261 §

Tietoturvapolitiikan päivitys

HA/501/00.01.01.01/2022

Perusteluosa

Tietoturvapolitiikka on organisaation tietoturvallisuutta ohjaavan dokumentaatiohierarkian ylin dokumentti, joka linjaa tietoturvan periaatteita sekä tietoturvan rooleja ja vastuita.

Päijät-Hämeen hyvinvointialueen voimassa oleva tietoturvapolitiikan versio 1.1 on hyväksytty 12.12.2022 aluehallituksessa.

Nykyinen tietoturvapolitiikka ei huomioi vuonna 2024 voimaan tullutta NIS2-direktiiviä (Directive (EU) 2016/1148 of the European Parliament and the Council) eikä vuonna 2025 voimaan astunutta kansallista kyberturvallisuuslakia (124/2025). Päivitetty versio huomioi lainsäädännön vaatimat muutokset.

Tietoturvapolitiikan keskeiset muutokset:

1. Lainsäädännön ja direktiivien päivitykset

    - Tietoturvapolitiikka päivitetty on vastaamaan vuonna 2024 voimaan tullutta NIS2-direktiiviä sekä vuonna 2025 voimaan astunutta kansallista kyberturvallisuuslakia (124/2025). Tietoturvapolitiikka on nyt lakisääteinen dokumentti.

    - Mukana myös uusi laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja CER-direktiivi (EU 2022/2557).

2. Rakenne

    - Politiikkaan on lisätty tarkentavia liitteitä (mm. lainsäädäntö, vastuut, käyttövaltuudet, lokienhallinta), joiden muutosten hyväksynnästä vastaa jatkossa tietoturvapäällikkö. Liitteitä voidaan lisätä tarpeen mukaan.

3. Sisällölliset muutokset

    - Tietoturvatavoitteet on määritelty aiempaa tarkemmin: painotetaan toiminnan jatkuvuutta (resilienssi), henkilötietojen

suojaa, tietojärjestelmien turvallisuutta, maineen ja luotettavuuden turvaamista sekä lainsäädännön vaatimustenmukaisuutta.
- Uusien teknologioiden ja palveluiden turvallinen hyödyntäminen sekä käyttäjälähtöinen tietoturvakulttuuri nostettu esiin.
- Vastuut ja organisointi
    - Ylin vastuu tietoturvallisuudesta on aluehallituksella (strateginen ohjaus ja lainmukaisuuden valvonta).
    - Hyvinvointialuejohtaja vastaa kokonaisvaltaisesta johtamisesta ja nimittää tieto- ja kyberturvallisuudesta vastaavan viranhaltijan.
    - Tietoturvapäällikkö vastaa operatiivisesta ohjauksesta ja kehittämisestä.
    - Jokainen työntekijä ja sidosryhmän edustaja on velvollinen noudattamaan tietoturvapolitiikkaa ja osallistumaan sen kehittämiseen.
- Tietoturvan johtaminen perustuu hallintamalliin, jossa kuvataan johtamisen, organisoinnin, valvonnan ja kehittämisen rakenteet. Tämä on lisätty tietoturvapolitiikkaan.
- Riskienhallinnan toimintamalli on kuvattu sisäisen valvonnan dokumentissa ja kuvattu tietoturvapolitiikkaan.
- Jatkuvuussuunnittelu ja poikkeustilanteisiin varautuminen on korostettu. Jatkuvuus taataan normaali- ja poikkeusoloissa sekä häiriötilanteissa.
- Riskienhallinta toteutetaan jatkuvalla arvioinnilla ja seurannalla. Riskienhallinnan toimintamalli on kuvattu sisäisen valvonnan dokumentissa ja tuotu tietoturvapolitiikkaan.
- Jatkuvuussuunnittelu ja poikkeustilanteisiin varautuminen on korostettu. Jatkuvuus taataan normaali- ja poikkeusoloissa sekä häiriötilanteissa.

Tietoturvapolitiikan päivityksen merkittävimmät muutokset on esitelty 13.11.2025 kokonaisturvallisuuden lautakunnalle yhdessä tietoturvan hallintajärjestelmän kanssa. Lisäksi heille on pidetty koulutus NIS2-direktiivistä ja sen vaatimuksista osana kokonaisuutta.

Kokonaisturvallisuuden lautakunta on merkinnyt 13.11.2025 tiedoksi tietoturvapolitiikan päivitysehdotuksen, joka siirrettiin aluehallituksen hyväksyttäväksi.

Liitteenä	Liite 1, Päijät-Hämeen hyvinvointialue tietoturvapolitiikka 1.2 Liite 2, Tietoturvapolitiikan Liite 1 – Tietoturvaa ohjaava lainsäädäntö ja suositukset Liite 3, Tietoturvapolitiikan Liite 2 – Tietoturvavastuut (salassa pidettävä) Liite 4, Tietoturvapolitiikan Liite 3 – Käyttövaltuus- ja pääsynhallinnan periaatteet (salassa pidettävä) Liite 5, Tietoturvapolitiikan Liite 4 – Lokienhallinnan periaatteet (salassa pidettävä)
Esittelijä	Hyvinvointialuejohtaja Petri Virolainen
Päätösehdotus	Aluehallitus hyväksyy tietoturvapolitiikan päivitykset ehdotuksen mukaisesti.
Päätös	Ehdotus hyväksyttiin yksimielisesti.
Toimivallan peruste	Hallintosääntö 66a §, kyberturvan järjestäminen
Asian valmistelija / Lisätietojen antaja	Toimialajohtaja Ismo Rautiainen, puh. 044 729 7982 Tietoturvapäällikkö Tanja Linnonmaa, puh. 044 482 5140
Toimenpiteet	Ote: toimialajohtaja Ismo Rautiainen, tietoturvapäällikkö Tanja Linnonmaa
Muutoksenhaku	Oikaisuvaatimus

Päijät-Hämeen hyvinvointialue

Tietoturvapolitiikka

1.10.2025

Versio 1.2

Päijät-Hämeen hyvinvointialueen tietoturvapolitiikka

Säädösperusta
Kappaleen 6 ja liitteen 1 mukaisesti

Korvaa/Muuttaa
Korvaa Päijät-Hämeen hyvinvointiyhtymän Digitaalisen turvallisuuden politiikka 25.03.2019 -dokumentin

Kohdistuvuus
Hyvinvointialueen henkilökunta ja hyvinvointialueen ympäristössä toimivat tahot.

Voimassa
Toistaiseksi

Muutoshistoria			
Päivämäärä	**Muutoksentekijä**	**Muutos**	**Versio**
8.6.2022	Tanja Linnonmaa	Ensimmäisen version kirjoittaminen	1.0
2.8.2022	Tanja Linnonmaa	Päijät-Soten joryn edellyttämät muutokset: laki 22.9.2000/812 lisätty ja täsmennetty voimaantulo Päijät-Sotessa heti hyväksynnän jälkeen	1.1
1.10.2025	Tanja Linnonmaa	Kyberturvallisuuslain edellyttämät muutokset, vastuiden täsmentäminen, tietoturvan hallintamalli	1.2

Päijät-Hämeen hyvinvointialue

1 Termit ja käsitteet

Tietoturvallisuus

Toimenpiteet ja periaatteet, joiden avulla suojataan ja varmistetaan tietojen ja tietojärjestelmien saatavuus, eheys ja luottamuksellisuus. Tietoturva kattaa sekä tekniset että hallinnolliset keinot, joilla suojataan tietoa luvattomalta käytöltä, muutoksilta ja häviämiseltä.

