Tietoturvapolitiikka

Itä UUSIMAA
Östra NYLAND

Hyvinvointialue
Välfärdsområde

Sisällysluettelo

1. Hyväksyntä

Itä-Uudenmaan hyvinvointialueen tietoturvapolitiikan hyväksyy hyvinvointialueen aluehallitus. Politiikka on voimassa toistaiseksi vahvistetusta käyttöönotosta alkaen. Politiikkaa päivitetään tarvittaessa ja uusi päivitysversio kumoaa vanhan politiikan hyvinvointialueen aluehallituksen erillisellä päätöksellä.

Käyttö: Itä-Uudenmaan hyvinvointialueen henkilöstön ja sidosryhmien käyttöön
Käyttöalue: Itä-Uudenmaan hyvinvointialueen organisaatio

Päiväys	**Hyväksyntä**	**Tekijä(t)**	**Hyväksyjä(t)**
xx.xx.2022	Tietoturvasuunnitelman käyttöönotto	Tietoturva-asiantuntija Tuomas Lintula	Itä-Uudenmaan hyvinvointialueen aluehallitus

2. Muutosloki

Tämän politiikan alkuperäinen versio 1.0 on laadittu 3.2.2022. Tehdyt muutokset:

3.2.2022 / Versio 1.0 / Tietoturva-asiantuntija Tuomas Lintula

-Laadittu politiikasta ensimmäinen versio.

8.6.2022 / Versio 1.1 / Tietoturva-asiantuntija Tuomas Lintula

-Muokattu tietoturvapolitiikka Itä-Uudenmaan hyvinvointialueen viralliselle asiakirjapohjalle.

23.6.2022 / Versio 1.2 / Tietoturva-asiantuntija Tuomas Lintula

-Korjattu asia- ja rakennevirheet.
-Lisätty kappaleet Liite 2, Käyttöoikeudet, Lokitiedot ja Hankinnat.
-Lisätty vastuisiin jokaisen työntekijän vastuut.

3. Johdanto

”Itä-Uudenmaan hyvinvointialueen tietoturvapolitiikassa määritellään tietoturvallisuutta koskevat periaatteet.”

3.1. Mitä on tietoturvallisuus?

Itä-Uudenmaan hyvinvointialueen toiminta ja palvelut perustuvat enenevässä määrin tietoon. Ollakseen tehokkaasti hyödynnettävissä tietoa tukevien järjestelyjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tämä edellyttää tehokasta johtamista luotettavien toteutusten ja osaavan henkilöstön tueksi.

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon:

- **Luottamuksellisuus**; tiedot ovat vain niiden käyttöön oikeutettujen saatavilla,
- **Eheys**; tietoja eivät voi muuttaa muut kuin siihen oikeutetut,
- **Saatavuus**; tiedot ovat niiden käyttöön oikeutettujen saatavilla ja hyödynnettävissä.

3.2. Tietoturvapolitiikka

Lain julkisen hallinnon tiedonhallinnasta (906/2019) 4 § nojalla Itä-Uudenmaan hyvinvointialueen tiedonhallinta ja tietoturvatoiminta tulee olla suunnitelmallista.

Itä-Uudenmaan hyvinvointialueen aluehallitus määrittelee tässä Itä-Uudenmaan hyvinvointialueen tietoturvapolitiikassa tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Politiikka on sisällöllisesti yleisluontoinen, josta viitataan toimialakohtaisiin tietoturvasuunnitelmiin ja -ohjeisiin.

Politiikka toimii perustana hyvinvointialueen tietoturvallisuutta koskeville toimialakohtaisille tietoturvasuunnitelmille ja -ohjeille, joiden tehtävänä on tarkentaa hyvinvointialueen tietoturvapolitiikassa annettuja määräyksiä sekä ohjeistaa niiden käytäntöön

soveltamisessa. Toimialoilla on omat tietoturvasuunnitelmansa, koska niitä koskevat omat erityislainsäädäntönsä sekä tietoturvavaatimuksensa. Lisäksi toimialakohtaisten suunnitelmien ja ohjeiden hallinta sekä ylläpito on helpompaa.

Itä-Uudenmaan hyvinvointialueen tietoturvapolitiikka koskee koko hyvinvointialueen organisaatiota sekä kaikkia sen sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät hyvinvointialueen omistamaa tai hallinnoimaa tietoa. Politiikka kattaa hyvinvointialueen käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta. Tietoturvapolitiikka on käyttäjien saatavilla sähköisessä muodossa hyvinvointialueen verkkosivuilla ja tarvittaessa paperiversiona.

