JULKINEN

TIETO-TILINPÄÄTÖS

Vuosi 2023

TIIVISTELMÄ

Kempeleen kunnan tietotilinpäätös vuodelle 2023.

Tietohallintopäällikkö

Sisällys

ESIPUHE

Digitaalinen aikakausi, erilaiset organisaationaaliset muutokset ja globaalit tapahtumat asettavat kunnan tiedonhallinnalle ja digiturvallisuudelle haasteita, jotka vaativat valppautta ja sopeutumista muuttuvassa ympäristössä. Digiturvallisuus vaatii niin hallinnollisten prosessien ja toimintamallien kehittämistä, taloudellisia panostuksia kuin uusien toimintatapojen ja teknologioiden omaksumista henkilöstöltä, jotta väistämättömässä muutoksessa voidaan ylipäätään pysyä mukana ja uhkiin löytää riittävän tehokkaita torjuntakeinoja.

Digitaalisen aikakauden erityispiirteitä ovat ulkoiset nopeasykliset ja monimuotoiset muutokset, jotka vaikuttavat kunnan toimintaan ja palveluihin. Uusien teknologioiden ja palveluiden käyttöönoton prosessit ovat tehty erittäin helpoksi loppukäyttäjille, mitkä aiheuttavat haasteita tiedonhallinnan suunnitelmalliselle kehittämiselle. Samalla, kun vanhoja teknologioita ajetaan alas, uutta teknologiaa otetaan käyttöön. Palveluiden hankinnoissa tuleekin pitää mielessä sanonta ”maltti on valttia”, jotta kaikki siihen liittyvät osa-alueet vaikutuksineen pystytään huomioimaan kuntaorganisaation toiminnassa.

Vuoden 2023 alussa voimaan tulleen lainsäädännön myötä hyvinvointialueet irtautuivat kuntien ja kaupunkien toiminnasta prosessiensa ja henkilöstönsä osalta. Kempeleen kunnan sosiaali- ja terveyspalveluihin kuuluvien ICT-palveluiden tuottamista jatkettiin hyvinvointialue Pohteelle ja siirtymätyö hyvinvointialueen omaan ICT-ympäristöön jatkuu edelleen myös vuoden 2024 aikana. Tämän merkittävän siirtymäprojektin kaikkia esiin tulevia muutostarpeita on ollut vaikea ennakoida etukäteen ja se on aiheuttanut paineita työn organisoimiselle ja viestinnälle. Kempeleen kunta on pyrkinyt tarjoamaan ICT-palvelut käytettävissä olevien resurssiensa puitteissa sosiaali- ja terveydenhuollon henkilöstölle, joka on joutunut taiteilemaan useiden eri IT-palvelutuottajien palveluviidakossa.

Venäjän vuonna 2022 aloittama hyökkäyssota Ukrainaan jatkuu edelleen ja se aiheuttaa haasteita myös eurooppalaisille valtioille esimerkiksi digiturvallisuuden näkökulmasta. Erilaiset tietojenkalastelujen kampanjat, hybridisodankäynnin keinot, informaatio-vaikuttaminen ja palvelunestohyökkäykset ovat läsnä myös suomalaisessa digiarjessa. Koko kuntaorganisaation henkilöstön tulee huomioida omassa toiminnassaan arjen digiturvallisuuden näkökulmat. Olennaisessa osassa on työntekijöiden tietoisuus vallitsevista riskeistä, kiinnostus digiturvalliseen toimintaan omassa työssä ja digiturmien torjuntakeinojen hyödyntäminen. Digiturvallisuus kuuluu meille kaikille.

Kokonaisuutena kunta pyrkii varmistamaan digiturvallisuuden ja tietosuojan toteutumisen haasteellisessa ympäristössä. Kiitän henkilöstöämme pyrkimyksistä tässä muutoksia värittäneessä vuodessa 2023.

Digiturvaterveisin,

Tietohallintopäällikkö, Kempeleen kunta

1. Johdanto

Korkealaatuinen tieto sekä toimivat menettelyt tietojen käsittelyssä ja digiturvassa vaikuttavat positiivisesti koko organisaation toimintaan. Hyödyntämällä tietoa voidaan luoda uudenlaisia palveluja tai kehitetään nykyisten tuottamaa arvoa. Uutta tietoa voidaan kerätä uusia teknologisia ratkaisuja ja palveluita käyttöönottamalla. Tieto tulee aina myös suojata riittävän tehokkaasti tietoteknisin ja hallinnollisin keinoin, jotta perusteeton pääsy ja tiedon hyödyntäminen voidaan estää.