Kyberturvallisuus

Toimenpiteet, joilla varmistetaan digitaalisten palveluiden, verkkojen ja järjestelmien häiriötön, turvallinen ja luotettava toiminta. Kyberturvallisuus sisältää kyberuhkien ennaltaehkäisyn, havaitsemisen ja torjumisen.

Tietosuoja

Tietosuoja tarkoittaa henkilötietojen käsittelyä lainmukaisesti, turvallisesti ja yksityisyyttä kunnioittaen. Tietosuojan tavoitteena on turvata rekisteröityjen oikeudet ja estää henkilötietojen väärinkäyttö.

2 Johdanto

Päijät-Hämeen hyvinvointialue käsittelee toiminnassaan runsaasti luottamuksellisia tai salaisena pidettäviä tietoja, joiden suojaamisesta hyvinvointialueen on huolehdittava lainsäädännön velvoittamana.

Hyvinvointialueen ydintehtävät sekä asiakas- ja potilasturvallisuus edellyttävät tietosuojan ja tietoturvallisuuden toteuttamista kaikissa olosuhteissa. Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden varmistamista.

Hyvinvointialueen tietoturvajärjestelyiden tehtävänä on varmistaa toiminnan jatkuvuus, tietoturvallisuus, henkilötietojen oikeudellisuus, vaatimustenmukaisuus sekä niiden saatavuus rooliperusteisesti niille työntekijöille, joilla on työperäinen tarve tietoon.

3 Tausta ja tarkoitus

Tämä tietoturvapolitiikka on hyvinvointialueen aluehallituksen hyväksymä julkinen asiakirja, jossa asetetaan tietoturvallisuuden ylätason tavoitteet ja linjaukset sekä määritellään hallintosäännössä määriteltyjen kyberturvavastuiden lisäksi tietoturvallisuuteen liittyvät vastuut, periaatteet ja seuranta. Tämän asiakirjan liitteet ovat osittain luottamuksellisia, ei-julkisia asiakirjoja ja näitä asiakirjoja voidaan päivittää tietoturvapäällikön hyväksynnällä. Tietoturvapolitiikkaa täydentävät tietoturvasuunnitelma sekä yksityiskohtaisemmat periaatteet ja ohjeet.

4 Soveltamisala

Tietoturvapolitiikka koskee koko hyvinvointialuetta ja kattaa kaikki toimintaan liittyvät tietojenkäsittelytehtävät riippumatta siitä, missä muodossa tieto on – digitaalisessa muodossa, paperilla tai suullisesti käsiteltynä/välitettynä. Tietosuoja ja tietoturvallisuus on otettava huomioon kaikessa tietojenkäsittelyssä koko sen elinkaaren ajan, alkaen jo hankinta- ja suunnitteluvaiheista. Hyvä tiedonhallintatapa

edellyttää toiminnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä, seurantaa ja varautumista erilaisiin uhka- ja poikkeustilanteisiin.

Tätä tietoturvapolitiikkaa sekä siihen liittyviä tarkempia periaatteita ja ohjeistuksia on noudatettava paitsi oman henkilöstön, myös hyvinvointialueen tytäryhtiöiden sekä kaikkien yhteistyö- ja sopimuskumppaneiden toimesta.

Yhteistyökumppaneiden tietoturvallisuutta koskevat velvoitteet määritellään sopimuksen tietoturvaliitteessä.

Tietoturvapolitiikka on keskeinen osa Päijät-Hämeen hyvinvointialueen tietoturvan hallintajärjestelmää, johon kuuluvat kaikki tarvittavat tietoturvan toimintatavat, hallintakeinot ja dokumentit. Tietoturvan hallintajärjestelmän tarkoituksena on varmistaa hyvinvointialueen tietojen luottamuksellisuus, eheys ja saatavuus kaikissa olosuhteissa johdonmukaisella, riskeihin perustuvalla ja jatkuvasti kehittyvällä tavalla.

5 Tietoturvatavoitteet

Tietoturvallisuuden ensisijaisena päämääränä on hyvinvointialueen vastuulla olevien toimintojen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tietoturvallisuutta ylläpidetään kaikissa työvaiheissa kaikkien toimijoiden osalta. Turvallista ympäristöä ylläpidetään jatkuvalla seurannalla, riittävällä suunnittelulla, erilaisiin uhkatilainteisiin varautumalla sekä henkilökuntaa säännöllisesti ja tarpeenmukaisesti kouluttamalla.

Päijät-Hämeen hyvinvointialueen johdon asettamat tieto- ja kyberturvallisuustavoitteet:

- toiminnan jatkuvuuden turvaaminen ja varautuminen kaikkiin olosuhteisiin (resilienssi)
- asiakas-, potilas- ja henkilötietojen suojaaminen
- hyvinvointialueen tietojen ja tietojärjestelmien tietoturvallisuuden varmistaminen
- hyvinvointialueen maineen ja luotettavuuden turvaaminen tietoturvallisuuden ja tietosuojan osalta
- tietoturva- ja tietosuojalainsäädännön sekä toimialan lakien ja määräysten vaatimustenmukaisuus
- uusien teknologioiden ja palveluiden tietoturvallisen, säädöstenmukaisen ja tehokkaan hyödyntämisen mahdollistaminen
- käyttäjälähtöinen tietoturvakulttuuri

6 Ohjaava lainsäädäntö ja säädökset

Päijät-Hämeen hyvinvointialue on yhteiskunnan toiminnan kannalta kriittinen toimija, joka edellyttää tietoturvan toteutumista kaikessa toiminnassa. Hyvinvointialuetta ja sen kumppaneita tietojen käsittelyssä ohjaavat keskeisimmät lait ja säädökset sekä muut suositukset on listattu liitteessä 1. Päijät-Hämeen hyvinvointialue myös ylläpitää THL:n vaatimaa tietoturvasuunnitelmaa, jota päivitetään säännöllisesti.

7 Tietoturvallisuuden vastuut ja organisointi

Tietoturvallisuuden ja tietosuojan toteutuminen hyvinvointialueella edellyttää selkeästi määriteltyjä rooleja ja vastuita. Selkeiden vastuiden avulla varmistetaan, että tietoturva on osa hyvinvointialueen jokapäiväistä toimintaa ja että

vaatimustenmukaisuus toteutuu koko organisaatiossa. Tietoturvallisuuden hallinta on osa hyvinvointialueen johtamisjärjestelmää ja riskienhallintaa.

Ylin vastuu hyvinvointialueen tietoturvallisuudesta on hyvinvointialueen aluehallituksella, joka vastaa tietoturvallisuuden strategisesta ohjauksesta ja lainmukaisuuden toteutumisen valvonnasta hallintosäännön mukaisesti. Hyvinvointialueen hallitus hyväksyy tietoturvallisuutta ohjaavan tietoturvapolitiikan.

