Nivalan kaupungin tietoturvapolitiikka 2021 - 2025

Kuinka toimimme tietoturvallisesti

20.10.2021

Arto Marjamaa
Tietohallintopäällikkö
Nivalan kaupunki

Anita Rättyä
Tietosuojavastaava
Joki ICT Oy

NIVALA
Kasvatamme tulevaisuutta

Sisällys

NIVALA
Kasvatamme tulevaisuutta

Johdanto

Julkisen hallinon digitalisointi edistyy vauhdilla. Digitaalisuus on kytköksissä fyysiseen ympäristöön kaikilla kaupungin toimialoilla ja siksi turvallisuuden ylläpitäminen on yhä haastavampaa. Tämä kehitys edellyttää huolellista varautumista ja hyvää riskienhallintaa sekä kykyä havaita tietoturvaan ja tietosuojaan liittyviä poikkeamia. Käytössä oleva tietoturvateknologia suojaa toimintaympäristöä, mutta se ei yksin riitä. Henkilöstön tietoturva koostuu oikeasta asenteesta ja arjen pienistä päätöksistä. Nivalan kaupungissa kehitetään ja ylläpidetään tietoturvallista työkulttuuria koulutusten ja tietoturvaharjoitusten avulla. Tietoturvallinen työkulttuuri ja tietoturvateknologia takaavat Nivalan kaupungille sellaisen toiminta- ja palveluympäristön, johon työntekijät, kuntalaiset ja sidosryhmät voivat sitoutua ja luottaa.

Tämä tietoturvapolitikka kuvaa Nivalan kaupungin tietoturvallisuuden tavoitteet, vastuut ja toteuttamiskeinot, jotka tiedonhallintayksikön johto (kaupunginjohtaja ja kaupunginhallitus, TiHL 609/2019, 4§,) on hyväksynyt. Johto sitoutuu noudattamaan tietoturvaan ja tietosuojaan liittyvää lainsäädäntöä, viranomaisvaatimuksia ja hyviä käytäntöjä. Tiedonhallintayksikkö edistää tietoturvallista työkulttuuria, jossa tietoturva huomioidaan kaikessa toiminnassa. Henkilökunnalta edellytetään tietoturvallisten toimintatapojen noudattamista. Nivalan kaupunki edellyttää samaa sisäänrakennettua tietoturvaa myös sidosryhmiltään.

Tietoturvan ensisijainen tarkoitus on varmistaa tietojen asianmukainen ja luotettava käsittely organisaatiossa. Päivittäisessä työssä tämä tarkoittaa sitä, että tietoja voivat käyttää ainoastaan ne henkilöt, joka tarvitsevat tietoja työtehtävissään. Järjestelmähankintoja ja järjestelmien käyttöönottoja suunniteltaessa huomioidaan järjestelmille asetettavat käytettävyys-, tietosuoja- ja tietoturvavaatimukset sekä vaikutustenarvioinnin Nivalan kaupungin hankintaohjeen ja -prosessin mukaisesti.

Tämä tietoturvapolitiikka on julkinen asiakirja. Johto sitoutuu parantamaan tietoturvaa jatkuvasti ja asettaa vuosittain tietoturvan kehittämistavoitteet.

Mahdolliset tietoturvapolitiikkaan liittyvät huomautukset ja kehittämiskohteet pyydetään toimittamaan Nivalan kaupungin tietohallintopäällikölle ja tietosuojavastaavalle. Tietoturva- ja tietosuojavastaavat raportoivat säännöllisesti tiedonhallinnasta, tietojen käsittelystä ja tietoturvan tilasta johdolle. Tietoturva- ja tietosuojavastaavat valmistelevat tarvittavat muutokset tietoturvapolitiikkaan ja tuovat ne johdolle hyväksyttäväksi.

NIVALA
Kasvatamme tulevaisuutta

Tietoturvaan liittyviä näkökulmia

Hallinnollista tietoturvaa toteutetaan luomalla periaatteet tietoturvatyölle. Johto arvioi riskit ja luo puitteet tietoturvan hallinnan muiden osa-alueiden menettelytavoille. Hallinnollisen tietoturvan toimenpiteitä ovat resurssien nimeämiset, vastuiden jakamiset, salassapito- ja turvallisuussopimusten tekeminen. Tietoturvallinen ajattelutapa pyritään sisällyttämään organisaation jokapäiväisiin toimiin.

