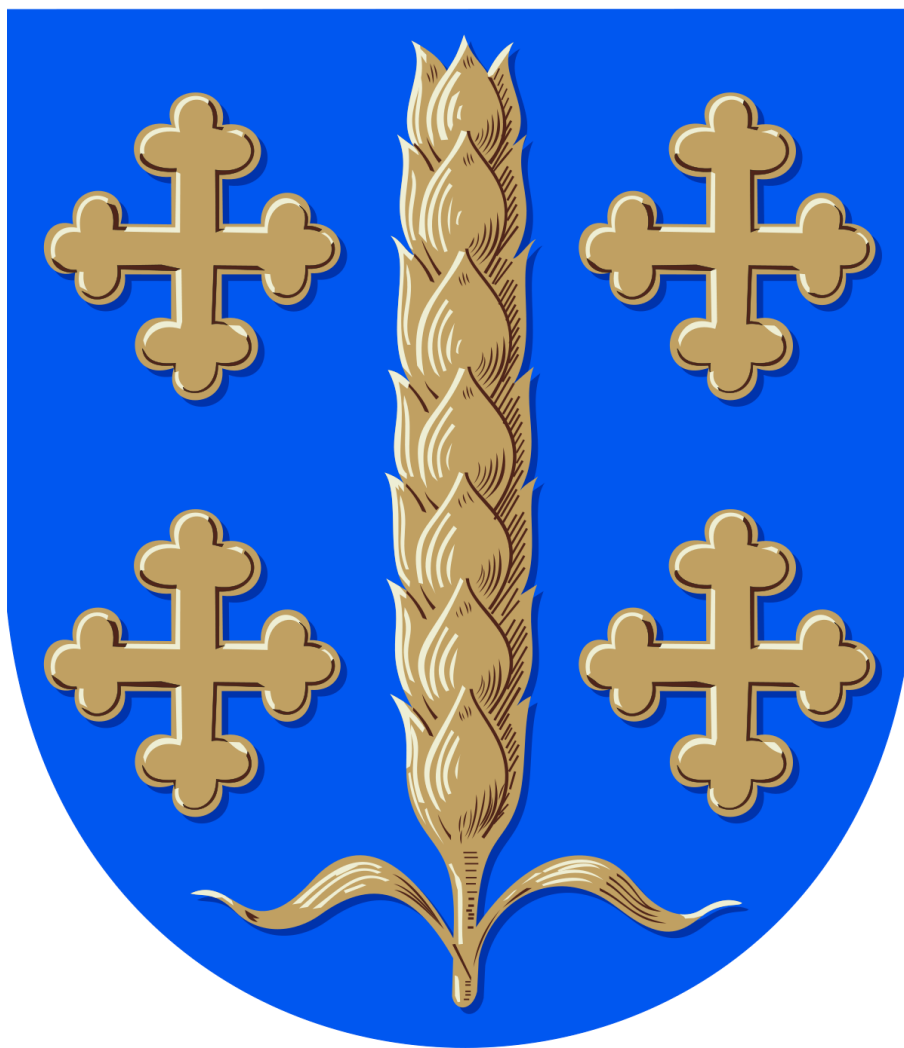


TIETOTILINPÄÄTÖS 2021



Jari Suvila, tietosuojavastaava

jari.suvila@loimaa.fi

Sisällys

TAUSTAA.....	3
Tietotilinpäättös.....	3
Tietoturvaloukkaukset.....	3
TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN	4
SEURANTA JA TIETOTURVALOUKKAUKSET.....	5
1. Verkkohyökkäys vaikeuttaa toimintaa	5
2. Palvelunestohyökkäys julkiseen oppilasverkkoon.....	5
3. Opiskelijan tunnus väärässä roolissa.....	5
4. Microsoft tuen yhteydenotot.....	6
5. Pankkitunnusten kalastelut.....	6
6. Päivitetyt tietoturvaselosteet.....	6
7. Valmiusharjoitus.....	6
8. Tietosuoja-asiaa Teho-ITssä.....	6
9. "Digitaalisen turvallisuuden edistäminen kuntien toiminnan ja johtamisen jatkuvuuden varmistamiseksi"	6
10. Tietosuojavastaavan koulutusohjelma.....	7
LÄHTEET.....	7

TAUSTAA

Tietotilinpäätös

Loimaan tietotilinpäätöksessä kuvataan tietosuojan ja -turvan tilannetta vuonna 2021. Tilinpäätökseen on koottu toimenpiteitä tietoturvan toteuttamisesta käytännössä ja mitä uusia toimenpiteitä on otettu käyttöön kuluvana vuonna. Lisäksi käydään läpi, onko mahdollisia tietoturvaloukkauksia tapahtunut ja mitä toimenpiteitä nämä ovat aiheuttaneet.

Tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, niitä luovutetaan eteenpäin ilman lupaa tai niihin pääsee käsiksi taho, jolla ei ole oikeutta kyseisiin tietoihin.