Hyvinvointialueen johtaja vastaa tietoturvallisuuden kokonaisvaltaisesta johtamisesta ja ohjauksesta. Hyvinvointialueen johtaja nimittää tieto- ja kyberturvallisuudesta vastaavan viranhaltijan, joka vastaa hyvinvointialueen teknisestä ja hallinnollisesta tietoturvasta kokonaisuutena sekä vastaa ICT-valmiussuunnittelun organisoinnista.

Jokainen työntekijä ja sidosryhmän edustaja on velvollinen noudattamaan tätä tietoturvapolitiikkaa sekä tarkempia tietoturva- ja tietosuojakäytäntöjä sekä ohjeistuksia ja osallistumaan niiden ylläpitoon ja kehittämiseen.

Tietoturvapäällikkö vastaa hyvinvointialueen tietoturvan operatiivisesta ohjaamisesta ja kehittämisestä sekä tietoturvaohjeiden ja -politiikan ylläpitämisestä.

Tietoturvallisuuden toteuttamiseen osallistuu vahvasti ICT-organisaatio ja palveluiden tuottamisen vastuuhenkilöt, jotka vastaavat omien toimintojensa tietoturvallisuuden toteuttamisesta sekä tietoturvapolitiikkojen ja -ohjeistusten noudattamisesta.

Yksityiskohtaiset tietoturvavastuut on määritelty tietoturvapolitiikan liitteessä 2.

Tietoturvan hallintamalli ja organisointi

Hyvinvointialueen tietoturvan johtaminen perustuu tietoturvan hallintamalliin, joka kuvaa tietoturvallisuuden johtamisen, organisoinnin, valvonnan ja jatkuvan kehittämisen rakenteet ja käytännöt. Hallintamallin tavoitteena on varmistaa:

- Tietoturvan vaatimustenmukainen ja johdonmukainen toteutus
- Tietoturvallisuustyön selkeä työn- ja vastuunjako
- Riskienhallinnan, poikkeamienhallinnan ja jatkuvuudenhallinnan yhteensovittaminen
- Dokumentoidut ja mitattavat toimintatavat, jotka tukevat auditointeja ja kehittämistä

Hallintamallin sisältö ja rakenne dokumentoidaan erilliseen tietoturvan hallintamallin kuvaukseen, jota ylläpitää tietoturvapäällikkö yhteistyössä tietohallinnon, johdon ja muiden avaintoimijoiden kanssa.

8 Tietoturvaperiaatteet ja linjaukset

Hyvinvointialuetta koskevat tietoturvalinjaukset

Tietoturvallisuus on osa hyvinvointialueen kokonaisturvallisuutta, jota johdetaan osana johtamisjärjestelmää ja riskienhallintaa.

Tietoturva- ja tietosuoja ovat johdon erityisen huomion kohteena, tietosuojaan ja tietoturvaan liittyviä riskejä hallitaan aktiivisesti johdon toimesta.

Tietosuoja ja tietoturva ovat koko henkilöstön asia ja rakentuvat vahvan turvallisuuskulttuurin varaan sekä ovat osa hyvinvointialueen päivittäistä toimintaa.

Esihenkilöt varmistavat omien alaistensa osalta tietoturvakoulutusten suorittamisen sekä tietoturvaan ja tietosuojaan liittyvien ohjeiden tuntemisen ja noudattamisen.

Kumppanisopimuksen vastuuhenkilö vastaa kumppaniin ja kumppanin palveluihin liittyvien tietoturva- ja tietosuojariskien hallinnasta ja kumppanin tietoturvallisuutta koskevien tietoturvavaatimusten ja -ohjeistusten noudattamisen seurannasta.

Hyvinvointialueen käsittelemillä tiedoilla ja tietojärjestelmillä on nimetyt omistajat ja muut tarpeen mukaiset vastuuhenkilöt, jotka vastaavat tietojen turvallisesta käsittelystä koko tiedon elinkaaren ajan.

Tietoja kerätään vain sen verran kuin määritellyn käyttötarkoituksen mukaan tarvitaan ja tietoja hyödynnetään vain määritellyn käyttötarkoituksen mukaisiin tarkoituksiin.

Tietoturvan eri osa-alueille on määritelty periaatteita, jotka ovat tämän tietoturvapolitiikan liitteenä. Tietoturvapolitiikan liitteenä olevia periaatteita voidaan päivittää tietoturvapäällikön hyväksynnällä.

9 Riskienhallinta

Kattavan tietoturvan toteuttaminen, ylläpitäminen ja kehittäminen toteutetaan jatkuvalla riskienarvioinnilla ja riskienhallinnalla. Tunnistettuja riskejä seurataan säännöllisesti ja niille asetetaan hallintatoimenpiteet sekä vastuut.

Henkilöstö tuntee ja tunnistaa omaan toimintaansa kohdistuvat tietoturvariskit ja pyrkii omalla toiminnallaan pienentämään niiden realisoitumisen mahdollisuuksia.

Tietoturvallisuuden riskienhallinta perustuu hyvinvointialueen yhteiseen riskienhallinnan toimintamalliin, jonka perusteet on kuvattu sisäisen valvonnan ja riskienhallinnan dokumentissa sekä siihen liittyvässä ohjeessa. Sisäinen riskienhallinnan ohje löytyy hyvinvointialueen dokumentinhallintajärjestelmästä.

10 Jatkuvuuden ja toipumisen varmistaminen

Toiminnalle kriittiset toiminnot tunnistetaan ja niiden jatkuvuussuunnittelua tehdään säännöllisesti. Lisäksi poikkeustilanteissa toimimista harjoitellaan säännöllisesti. Jatkuvuuden tulee olla taattu normaali- ja poikkeusoloissa sekä häiriötilanteissa.

Valmius- sekä toipumissuunnitelma on luotuna erilaisille poikkeusoloille, ja niitä harjoitellaan ja katselmoidaan säännöllisesti. Hyvinvointialueen ympäristössä toimivat tahot sitoutetaan jatkuvuudenhallintaan ja poikkeusoloihin varautumiseen sopimuksellisesti. Jatkuvuuden hallinnassa huomioidaan keskeisenä elementtinä toiminnan tietoturvallisuus.

11 Työntekijöiden koulutus

Työntekijöille järjestetään säännöllisiä tietoturvakoulutuksia. Osa koulutuksista on pakollista kaikille työntekijöille ja nämä koulutukset on myös uusittava määritellyin väliajoin.

12 Tietoturvapoikkeamat

Tietoturvapoikkeamien käsittelyyn ja raportointiin on määritelty omat toimintamallit.

Tietoturvan tahallinen vaarantaminen on rangaistava teko. Mikäli tietoturvapoikkeamia tai -rikkomuksia havaitaan, niistä ilmoitetaan pikimmiten omalle esihenkilölle, palveluvastaavalle tai tietoturvavastaavalle. Tarvittaessa poikkeamista ilmoitetaan lain vaatimalla tavalla tietosuojavaltuutetulle, poliisille ja muille viranomaisille.