4. Hyvinvointialueen tietoturvallisuutta koskevat velvoitteet

”Itä-Uudenmaan hyvinvointialueen tietoturvatoimintaa ohjaavat lainsäädäntö, ohjeet, viitekehykset ja linjaukset.”

Hyvinvointialueen tietoturvallisuuden kehittämisen ja ylläpitämisen toimintaa ohjaavat soveltuvilta osin lainsäädäntö, ohjeet ja viitekehykset. Käytännössä nämä ohjaavat tekijät voidaan jakaa kolmeen tärkeään kokonaisuuteen:

- Lainsäädäntö
- Ohjeet ja viitekehykset
- Toimialakohtaiset linjaukset

4.1. Lainsäädäntö

Hyvinvointialueen tietoturvallisuuden yleisistä periaatteista säädetään **tiedonhallintalaissa** (906/2019). Lisäksi **Euroopan parlamentin ja neuvoston yleinen tietosuoja-asetus** (2016/679, GDPR) asettaa vaatimuksia henkilötietojen tietoturvallisesta käsittelystä hyvinvointialueen toimiessa rekisterinpitäjänä. Tietosuoja-asetusta täydentävää kansallista lainsäädäntöä henkilötietojen käsittelystä käsitellään **laissa työelämän tietosuojasta** (759/2004) sekä **tietosuojalaissa** (1050/2018).

4.2. Ohjeet ja viitekehykset

Hyvinvointialueen tietoturvallisuutta ohjaavat soveltuvilta osin seuraavat viitekehykset:

- Hyvinvointialuetta velvoittava lainsäädäntö
- Hyvinvointialueen strategia ja siitä johdetut vaatimukset
- Hyvinvointialueen tietoturvapolitiikka, toimialojen tietoturvasuunnitelmat ja -ohjeet
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Valtionhallinnon tietoturvallisuuden (VAHTI) ohjeet

- Valtion tieto- ja viestintätekniikkakeskuksen (Valtori) ohjeet ja suositukset

4.3. Toimialakohtaiset linjaukset

Toimialakohtaiset linjaukset ja tietoturvallisuutta koskevat yksityiskohtaiset vaatimukset on kirjattu hyvinvointialueen toimialueiden omiin tietoturvasuunnitelmiin sekä ohjeisiin.

5. Tietoturvallisuustavoitteet

”Tietoturvallisuus vähintään perustasolle koko hyvinvointialueella.”

Tietoturvasta tinkiminen vaarantaa hyvinvointialueen toiminnan jatkuvuuden ja palveluiden saatavuuden. Tietoturvapoikkeama aiheuttaa korjauskuluja, palvelukatkoja, huonoa mainetta ja voi johtaa oikeudellisiin seuraamuksiin.

5.1. Riskiperusteinen lähestymistapa

Tietoturvallisuustoimet tulee aina suhteuttaa suojattavaan tietoon; julkisen tiedon suojaamiseksi ei tarvita samanlaisia toimenpiteitä kuin salassa pidettävien tietojen suojaamiseksi. Tietoturvauhkien kartoittamisen kautta muodostetaan käsitys suojattavaan tietoon kohdistuvista riskeistä, jotka arvioidaan ja joiden perusteella tietoturvallisuustoimenpiteet toteutetaan.

Riskiarvioon perustuvat tietoturvajärjestelyt toteutetaan monitasoisen suojaamisen periaatetta noudattaen. Tietoturvajärjestelyiden riittävyyttä arvioidaan julkishallinnon yleisiä vaatimustasoja ja alan vakiintuneita standardeja vasten. Tällaisia ovat esimerkiksi kansallinen (tieto)turvallisuuden arviointikriteeristö (Katakri) ja pilvipalveluiden turvallisuuden arviointikriteeristö (Pitukri).

Tieto- ja ICT-riskien hallinnassa sovelletaan hyvinvointialueen riskienhallinnasta annettuja ohjeita ja määräyksiä. Toimialat arvioivat tietojensa ja tietojärjestelmiensä vaatimien turvatoimien tarpeen ja määrittelevät tietoturvajärjestelyt.

5.2. Tietoturvan tasot

Tietojärjestelmän suojaustaso määräytyy siinä käsiteltyjen tietojen eniten suojausta vaativan tiedon mukaan. Tietoaineiston suojaamistarpeista on huolehdittava tarvittavien teknisten ratkaisujen ja hallinnollisten prosessien avulla siten, että ne mitoitetaan aina

suojattavan kohteen merkityksen mukaan. Tietoaineiston saatavuudesta tulee huolehtia, vaikka sen luottamuksellisuuteen liittyisikin tiukkoja vaatimuksia.