Henkilöturvallisuus pyritään pitämään korkealla tasolla valitsemalla oikeat henkilöt työtehtäviin, perehdyttämällä ja kouluttamalla henkilöt toimimaan oikein prosessien mukaan sekä noudattamalla sovittuja menettelyjä irtisanomistilanteissa. Näitä periaatteita sovelletaan sekä vakituisiin että tilapäisiin työntekijöihin.

Tietotekniikan käyttöympäristö laitteineen ja tiedonsiirtovälineineen suojataan fyysisin turvallisuustoimenpitein. Kiinteistöt, toimitilat, laitteet ja tietovarastot suojataan asiaankuulumattomilta henkilöiltä sekä erilaisilta vahingoilta ja onnettomuuksilta. Jotta toiminnan jatkuminen voidaan taata ajan kuluessa, riskien havaitsemiseen ja vähentämiseen tähtääviä toimenpiteitä kehitetään siten, että ne muodostuvat arkirutiineiksi. Työntekijä huomioi ja huolehtii tietoturvasta ja tietosuojasta myös kotitoimistossa ja etätöissä.

Laitteistoturvallisuudessa otetaan huomioon laitteiden koko elinkaari, takuut, sopimukset ja tukipalvelut. Laitteistoturvallisuus taataan laitteiston suojauksella ja asianmukaisilla asennus-, ylläpito- ja poistotoimenpiteillä. Lisäksi laitteille määritellään omistaja ja laitteen turvaluokka sekä suunnitellaan laitteiden valvonta ja kapasiteetit.

Ohjelmistoturvallisuus taataan ohjelmistopäivityksillä, pääsynvalvonta- ja lokimenettelyillä sekä varmuuskopioinnilla. Ohjelmistopäivitysten julkaisuja seurataan aktiivisesti ja päivitysten kriittisyys arvioidaan ennakolta, jos mahdollista. Kriittiset päivitykset asennetaan viipymättä.

Tietoliikenneturvallisuudessa huolehditaan turvallisesta tietojen siirrosta. Kriittiset viestit ja dokumentit välitetään luokitusten vaatimin salausmenettelyin. Viestinvälityksen tietosuojaa koskevat vaatimukset ja vastuut on määritelty organisaation ja viestinvälitysoperaattorin välisissä sopimuksissa.

Tietoaineistoturvallisuutta pidetään yllä luokittelemalla tietoja niiden kriittisyyden perusteella ja antamalla käsittelyoikeudet työtehtävien perusteella sekä valvomalla tiedonkäsittelyä.

Käyttöturvallisuutta parannetaan luomalla ja ylläpitämällä turvallisia toimintaolosuhteita. Organisaatiossa huolehditaan käytön ja tekniikan toimivuudesta, käyttöoikeuksista, ohjelmistotuesta, ja varmuuskopioinnista. Käyttöturvallisuus huomioidaan elinkaaren kaikissa vaiheissa sekä kehittämistoiminnoissa. Käyttäjät ovat velvollisia ilmoittamaan havaitsemistaan häiriöepäilyistä tai häiriöistä välittömästi pääkäyttäjille ja IT-tuelle. Tietoturvapoikkeamista, haitallisista ja toimintaa vaarantavista tapahtumista raportoidaan kaikilla tasoilla viivytyksettä poikkeamien hallintaprosessin mukaisesti. Poikkeamaraporttien tilastoja seurataan ja niitä hyödynnetään tietoturvan kehittämisessä.

1. Tietoturvapolitiikan tavoite

Tietoturvapolitiikan tavoitteena on kuvata yleisellä tasolla ja ymmärrettävästi, kuinka Nivalan kaupungilla toteutetaan tietoturvallisuuden periaatteita.

1.1 Tietoturvallisuuden periaatteet

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä, käytettävyydestä, kiistämättömyydestä sekä tunnistettavuudesta eli pääsynvalvonnasta. Tietoturvatoimet koskevat tiedon käsittelyä, kuten tallennusta, luovutusta, siirtoa ja suojausta tiedon koko elinkaaren ajan.