13 Auditointi

Auditointi ja tarkastaminen ovat keskeinen osa kyberturvallisuuden riskienhallintaa, jonka avulla johto voi varmistaa kyberturvallisuuslain mukaisen velvollisuutensa arvioida ja tarkastaa organisaation kyberturvallisuustoimien ja politiikkojen toimivuutta.

Auditointien avulla varmennetaan kyberturvallisuuden riskienhallinnan arviointi, poikkeamanhallinnan testaus ja arviointi sekä toimitusketjun turvallisuus. Tieto- ja kyberturvallisuuden auditointeja toteutetaan erillisen auditointisuunnitelman mukaisesti, auditointien toimeenpanosta vastaa tietoturvapäällikkö tai tietohallinto.

14 Seuranta ja sanktiointi

Tietoturvan toteutumista seurataan mittareiden, auditointien, ja katselmuksien avulla. Poikkeamat politiikkoihin tai vaatimuksiin dokumentoidaan ja käsitellään määritellyn prosessin mukaisesti.

Politiikan tai sitä täydentävien tietoturvaohjeiden tietoinen rikkominen voi johtaa kurinpidollisiin toimenpiteisiin, rikostutkintaan tai sopimusoikeudellisiin seuraamuksiin. Hyvinvointialueen työsopimuksen osana oleva tietoturva- ja tietosuojasitoumus määrittelee täsmällisemmin tietoturvaohjeiden rikkomisen seuraamukset.

15 Liitteet

Tietoturvapolitiikan liite 1:

Tietoturvaa ohjaava lainsäädäntö ja suositukset

Tietoturvapolitiikan liite 2:

Tietoturvavastuut (luottamuksellinen, ei-julkinen dokumentti)

Tietoturvapolitiikan liite 3:

Käyttövaltuus- ja pääsynhallinnan periaatteet (luottamuksellinen, ei-julkinen dokumentti)

Tietoturvapolitiikan liite 4:

Lokienhallinnan periaatteet (luottamuksellinen, ei-julkinen dokumentti)

Tietoturvapolitiikan liite 5:

Tietoturvasuunnitelma (Ajantasainen suunnitelma on saatavilla tietohallinnosta. Liite on luottamuksellinen dokumentti)

Päijät-Hämeen hyvinvointialue

Tietoturvapolitiikan liite 1:
Tietoturvaa ohjaava lainsäädäntö ja suositukset

Keskeinen hyvinvointialueen tietoturvallisuutta ohjaava lainsäädäntö

Laki julkisen hallinnon tiedonhallinnasta (906/2019) – velvoittaa tiedonhallintaan, tietoturvallisuuteen ja tiedonhallintayksikön vastuisiin.

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) – säätelee potilas- ja asiakastietojen käsittelyä ja varmistaa yhteen toimivuuden Kanta-palveluiden kanssa.

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) – määrittelee terveystietojen käytön tutkimukseen, tilastointiin ja kehittämiseen.

Laki potilaan asemasta ja oikeuksista (785/1992) ja **Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)** – takaavat asiakkaiden ja potilaiden tiedolliset ja yksityisyyden suojan oikeudet.

Tietosuojalaki (1050/2018) ja GDPR (EU 2016/679) – yleiset henkilötietojen käsittelyn ja tietosuojan säännökset.

Kyberturvallisuuslaki (124/2025) – kansallinen toimeenpano NIS2-direktiivistä, velvoittaa hyvinvointialueet kriittisen toiminnan suojaamiseen ja tietoturvasta raportointiin.

Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025) sekä **CER-direktiivi (EU 2022/2557)** – ohjaavat kriittisten palveluiden jatkuvuuden turvaamista ja resilienssiä.

Tärkeimmät tietoturvallisuutta ohjaavat suositukset:

- Tiedonhallintalautakunnan suositukset
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
- ISO-standardit tietoturvallisuudesta, riskienhallinnasta, tekoälyn hallinasta, jatkuvuudesta mm. ISO 27001, 27002, 27005, 27701, 31000, 42001
- CIS Benchmark and controls -tietoturvasuositukset

Päijät-Hämeen hyvinvointialue

Päijät-Hämeen hyvinvointialueen tietoturvapolitiikan liite 2: Tietoturvavastuut (luottamuksellinen, ei-julkinen)

ROOLI	VASTUUALUEET
Aluehallitus	• Tietoturvapolitiikan hyväksyminen • Strateginen tietoturvan ohjaaminen ja tietoturvatavoitteiden asettaminen
Hyvinvointialueen johtaja	• Vastaa tietoturvallisuuden kokonaisvaltaisesta johtamisesta ja ohjauksesta • Varmistaa, että hyvinvointialue on määritellyt toiminnan kannalta kriittiset toiminnot, omaisuuserät, viestintäverkot, järjestelmät, fyysiset ympäristöt ja henkilöstön (NIS2) • Seuraa kyberturvan kokonaistilannetta ja kyberturvariskejä • Nimittää tieto- ja kyberturvallisuudesta vastaavan viranhaltijan
Kyberturvallisuudesta vastaava viranhaltija	• Vastaa hyvinvointialueen teknisestä ja hallinnollisesta tietoturvasta kokonaisuutena sekä vastaa ICT-valmiussuunnittelun organisoinnista.
Toimialajohtaja	• Vastaa tietoturva- ja tietosuojaohjeistuksen noudattamisen valvonnasta omalla toimialallaan • Vastaa toimialaa koskevien tietoturva- ja tietosuojariskien hallinnasta ja hyväksymisestä
Tietoturvapäällikkö (CISO)	• Tietoturvan ohjaaminen operatiivisella tasolla ja tietoturvan kehittäminen • Johdon tukeminen tietoturvan osalta • Tietoturvan hallintamalli (ISMS), Digiturvamalli • Tietoturvariskien hallinnan ohjaaminen • Jatkuvuus, ICT-varautuminen ja poikkeamatilanteiden hallinta • Tietoturvatietoisuus, koulutus, tietoturvaohjeet • Teknisten tietoturvapalvelut: tietoturvavalvomo (SOC), tekniset tietoturvaratkaisut • NIS2-compliance-seuranta ja raportointi
Tietosuojavastaava (DPO)/tietosuojatiimi	• Tietosuojatyön johtaminen ja seuranta • Tietosuojan valvonta • Tietosuojan ohjeistus ja koulutus • GDPR-compliance-seuranta ja raportointi
Tiedonhallintapäällikkö	• Tiedonhallintamalli
Rekisterinpitäjä (rekisterin omistaja)	• Hyväksyy omaa rekisteriä koskevat tietosuojan vaikutusten arvioinnit • Tekee päätökset tietosuojaa koskevien riskien hyväksymisestä
Tietohallintojohtaja (CIO)	• Vastaa tietoturvallisesta ja toiminnan jatkuvuuden mahdollistavasta ICT-kokonaisuudesta • Tietoturvallinen järjestelmien hankinta ja kehitys • IC- toimitusketjun riskienhallinta, kumppanihallinta • Tietoturvan ja tietosuojan mahdollistavat prosessit/toimintamallit (privacy by design, cybersecurity by design) • Tietoturvan budjetti