Tietotilinpäätöksen tehtävänä on organisaation tietoturvan, tietosuojan ja tiedonhallinnan tilannekuvan tarjoaminen. Tietotilinpäätös osoittaa osaltaan, että organisaatiossa noudatetaan tiedonhallintaan, tietosuojaan ja tietoturvaan liittyviä lakeja ja määräyksiä. Tietotilinpäätöksessä kuvataan myös henkilötietojen käsittelyyn ja digiturvallisuuteen liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuoja- ja digiturvatyön tekemistä ja lisätä tekemisen vaikuttavuutta arjessa.

Kempeleen tietoturvan ja tietosuojan toteutusta ohjataan erityisesti kunnan tietoturvapolitiikan avulla. Kuntaan tulevien uusien työntekijöiden tulee allekirjoittaa tietoturva-, tietosuoja ja salassapitositoumus osana virka- tai työsopimusta. Tietoturva- ja tietosuojatyötä tarkastellaan toistuvammin kunnan tietoturvaryhmässä. Tietoturvan asiantuntijana toimii nimetty tietoturvavastaava ja tietosuojan asiantuntijana nimetty tietosuojavastaava. Kempeleen kunnan tietotilinpäätöksen 2023 laadintaan ovat osallistuneet tietoturvavastaava, tietosuojavastaava ja tietohallintopäällikkö.

2. Riskien, tietoturvan ja tietosuojan hallinta

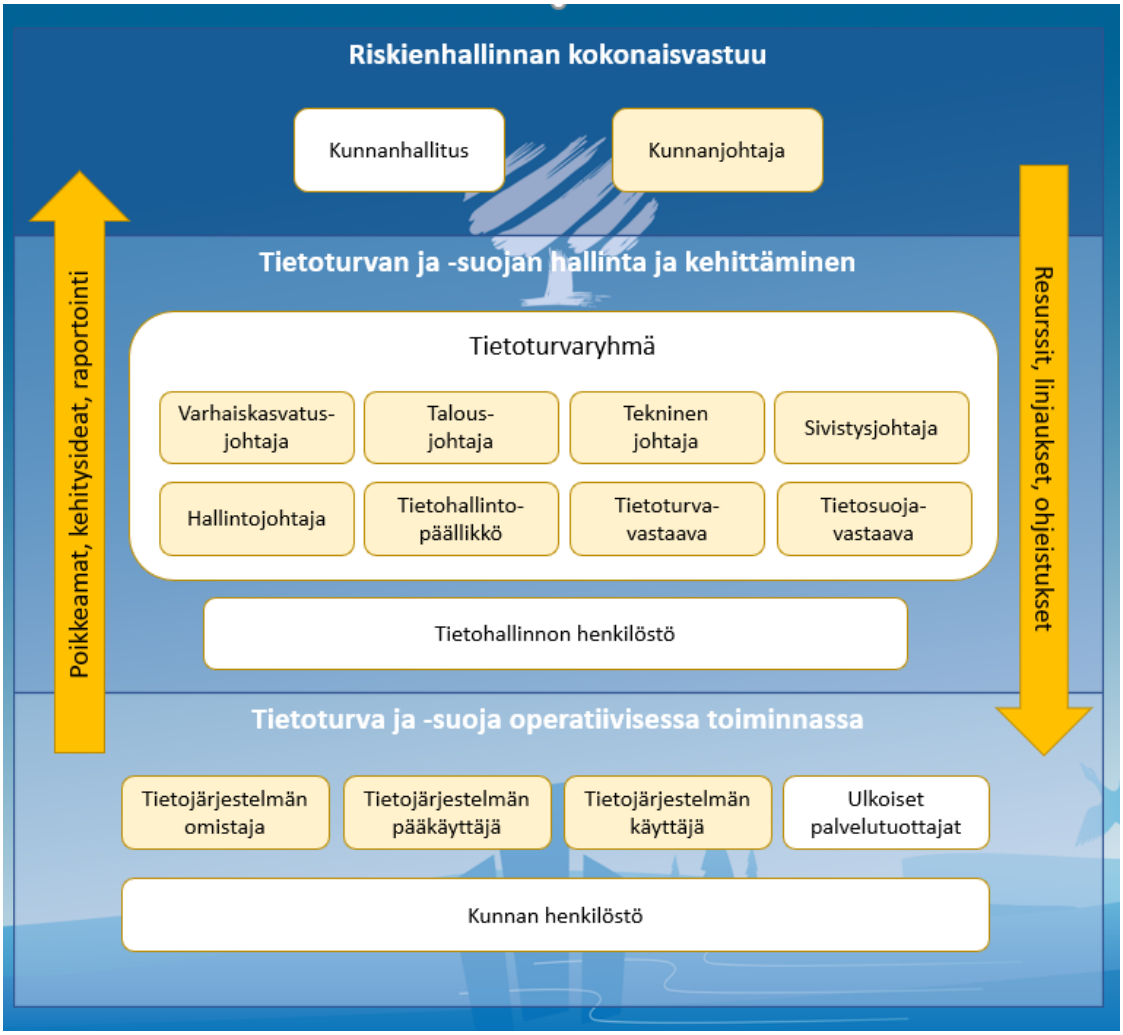
Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä on vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, käytönvalvontaa, pääsynhallintaa, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytännesääntöjen sekä sertifikaattien käyttöä.