Luottamuksellisuus tarkoittaa sitä, että erilaiset tiedot, kuten salasanat ja organisaatiossa käsiteltävät tiedot ovat vain sellaisten henkilöiden käytettävissä, joilla on oikeus niiden käyttöön.

Eheys tarkoittaa sitä, että tietoa ei pääse muokkaamaan kuka tahansa ilman asianmukaista valtuutusta. Tieto ei myöskään muutu matkan varrella tahattomasti tai tietoturvahyökkäyksen takia. Eheys tarkoittaa myös tietojen loogisuutta ja sitä, että tieto pitää paikkansa.

Käytettävyys tarkoittaa tiedon saatavuutta oikeassa muodossa oikeaan aikaan. Tietojen tulee olla sellaisten henkilöiden käytettävissä, jotka sitä tarvitsevat ja jotka ovat niihin oikeutettuja.

Kiistämättömyys tarkoittaa tapahtuman todentamista oikeaksi jälkikäteen esimerkiksi seuraamalla järjestelmän käyttöä. Lokipalvelimelta on mahdollista todentaa käyttäjien tekemiä muutoksia.

Tunnistaminen (todentaminen, autentikointi) tarkoittaa osapuolten (henkilön tai järjestelmän) luotettavaa tunnistettavuutta. Todentamisessa käytetään esim. salasanoja, sertifikaatteja ja muuttuvia avaintunnuksia.

Tietoturvatoimilla suojataan tietoaineistot ja tietojärjestelmät sekä turvataan niiden toiminta ja sisältö. Tietoturvan tiekartta visualisoi Nivalan kaupungin tietoturvatoimenpiteet ja tavoitteet. Tietoturvatoimenpiteet-dokumentissa luetellaan konkreettiset toimenpiteet, joilla edistetään tietoturvallista työkulttuuria.

Päämääränä on tiedonhallintayksikön keskeytymätön ja luotettava toiminta. Tietoturvan osalta tätä päämäärää tavoitellaan siten, että estetään tietojen ja tietojärjestelmien valtuudeton käyttö sekä tiedon tahaton tai tahallinen tuhoaminen tai vääristyminen. Nivalan kaupungin kriittiset tiedot, tietojenkäsittelyjärjestelmät ja palvelut pidetään asianmukaisesti suojattuna sekä normaali- että poikkeustilanteissa. Luettelo kriittisistä kohteista ja

niiden suojauksista on salassa pidettävä asiakirja. Uhka- ja poikkeustilanteisiin varaudutaan etukäteen riskianalyysillä ja toipumissuunnitelmalla, jotta mahdolliset vahingot saadaan minimoitua.

1.2 Tavoitteet

Tavoitteena on tietoturvallinen työkulttuuri. Tietoturvallinen työkulttuuri tarkoittaa turvallista, sujuvaa ja häiriötöntä tietojenkäsittelyä ja vastuullista asennetta tietoturva- ja tietosuoja-asioihin. Tietoturvallisen työkulttuurin ansiosta asiakkaat, henkilökunta ja sidosryhmät voivat luottaa Nivalan kaupungin tietojenkäsittelyn asianmukaisuuteen. Tietoturvallisessa työkulttuurissa tietoturva on sisäänrakennettu ja luonteva osa arjen työntekoa.

Näiden päämäärien saavuttamiseksi kaikkien tietoa käsittelevien henkilöiden

- on tiedettävä tehtävänsä ja velvollisuutensa
- on ymmärrettävä tietojenkäsittelyn periaatteet: mitä, missä tarkoituksessa, miten ja milloin tietoja käsitellään
- on tiedettävä, kenelle ja millä perusteella tietoa voidaan luovuttaa
- on omalta osaltaan huolehdittava tietoturvallisesta työkulttuurista
- on osallistuttava omiin tehtäviin liittyvän tietoturvallisuuden ja tietosuojan jatkuvaan kehittämiseen
- ilmoittaa viipymättä havaitut tietoturvapoikkeamaepäilyt esimiehelle

Tietoturvallinen työkulttuuri syntyy seuraavilla tekijöillä:

- Organisaatiossa kehitetään tietoturva- ja tietosuojapoikkeamien tunnistamista
- Tietoturvasta keskustellaan avoimesti ja havaitut epäkohdat korjataan.
- Kaikki ymmärtävät oman merkityksensä, tehtävänsä ja velvollisuutensa tietoturvallisuuden ylläpidossa.
- Tietojen luottamuksellisuuden, eheyden, käytettävyyden, kiistämättömyyden ja tunnistamisen vaatimuksia toteutetaan kaikessa tietojenkäsittelyssä, mikä mahdollistaa tietoturvallisen asioinnin ja tietojen käytön.
- Tietoturvavaatimukset otetaan huomioon kaikessa kehittämistoiminnassa.
- Tietoturvallinen toimintatapa on mukana jokapäiväisessä työssä sekä toimintaprosesseissa ja tietojärjestelmissä koko organisaatiossa.
- Tietoturvallisia työtapoja suunniteltaessa huomioidaan joustavat työtavat. Liian jäykät tietoturvakontrollit eivät saa johtaa siihen, että tietoturvaa kierretään ja aiheutetaan uusia tietoturvauhkia.

1.3 Mittarit

Havainnointikyvyn, tietoturvallisen työkulttuurin kehittymisen ja tietoturvan laadun kehittymisen seuraamiseksi laaditaan laadulliset mittarit. Tietoturvan nykytilan ja tietoturvan toteutumisen mittaamiseen otetaan käyttöön kyberturvallisuuskeskuksen kehittämä Kybermittari. Kybermittari auttaa parantamaan kykyä torjua kyberuhkia. Mittareita seurataan säännöllisesti. Tietoturvan hallinnan laatua seurataan ja mittareita kehitetään aktiivisesti.

1.4 Tietoturvan ohjaus

Nivalan kaupungin tietoturvallisuus pohjautuu kansallisiin ja kansainvälisiin lakeihin ja asetuksiin. Keskeisimmät lait ovat Laki julkisen hallinnon tiedonhallinnasta (906/2019) ja Tietosuoja-asetus (EU, 679/2016). Lakeja täydentää Digi- ja väestötietoviraston kyberturvallisuuskeskuksen suositukset ja Nivalan kaupungin tietoturvaohjeet.

2. Tietoturvavastuut ja organisointi

Tietoturvallisen toimintaympäristön luomisessa avainasemassa on henkilöstö. Jokainen yksilö on vastuussa omalta osaltaan tietoturvallisen toimintakulttuurin luomisessa huolimatta siitä, missä paikassa työtehtäviä suoritetaan.

2.1 Organisaatio

Tietoturvallisuus on osa Nivalan kaupungin kokonaisturvallisuutta ja tietoturvan eri osa-alueille määritellään vastuuviranhaltijat tiedonhallintalain (TiHL 906/2019) ja hallintosäännön mukaisesti.

2.2 Johdon vastuut

Tiedonhallintayksikön johto on vastuussa tietoturvallisesta työkulttuurista, tietoturvan linjauksista ja johtamisesta. Se määrittelee tietoturvan tavoitetason ja ne hyödyt, joita tieto-omaisuuden turvaamisella saavutetaan. Johto nimeää vastuuhenkilöt, joiden tehtävänä on toteuttaa turvallisuusjohtamiseen liittyviä tehtäviä. Johto on vastuussa siitä, että kaikki työntekijät ovat tietoisia organisaation tietoturvapolitiikasta ja -periaatteista. Johto on vastuussa siitä, että tietoturvavastuut ovat sidosryhmien tiedossa ja tietoturvaohjeita noudatetaan. Sopimuksissa tulee olla kirjattuna tietoturva- ja henkilötietojen käsittelyyn liittyvät toimintatavat. Kaupunginhallitus hyväksyy tiedonhallintamallin, tietoturvapolitiikan ja niihin tehtävät muutokset.