Esimerkkejä tietoturvaloukkauksista ovat esimerkiksi

- Toisen henkilön potilastietojen tarkastelu ilman hoitosuhdetta
- Kadonnut muistitikku, joka sisältää henkilötietoja tms. arkaluontoista tietoa
- Hakkerointi
- Haittaohjelmatartunta

Tietoturvaloukkauksiin on kyettävä reagoimaan nopeasti ja tämän vuoksi onkin laadittava toimintaohjeet mahdollisia tietoturvaloukkaustilanteita varten.

Rekisterinpitäjän tulee arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu, esimerkiksi

- Ei riskiä
- Aiheutuu riski
- Aiheutuu korkea riski

Toimenpiteet tietoturvaloukkauksen jälkeen riippuvat riskin tasosta, mutta kaikki loukkaukset tulee dokumentoida.

Mikäli tietoturvaloukkauksesta aiheutuu riski luonnollisten henkilöiden oikeuksille ja vapauksille, tulee tietosuojavaltuutetun toimistoon tehdä ilmoitus 72 tunnin kuluessa. Ilmoitus tehdään sähköisellä lomakkeella (<https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta>). (<https://tietosuoja.fi/tietoturvaloukkaukset>)

TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Loimaan kaupungille on laadittu tietoturvapoliittika. Tiedon turvaaminen on tärkeä osa kaupungin toiminnan ja sen järjestämien palvelujen laatua. Tietoturvan hyvä hallinta edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja resursointia erilaisten uhkatilanteiden varalta. Tietoturvan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää. Tietoturvapoliittika määrittelee Loimaan kaupungin tietoturvan tavoitteet, vastuut, tietoturvyön organisoinnin ja toteutuskeinot. Se kuvaa myös seurannan ja tiedottamisen yleisperiaatteet.

Henkilöstölle on laadittu tietoturvaohje, joka löytyy verkkolevyllä (L:\tietopankki\Tietohuolto\Tietoturvyöryhmä\dokumentit\Henkilöstön tietoturvaohje.pdf). Ohjeessa otetaan kantaa mm. toimitilaturvallisuuteen sekä tunnuksiin ja salasanoihin. Tietoturvaohje päivitettiin vuonna 2020.

Varhaiskasvatuksen ja perusopetuksen henkilöstölle on laadittu erillinen tietosuojaohje.

Käyttäjiä on aiemmin ohjeistettu tekemään Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) toteuttama Arjen tietosuojan nettitestin (<https://arjentietosuoja.fi/fi/#/quiz>). Tämän ohjeistuksen noudattamista tulee jatkaa myös uusien työntekijöiden kohdalla.

Tietosuojaoselosteet löytyvät kaupungin kotisivuilta.

Salatun sähköpostin lähetyks on ollut käytössä jo useamman vuoden. Kaupungin sisällä liikkuva posti (loimaa.fi -> loimaa.fi) on aina salattua, mutta ulkopuolisille tahoille lähetävä sähköposti, joka sisältää arkaluonteista tietoa, tulee salata F-Securen suojausratkaisulla. Ohje salaukseen löytyy verkkolevyllä, johon kaikilla on pääsy. (L:\tietopankki\Tietohuolto\ATK-opaat ja ohjeet\sähköposti\Salatun sähköpostin lähettäminen.pdf)

Kaupungissa on käytössä suurissa monitoimilaitteissa turvatulostus. Tulostettaessa työasemalta monitoimilaitteelle, pitää käyttäjän mennä fyysisesti laitteen luokse ja heilauttaa kulkuläpyskäänsä lukijan luona. Vasta tämän jälkeen tulostustyö tulostuu paperille.

Arkaluonteiset tiedostot tallennetaan omalle verkkolevyllä, jossa pääsyoikeuksia on jaettu kansiokohtaisesti. Lisäksi tiedostojen käytöstä muodostuu käyttöloki.

Esimiehillä on käytössä kaksivaiheinen tunnistautuminen tietoturvan korottamiseksi. Kaksivaiheista tunnistautumista laajennetaan hyvinvointialueen toteuduttua.

Maaseutupalveluissa tietoturva-asioissa toimitaan oman kuvion mukaisesti. Maaseutupalveluissa noudetaan Ruokaviraston sanelemaa ISO-Standardia ja sen mukaisesti laaditaan omat asiakirjat.

Kaupunki on hankkinut Luuppi-tietosuoja palvelun (Cloudpoint), jolla hallitaan opetuksessa käytettävien tietoteknisten sovellutusten ja palveluiden tietosuojariskiä.

SEURANTA JA TIETOTURVALOUKKAUKSET

1. Verkkohyökkäys vaikeuttaa toimintaa

19.2.2021 havaittiin verkkohyökkäys, jolla oli vaikutusta organisaation tietoliikenteeseen. Hyökkäyksen johdosta rajoitustoimenpiteet on aloitettu klo 14. Tilanteeseen reagoitu palauttamiseksi mutta verkon käyttöä ei hallinnollisesti eikä ohjeistuksellisesti estetty.