Kempeleen kunnan ohjeistuksen mukaan sisäisen valvonnan ja riskienhallinnan asianmukainen järjestäminen koskee kaikkia kunnan ja kuntakonsernin toimielimiä ja tilivelvollista johtoa. Sisäinen valvonta on osa kuntakonsernin johtamisjärjestelmää sekä kunnan poliittisen johdon, viranhaltijajohdon ja hallinnon työväline, jonka avulla arvioidaan asetettujen tavoitteiden toteutumista, toimintaprosesseja ja riskienhallinnan tuloksellisuutta sekä vaikuttavuutta. Valvonnan tarkoituksena on edistää organisaation tehokasta johtamista, riskien hallintaa ja toiminnan tuloksellisuuden arviointia sekä vahvistaa hyvää johtamis- ja hallintotapaa.

Kempeleen kunnassa on käytössä tietoturvapolitiikka, joka on hyväksytty kunnanhallituksessa vuonna 2021. Tietoturvapolitiikassa määritellään tietoturvatyön tavoitteet ja strategiset

painopisteet, tietoturvaviestinnän periaatteet, organisointi ja vastuut, tietoturvan ja tietosuojan varmistamisen periaatteet hankinnoissa sekä arviointi- ja seurantamenetelmät.

Kunnanhallituksen ja -kunnanjohtajan vastuulla on riskienhallinnan kokonaisvastuu ja poikkeus-, erityis- ja kriisitilanteissa toimimisen edellytysten varmistaminen (katso kuva 1). Kunnanhallitus ja kunnanjohtaja vastaavat tietoturvan sekä tietosuojan resursoinnista, linjauksista ja yleisten ohjeistuksien antamisesta.



Kuva 1. Riskienhallinnan kokonaisvastuu sekä tietoturvan ja tietosuojan hallinta.

Tietoturvaryhmän tarkoituksena on käsitellä tietoturvan linjaukset ja ohjeet ennen kuin ne pannaan toimeen operatiivisessa toiminnassa. Tietoturvaryhmä voi pyytää tarvittaessa tarkennuksia ja linjauksia kunnanhallitukselta ja -johtajalta. Ryhmä arvioi myös tietoturvan ja tietosuojan tason ja toteutuksen sekä käsittelee esiin tulleet poikkeamat. Tietohallinnon henkilöstö kehittää omalta osaltaan tietoturvaa ja tietosuojaa teknologian ja toimintamallien avulla käytännön työssä ja operatiivisessa ympäristössä. Tietosuojavastaava tuottaa tietosuojaan liittyvää informaatiota tietoturvaryhmälle päätöksentekoa varten.

Operatiivisella tasolla tietoturvaa toteuttavat tietojärjestelmien omistajat, pääkäyttäjät, käyttäjät ja kunnan henkilöstö, jotka ovat toimintansa osalta tekemisissä henkilötietojen kanssa ja huolehtivat tietoturvasta sekä tietosuojasta omassa toiminnassaan. Operatiiviseen toimintaan liittyvien ulkoisten palvelutuottajien kanssa sovitaan toimintatavoista ja säännöistä henkilötietojen käsittelyyn liittyen palvelusopimuksien ja ohjeistuksien kautta.

Tietohallintopäällikkö vastaa kunnan tietojärjestelmäkokonaisuudesta sekä tietoturvaan liittyvästä viestinnästä kunnassa. Tietohallinto vastaa poikkeamatilanteisiin ja pyrkii palauttamaan toiminnan normaaliksi poikkeamatilanteissa. Tämän lisäksi tietohallinto ehkäisee poikkeavien tilanteiden syntymistä tietoverkon ja laitteiston seurannan ja muiden ennalta ehkäisevien teknisten ja hallinnollisten toimien avulla.

