsittelyä ohjaavat mm. seuraavat dokumentit:
Tietoturva- ja tietosuojapolitiikka
Tietoturvasäännöt, -ohjeet ja -prosessit
Tiedonluokittelu- ja käsittelyohjeet
Tietosuojaselosteiden mallipohjat
Vaikutustenarvioinnin ohjeet ja mallipohjat

6. SEURANTA JA MITTAAMINEN

Tietosuojan ja tietoturvan tilaa DigiFinlandissa vuonna 2020 voidaan kuvata seuraavin tunnusluvuin.

Aihe	Määrä
Henkilötietojen tarkastus-, oikaisu- ja poistopyynnöt Tarkastuspyynnöt Oikaisupyynnöt Poistopyynnöt	1 kpl poistopyyntöä
Kieltäytymiset automaattisesta päätöksenteosta	0
Valvontaviranomaisten selvitys- ja tietopyynnöt	0
Tarpeelliset ilmoitukset valvontaviranomaiselle Tietoturvaloukkausilmoitukset	0
Käyttö- ja luovutuslokipyynnöt	0
Vakavat tietoturvapoikkeamat	0

Esille tulleet tietosuojarikkomukset ja niiden epäilyt	1
Tietojärjestelmien käyttökatkot ja niiden laajuudet	0
Tietojärjestelmien määrä	20 (13 sisätää henkilötietoja)
Harjoituksiin osallistuminen	1
Rekisterit	6
Auditoinnit	4
Koulutukset • Henkilötön tietoturva- ja tietosuojakoulutus • Johdon ja esimiesten tietoturvakoulutus • Palvelutuotannon tietoturva- ja tietosuojakoulutus	6

Sidosryhmäyhteistyön osalta DigiFinland on mukana seuraavissa tietosuoja- ja tietoturvaryhmissä:
Jenni Siermala Vahti Toiminnan jatkuvuudenhallinta asiantuntijaryhmä VPJ

7. VARAUTUMINEN ja JATKUVUUDENHALLINTA

DigiFinland osallistui vuonna 2020 TAISTO20 harjoitukseen. Harjoituksessa harjoitellaan tietoturvan ja tietosuojahallintaa erilaisten toiminnanjatkuvuutta uhkaavien tilanteiden vallitessa.

Vuonna 2020 harjoituksessa harjoiteltiin toimintaa, kun organisaation toimintaa uhattiin louhintahaittaohjelman avulla sekä valeuutisten vallitessa. Harjoitukseen osallistuttiin 12.11.2020. Osallistujat olivat Mirva Antila, Eila Neitola, Juhani Vuorijärvi, Jonna Piiroinen (harjoituksen kulun ja toimenpiteiden kirjaaminen), Laura Auvinen (tarkkailija), Jenni Siermala (harjoituksen ohjaaminen ja näyttövastaava) ja Anssi Virtanen. Lähtökohta oli osallistua harjoitukseen oppimisen näkökulmasta. Organisaatiomme on muotoutumassa ja tämä on erinomainen tapa kehittää toimintaa. Oli selvästi havaittavissa, että yhtiössä on kehitettävä varautumista ja jatkuvuudenhallintaa.

8. ARVIOINTI JA KEHITTÄMINEN

Vuonna 2020 toteutettiin käytännön toimet SoteDigi Oy:n ja Vimana Oy:n yhdistymistä varten. Yhtiössä toteutettiin laajasti muutoksia, jotta uusi monialainen toiminta otettiin käyttöön.

Vuotta 2020 kosketti maailman laajuinen koronavirus pandemia. Sen johdosta yhtiössä otettiin käyttöön laajasti etätyö. DigiFinlandissa tiedot luokitellaan julkinen, sisäinen, salainen. Luokittelu on riskiperusteinen. Salaiseksi luokitellun tiedon tallentamiseen otettiin

käyttöön tweb asianhallintajärjestelmä. Lisäksi yhtiölle tuli tehtäväksi rakentaa koronavilkkusovellukseen ammattilaisen käyttöliittymä, joka avustaa terveydenhuollon ammattihenkilöitä koronavirus tartuntaketjujen jäljittämistä. Tämän vuoksi DigiFinlandissa tiivistettiin toimintaa eikä edellisen vuoden 2019 tietotilinpäätöksen ja johtoryhmässä käsiteltyä esiselvityksen mukaista ISO22031 standardin mukaista jatkuvuuden ja varautumisenhallintaa jatkettu.

Tämän vuoksi on tärkeää saattaa jatkuvuudenhallinta ja varautuminen yhtiön tasolla vaatimusten mukaiseksi. Sen avulla varmistetaan yhtiön tarjoamien digitaalisten palvelujen jatkuvuudenhallinta ja yhtiön toiminnanjatkuminen kaikissa oloissa.

Monialaisessa yhtiössä on huomioitava tietoturvavaatimukset riskilähtöisesti. Sen vuoksi DigiFinlandissa tulee kehittää tietoturvavaatimuksia sen mukaisesti, että yhtiössä jokainen tietää mitä vaatimuksia hänen tulee noudattaa jokapäiväisessä työssään, hankinnoissa sekä palvelutuotannossa.

Jotta osaamisen vahvistamista tuetaan ja lisätään henkilöstössä, on yhtiöön hankittu koulutusjärjestelmä. Kaikki yhtiön koulutukset viedään tähän verkkokoutusympäristöön. Tietoturvan ja tietosuojan sitoutumista tuetaan lisäksi erilaisilla Teams ja mahdollisesti kasvokkain tapahtuvilla tietoturva- ja tietosuojakoulutuksilla sekä keskusteluilla.

Palvelutuotannon tietoturva-, tietosuoja ja jatkuvuudenhallintaohjeen toimeenpano hankkeissa on tarpeen vahvistaa. Jatkossa on tarpeen kasvattaa hankkeen sisällä tietoturvan, tietosuojan ja jatkuvuudenhallintaa, jotta aidosti toteutuu sisäänrakennettu tietoturva- ja tietosuoja sekä palvelut toimivat kaikissa tilanteissa.