5.2.1. Tietoturvan perustaso

Toimintaan liittyvät tietoturvallisuusriskit tulee olla kartoitettu ja tietoturvallisuuden hoitamista ja asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritelty. Tietojen saanti ja käytettävyys tulee turvata eri tilanteissa, myös poikkeustilanteissa.

Mikäli järjestelmässä on julkisuuslaissa (JulkL 24.1 1–32) tai erillislaeissa säädettyä salassa pidettävää tietoa, sen tietoturva tulee toteuttaa vähintään VAHTI-ohjeistuksissa kuvatun perustason mukaan (ohjeissa käytetty tason vaatimuksista nimikettä turvallisuusluokka IV, suojaustaso IV tai käyttö rajoitettu).

Viranomaisen turvaluokittelemaa tietoa tulee käsitellä kyseiselle turvaluokalle annettujen vaatimusten mukaisesti. Turvaluokitellun tiedon käsittelyä voi tapahtua sekä sähköisesti että muutoin (esimerkiksi paperilla).

5.2.2. Tietoturvan korotettu taso

Osassa hyvinvointialueen toimintoja tavoitetason tulee olla perustasoa korkeampi.

Yleistä tietoturvan perustasoa korkeampaa kyvykkyyttä tietoturvaosaamisessa saatetaan tarvita raha- ja maksuliikenteessä, salassa pidettävien ja erityisiin henkilötietoryhmiin kuuluvien henkilötietojen (esim. terveystietojen) käsittelyssä, turvallisuuteen, tietoturvallisuuteen ja varautumiseen liittyvässä toiminnassa sekä silloin, kun käsitellään valtionhallinnon salassa pidettäväksi merkitsemiä asiakirjoja tai muuta salassa pidettävää aineistoa.

Tällaisia erityisjärjestelyitä ovat käytännössä esimerkiksi korotetun tietoturvatason viestintäjärjestelmät (suojattu sähköposti, suojattu matkapuhelin), ryhmätyöympäristöt (suojattu ryhmätyöympäristö), tallennusalustat tai korotetun turvatason työasemat.

6. Tietoturvallisuuden organisointi ja vastuut

”Tietoturvallisuuden vastuut ja velvollisuudet on määritelty.”

Itä-Uudenmaan hyvinvointialueen keskeisimmät tietoturvallisuuteen liittyvät toimijat ja roolit vastuineen on määritelty alla.

Hyvinvointialueen aluehallitus on hyvinvointialueen ylin kokonaisturvallisuudesta päättävä taho. Aluehallitus hyväksyy tähän tietoturvapolitiikkaan ehdotetut muutokset.

Hyvinvointialueen johtaja toimii tietoturvallisuuden ja -suojan omistajana hyvinvointialueella luoden edellytykset niiden asianmukaiselle toteuttamiselle.

Hyvinvointialueen tietoturvavastaava vastaa hyvinvointialueen tietoturvallisuuden toteutumisesta ja integroitumisesta muihin kokonaisturvallisuuden osa-alueisiin. Vastuuseen sisältyy tarvittava suunnittelu, ohjaus, seuranta ja kehittäminen sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi. Tietoturvavastaava raportoi hyvinvointialueen johdolle.

Toimialojen johto vastaa tietoturvallisuuden ja -suojan toteutumisesta alaisessaan toiminnassa. Lisäksi toimialojen johto hyväksyy toimialansa käyttöönotettavat tietoturvasuunnitelmat ja -ohjeistukset.

Toimialojen tietoturvavastaavat vastaavat toimialojensa tietoturvallisuuden toteutumisesta ja integroitumisesta hyvinvointialueen tietoturvakokonaisuuteen. Vastuuseen sisältyy tarvittava suunnittelu, ohjaus, seuranta ja kehittäminen sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi.

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta alaisessaan toiminnassa.

Tiedon ja tietojärjestelmien käyttäjä vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen käyttäjän vastuulla on lisäksi tietoturvaan ja -suojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen erillisen ohjeistuksen mukaisesti.

Tiedon, tietojärjestelmän tai palvelun omistaja vastaa omistukseensa liittyvästä:

- Käyttäjien ja käyttöoikeuksien määrittelystä, hyväksynnästä ja valvonnasta
- Riskienhallinnan toteuttamisesta
- Tiedon eheyden varmistamisesta
- Tietojen luokittelusta (julkisuuden ja salassapidon määrittely sekä arkistonmuodostus).