Kempeleen kunnan tietosuojavastaavan tehtävät on ulkoistettu Joki ICT Oy:lle, joka on kunnan osaomistuksessa. Tietosuojavastaavan tehtävänä on valvoa tietosuojan toteutumista kunnan toiminnassa. Tietosuojavastaava tekee yhteistyötä palvelualueiden kanssa henkilötietojen käsittelytoimien suunnittelussa sekä tietohallinnon kanssa tietosuojan huomioimiseksi tietoteknisissä toimissa. Palvelualueet vastaavat hyvin itsenäisesti henkilötietojen tarkastus- ja korjauspyyntöihin kunnassa ja tietosuojavastaava antaa neuvoja haastavimmissa kysymyksissä.

Kuntaan nimetyn tietoturvavastaavan tehtävänä on kehittää tietoturvaa, valvoa sen toteutusta sekä edistää tietoturvatietoutta tietohallintopäälliköltä saamiensa resurssien ja toimintavaltuuksien puitteissa. Tietoturvavastaava osallistuu yhdessä tietosuojavastaavan kanssa kunnan turvallisuus-, tietoturva- ja tietosuoja-asioiden kokonaisuuden koordinointiin.

3. Tilannekuva

3.1 Lainsäädäntö

Tiedonhallintalain mukainen asiakirjajulkisuuskuvaus on julkaistu kuntalaisille kunnan internet-sivulle. Tiedonhallintalain mukaista tiedonhallintamallia, joka kuvaa kunnan digitaalista toimintaympäristöä, ylläpidetään ja hallitaan Digiturvamalli-palvelussa. Tiedonhallintalain vaatimukset on huomioitu tietojärjestelmien hankinnassa ja palveluiden tarjoamisessa.

Kempeleen kunta ylläpitää henkilötietorekistereiden tietosuojaselosteita verkkosivuillaan, josta ne ovat kuntalaisten ja muiden rekisteröityjen nähtävissä. Näin kunta toteuttaa informointivelvoitettaan rekisteröidyille. Rekisteröity voi halutessaan olla yhteydessä rekisterin yhteyshenkilöön, vastuuhenkilöön tai tietosuojavastaavaan. Rekisteröidyillä on mahdollisuus jättää henkilötietojensa tarkastus- ja korjauspyyntö kunnan kirjaamon kautta www-sivuilta löytyvien lomakkeiden avulla tai suoraan palvelun yhteydessä.

Euroopan Unionin NIS2-direktiivi on tullut voimaan 2023 vuonna. Kansallisia lainsäädännön muutoksia ei ole vielä tullut toteuttavaksi kuntatasolle. Direktiivin tarkoituksena on päivittää erilaisia kyberturvallisuussäännöksiä esimerkiksi tietoverkkoon liittyen.

Joulukuussa 2023 tuli voimaan Euroopan Unionin ”The AI Act” tekoälysäädös, jonka tarkoituksena on asettaa rajoituksia tekoälyn väärinkäytölle ja ennaltaehkäistä käytöstä syntyviä riskejä. Tätä säädöstä ei vielä kuitenkaan käsitelty kansallisella tasolla.

3.2 Toimintaprosessit, tietovarannot ja tietojärjestelmät

Kempeleen kunnan toiminta perustuu pääosin lainsäädäntöön, jossa kuntaa velvoitetaan tuottamaan palveluita kuntalaisille. Palvelun tuottamiseksi kunta käyttää hyväkseen erilaisia sidosryhmien, kuten viranomaisten, rekistereitä ja luovuttaa myös itse tilastotietoja viranomaisten käyttöön.

Henkilötietojen lähteitä Kempeleen kunnalle ovat kuntalaiset, kuntalaisten huoltajat, omaiset tai edunvalvojat, työnhakijat, yrittäjät, väestörekisterikeskus, asemakaava, eläketurvakeskus, eläkeyhtiöt, kameravalvonta, Kansaneläkelaitos, kiinteistörekisteri, Opetushallitus, lääkärintodistukset, ostopalveluiden tuottajat, poliisi, työnantajat, työtoimintapaikat, työvoimatoimisto ja veroviranomaiset. Kempeleen Kunta luovuttaa tietoja säännönmukaisesti Kansaneläkelaitokselle, KEHA-keskukselle, Opetushallitukselle, pankeille (maksatustietoja), perintätoimistoille, rakennuslupahankkeiden sidosryhmille, tilastokeskukselle ja Ylioppilaslautakunnalle.