Infrapalveluiden tuotepäällikkö	• Pääsynhallinta ja tunnistautuminen • Infrajärjestelmien hallinta, haavoittuvuuksien hallinta, verkon turvallisuus, varmuuskopiointi
Palveluiden ja järjestelmien omistajat/tuotepäälliköt	• Järjestelmien ja tietojen luokittelu, järjestelmien suojaus, pääsynhallinta, haavoittuvuuksien hallinta ja korjaaminen, riskien tunnistaminen ja hallinta
Riskienhallinta/fyysinen turvallisuus ja henkilöstöturvallisuus	• Riskienhallinnan toimintamalli • Fyysinen turvallisuus: kiinteistöjen turvallisuus, laitteiston suojaus, turvallisuusalueiden hallinta • Henkilöstöturvallisuus: digiturva sopimuksissa, työsuhteen muutoshetket
Esihenkilö	• Vastaa omien alaistensa tietoturvaohjeiden noudattamisesta • Vastaa omien alaistensa tietoturvakoulutusten toteutumisen seurannasta
Henkilöstö	• Tietoturvaohjeistuksen noudattaminen, poikkeamien havainnointi ja niistä ilmoittaminen, tietoturvakoulutusten suorittaminen määräajoin

Päijät-Hämeen hyvinvointialue

Päijät-Hämeen hyvinvointialueen tietoturvapolitiikan liite 3:

Päijät-Hämeen hyvinvointialueen Käyttövaltuus- ja pääsynhallinnan periaatteet (ei-julkinen)

1 Tarkoitus ja soveltamisala

Tämä dokumentti kokoaa yhteen keskeiset hallintaperiaatteet ja käytännöt, joiden avulla Päijät-Hämeen hyvinvointialue varmistaa käyttövaltuus- ja pääsynhallinnan turvallisuuden, vaatimustenmukaisuuden ja valvottavuuden. Dokumentti tukee Suomen kyberturvallisuuslain 124/2025, NIS2-direktiivin, GDPR:n ja ISO/IEC 27001 -standardin mukaisia velvoitteita. Tietoturvapolitiikan liitteenä olevia periaatteita, kuten tätä käyttö- ja pääsynhallinnan periaatteet dokumenttia voidaan päivittää tietoturvapäällikön hyväksynnällä.

Käyttöoikeuksien hallinta

- Käyttöoikeudet ovat henkilökohtaisia, eikä niitä saa luovuttaa kenellekään toiselle.
- Jaetut/yhteiskäyttöiset käyttöoikeudet vaativat aina erillisen tietoturvatiimin hyväksynnän.
- Palvelu/järjestelmätunnukset vaativat aina dokumentoinnin, riskiarvioinnin ja erillisen tietoturvatiimin hyväksynnän.
- Järjestelmätunnusten oikeudet on rajoitettava vähimmän oikeuden periaatteen mukaisesti aivan minimiin.
- Käyttöoikeudet myönnetään vain työtehtävien edellyttämässä laajuudessa ja vain niihin tietoihin, mihin on tarpeellista päästä, vähimmän oikeuden periaatteella.
- Käyttöoikeudet ovat voimassa enintään sopimuksen päättymiseen saakka tai kunnes ne poistetaan tarpeettomina tehtävien muuttuessa tai viimeistään katselmoinnissa.
- Käyttöoikeudet luokitellaan automaattisesti myönnettäviin (rooli-, nimike- tai organisaatioperusteisiin) ja erikseen anottaviin.
- Hyväksyntäprosessin osapuolia ovat esihenkilöt, sovellusomistajat, pääkäyttäjät ja nimetyt hyväksyjät.
- Käyttöoikeuksien katselmointi tulee suorittaa vähintään kerran vuodessa.
- Käyttöoikeudet ja niiden myöntämiset ja poistamiset dokumentoidaan ensisijaisesti IAM-järjestelmään. Tukidokumentaatio sijoitetaan saataville IT-organisaation tarjoamaan paikkaan. Käyttöoikeuden dokumentointi on sovelluksien pääkäyttäjien ja IAM-pääkäyttäjän vastuulla. Käyttöoikeuden myöntämisestä tallennetaan peruste, hyväksymispäivä, hyväksyjä ja toteutustapa. Poistamisesta tallennetaan peruste, päivämäärä ja toteuttaja. Käyttöoikeuksien hallinnan dokumentaation tulee olla saatavissa auditointeja varten.
- Viitteet: NIS2: Art. 24 | GDPR: Art. 25 | ISO/IEC 27001: A.9.1.1, A.9.2.3

2. Tunnusten hallinta

- Tunnukset luodaan keskitetysti rooliperusteisesti IDM-järjestelmän kautta.
- Käyttäjätunnusten elinkaari perustuu tulo–muutos–lähtö prosessiin.
- Ulkoisten käyttäjien tunnukset ja korkean käyttöoikeustason tunnukset ovat aina määräaikaisia.
- Poistuvien käyttäjien tunnukset suljetaan viimeistään kahden (2) vuorokauden kuluttua sopimuksen päättymisen jälkeen.
- Viitteet: NIS2: Art. 21 | GDPR: Art. 32 | ISO/IEC 27001: A.9.2.1, A.9.2.6

3. Korkean käyttöoikeustason tunnusten hallinta

- Korkean käyttöoikeustason tunnukset tulee erotella normaaleista käyttäjätunnuksista. Korkean käyttöoikeustason tunnuksia saa käyttää ainoastaan ylläpitotehtäviin.
- Korkean käyttöoikeustason tunnukset myönnetään vain tilapäisesti, perustuen Just-in-Time-malliin.
- Korkean käyttöoikeustason tunnusten aktivointi vaatii dokumentoidun hyväksynnän ja tunnusten käyttäminen soveltuvilta osin monivaiheisen tunnistautumisen (MFA).
- Kaikki korkean käyttöoikeustason tunnusten käyttö tulee kirjata audit trailiin ja siirretään valvontaan SOC/SIEM-järjestelmiin.
- Hätätunnukset on talletettava turvallisesti joko suljettuun kirjekuoreen tai salasanahallintaan ja säilytettävä turvallisesti (esim. kassakaapissa). Hätätunnuksen salasana on muutettava käytön jälkeen ja talletettava uudelleen seuraavaa käyttöä varten.
- Viitteet: NIS2: Art. 24 | ISO/IEC 27001: A.9.2.3, A.9.4.4

4. Auditointi ja lokitus

- Tunnusten ja käyttöoikeuksien lokituksessa noudatetaan lokienhallinnan periaatteita ja tässä esitettyjä täsmennyksiä.
- Kaikki käyttäjähallintaan ja järjestelmäkäyttöön liittyvät tapahtumat tulee kirjata ja säilyttää valvottavassa ja jäljitettävässä muodossa esim. SIEM-järjestelmässä. Näihin kuuluvat:
    - Tunnistautumistapahtumat (esim. kirjautumiset, epäonnistuneet kirjautumiset, vahva tunnistautuminen)
    - Käyttäjätunnustapahtumat (esim. tunnuksen luonti, muokkaus, poistaminen)
    - Käyttövaltuustapahtumat (esim. oikeuksien ja roolien myöntäminen, poistaminen ja muutokset)
- Säilytyspaikka ja suojaus:
    - Tiedot pyritään tallentamaan keskitettyyn, tietoturvalliseen järjestelmään, joka takaa eheyden ja muuttumattomuuden esimerkiksi SIEM järjestelmä.
    - Lokitiedot ovat käytettävissä ainoastaan valtuutetuille henkilöille ja vain tietoturva-, valvonta- ja auditointikäyttöön.
- Viitteet: NIS2: Art. 23 | GDPR: Art. 30 | ISO/IEC 27001: A.12.4.1