2.3 Esimiesten vastuut

Esimies tai toimialajohtaja, joka on vastuussa prosessi- tai järjestelmämuutoksista, muutosvaikutusarvioinnin ja henkilötietojen käsittelyn vaikutustenarvioinnin käynnistämisestä ja tekemisestä. Esimies huolehtii, että työntekijät saavat tietoturva- ja tietosuojakoulutusta ja tuntevat ohjeistuksen. Esimies ohjaa ja valvoo tietoturvallisten työtapojen ja ohjeiden noudattamista. Esimiehen vastuulla on tehdä virallinen ilmoitus tietoturvaan ja tietosuojaan liittyvistä poikkeamaepäilystä. Esimiehet huolehtivat, että työntekijät suorittavat vuosittaisen tietoturvakyselyn.

2.4 Tietoturvaorganisaation vastuut

Tietoturva- ja tietosuojavastaavat seuraavat tietoturvan toteutumista ja henkilökunnan koulutusta. He ylläpitävät käytössä olevaa tietoturvaohjeistusta. Tietoturvatyöryhmä ohjeistaa ja antaa lausuntoja muutosvaikutusarviointeihin. Tietoturvavastaava raportoi johtoryhmälle neljännesvuosittain tietoturvan tilan ja koostaa kerran vuodessa tietotilinpäätöksen.

2.5 Työntekijöiden vastuut

Jokaisella työntekijällä on vastuu toimia siten, että tietoturva ja henkilötietojen käsittely noudattaa organisaation tietoturvapolitiikkaa ja -ohjeita. Käyttäjätunnus ja salasana on aina henkilökohtainen. Jokaisen velvollisuus on huolehtia, että omat käyttäjätunnukset ja salasanat eivät päädy ulkopuolisen käsiin. Työntekijän on huolehdittava tilaturvallisuudesta siten, että tuntemattomat henkilöt eivät pääse henkilökunnalle tarkoitettuihin tiloihin ilman saattajaa. Jokainen työntekijä on velvollinen raportoimaan havaituista poikkeamaepäilyistä ja tietoturvaan liittyvistä puutteista esimiehelleen.

2.6 Tietoturvapalvelun tuottajan vastuut

Joki ICT Oy:n tietosuoja- ja tietoturvapalvelulla on Nivalan kaupungin johdon antama valtuutus tehdä organisaation tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi. Palvelujen tuottaja tekee yhteistyötä kaupungin johdon, tietoturva- ja tietosuojavastaavien kanssa. Palvelujen tuottaja huolehtii omalta osaltaan tietosuojaan ja tietoturvaan liittyvän dokumentaation ylläpidosta sekä tarjoaa asiantuntemusta ja koulutusta.

2.7 Organisaation yhteistyökumppaneiden vastuut

Sidosryhmät ja yhteistyökumppanit sitoutuvat omalta osaltaan turvalliseen tiedonkäsittelyyn asioidessaan Nivalan kaupungin kanssa. Sopimuksissa sovitaan tietoturvaan, salassapitoon ja henkilötietojen käsittelyyn liittyvät vastuut.

3. Häiriöt ja varautuminen

3.1 Häiriöt ja niiden hallinta

Häiriöitä voivat aiheuttaa mm. ihmisten huolimattomuus, laiteviat, tahallinen ilkivalta, järjestäytyneet rikolliset, ennakoimattomat tapahtumat, onnettomuudet tai luonnonmullistukset. Häiriöitä hallitaan arvioimalla näiden riskien esiintymisen todennäköisyyttä, tiheyttä ja vakavuutta. Riskiarvion perusteella valitaan sopivat hallintakeinoja, joilla ehkäistään, lievennetään tai siirretään riskejä.

3.2 Varautuminen

Varautumissuunnitelma on salassa pidettävä asiakirja. Se päivitetään säännöllisesti, koska digitaalinen toimintaympäristö kehittyy ja monimutkaistuu vauhdilla. Varautumissuunnittelulla ehkäistään riskien toteutumista, pienennetään riskin vaikutusta tai kestoa. Ennakoimattomien ja suurten riskien aiheuttamia vahinkoja hallitaan vakuutuksilla. Toipumissuunnitelmalla varmistetaan toiminnan mahdollisimman nopea palautuminen.