Kempeleen kunta toteuttaa palveluitaan 44 erilaisen toimintaprosessin kautta. Kunnan prosesseista, tietovarannoista, tietoaineistoista ja tietojärjestelmistä on muodostettu tiedonhallintamalli, joka kuvaa kunnan tiedonhallintaa.

Kunnalla on hallussaan 57 erilaista palvelualueisiin liittyvää, henkilötietoja sisältävää tietovarantoa. Suurin osa kunnan toteuttamasta henkilötietojen käsittelystä tapahtuu 72:n käytössä olevan tietojärjestelmän avulla. Henkilötietojen hallinta perustuu olennaisesti ulkoisten palveluntarjoajien ja henkilötietojen käsittelijöiden tekemään työhön. Kempeleen kunta varmistaa asianmukaisen henkilötietojen käsittelyn erityisesti hankintojen yhteydessä asetettavin sopimusehdoin.

Alla olevassa taulukossa on kuvattu yhteenveto avainluvuista tiedonhallintamallista.

	Vuosi 2023
Toimintaprosesseja	44
Tietovarantoja	57
Tietoaineistoja	217
Tietojärjestelmiä	72
Tietojärjestelmätoimittajia	69

3.3 Toimintavuoden merkittävimmät muutokset

Vuoden 2023 alusta alkaen sosiaali- ja terveyspalvelun toimintaprosessit siirtyivät hyvinvointialue Pohteelle. Samassa yhteydessä toimintaprosesseihin liittyviä tietojärjestelmiä, ohjelmistoja, tietoliikenneliittymiä, palveluita ja laitteistoja on siirretty siirtosopimuksin hyvinvointialue Pohteen hallinnoitavaksi. Osa tietoteknisistä ratkaisuista jatkaa edelleen Kempeleen kunnan ICT-palveluiden tuottamisvastuulla siihen saakka, kunnes siirtymäprojektit ovat saatu toteutettua loppuun. Muutoksen myötä kahden organisaation välisessä viestinnässä ja toimintamallien yhteensovittamisessa on ollut haasteita, jotka ovat aiheuttaneet ylimääräitä työtä niin kunnan tietohallinnolle kuin Pohteen ICT-palvelutuottajille ja loppukäyttäjille.

Vuoden 2023 kesällä Kempeleen kunta teki hankintapäätöksen uudesta maankäytön toiminnanohjausjärjestelmästä Kuntien Tiera Oy:ltä. Käyttöönottoprojekti käynnistyi vuoden 2023 syksyllä ja tavoitteena on saada uusi järjestelmä käyttöön vuoden 2024 aikana. Uusi toiminnanohjausjärjestelmä korvaa vanhentuneen maankäytön järjestelmäympäristön.

3.4 Tietoturva- ja tietosuojahavainnot

Kempeleen kunnan tietoturvatyöryhmä kokoontui vuoden 2023 aikana kaksi kertaa. Kokouksissa käsiteltiin tietoturvan ja tietosuojan yleistilannetta ja poikkeamia, tietoturvan

kehittämistoimenpiteitä sekä tietoturvavastaavan ja tietosuojavastaavan havaintoja huomioita tietoturvaan ja tietosuojaan liittyen.

Vuoden 2023 aikana tietohallinto rekisteröi yhteensä 31 tietoturvahavaintoa eri lähteistä, kuten kunnan työntekijöiltä ja palvelutoimittajilta tulleista ilmoituksista sekä oman seurannan kautta. Rekisteröidyt tietoturvahavainnot ovat luokiteltu seuraavassa taulukossa:

Havainnon luokka	**Määrä**
Laitteeseen liittyvä	3
Ohjelmistoon liittyvä	8
Toimintatapaan liittyvä	3
Muu	17
Yhteensä	**31**

Merkittävimmät tietoturvahavainnot liittyivät tietojärjestelmissä oleviin käyttäjärekisterien käyttöoikeuksiin, joista on ilmoitettu ohjelmistotoimittajille. Lisäksi toimintavuoden aikana tapahtui yksi kunnan toimintaan vaikuttava tietoliikenteen häiriötilanne. Vuoden 2022 aikana tietoturvahavaintoja kirjattiin 39 kappaletta. Arvio tietoturvan yleistilanteesta on hyvä.