5. Tunnistautumiskäytännöt

- Tunnistautumismenetelminä tulee käyttää menetelmiä, jotka ovat yleisesti luotettavia. Lähtökohtaisesti käytetään EntraID-pohjaisia tunnistautumisratkaisuja. Uuden järjestelmän käyttöönoton yhteydessä järjestelmän tunnistautumismenetelmä hyväksytetään arkkitehtuurimenettelyssä.
- Salasanavaatimukset on dokumentoitu tietoturvaohjeissa
- LDAP-tunnistautuminen on lähtökohtaisesti kielletty.
- MFA:ta tulee käyttää lähtökohtaisesti kaikessa tunnistautumisessa.
- Viitteet: NIS2: Art. 21, 24 | ISO/IEC 27001: A.9.4.2, A.9.4.3

Päijät-Hämeen hyvinvointialue

Päijät-Hämeen hyvinvointialueen tietoturvapolitiikan liite 4:

Päijät-Hämeen hyvinvointialueen lokienhallinnan periaatteet (ei- julkinen)

Säädösperusta:

Laki viranomaisen toiminnan julkisuudesta (621/1999) 11§

Laki sähköisen viestinnän palveluista (917/2014)

Rikoslaki (39/1889)

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)

Laki yksityisyyden suojasta työelämässä (759/2004)

Pelastuslaki (616/2022) 27§

EU:n yleinen tietosuoja-asetus (EU 2016/679)

Tietosuojalaki (1050/2018)

Kyberturvallisuuslaki (124/2025) ja NIS2 direktiivi (EU 2022/2555)

Laki sosiaali- ja terveydenhuollon asiakastietojen toissijaisesta käytöstä (552/2019, ns. toisiolaki)

Laki sähköisestä lääkemääräyksestä (61/2007)

Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan kansalliset vaatimusmäärittelyt 1.2, 4/2023

Kanta-palveluiden vaatimukset (kaikkien kanta- tapahtumien lokittaminen)

Päijät-Hämeen hyvinvointialue

1 Tarkoitus ja soveltamisala

Tämä periaatedokumentti määrittää vaatimukset lokitietojen keräämiselle, säilyttämiselle, käytölle ja raportoinnille hyvinvointialueella. Periaatteet koskevat kaikkia järjestelmiä ja palveluita, joissa syntyy lokitietoja: sote-asiakas- ja potilastietojärjestelmät (EHR/EMR), sosiaalihuollon järjestelmät, integraatio- ja rajapintapalvelut, pilvi- ja SaaS-palvelut, verkko- ja tietoturvatuotteet, käyttöjärjestelmät ja tietokannat sekä työasemat ja mobiilipäätelaitteet.

Periaatteet tukevat EU:n ja kansallisen sääntelyn (mm. asiakas- ja potilastietojen sääntely, GDPR ja kansallinen tietosuojalaki, Tiedonhallintalaki) sekä kyberturvallisuuslain tavoitteita.

2 Määritelmät

Lokitieto (loki): aikajärjestyksessä tallennettu merkintä järjestelmissä, sovelluksissa, verkoissa tai tietosisällöissä tapahtuneista toiminnoista ja muutoksista sekä niiden tekijöistä.

Käyttöloki / käytönvalvontaloki: henkilö- ja asiakastietojen katselut, haut, muutokset ja luovutukset (sis. käyttötarkoitus/konteksti).

Luovutusloki: tietojen luovutukset rekisterinpitäjien välillä ja kansallisiin palveluihin.

Ylläpitoloki (admin): järjestelmänvalvojan toimet ja konfiguraatiomuutokset.

Tietoturvaloki: tietoturvatuotteiden ja -palveluiden tuottamat tapahtumat (EDR/XDR, IDS/IPS, palomuuri, DLP, sähköpostisuodatus jne.).

Tekninen loki: virheet, suorituskyky, job-run ja integraatiotapahtumat.

Meta-loki: lokien katselun ja käsittelyn oma audit trail.

SIEM: keskitetty tietoturvalokienhallinta- ja analytiikkajärjestelmä.

Audit trail: järjestelmän tai prosessin tapahtumaketju ja siihen liittyvä todentava tieto, joka mahdollistaa toimenpiteiden jäljitettävyyden ja todennettavuuden, koostuu useista lokilähteistä ja tukee osoitusvelvollisuutta, poikkeamien tutkintaa ja auditointeja.

Audit loki: auditointitarkoitukseen ylläpidettävä loki tai kuratoitu lokinäkymä, joka korostaa valvontaa ja muutosten jäljitettävyyttä

Päijät-Hämeen hyvinvointialue

3 Lokienhallinnan periaatteet

Päijät-Hämeen hyvinvointialueen lokienhallinnan periaatteet määrittelee vaatimukset tietojärjestelmien käytöstä syntyvien lokitietojen käsittelylle. Lokiperiaatteissa otetaan kantaa tietojärjestelmien lokienhallinnan suunnitteluun, kuvaamiseen, säilytystapaan ja -aikaan, lokien käsittelyyn liittyviin rooleihin sekä vastuisiin.

Keskeiset hyvinvointialueen toiminnassa sovellettavat lokienhallinnan periaatteet:

Lainmukaisuus: Lokien käsittely toteutetaan sovellettavan lainsäädännön, asetusten ja viranomaisohjeiden mukaisesti. Henkilötietoja sisältäviä lokitietoja on käsiteltävä tietosuojalainsäädännön mukaisesti ja henkilötietoa sisältävät lokitiedot on liitettävä osaksi henkilörekisteriä ja ne on mainittava tietosuojaselosteessa.

Tarkoitussidonnaisuus: Lokeja kerätään vain määriteltyihin tarkoituksiin: tietoturva, väärinkäytösten selvittäminen, vianselvitys ja palvelutason seuranta, toiminnan valvonta ja auditointi ja viranomaisvelvoitteet.

Tietojen minimointi: Lokeihin tallennetaan vain tarkoituksen kannalta tarpeelliset tiedot.

Eheys ja muuttumattomuus: Lokien muuttumattomuus varmistetaan (esim. salaamalla). Luvaton muokkaus tai poistaminen estetään. Myös järjestelmän ylläpitäjiltä on estetty lokitietojen muokkaaminen.

Luottamuksellisuus ja pääsynhallinta: Lokit ovat salassa pidettäviä. Pääsy on rajattu nimetyille rooleille vähimmän oikeuden periaatteella, ja lokien katselu lokitetaan.

Keskitetty hallinta: Kaikki lokit tulisi ohjata keskitettyyn lokijärjestelmään/palveluun reaali- tai lähes reaaliaikaisesti, ellei kirjallisesti hyväksytty poikkeus toisin määrää.

