Pohjois-Savon hyvinvointialue

NIS 2 direktiivin / kyberturvallisuuslain toimeenpano PSHVA:lla. - riskienhallinnan toimintamallin käsittely

Aluehallitus 9.6.2025

15.4.2025

Pohjois-Savon hyvinvointialue

Esityksestä

- Esittelijä tietoturvapäällikkö Marko Ruotsala
- Yleiskatsaus NIS 2 direktiiviin ja kyberturvallisuuslakiin
  - Keskeisimmät huomiot
- Kyberturvallisuuslain toimeenpanon tilanne PSHVA:lla
- ”Kyberturvallisuuslain mukainen riskienhallinnan toimintamalli”
  - Käsittely ja hyväksyntä

Pohjois-Savon hyvinvointialue

NIS 2 direktiivi

- Direktiivi toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa (NIS2-direktiivi) Linkki
- Annettu 14.12.2022
- NIS 2 -direktiivillä luodaan yhtenäinen oikeudellinen kehys kyberturvallisuuden ylläpitämiseksi 18 kriittisellä alalla kaikkialla EU:ssa
- Edeltäjänä direktiivi NIS1 (2016/1148)
- Verkko- ja tietoturvadirektiivi **nostaa kyberturvallisuutta koskevaa EU:n yhteistä tavoitetasoa laajemmalla soveltamisalalla, selkeämmillä säännöillä ja vahvemmilla valvontavälineillä**

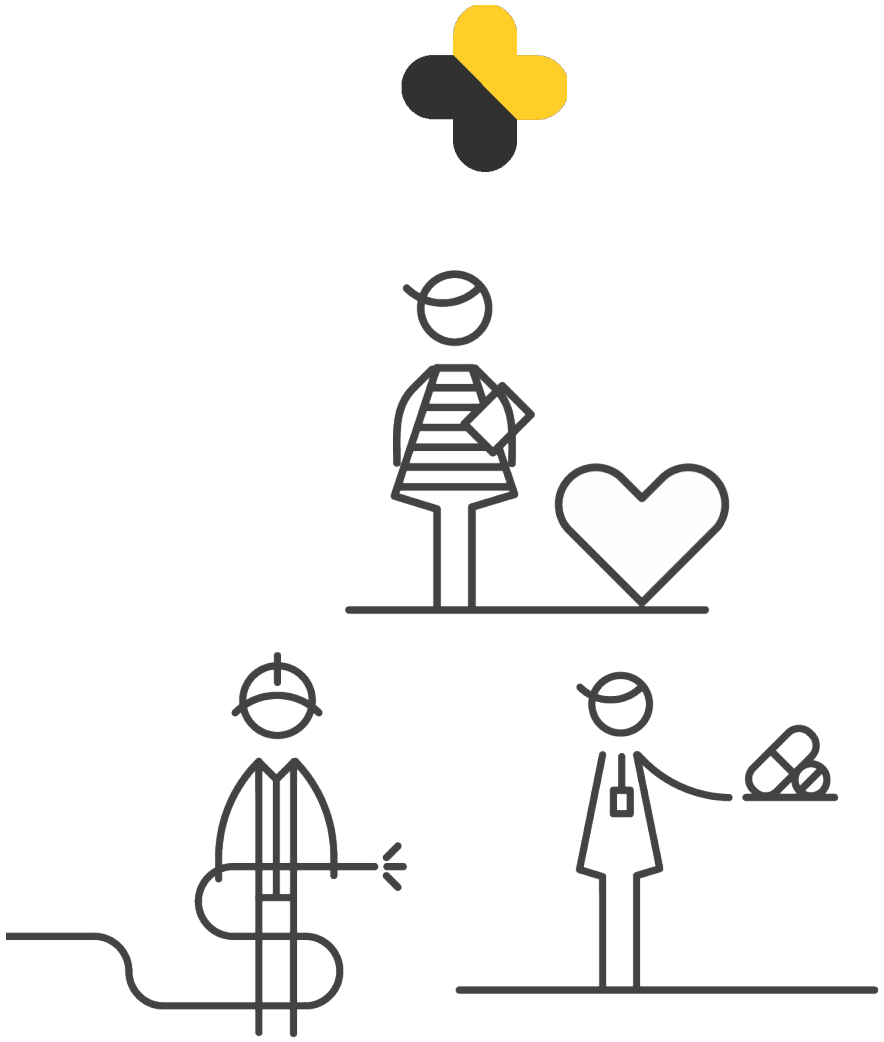
Kyberturvallisuuslaki

- Eduskunnan täysistunto, tiistai 11.3.2025
- ”*Eduskunta hyväksyi ensimmäisessä käsittelyssä sisällöltään päätetyt, hallituksen esitykseen HE 57/2024 vp sisältyvät 1.-17. lakiehdotuksen. Lakiehdotusten toinen käsittely päättyi. Eduskunta hyväksyi mietintöön sisältyvät lausumaehdotukset. Asian käsittely päättyi*.” PTK 20/2025 vp
- Kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskeva lainsäädäntö (tärkeimpänä uusi Kyberturvallisuuslaki)
- Kyberturvallisuuslaki voimaan 4.4.2025
- 124/2025 | Suomen säädöskokoelma | Finlex

Pohjois-Savon hyvinvointialue

Soveltamisala: hyvinvointialue

- NIS 2 liite 1. Erittäin kriittiset toimialat
  - Kohta 5. Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU (18) 3 artiklan g alakohdassa määritellyt terveydenhuollon tarjoajat
    - L_2022333FI.01008001.xml
- NIS2-direktiivin soveltamisalaan kuuluvat terveydenhuollon tarjoajat, EU:n vertailulaboratoriot, lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat, eräät lääkeaineiden ja lääkkeiden valmistusta harjoittavat toimijat sekä vakavan kansanterveysuhan aikana kriittisiksi katsottuja lääkinnällisiä laitteita valmistavat toimijat
  - Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi HE 57/2024



Mikä muuttui / muuttuu hyvinvointialueen näkökulmasta?

- Aiempaa regulaatiota (osittainen listaus keskeisimmistä)

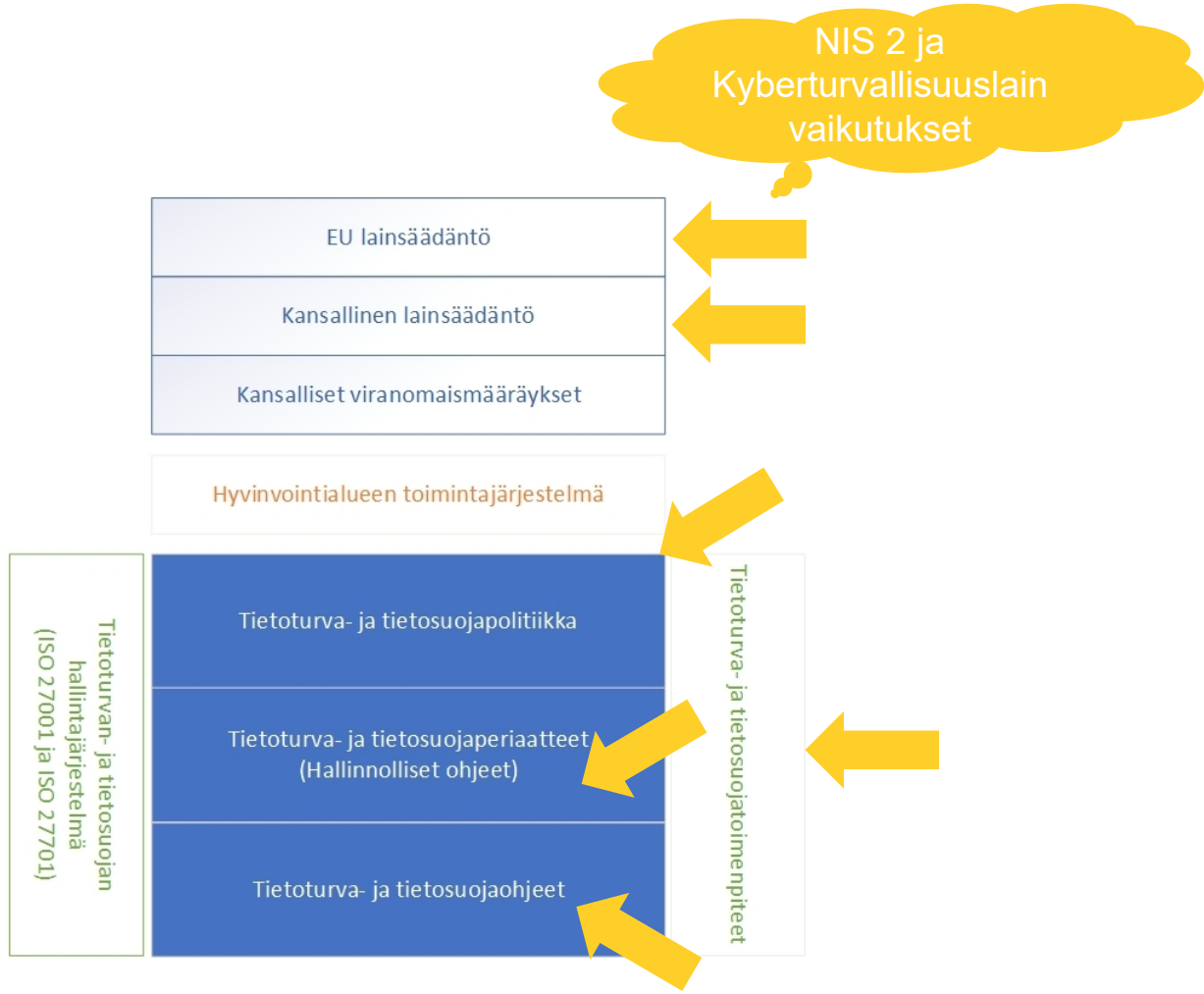
- Yleinen tietosuoja-asetus vuodelta 2016 (soveltaminen 25.5.2018)
  - Samankaltainen riskilähtöinen lähestymistapa, kuin NIS 2, ISO 27000 sarjan standardit ym. parhaat käytännöt
- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (2023/703)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki lääkinnällisistä laitteista (719/2021)
- Laki hyvinvointialueesta (611/2021)
- Kyberturvallisuuslaki (2025)

- Sosiaali- ja terveydenhuollon tiedonhallintaa ja asiakastietojen sähköistä käsittelyä ohjataan asiakastietolakiin pohjautuvilla THL:n määräyksillä. mm.
  - Määräys 3/2024 tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista
  - Määräys 4/2024 sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta ja sertifioinnista
  - Määräys 5/2024 sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten olennaisista vaatimuksista
- Sosiaali- ja terveysministeriön asetus sosiaali- ja terveydenhuollon asiakastietojen käsittelystä

Tietoturvan ja tietosuojan hallintamalli Pohjois-Savon hyvinvointialueella – pohjalla parhaat käytännöt ja regulaatio

- *”Ylin ohjaava taso hyvinvointialueen tietoturvallisuuden ja tietosuojan hallinnassa on lainsäädäntö. Soveltuvaa lainsäädäntöä on sekä EU-tasolla että kansallisella tasolla. Keskeinen lainsäädäntö on kuvattu tietoturva- ja tietosuojapolitiikan liitteessä 2. Lainsäädännön lisäksi toiminnassa huomioidaan toimivaltaisten viranomaisten määräykset ja standardit.”*
- *”Toimintajärjestelmän keskeisiä osa-alueita ovat toimintajärjestelmän kuvaus, prosessit ja ohjeet. Tietoturvallisuuden ja tietosuojan hallintajärjestelmässä noudatetaan soveltuvin osin ISO 27001 ja ISO 27701 standardeja. Standardeilla pyritään varmistamaan laadukas, ajantasainen ja vaatimustenmukainen tietoturvan ja tietosuojan hallintajärjestelmä.”*

- PSHVA tietoturva- ja tietosuojapolitiikka joulukuulta 2022



Pohjois-Savon hyvinvointialue

Keskeistä kyberturvallisuuslaissa - Riskienhallinta (7,8,9 §)

- Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen
- Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin
- Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta
- Toimijalla on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta

Pohjois-Savon hyvinvointialue

Keskeistä kyberturvallisuuslaissa - Riskienhallinnan toimintamallin keskeinen sisältö

- 1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;
- 2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;
- 3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;
- 4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
- 5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;
- 6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;
- 7) pääsynhallinnan ja todentamisen menettelyt;
- 8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;
- 9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;
- 10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;
- 11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä
- 12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

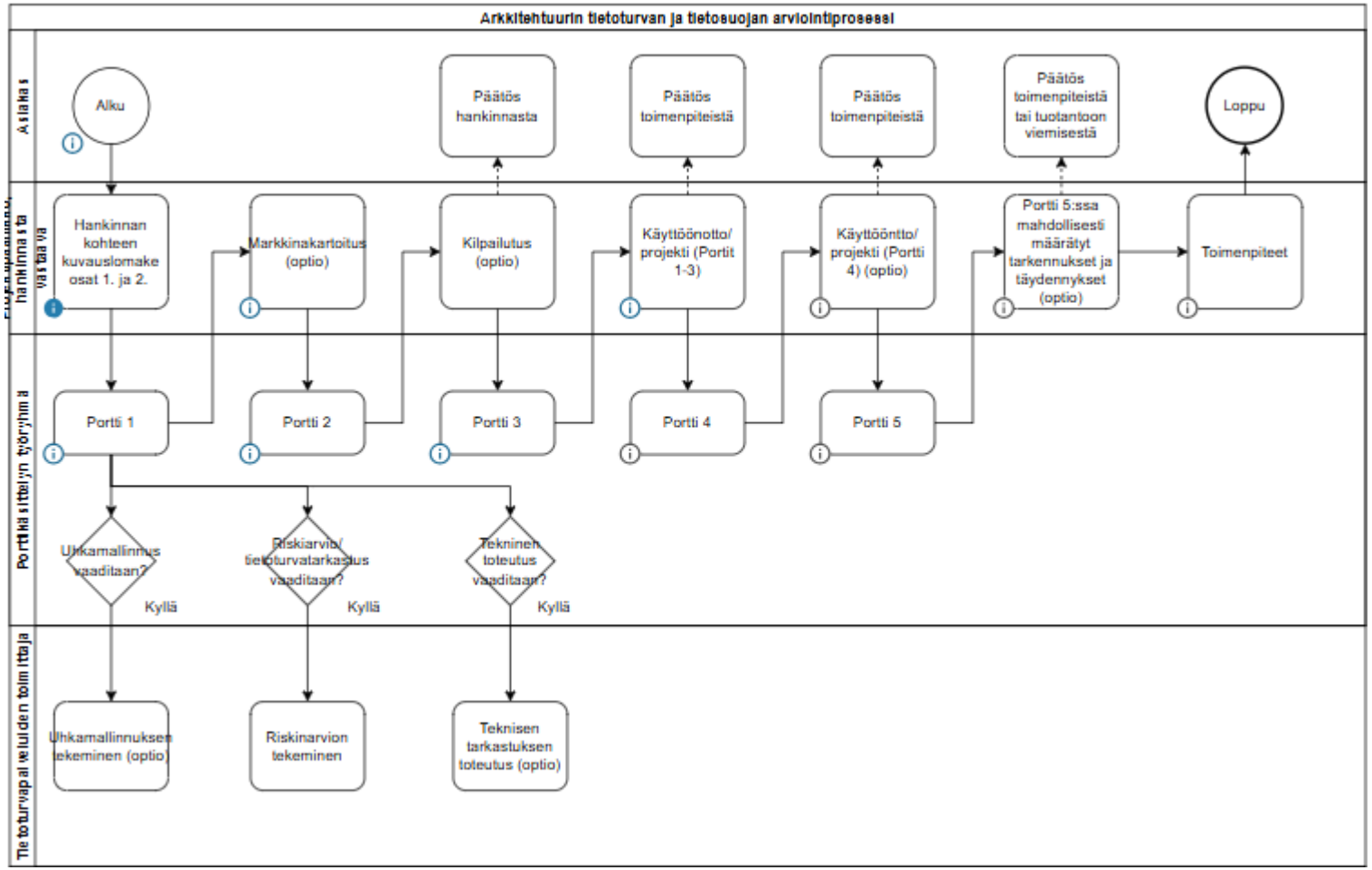
Pohjois-Savon hyvinvointialue

Riskienhallinnan toimintamalli PSHVA:lla versio 1.0

Riskienhallinnan toimintamalli PSHVA:lla versio 1.0

- Kuvataan ylätasolla Kyberturvallisuuslain 7, 8 ja 9 §:ien mukainen riskienhallinnan toimintamalli
- Kyberturvallisuuden riskienhallinnan toimintamalli täydentää tietoturvan ja tietosuojan politiikan ja sen liitteiden, periaatedokumenttien, ohjeiden ja määräysten kokonaisuutta
- Kyseessä on ensimmäinen versio Kyberturvallisuuden riskienhallinnan toimintamallista, ja se tulee täydentymään seuraavissa versioissa
  - Tämä toimintamalli katselmoidaan vuosittain ja mahdolliset päivitykset käsitellään hyvinvointialueen aluehallituksessa
- Pohjois-Savon hyvinvointialueen tietoturvallisuuteen ja rekisterinpitoon liittyvät vastuut ovat määritetty hallintosäännössä ja sitä täydentävässä tietoturva- ja tietosuojapolitiikan liitteessä 3.
  - Liite 3. on päivitetty vastaaman kyberturvallisuuslain vaatimuksia 5.2.2025
- 5.2.2025 päivätyssä versiossa on lisätty aluehallituksen osalta seuraavaa: ”Hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista” ja ”Aluehallituksen jäsenillä tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan”. Lisäksi hyvinvointialueen johtajan ja hyvinvointialueen johtoryhmän osalle on lisätty vastaavasti: ”Tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan

Arkkitehtuurin tietoturvan ja tietosuojan arvioprosessi



Pohjois-Savon hyvinvointialue

Toimenpiteitä riskienhallinnan osalta

- Organisaatiokohtaiset riskiarviot (määräajoin)
  - Digiturvan kokonaispalvelu
  - Kybermittari
  - Kysymyksiä osana yksikkökohtaista riskiarviota
- Järjestelmäkohtaiset riskiarviot laatuporttiin
  - Osana porttikäsittelyä ja muutoksenhallintaa
  - Uusi riskienhallinnan tietojärjestelmä (muuttaa Excelit ja pdf:t seurattavaksi kokonaisuudeksi mm. vastuineen) ja tuo myös ulkopuoliset arviot samaan kokonaisuuteen
  - Uudet riskienhallinnan väittämät
- Riskien arviointi on yhteistyötä eri asiantuntijoiden muodostama työryhmänä
  - Esim. Palvelun omistaja, tuotevastaava, tuotepäällikkö, tietosuoja-asiantuntija, tietoturva-asiantuntija, juristi jne.
    - Jokaisella on oma vastuunsa ja velvollisuutensa tukea riskienarvioinnin tekijää, etenkin jos arviointia tehdään ensimmäistä kertaa kattavasti
- Uudet vaatimukset kilpailutuksiin erityisesti toimitusketjun riskienhallinnan ja raportoinnin osalta
- Kyberriskien raportoinnin jatkokehitys

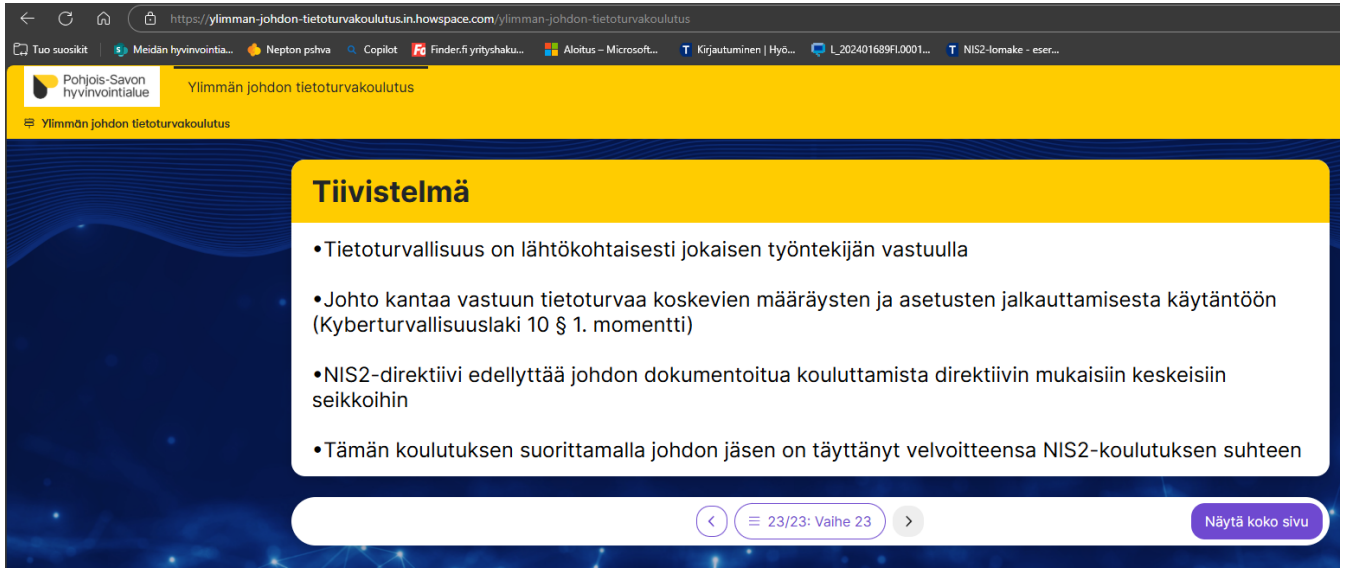
Pohjois-Savon hyvinvointialue

Keskeistä kyberturvallisuuslaissa - johdon vastuut (§ 10)

- Toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista
- Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan
- Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa

Ylimmän johdon koulutus

- PSHVA:n tietoturvapalvelut yksikön toimesta valmistellun ylimmän johdon kyberturvallisuuskoulutuksen suorittavat hyvinvointialueen aluehallituksen jäsenet ja hyvinvointialueen johtotiimin jäsenet
- Koulutus on pakollinen ja suoritukset koordinoi hallintopäällikkö

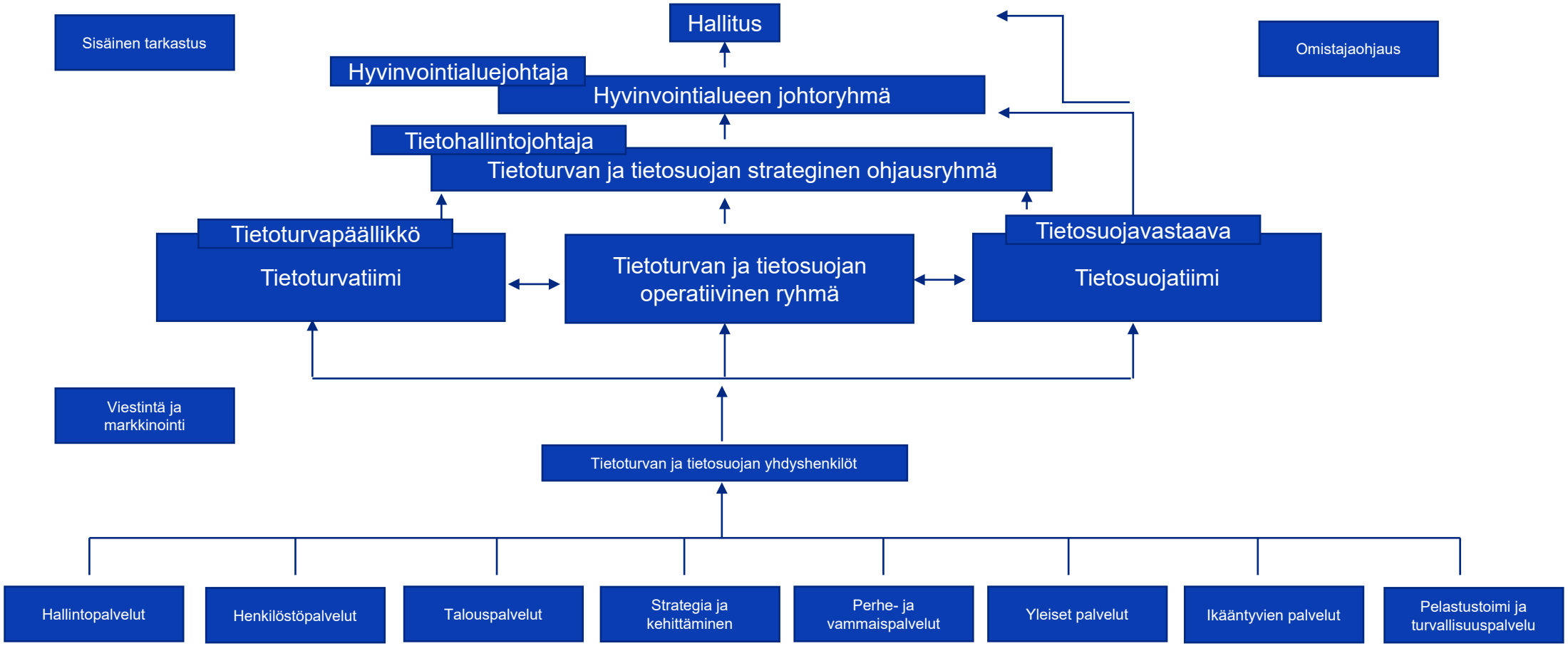


Raportointi Kyberturvallisuuden riskeistä, poikkeamista, toimenpiteistä ym. johdolle

- ”Kyberturvallisuuslain mukainen riskienhallinnan toimintamallin” luvun 2. alakohdissa osin kuvatusta kokonaisuudesta muodostuva Kyberturvallisuuden tilannekuva ja riskitaso raportoidaan aluehallitukselle ja hyvinvointialueen johtotiimille osavuosikatsausten riskienhallinnan raportoinnin yhteydessä
  - Tietoturvapäällikkö koostaa tämän raportin osaksi tätä kokonaisuutta.
- Kyberturvallisuutta vakavasti vaarantavista poikkeamatilanteista informoidaan aluehallitusta, kuten muistakin mahdollista vakavista poikkeamatilanteista osana päivittäisjohtamista ja viestintäsuunnitelmia

Pohjois-Savon hyvinvointialue

Tietoturvan ja tietosuojan organisoituminen ja raportointivastuut (kyberturvallisuuslailla ei vaikutuksia)



Vastuiden ja hallintamallin määrittely

- *” 6.1.1 Tietoturvaroolit ja –vastuut: Kaikki tietoturvavastuut on määriteltävä ja jaettava.” – ISO/IEC 27002:2017*
- Tietoturva- ja tietosuojapolitiikan liite 3.
  - Luku 2. kuvaa hyvinvointialueen tietoturva- ja tietosuojatehtävät, sekä niiden organisoinnin ja vastuut
  - Luku 3. kuvaa käsittelytarkoituksen mukaiset henkilötietojen käsittelyn ja henkilörekisterien vastuut

2.30 Tietoturvapäällikkö

- Vastaa tietoturvan operatiivisesta johtamisesta hyvinvointialueella
- Vastaa tietoturvaan liittyvien yleisten ohjeiden, politiikkojen ja periaatteiden valmistelusta ja ylläpitämisestä yhteistyössä sidosryhmien kanssa
- Vastaa tietoturvan hallintamallin kehittämisestä ja ylläpidosta
- Vastaa tietoturvariskien hallintamallin kehittämisestä ja ylläpidosta
- Suorittaa kehittämistä kansallisessa ja kansainvälisessä yhteistyössä
- Valmistelee tietoturvallisuuteen liittyviä kehittämishankkeita ja budjetointia yhdessä muiden sidosryhmien kanssa
- Osallistuu teknisten tietoturvallisuuden kehitystoimien suunnitteluun, arviointiin, priorisointiin ja budjetointiin
- Ohjeistaa yleiset tietoturvallisuusasiat ja huolehtii, että niistä tiedotetaan ja koulutetaan
- Vastaa tietoturvapoikkeamien seurannasta ja tilastoinnista
- Tiedottaa tietoturvallisuusasioista ja –ongelmista
- Valmistelee tietoturvaan liittyvän viestinnän koko organisaation, sidosryhmien ja erityisesti esimiesten kanssa
- Osallistuu hyvinvointialueen turvallisuus-, tietosuoja- ja tietoturva-asioiden kokonaisuuden koordinointiin tietoturvan ja tietosuojan strategisen ohjausryhmän esittelijänä
- Toimii tietoturvan ja tietosuojan operatiivisen ryhmän puheenjohtajana
- Raportoi tietoturvallisuudesta tietohallintojohtajalle, operatiiviselle tietosuoja- ja tietoturvaryhmälle ja tietoturvan ja tietosuojan strategiselle ohjausryhmälle
- Vastaa tietoturvaprosessien ja hallintakeinojen osalta seuranta-, mittaus-, analysointi- tai arviointimenetelmien suunnittelusta

Poikkeamailmoitukset viranomaiselle - (§ 11, 12, 13, 14)

- Toimijan on viipymättä ilmoitettava valvovalle viranomaiselle merkittävästä poikkeamasta
- Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia… voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa
- Ensi-ilmoitus on tehtävä 24 tunnin kuluessa poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa poikkeaman havaitsemisesta
- Ensi-ilmoitus, jatkoilmoitus, väliraportti ja loppuraportti
- Toimijan on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa toimijan palvelujen tarjoamista
- Toimijat voivat vapaaehtoisesti tehdä valvovalle viranomaiselle ilmoituksia muista kuin 11 §:ssä tarkoitetuista poikkeamista, kyberuhkista ja läheltä piti –tilanteista

- Aiemmin ohjeistettua ilmoittamista
  - Tietosuojavaltuutetun toimisto
  - Tietojärjestelmän valmistaja
  - Sosiaali- ja terveysalan lupa ja valvontavirastolle (Valvira)
  - Rikosilmoitus tai tutkintapyyntö toimivaltaiselle esitutkintaviranomaiselle, eli poliisille
  - Kyberturvallisuuskeskukselle
    - Ilmoitus voidaan tehdä, joko suoraan kyberturvallisuuskeskuksen päivystäjälle puhelimitse tai sähköisesti. NIS direktiivin mukainen ilmoitus voidaan tehdä samalla, jolloin tieto ohjautuu myös valvoville viranomaisille
  - Lisäksi voidaan lähettää tietoa SOTE-ISAC tiedonvaihtoryhmälle esimerkiksi tiettyyn lääkinnälliseen laitteeseen kohdistuvasta tai potilastietojärjestelmään kohdistuvasta uhkasta.
- Ensi-ilmoituksen tekeminen Istekki Oy:n tietoturvavalvomolla 24/7, HVA:n tietoturvapalvelut huolehtivat jatkoilmoitukset, väliraportit ja loppuraportit yhdessä ICMT-palveluntarjoajien kanssa

Valvovat viranomaiset (§ 26),valvonnan kohdistaminen (§ 27), tiedonsaantioikeus (§ 28)

- Kyberturvallisuuslain ja, sen nojalla annettujen määräysten ja NIS 2 –direktiivin nojalla annettujen säännösten noudattamista valvoo:
  - Sosiaali- ja terveysalan lupa- ja valvontavirasto siltä osin kuin kyse on liitteen I kohdan 13 alakohdissa a ja b tarkoitetuista toimijoista
- Valvonta on kohdistettava keskeisiin toimijoihin
- Valvova viranomainen voi kuitenkin kohdistaa valvontaa myös muuhun kuin keskeiseen toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säännöksiä
- Tiedostetaan, että valvontaa voi olla tulossa, mutta sinällään ylin johto on ollut sitoutunut vastaaviin asioihin jo HVA:n alkumetreiltä vuodesta 2022 ja osoittanut resursseja sekä sitoumusta. Työtä tehdään asiakkaiden, henkilökunnan ja yhteiskunnan eteen. Ei niinkään valvonnan vuoksi!

- Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot
- Valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten

§ 31 Valvontapäätös ja varoitus
§ 32 Johdon toiminnan rajoittaminen

- Valvova viranomainen voi velvoittaa toimijan määräajassa korjaamaan puutteet tässä laissa tai sen nojalla annetuissa määräyksissä taikka NIS 2 -direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisessa. Valvova viranomainen voi päätöksellä velvoittaa toimijan julkistamaan kyseiset puutteet tai muut seikat…
- Valvova viranomainen voi antaa toimijalle varoituksen, jos tämä ei ole noudattanut tätä lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säännöksiä
- Valvova viranomainen voi kieltää määräajaksi henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä tai varajäsenenä, hallintoneuvoston jäsenenä tai varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, jos tämä on toistuvasti ja vakavasti rikkonut 10 §:ssä säädettyjä velvollisuuksia.
- .. johdon toimintaa ei saa rajoittaa, jos kyse on yksityisestä elinkeinonharjoittajasta, avoimesta yhtiöstä, kommandiittiyhtiöstä, valtion viranomaisesta, valtion liikelaitoksesta, hyvinvointialueesta tai –yhtymästä…

§ 35 Hallinnollinen seuraamusmaksu

- Toimijalle voidaan määrätä hallinnollinen seuraamusmaksu, jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö:
- 1) 7 §:ssä tarkoitetun velvollisuuden hallita riskejä, 8 §:ssä tarkoitetun kyberturvallisuutta koskevan riskienhallinnan toimintamallin laatimisen tai 9 §:n 1 momentissa tarkoitettujen osa-alueiden huomioimisen osana kyberturvallisuuden riskienhallinnan toimintamallia;
- 2) toteuttaa 9 §:n 2 momentissa tarkoitetut toimenpiteet;
- 3)antaa 11 §:ssä tarkoitetun poikkeamailmoituksen, 12 §:ssä tarkoitetun väliraportin tai 13 §:ssä tarkoitetun loppuraportin valvovalle viranomaiselle;
- 4) antaa 41 §:ssä tarkoitetut tiedot valvovalle viranomaiselle.

- Seuraamusmaksua ei voi määrätä valtion viranomaisille, valtion liikelaitoksille, hyvinvointialueille eikä –yhtymille…
- Keskeiselle toimijalle määrättävän hallinnollisen seuraamusmaksun enimmäismäärä on 10 000 000 euroa tai kaksi prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Toimijaluettelo (§ 41)

- Valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa.
- Toimijoiden on ilmoitettava valvovalle viranomaiselle:
  - Toimijan nimi;
  - Osoitteensa, sähköpostiosoitteensa, puhelinnumeronsa ja muut ajantasaiset yhteystietonsa;
  - IP-osoitealueensa;
  - NIS 2 -direktiivin liitteessä I tai II tarkoitettu asiaankuuluva toimialansa ja sen osa;
  - Tieto siitä, onko se keskeinen toimija;
  - Luettelo niistä Euroopan unionin jäsenvaltioista, joissa se tarjoaa NIS 2 -direktiivin soveltamisalaan kuuluvia palveluja; ja
  - Osallistumisesta 23 §:ssä tarkoitettuun kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn
- Ilmoitukset tehty Valviralle ja Traficomille

Pohjois-Savon hyvinvointialue

Mitä on/oli NIS 2 / kyberturvallisuuslain toimenpidelistalla?

- Toimijaluetteloon ilmoittaminen (valmis)
- Riskienhallinnan toimintamalli (versio 1.0 valmis, käsittelyssä 9.6.2025 aluehallituksessa)
- Työkalut riskienhallintaan mm.
  - Organisaation laajuinen (osin tehty)
  - Yksikkökohtainen (osana laajempaa arviointia) (valmistumassa)
  - Tietojärjestelmäkohtainen (valmistumassa)
- Jatkuva ICT-Infran arvioinnin ja testauksen mallin jatkokehitys (mm. haavoittuvuusskannaukset ja muu testaaminen) (otettu käyttöön mm. Hyöky-palvelu sekä vuosittaiset skannaukset /tarkastukset), (valmistumassa)
- Toiminnan ja tietojärjestelmien kriittisyysluokittelun jatkokehitys (järjestelmien tarkempi luokittelu valmistumassa)
- Ylimmän johdon koulutusympäristö (valmis)
- Henkilöstön koulutuksen päivitys (viimeistään 2026 alkuun)
- Tietoturva- ja tietosuojapolitiikan liite 3. päivitys (valmis)
- Kilpailutusvaatimusten kehitys ja sopimuksellisten vaatimusten tarkastus / kehitys (työn alla)
- Riskienhallinnan vaatimukset sopimuksiin ja kilpailutusvaatimuksiin (tarkastelu kesän/syksyn 2025 aikana)
- Pääsynhallinnan periaatteiden päivitys (valmis)
- Poikkeamien havainto ja käsittelyohjeen päivitys (valmis)
  - 24/7 ensi-ilmoitukset erityisesti
- Periaatteiden päivitykset: Varmistukset, palautukset, jatkuvuus ja varautuminen (työ jatkuu)
- Turvallisuusselvitykset, pääsy tekniseen dokumentaatioon vain selvitetyillä henkilöillä (osin valmista)
- Hätäviestintäjärjestelmän jatkokehitys (työn alla)

Kiitos!

- **Kysymyksiä / kommentteja?**
- tietoturva@pshyvinvointialue.fi
- marko.ruotsala@pshyvinvointialue.fi

- Mikäli havaitset aktiivisen tietoturvaloukkauksen, kuten haittaohjelman, tietomurron tai käyttäjätunnuksesi päätyneen vääriin käsiin, ota yhteys ensimmäisenä Istekki Oy:n palvelupisteeseen puhelimitse.
- Numerot ovat virka-aikana: 017 17 3900 ja virka-ajan ulkopuolella samaan numeroon, ja valitse numero 1, jolla yhdistetään varallaoloon.