Tietosuojavastaavan palvelutuottaja Joki ICT Oy:n palveluun nimetty henkilö vaihtui toimintavuoden aikana.

Tietosuojavaltuutetulle on tehty yksi ilmoitus vuonna 2023 koskien sähköpostin lähettämistä väärään osoitteeseen.

Tietosuojavastaavalle on tullut kaksi kirjallista kysymystä. Toinen kysely tuli rekisteröidyltä koskien omien potilastietojen luovuttamista ja toinen kunnan työntekijältä koskien tietojen siirtoa. Puhelimitse tulleita yhteydenottoja ei ole kirjattu.

Tietosuojavastaavalle ei ole tullut pyyntöjä osallistua tietosuojan vaikutustenarvioiden laatimiseen vuonna 2023. Digitaalisen palvelun kartoittamisen yhteydessä on käyty läpi Joki ICT:llä tehtyjä tietosuojan vaikutusten arviointeja yhdessä kunnan ja tietosuojavastaavan kanssa.

4. Kehittämistoimenpiteet

4.1 Toteutetut toimenpiteet

Digiturvallisuutta on kehitetty opetushenkilöstön työpuhelinten hallintaa laajentamalla laitteiden uusinnan yhteydessä. Opetushenkilöstön työpuhelimissa käytettävissä olevat sovellukset ja asetukset ovat tietokoneiden tapaan hallittavissa keskitetyn hallintajärjestelmän kautta.

Henkilöstön tunnusten tietoturvavaatimuksia on tiukennettu tunnistautumiseen liittyen. Salasanojen vaatimuksia on muutettu (esim. pituus) ja monivaiheista tunnistautumista otettu käyttöön henkilöstössä. Tietohallinto on lisäksi suorittanut täsmäviestintää arjen digiturvataitoihin liittyen ja tavoitteena on jatkaa säännönmukaista viestintää ennalta suunnitelluissa aihealueissa. Täsmäviestintää on tehty esimerkiksi salasanakäytänteisiin ja kalasteluviestiepäilyksissä toimimiseen liittyen.

Palomuuri on uusittu palvelutuottajan vaihdoksella sekä infran palveluita on ajettu alas osana konesalipalveluiden siirtymistä palvelutuottajalle. Palomuurin uusinnan myötä käyttäjien

kirjautumistapahtumia ja liikennettä saadaan logitettua paremmin. Infrapalveluista on ajettu alas palveluita, joiden käyttö on vähäistä ja teknologia vanhentunutta.

WhistleBlower-direktiiviä varten hankittu väärinkäytösten ilmoituskanava. Tietoliikenteen valvontapalvelun pilotointiprojektiin osallistuttu yhteistyössä kansallisen toimijan kanssa. Toimialueympäristön kartoitus toteutettu yhteistyössä ulkoisen kumppanin kanssa tietoturvan kehittämiseksi. Kartoituksen myötä on saatu toimenpidelistaa infran ja palveluiden tietoturvan kehittämistoimenpiteille. Osa toimenpiteistä on toteutettu aikataulun mukaisesti toimintavuoden aikana ja osa toimenpiteistä tehdään vuoden 2024 aikana.

Kunnan tietohallinto osallistunut digiturvallisuutta parantaviin projekteihin ja harjoituksiin niin paikallisesti (Digityy) kuin kansallisella tasolla (TAISTO23) ja suorittanut tietoturvatestausta omaan ympäristöön ja henkilöstölle (FISU-hanke). Projektien ja harjoituksien kautta on saatu lisää tietoa ja kokemusta prosesseista, menetelmistä ja työvälineistä digiturvallisuuden parantamiseksi niin hallinnollisella kuin operatiivisellakin tasolla.

4.2 Tunnistetut toimenpiteet

Kunnan tietohallinnossa on tunnistettu seuraavia digiturvallisuuden kehittämiseen liittyviä kohteita ja toimenpiteitä:

- Ratkaisun hankinta tietoturvallisuuden parantamiseen
- Ratkaisun hankinta tietoturvauhkien havaitsemiseen ja torjuntaan
- Tietoliikenneverkon liikenteen ohjaukset ja rajoitukset
- Pääsynhallinnan jatkokehittäminen
- Digi- ja toimintaympäristön dokumentaation päivittäminen
- Tekoälykäyttöön liittyvät periaatteet ja ohjeistukset
- Kameravalvontaan liittyvät periaatteet ja ohjeistukset
- Teknologioiden ja palveluiden korvaaminen uusilla tai vaihtoehtoisilla tavoilla