Oppilas oli saanut selville salasanoja. Hän on ollut yhteyksissä ulkopuolisiin tahoihin ja oli suunnitellut mahdollista hyökkäystä. JMJ pingiltä saatiin tieto, että kouluverkkoon yritettiin murtautua.

Oli juuri alkamassa hiihtolomaviikko. Päätimme alas ajaa verkon viikonlopuksi. Loppujen lopuksi verkko oli alhaalla koko hiihtoloman ajan.

Henkilökunta informoitiin laajalla jakelulla asiasta.

Asiasta pidettiin palaveria ja totesimme asian olevan likipitään rikosasia. Päätimme jäädä seuraamaan tilannetta ja rikosasiaa ei asiasta tehty.

2. Palvelunestohyökkäys julkiseen oppilasverkkoon

12.11.2021 iltapäivällä oppilasverkkoa kohtaan hyökättiin laajasti ja voimalla rajoitetun ajan. Tavoitteena lienee ollut estää verkon käyttö. Hyökkäys loppui ja tilanne normalisoitui. Tilannetta tutkittiin ja saatiin hyökkäystavasta kattavasti tietoa. Tilannetta jäätettiin seuraamaan.

Riskiarvion tekemisen jälkeen todettiin, että tietoturvaloukkausta ei ollut tapahtunut tai se todettiin niin vähäiseksi, että ilmoitusta tietosuojavaltuutetun toimistoon tai rikosilmoitusta poliisille ei tehty.

3. Opiskelijan tunnus väärässä roolissa

Perhekoti ilmoitti 30.11, että heiltä postia lähetettäessä lähtee posti erään opiskelijan nimissä. Asiaa tutkittaessa ilmeni, että perhekodilla olisi ollut mahdollisuus nähdä Wilmassa olevia opiskelijan tietoja. Lokitietoja tutkittaessa selvisi, että näin ei ollut tapahtunut eikä siis tietoturvuoto ollut tapahtunut.

Asiakokonaisuuden kuvio on selvillä ja koostuu yhteensattumista sekä inhimillisistä tekijöistä. Tahallisuudesta ei ole merkkejä. Asianosaisia on informoitu sekä tarvittavat muutokset on tehty.

Tapahtumalla on vaikutusta toiminnan kehittämiseen. (käyttöoikeuksien tarkempi määrittely)

Riskiarvion tekemisen jälkeen todettiin, että tietoturvaloukkausta ei ollut tapahtunut tai se todettiin niin vähäiseksi, että ilmoitusta tietosuojavaltuutetun toimistoon tai rikosilmoitusta poliisille ei tehty.

4. Microsoft tuen yhteydenotot

Henkilöstöä on lähestytty pitkin vuotta naamioituneena Microsoftin tukeen. Kieli on ollut englanti. Asian tullessa ilmi, on henkilöstöä tiedotettu laajalla jakelulla.

Tiedossa ei ole soitoista aiheutuneita seuraamuksia.

5. Pankkitunnusten kalastelut

Henkilöstöltä on eri tavoin pyritty saamaan pankkitietoja luovutetuksi. Asian tullessa ilmi, on henkilöstöä tiedotettu laajalla jakelulla.

Tiedossa ei ole kalasteluista aiheutuneita seuraamuksia.

6. Päivitetyt tietoturvaselosteet

Henkilömuutosten sekä puhelinnumeroiden muuttumisen vuoksi tietosuojaselosteet on käyty lävitse syksyn aikana. Samassa yhteydessä tietosuojavaltuutetun toimistoon on ilmoitettu ajantasaiset tiedot.

7. Valmiusharjoitus

Johtoryhmän sekä tietohuolto osallistui valtakunnalliseen Taisto -harjoitukseen 18.11.2021.

8. Tietosuoja-asiaa Teho-ITssä

Miten tietosuoja vaikuttaa arjen toimeen Sotessa -keskustelua käytiin Tietosuojavaltuutetun laatiman oheistuksen pohjalta. 3.12.2021

9. "Digitaalisen turvallisuuden edistäminen kuntien toiminnan ja johtamisen jatkuvuuden varmistamiseksi"

Loimaan kaupunki osallistui hakemukseen, jossa Valtiovarainministeriö avustaa digitalisaatiota. Hakemus meni lävitse ja olemme mukana digi- ja kyberturvallisuushankkeessa, joka alkaa vuoden alusta 2022.

10. Tietosuojavastaavan koulutusohjelma

Tietosuojavastaava osallistui ja suoritti FCG:n järjestämän tietosuojavastaavan koulutusohjelman 1.9 – 11.11.2021.

LÄHTEET

Tietosuojavaltuutetun toimisto, 2021. <https://tietosuoja.fi/tietoturvaloukkaukset>

Yleinen tietosuoja-asetus, artikla 33, 2021. <https://gdprinfo.eu/fi/fi-article-33>