Hyvinvointialueen IT-palveluiden tuottaja vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

Pääkäyttäjät valvovat tietoturvan toteutumista omilla vastuualueillaan. Pääkäyttäjät huolehtivat sovelluksen ylläpitotoiminnoista ja varmistavat, että järjestelmää käytetään lakien, säädösten ja ohjeiden mukaisesti.

Tietosuojavastaavan tehtävänä on antaa asiantuntija-apua sekä organisaation henkilöstölle että johdolle tietosuoja-asioissa. Tietosuojavastaava raportoi hyvinvointialueen johdolle.

Työntekijä on velvollinen noudattamaan annettuja ohjeistuksia ja määräyksiä. Lisäksi jokainen työntekijä on velvollinen ilmoittamaan tietoturvapoikkeamista.

7. Tiedon ja tietojärjestelmien tietoturvallinen käyttö

”Varmistetaan tietojen luottamuksellisuus, eheys ja saatavuus.”

Hyvinvointialueen käytössä oleva tieto sekä tietojärjestelmät, laitteet ja ohjelmistot on tarkoitettu työtehtävien hoitamista varten. Hyvinvointialueen tietojärjestelmäympäristössä saa käyttää ainoastaan IT-palveluiden tuottajan hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja. Asennustyön saa suorittaa vain hyvinvointialueen valtuuttama taho.

7.1. Käyttöoikeuksien hallinta

Käyttöoikeudet hyvinvointialueen tietoon ja tietojärjestelmiin myönnetään työtehtävien hoitoon roolipohjaisesti ja työtehtävien käyttötarpeiden mukaisessa laajuudessa. Käyttöoikeudet hyväksyvät hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho. Peruskäyttöoikeudet muodostuvat henkilöstöjärjestelmän tietojen perusteella automaattisesti.

Vastuu käyttöoikeuksista on aina sillä toimialalla, joka ne myöntää. Esimiehen tulee huolehtia alaistensa käyttöoikeuksien asianmukaisuudesta ja ajantasaisuudesta.

7.2. Lokitietojen kerääminen

Lokitieto tarkoittaa dokumenttia (tapahtumakirjanpitoa) jonkin tapahtuman toteutumisesta tiettynä hetkenä. Silloin kun tieto- ja viestintäjärjestelmän toiminta tai todennetun käyttäjän toimet pitää osoittaa kiistämättömästi, tulee tarvittava tapahtumakirjanpito toteuttaa tietojen eheyden säilyttävillä teknisillä ratkaisuilla (lokijärjestelmät).

Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi hyvinvointialueen normaalein kurinpidollisin keinoin tai lainsäädännön edellyttämällä tavalla. Tiedon turvalliset käsittelytavat ja tietoturvapoikkeamien hallinta kuvataan erillisissä ohjeissa.

8. Tietoturvaosaamisen ja -tietoisuuden ylläpito

”Henkilöstön koulutus on edellytys tietoturvallisuuskulttuurin luomiselle ja ylläpidolle.”

Jokainen uudessa tehtävässä aloittava työtekijä perehdytetään hyvinvointialueen perehdytyskäytäntöjen mukaisesti tietoturvan perusteisiin ja tietoturvan toteuttamiseen hänen omissa työtehtävissään. Uuden työntekijän tulee suorittaa hyvinvointialueen tietoturvakoulutus mahdollisimman nopeasti tehtävässä aloittamisesta, jotta hänelle voidaan myöntää käyttöoikeuksia hyvinvointialueen tietojärjestelmiin ja -palveluihin. Lisäksi ajantasaiset tietoturvaohjeet ovat kaikkien työntekijöiden saatavilla ja tietoturvallisuuden jatkokoulutusta järjestetään säännöllisesti.

Tietoturvaosaamisen ylläpito kuvataan yksityiskohtaisemmin toimialakohtaisissa tietoturvasuunnitelmissa ja ohjeissa. Tietoturvallisuuden ja -suojan ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan riittävä hallinnollinen ja tekninen koulutus.

9. Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

”Ihmiset, prosessit ja teknologia.”

Tämä Itä-Uudenmaan hyvinvointialueen tietoturvapolitiikka katselmoidaan vuosittain ja päivitetään hyvinvointialueen tietoturvavastaavan toimesta tarvittaessa.