Suojattavat kohteet tunnistetaan ja tietoturvakriittisyys arvioidaan ja perustellaan. Kriittiset kohteet luetteloidaan ja priorisoidaan. Kohteille tehdään riski- ja vaikutustenarviointi kriittisyysjärjestyksessä. Riskien kontrollit arvioidaan ja valitaan toimintaympäristöön parhaiten soveltuvat tietoturvakontrollit. Tietoturvakontrollien toteuttamiseen osoitetaan vastuutahot. Riskien hallinta ja tietoturvakontrollien käyttöönotto ja vastuut kuvataan riskienhallintasuunnitelmassa.

Johtokeskustilat suunnitellaan ja dokumentoidaan. Tilat ja kalusto katselmoidaan säännöllisesti. Johtokeskuksen tarvitsemat tietoliikenneyhteydet, tietotekniikka ja AV-laitteet ovat mahdollisuuksien mukaan päivittäisessä käytössä ja niiden käyttöä harjoitellaan. Säännöllisellä harjoittelulla varmistetaan, että työntekijät osaavat toimia kriisitilanteessa luontevasti, tuntevat kriisitilanteen ohjeet ja osaavat käyttää niitä työkaluja, joita varautumissuunnitelmassa on määritelty käytettäväksi kriisitilanteissa. Harjoittelutilanteissa harjoitellaan myös sisäistä ja ulkoista viestintää. Harjoitelutilanteissa esiin tulevat puutteet kirjataan ylös ja käsitellään.

4. Sopimusten hallinta

Organisaatio huolehtii asianmukaisesta sopimustenhallinnasta. Sopimuksia saavat tehdä vain ne henkilöt, joilla on sopimustenteko-oikeus. Sopimuksissa edellytetään tietoturva- ja henkilötietojen käsittelysopimusta. Tietoturvavastuista tehdään laite- ja sovellustoimittajien sekä palveluntarjoajien kanssa erilliset sopimukset.

Sopimuksissa organisaatio kiinnittää erityisesti huomiota siihen, että koko palvelutuotannon ketju huolehtii tietoturvasta ja henkilötietojen käsittelystä, kuten tietojen siirrosta ja säilytyksestä Euroopan ja Suomen lain mukaisesti.

5. Tiedonhallintamallin merkitys turvallisuuteen

Tietoturvallisuuden toteuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Tiedonhallintamallissa kuvataan organisaation toimintaympäristö: kuten prosessit, tietoaineistot sekä tietojärjestelmät ja niiden yhteydet toisiinsa. Tiedonhallintamalli tukee organisaatiota kehittämään toimintaympäristöään hallitusti. Kun toimintaympäristöön tehdään muutoksia (esim. prosesseja digitalisoidaan tai hankitaan uusia tietojärjestelmiä) tiedonhallintamalliin kuvataan suunnitellut muutokset jo varhaisessa vaiheessa. Lait edellyttävät organisaatiota tekemään muutostenvaikutusarviointeja ja tietosuojan vaikutusten arviointeja muutostilanteissa. Kuvaukset tiedonhallintamallissa auttavat hahmottamaan monimutkaisten prosessien ja tietojärjestelmien mahdollisia riskejä ja muita vaikutuksia. Se taho, joka käynnistää kehitysprojektin tai hankintaprojektin on velvollinen käynnistämään kuvaukset tiedonhallintamalliin ja käynnistämään muutostenvaikutusarviointiprosessi sekä tietosuojan vaikutusten arvioinnin.

Tiedonhallinnan muutosten hyödyllisyys, vaikuttavuus ja turvallisuus sekä muutoksen toimivuus esitellään tiedonhallintamallin avulla johdon katselmoinnissa ja johto päättää tarvittavista laajavaikutteisista muutoksista.

6. Tietoturvakoulutus ja -ohjeet

Nivalan kaupunki kouluttaa johtoa ja henkilökuntaa säännöllisesti tietoturvaan ja tietosuojaan liittyvissä asioissa. Henkilökunta osallistuu säännöllisesti verkkokoulutuksiin ja tarpeen mukaan luokkahuonekoulutuksiin sekä seminaareihin tai työpajoihin. Koulutukset kuvataan tarkemmin koulutussuunnitelmassa. Uusien työntekijöiden perehdytyskoulutuksiin sisältyy tietoturvakoulutus. Mikäli tietojärjestelmiin tai organisaatiorakenteisiin tehdään merkittäviä uudistuksia tai hankintaan uusia tietojärjestelmiä, arvioidaan tietoturvakoulutuksen tarve erikseen näissä tilanteissa. Voimassa olevat tietoturva- ja tietosuojaohjeet löytyvät intranetistä.

7. Tietoturvallisuuden seuranta

Jokainen työntekijä on velvollinen ilmoittamaan havaitsemistaan tietoturvapuutteista. Tietoturvailmoitusten määrää seurataan ja ne käsitellään Tiedonhallintaryhmässä. Osastojen vastuuhenkilöiden tehtävänä on valvoa, että tietoturva toteutuu käytännössä ja ryhtyä toimiin, mikäli henkilökunta ilmoittaa tietoturvaan liittyvästä epäilystä tai epäkohdasta. Tietoturvaohjeistukseen liittyvien laiminlyöntien seurauksena voi olla huomautus tai kirjallinen varoitus, rikosilmoitus tai jopa palvelussuhteen purkaminen.

Tietoturvakäytännöille tehdään vertaisarviointeja saman toimialueen toimijoiden kanssa ja/tai niitä katselmoidaan erillisissä auditointitilaisuuksissa.

8. Poikkeamien hallinta

Poikkeamien käsittely on kuvattu Poikkeamienhallinta -dokumentissa. Kaikista epäilyttäväistä tapahtumista kannattaa ilmoittaa esimiehelle ja tehdä tietoturvapoikkeamailmoitus. Vakavissa tilanteissa asiasta ilmoitetaan ylimmälle johdolle ja tietohallintoon, joka kutsuu koolle poikkeamaryhmän, jossa on mukana henkilöt, joiden toimialaa tai työtehtävää poikkeama koskee. Esimies huolehtii, että viranomaisilmoitukset tulee tehtyä

Poikkeamatilanteessa toimitaan nopeasti tilanteen edellyttämällä tavalla vahinkojen minimoimiseksi. Jokainen poikkeamatilanteeseen osallistuva dokumentoi tilannetta vaihe vaiheelta kirjaamalla päiväyksen, kelloajan ja tehtävän, jonka tehnyt liittyen poikkeamaepäilyyn. Viestintä tapahtuu kaupungin kriisi- ja häiriötilanteiden ohjeiden mukaisesti.

Poikkeamat kirjataan tulevien kehittämistoimien perustaksi. Myös ns. ”läheltä piti” –tapaukset rekisteröidään. Onnettomuuksien, turvallisuusrikkomusten ja palvelujen keskeytysten seuraukset analysoidaan. Tietoturvatapahtumista kerätään jatkuvasti ajan tasalla olevaa tilannekuvaa yhdyshenkilö-verkoston ja teknisten valvontajärjestelmien avulla. Tilannekuva havainnollistaa tietoturva-poikkeamatilanteen ja niiden aiheuttamat vaikutukset. Kerättyä dataa käytetään tulevissa arvioinneissa apuna tietoturvatoimien suunnittelussa ja priorisoinnissa.

Tietoturvaloukkauksesta ilmoitetaan tarpeen vaatiessa myös Digi- ja Viestintäviraston Kyberturvallisuuskeskukseen nettilomakkeella. Tietosuojaloukkauksesta ilmoitetaan tiedonhallintalain mukaisesti Tietosuojavaltuutetun toimistoon ja tarvittaessa loukkauksen kohteeksi joutuneille henkilöille. Rikoksista tehdään rikosilmoitus poliisille.

8.1 Viestintä poikkeamatilanteissa

Häiriötilanteiden viestinnässä noudatetaan Nivalan kaupunginhallituksen hyväksymää Nivalan kaupungin viestintäohjetta. Ohje on henkilökunnan saatavilla Nivalan kaupungin intrassa. Organisaation johto tiedottaa ja ohjeistaa henkilökuntaa, mikäli organisaatiossa esiintyy tietoturvapoikkeamia. Johto varoittaa ja ohjeistaa henkilökuntaa, mikäli tietyt tietoturvaloukkaukset lisääntyvät.