Raportointi ja läpinäkyvyys: Organisaatiolla on kyvykkyys tuottaa lakien edellyttämät raportit sekä sisäiset valvontaraportit. Lokituksen toteutus dokumentoidaan osana järjestelmädokumentaatiota.

Säilytys ja poistaminen: Säilytysajat määritetään erityislainsäädännön tai Tiedonhallintalain §21 perusteella; säilytysajan päätyttyä lokit poistetaan tai anonymisoidaan turvallisesti ja poistosta jää todenne.

Toimittajavelvoitteet: Toimittajasopimuksiin sisällytetään vaatimukset lokien syntymisestä, muodosta, siirrettävyydestä, saatavuudesta ja luovutuksesta.

Jatkuva parantaminen: Lokien kattavuutta, laatua ja käytettävyyttä seurataan mittareilla ja arvioinneilla; puutteet korjataan ohjatusti.

Päijät-Hämeen hyvinvointialue

3 Lokienhallinnan roolit ja vastuut

ROOLI	VASTUU
Tietohallinto	operatiivinen lokituksen toteutus, toiminnalliset lokivaatimukset järjestelmille, sopimustekniset vaatimukset järjestelmien toimittajille ja toimittajien lokitusvaatimusten toteutumisen valvonta
Tietoturvapäällikkö	lokienhallinnan periaatteiden omistajuus ja poikkeamien käsittely/hyväksyntä, tietoturvalokienvalvonnan määrittely ja ohjaus sekä tietoturvalokien valvonta ja poikkeamien käsittelyprosessi.
Tietosuojavastaava	Sote-lokien sisältö ja käsittelyprosessit, rekisteröidyn oikeudet, ohjeistus asiakkaille ja tietohallinnolle sekä omavalvonta.
Järjestelmän omistaja/tuotepäällikkö	varmistaa lokivaatimusten toteutuksen ja säilytyspäätöksen (Tiedonhallintalaki §21) dokumentoinnin
Tietohallinnon järjestelmien vastuuhenkilö/tuotepäällikkö	vastaa lokienhallinnan periaatteiden vaatimuksien toteutumisesta omistamiensa järjestelmien osalta
Toimittajat/kumppanit	noudattavat sopimuksen tietoturva- ja lokitusvaatimuksia sekä lokienhallinnan periaatteita. Tuottavat sovitut lokit ja luovuttavat ne vaatimusten mukaisina hyvinvointialueen käyttöön.

4 Yleisimmät lokityypit ja käyttötarkoitukset

Sote-käyttö- ja luovutuslokit: potilas- ja asiakastietojen katselut, haut, muutokset ja luovutukset (sisältäen käyttötarkoitus/asiayhteys).

Tietoturvalokit: hyökkäysten ja poikkeamien havaitseminen (EDR/XDR, IDS/IPS, palomuuri, sähköposti/web-suodatus, DLP, haavoittuvuusskannaus jne.).

Ylläpitolokit: admin- ja konfiguraatiotoimet, käyttöoikeus- ja pääsynhallinnan muutokset.

Käyttäjähallinta- ja kirjautumislokit: AD/AAD, IAM, SSO/MFA, VPN, etäyhteydet.

Tekniset lokit: virheet, integraatiot, suorituskyky, tietokanta- ja OS-tapahtumat.

5 Vähimmäisvaatimukset lokitapahtumille

Pakolliset lokitietoihin tallennettavat kentät:

Päijät-Hämeen hyvinvointialue

- aikaleima
- tapahtuman tyyppi (katselu, haku, muutos, luovutus, kirjautuminen, epäonnistunut kirjautuminen…)
- käyttäjätunnus/toimija (user.id + user.role kun saatavilla)
- tapahtuman lähde komponentti/järjestelmä, ip-osoite, cliend.id (kun saatavilla)
- tapahtuman kohde id/tunniste/tyyppi
- tapahtuman lopputulema/tila (outcome, success/failure + virhekoodi)
- tapahtuman käyttötarkoitus (context.purpose)

Erityismerkinnät (tarvittaessa):

- erityissuoja / vahvistus, hoitosuhteen tekninen todennus, hakuehdot (ml. “ei tulosta” -haut).

Lähtökohtaisesti kielletty tietosisältö lokeissa: henkilötunnukset, tietosuoja-asetuksen tarkoittamat erityiset henkilötiedot, maksukorttitiedot, salasanat (myös tiivisteet), järjestelmäsalaisuudet, API-avaimet, valtuutustiedot ja henkilöiden välisen viestiliikenteen viestien sisältö.

Poikkeukset lokien sisältövaatimuksille tulee käsitellä yhdessä tietoturvan ja tietosuojan kanssa.

6 Tekniset lokitusvaatimukset

Keskitetty keräys: tietoturvalokit ohjataan keskitettyyn SIEM:iin reaali- tai lähes reaaliaikaisesti, tavoiteviive ≤ 5 min. Käyttövaltuushallinnan lokit tulisi ohjata keskitettyyn käyttövaltuushallinnan lokijärjestelmään.

Aikaleima ja kellonsynkronointi: kaikki lokittavat komponentit käyttävät yhteistä NTP-lähdettä ja kirjaavat lokitiedot UTC-ajassa.

Salaus: lokien siirto TLS salattuna ja säilytys salattuna.

Eheys: WORM/append-only tai kryptografinen sinetöinti; lokien katselu tuottaa meta-lokin.

Lokiformaatti: tavoitteellisesti RFC5424/syslog tai strukturoitu JSON dokumentoidulla kenttämapilla.

Pilvi/SaaS palveluiden lokitus: toimittaja tarjoaa rajapinnan lokien hakuun/siirtoon (API/webhook/syslog) ja noudattaa samoja formaatti- ja saatavuusvaatimuksia.

7 Lokien säilytys ja poistaminen

Lainsäädäntö edellyttää SOTE-käyttö- ja luovutuslokien säilyttämistä 12 vuotta lokitapahtumasta. Muiden lokien osalta hyvinvointialue päättää lokien säilytysajasta

Päijät-Hämeen hyvinvointialue

itsenäisesti tiedonhallintalain perusteella (tarpeellisuus, oikeuksien todentaminen, sopimukset, vanhentumisajat).

Lokien säilytysaikoja koskevat päätökset dokumentoidaan järjestelmäkohtaisesti järjestelmädokumentaatioon.

Lokien säilytysajan päätyttyä lokit poistetaan lopullisesti luotettavaa ja turvallista tietoturvapäällikön hyväksymää menetelmää käyttäen.

Ohjeelliset lokien vähimmäissäilytysaikavaatimukset, joista poikkeaminen edellyttää tietoturvapäällikön hyväksyntää:

Lokiryhmä	esimerkkejä	Säilytysaika	Peruste
Sote-käyttö- & luovutuslokit	Potilas-/asiakastietojen katselut/käyttäminen ja luovutukset	12 vuotta	Erityissääntely
Tietoturvalokit	EDR/XDR, palomuuri, IDS/IPS, DLP	3 -12kk	Tietoturvan valvonta, NIS2
Käyttäjähallinta- & kirjautumislokit	AD/AAD, IAM, SSO/MFA, VPN	3–12 kk	Tietoturvan valvonta, NIS2
Ylläpitolokit	Admin-toimet, konfiguraatiomuutokset	3–12 kk	Tietoturvan valvonta, NIS2
Tekniset virhelokit	Sovellus-/OS-virheet	3–6 kk	Vianselvitys ja teknisen toimivuuden varmistaminen

8 Lokien valvonta ja poikkeamien hallinta

Lokien valvonta toteutetaan keskitetyssä lokijärjestelmässä tietosuojan, SOC-palvelun tarjoajan, IT- infrapalveluiden toimittajien tai tietoturvan toimesta. Lokivalvonnan tavoitteena on havaita tietoturva- ja tietosuojapoikkeamat sekä reagoida niihin tehokkaasti.

Poikkeamien käsittely: dokumentointi, vaikutusarvio, korjaavat toimet, oppien läpikäynti; vakavista tapauksista viranomaisraportointi säänteIyn mukaan.

9 Raportointi ja rekisteröidyn oikeudet

- **Sisäinen raportointi:** kvartaaliraportit tietoturvalle ja tietosuojalle, raportointi johdolle tarvittaessa osana säännöllistä johdon raportointia
- **Rekisteröidyn tietopyyntö:** asiakas saa tiedon **omien tietojensa käytöstä** lain edellyttämässä määräajassa. Prosessi kattaa henkilöllisyyden varmistamisen, tietojen koonnin ja toimituksen. (erillinen ohjeistus hyvinvointialueen verkkosivuilla)

Päijät-Hämeen hyvinvointialue

10 Toimittajavaatimukset (sopimuksiin)

- Lokien omistus ja pääsy säilyvät rekisterinpitäjällä, toimittajan on annettava pyynnöstä pääsy myös ns. raakalokiin.
- Toimittajan ylläpitäjien tulee tehdä ylläpitotoimet henkilökohtaisilla tunnuksilla, ja ylläpitotoimenpiteet on lokitettava.
- Osana järjestelmädokumentaatiota dokumentoidaan myös lokituksen toteutus sekä lokitietojen säilytysajat ja tarkemmat määrittelyt lokitietojen valvonnasta.
- Toimittajan on toimittava hyvinvointialueelle pyydetyt sopimuksen mukaiset lokitiedot alle 24 tunnissa sekä sallittava lokitietojen integrointi keskitettyyn hyvinvointialueen omistamaan lokijärjestelmään/SIEM valvontaan.
- Lokitiedot on säilytettävä kaikissa tilanteissa EU/ETA alueella, josta on mahdollista poiketa vain erikseen kirjallisesti, hyväksyn poikkeaman perusteella.
- Lokitietoja on säilytettävä suojattuna, ja niiden päätyminen ulkopuolisille on estettävä. Ainoastaan erikseen lokitietojen käyttämiseen hyväksytyt henkilöt saavat perustellusta syystä tarkastella lokitietoja. Lokitietojen muuttaminen on estettävä kaikissa tilanteissa.
- **Muoto ja laatu:** yhteismuotoiset, dokumentoidut kentät; NTP/UTC; eheys ja salaus.

11 Poikkeamat lokienhallinnan periaatteisiin

Poikkeamat periaatteista hyväksyy tietoturvapäällikkö ja tietosuojavastaava yhteisesti, dokumentoidulla riskiperustelulla, määräaikaisina ja seurattavina.

Päijät-Hämeen aluehallitus

OIKAISUVAATIMUSOHJEET **Liitetään pöytäkirjanotteeseen**
Päijät-Hämeen hyvinvointialue

Oikaisuvaatimus-oikeus	Päätökseen tyytymätön voi tehdä kirjallisen oikaisuvaatimuksen. Oikaisuvaatimuksen saa tehdä se, johon päätös on kohdistettu tai jonka oikeuteen, velvollisuuteen tai etuun päätös välittömästi vaikuttaa (asianosainen) sekä hyvinvointialueen jäsen.

Oikaisuvaatimus-viranomainen	Viranomainen, jolle oikaisuvaatimus tehdään ja sen yhteystiedot **Toimielin:** **Päijät-Hämeen aluehallitus** **Postiosoite:** **Keskussairaalankatu 7, 15850 Lahti** **Puh.:** **(03) 819 11** **Sähköpostiosoite:** **kirjaamo@paijatha.fi** **Aukioloaika:** **Arkisin klo 9 - 15**
Oikaisuvaatimusaika ja sen alkaminen	Oikaisuvaatimus on tehtävä 14 päivän kuluessa päätöksen tiedoksisaannista ennen viraston aukioloajan päättymistä. Hyvinvointialueen jäsenen katsotaan saaneen päätöksestä tiedon seitsemän päivän kuluttua siitä, kun pöytäkirja on nähtävänä yleisessä tietoverkossa. Annettaessa päätös asianosaiselle tiedoksi hänen suostumuksellaan sähköisenä viestinä hänen katsotaan saaneen päätöksestä tiedon kolmantena päivänä viestin lähettämisestä, jollei muuta näytetä. Muuta tiedoksiantotapaa käytettäessä asianosaisen katsotaan saaneen päätöksestä tiedon, jollei muuta näytetä, seitsemän päivän kuluttua kirjeen lähettämisestä, saantitodistuksen osoittamana aikana tai erilliseen tiedoksisaantitodistukseen merkittynä aikana. Oikaisuvaatimusaika taloudellisin ja tuotannollisin perustein tehdystä irtisanomista koskevasta päätöksestä alkaa kulua vasta irtisanomisajan päättymisestä.

Pöytäkirjan nähtäväksi asettaminen	**Pvm:**
Tiedoksianto asianosaiselle	Asianosainen: toimialajohtaja Ismo Rautiainen, tietoturvapäällikkö Tanja Linnonmaa ☐ Annettu tiedoksi sähköisesti, pvm: ☐ Lähetetty tiedoksi kirjeellä, joka on annettu postin kuljettavaksi, pvm: (hyvinvointialuelaki 144 §) Tiedoksiantaja: ☐ Luovutettu asianosaiselle Paikka ja pvm: _____ Vastaanottajan allekirjoitus ☐ Muulla tavoin, miten Tweb
Oikaisuvaatimuksen sisältö ja sen toimittaminen	Oikaisuvaatimuksesta on käytävä ilmi vaatimus perusteluineen sekä sen tekijä ja yhteystiedot. Oikaisuvaatimus on toimitettava oikaisuvaatimusviranomaiselle oikaisuvaatimusajan kuluessa ennen sen viimeisen päivän virka-ajan päättymistä riippumatta tavasta, jolla se toimitetaan. Jos oikaisuvaatimusajan viimeinen päivä on pyhäpäivä, itsenäisyyspäivä,

	vapunpäivä, joulu- tai juhannusaatto tai arkilauantai, saa oikaisuvaatimuksen toimittaa ensimmäisenä sen jälkeisenä arkipäivänä. Omalla vastuulla oikaisuvaatimuksen voi lähettää postitse tai lähetin välityksellä. Postiin oikaisuvaatimus on jätettävä niin ajoissa, että se ehtii perille oikaisuvaatimusajan viimeisenä päivänä ennen viraston aukioloajan päättymistä.