Itä-Uudenmaan hyvinvointialueen toimialojen tietoturvasuunnitelmat sekä ohjeistukset katselmoidaan vuosittain ja päivitetään kyseisen toimialan tietoturvavastaavan toimesta tarvittaessa.

Itä-Uudenmaan hyvinvointialueen tietoturvallisuustyö perustuu ihmisten, prosessien ja teknologian jatkuvaan kehittämiseen seuraavien vaiheiden mukaisesti:

- **Suunnittelu**; tuotetaan analyysien ja arvioiden perusteella suunnitelmia ja ohjeita.
- **Toteutus**; suunnitteluvaiheen tuotokset otetaan käyttöön hyvinvointialueen toiminnassa.
- **Seuranta**; suoritetaan teknistä valvontaa sekä hallinnollista seurantaa.
- **Muutoshallinta**; seurantavaiheessa opittujen asioiden perusteella toteutetaan muutoshallintaa hyvinvointialueen muutoshallintaprosessin mukaisesti.

10. Hankinnat ja sopimukset

”Tietoturvallisuus otetaan huomioon hankinnoissa ja sopimuksissa.”

Hankinnoissa tulee noudattaa hankintalainsäädäntöä, hyvinvointialueen hankintaohjeistusta sekä julkishallinnon yleisiä suosituksia ICT-hankintojen ja hankinnan kohteiden tietoturvan huomioimisesta.

Erityistä huomiota tulee kiinnittää siihen, että tieto- ja viestintätekniset hankinnat sopivat hyvinvointialueen kokonaisarkkitehtuuriin. Tieto- ja viestintäteknisissä hankinnoissa tulee hankintalainsäädännön asettamissa puitteissa pyrkiä mahdollisimman yhdenmukaisiin, olemassa olevaa osaamista hyödyntäviin hankintoihin kokonaistaloudellisuus ja riskit huomioon
ottaen.

Jo hankintaa suunniteltaessa tulee määritellä, millaista tietoturvan tasoa tavoitellaan, mitkä ovat asianmukaiset tietoturvajärjestelyt ja kuinka tietoturvan toteutumista valvotaan.

Tietosuojan osalta tietosuoja-asetus edellyttää, että hyvinvointialue saa käyttää ainoastaan sellaisia palvelutuottajia tai muita henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset ja varmistettava rekisteröidyn oikeuksien suojelu.

Liite 1 Hyvinvointialueen tietoturvaohjeet

Tähän liitteeseen on kerätty hyvinvointialueen tietoturvallisuutta koskevat ohjeet. Alla olevien ohjeiden lisäksi toimialoilla voi olla omia tarkentavia ohjeita.

- Esimiehen tietoturvaohje
- Henkilöstön tietoturvaohje
- IT-henkilöstön tietoturvaohje
- Tietojärjestelmän omistajan tietoturvaohje
- Tietoturvapoikkeamien hallintaohje
- Salasanaohje

Liite 2 Lisätietoa

Keskeisiä lakeja tietoturvan kannalta ovat:

- Laki julkisen hallinnon tiedonhallinnasta 906/2019
- Laki digitaalisten palvelujen tarjoamisesta 306/2019
- Laki sähköisen viestinnän palveluista 917/2014
- Laki viranomaisten toiminnan julkisuudesta 621/1999

Tiedonhallintalautakunnan ohjeet ja suositukset, esimerkiksi seuraava:

- Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta

Keskeisiä julkishallinnolle annettuja yleisiä tietoturvaohjeita (Vahti-ohjeet) ovat tuoreimmat ohjeet, esimerkiksi seuraavat:

- Vahti 22/2017 Ohje riskienhallintaan
- Vahti 8/2017 Tietoturvapoikkeamatilanteiden hallinta
- Vahti 2/2016 Toiminnan jatkuvuuden hallinta
- Vahti 2/2014 Tietoturvallisuuden arviointiohje
- Vahti 2/2012 ICT-varautumisen vaatimukset
- Vahti 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, jonka liitteissä kuvattu käsittelyvaatimuksia

Julkishallinnon tietoturvan arviointiin keskeisiä ovat seuraavat:

- Katakri: Tietoturvallisuuden auditointityökalu viranomaisille
- Pitukri: Pilvipalveluiden turvallisuuden arviointikriteeristö

Eräitä muita julkishallinnon ohjeita ovat seuraavat:

- Turvallisen sovelluskehityksen käsikirja, Väestörekisterikeskus
- Turvallinen tuotekehitys -opas, Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom