Tiedonhallintalautakunta
Informationshanteringsnämnden

Tiedonhallintalautakunnan webinaari 09.10.2023 klo: 09.00 – 11.00

Suositus tietoturvallisuudesta hankinnoissa

Mika Kuronen, pj.
Tuula Seppo, siht.

Esittäytyminen

- Mika Kuronen
  - Neuvotteleva virkamies
    - Valtiovarainministeriön JulkICT-osaston palveluiden ja turvallisuuden ohjausyksikön digiturvatiimin jäsen
    - Tiedonhallintalautakunnan sihteeristön jäsen ja tietoturvallisuusjaoston puheenjohtaja
      - Suositustyöhön osallistuminen ja jaoston toiminnan kehittäminen
    - Tieto-, digiturvallisuuden sekä jatkuvuudenhallinnan ja varautumisen ohjaus
    - KV- asiat: Siviiliresielienssi, kriisivarautuminen ja hybridiuhat
    - Muut erikseen sovitut yksikön ja tiimin tehtävät.

Tietoturvallisuusjaoston ajankohtaiset kuulumiset – suositus työn tilanne

Vuonna 2023 hyväksytyt / julkaistut

Suositus salassa pidettävien asiakirjojen käsittelystä

- Hyväksyttiin Tiedonhallintalautakunnassa 15.12.2022
- Suomenkielinen julkaisu 19.1.2023
- Ruotsinkielinen käännös 24.3.2023

eOppiva-koulutus Julkrista

- Koulutus hyväksyttiin Tiedonhallintalautakunnassa 2.3.2023
- Suomenkielinen julkaisu 3.3.2023
- Julkaisun jälkeen on julkaistu ru + en tekstitys

Selvitys digitalisaation ja uusien teknologioiden vaikutuksista tiedonhallintalakiin pohjautuvaan tietoturvallisuussääntelyyn ja suosituksiin

- Suomenkielisen selvityksen julkaisu 17.5.2023
- Käännökset mahdollisesti 2024

Suositus tietoturvallisuudesta hankinnoissa

- Suositus hyväksyttiin 13.6.2023 Tiedonhallintalautakunnassa
- Suomenkielinen julkaisu 4.8.2023
- Ruotsinkielinen käännös 2023
- Englanninkielinen käännös 2024.

Vuonna 2023 aloitetut uudet suositukset

Suositus tietoturvallisuuden vähimmäisvaatimuksista

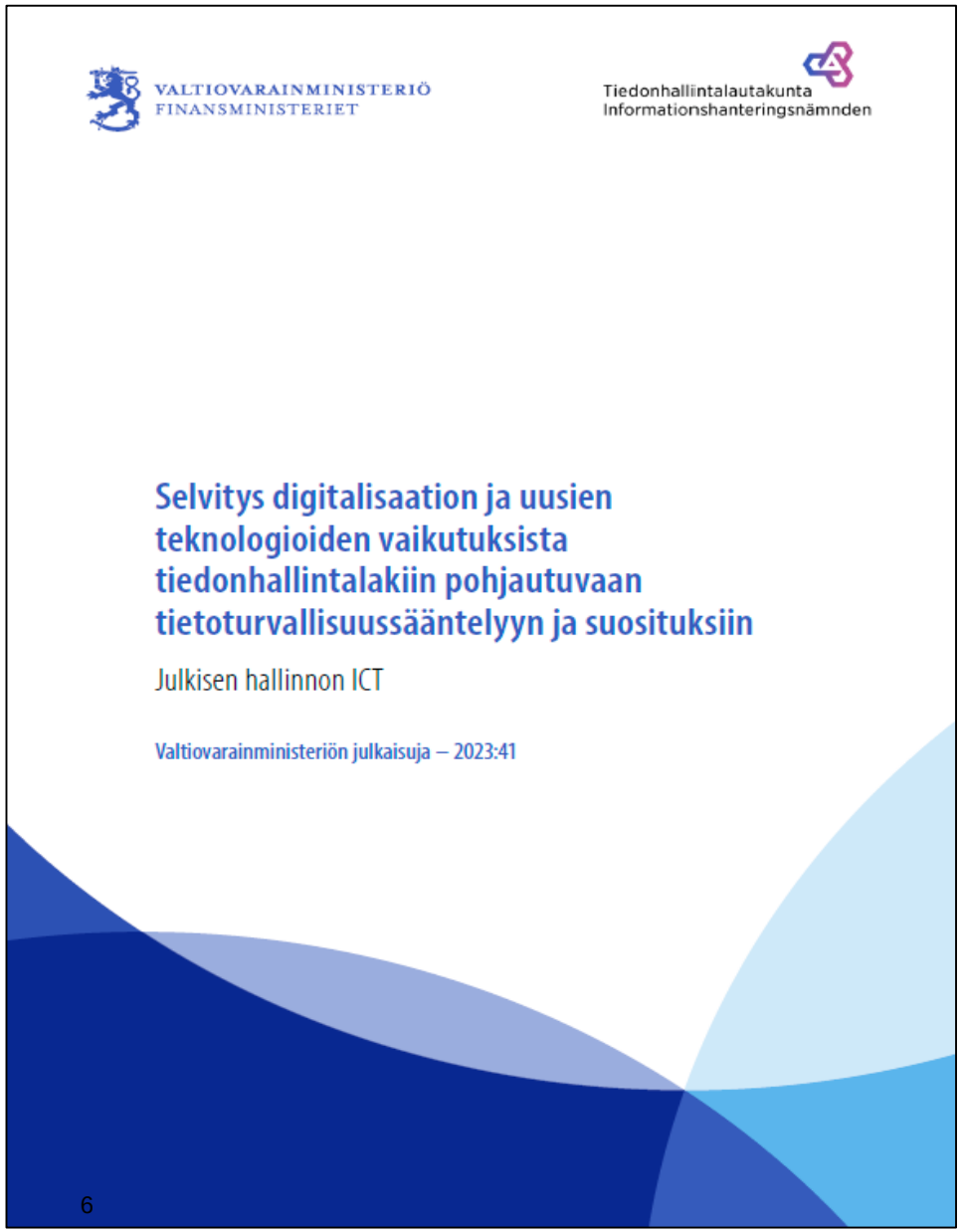
- Työtä on tehty kesken olevien muiden julkaisujen ohessa.
- Pääpainoisesti työtä on ollut mahdollista tehdä loppuvuosi 2023
- Tavoitteena on saada julkaisu valmiiksi tai vähintään lausunnolle loppuvuoden aikana.
- Suositus korvaa suosituskokoelmat tiettyjen tietoturvallisuussäännösten soveltamisesta (versiot VM 2021:65, VM 2020:61 ja VM 2020:21).
- Vähimmäisvaatimussuositus muodostaa yhdessä muiden tiedonhallintalautakunnan tietoturvallisuussuositusten kanssa kokonaisuuden.

Jatkopohdinnassa

- Uusi suositus häiriötilanteista tiedottamisesta ja varautumisesta häiriötilanteisiin
  - Asiaa käsitellään vähimmäisvaatimussuosituksessa (minimi-asiat)
  - Erillisen suosituksen tarve arvioidaan yhteistyössä APT-jaoston/ Tiedonhallintalautakunnan pääsihteerin kanssa.
- Vuoden lopussa arvioidaan myös muiden suositusten kehittämistarpeet.

Digitalisaation ja teknologian vaikutuksia koskeva selvitys

Digitalisaatiota ja teknologioita koskeva selvitys julkaistu 17.5.2023



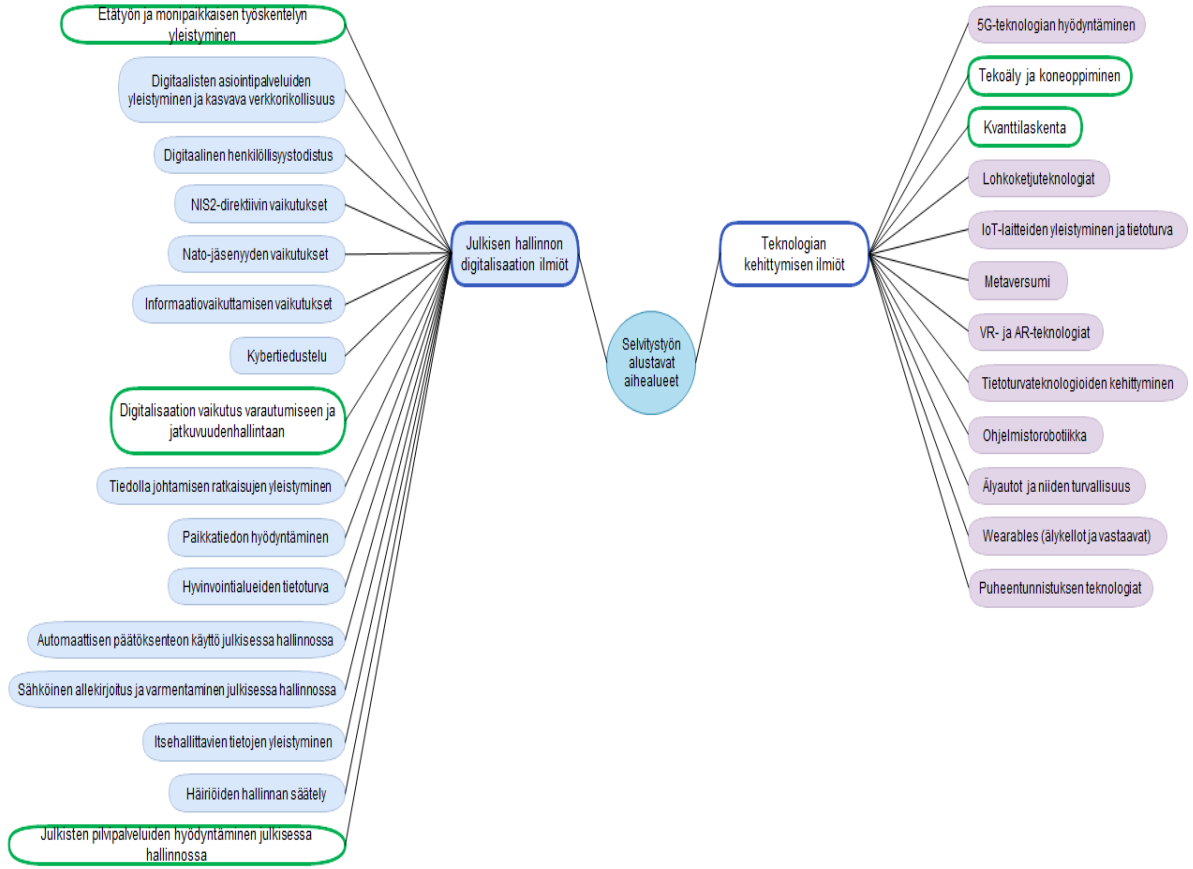
Sisältö

Selvityksen yleiskuvaus

- Tavoitteena oli ennakoivasti tunnistaa tiedonhallintaan ja tietoturvallisuuteen kohdistuvia muutoksia
- Tarkasteltavana julkisen hallinnon digitalisaation ja teknologian kehittymisen ilmiöitä ja niiden vaikutuksia
- Selvitys toteutettiin haastatteluilla, tutkimalla erilaisia aineistoja sekä työpajatyöskentelyllä.

Selvitykseen valittiin seuraavat asiat/aihealueet

1. Uuden teknologian hyödyntäminen julkisessa hallinnossa (erityisesti tekoäly ja kvanttilaskenta)
2. Julkisten pilvipalveluiden hyödyntäminen julkisessa hallinnossa
3. Etätyön ja monipaikkaisen työskentelyn yleistyminen julkisessa hallinnossa
4. Digitalisaation vaikutus varautumiseen
5. Suositusten kehittäminen yleisesti.



Salassa pidettävien tietojen käsittely ja suojaaminen -
eOppiva – koulutus

Sisältö

Salassa pidettävien asiakirjojen käsittely suosituksen sisältö…

- Julkaistu 19.1.2023
- Ruotsinkielinen käännös 24.3.2023

Tässä tiedonhallintolautakunnan antamassa suosituksessa kuvataan salassa pidettävien asiakirjojen (tietojen) käsittelyssä sekä käsittelyä koskevien vaatimusten täyttämisessä. Suositus sisältää lainsäädännön vaatimuksia, suosituksia sekä käytännön esimerkkejä salassa pidettävien asiakirjojen käsittelystä. Liitteeseen 1 on koostettu dokumentissa olevat suositukset ja niihin liittyvät lakiperusteet.

Aikaisemmin julkaistu tiedonhallintalautakunnan suosituskokoelma tiettyjen turvallisuussääntöjen soveltamisesta (VM 2021:65) sisältää julkisessa hallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset. Näitä vähimmäisvaatimuksia suositellaan sovellettavaksi myös salassa pidettävien asiakirjojen käsittelyssä.

Suositus on tarkoitettu ensisijaisesti viranomaisille, mutta niiden lisäksi suositusta voivat hyödyntää elinkeinoelämän toimijat ja kaikki muutkin, jotka käsittelevät viranomaisten salassa pidettäväksi määrittelemiä asiakirjoja.

Tiedonhallintalautakunta hyväksyi suosituksen 15.12.2022.

Tiedonhallintalautakunta
Informationshanteringsnämnden

eOppiva: Salassa pidettävien tietojen käsittely ja suojaaminen

Tämä eOppiva koulutus koostuu 5 osiosta, joiden suorittaminen kestää arviolta 6-7 minuuttia, sekä kertaustehtävistä. Koulutuksen kokonaiskesto on siis noin 40 minuuttia. Käytä koulutukseen kuitenkin juuri sen verran aikaa kuin tarvitset, keskeytä, palaa ja liiku osioiden välillä vapaasti. Meistä jokainen oppii omalla tyylillään ja omaan tahtiinsa.

Kun olet suorittanut kertaustehtävät hyväksytysti, pääset kirjaamaan suorituksesi, antamaan palautetta ja tilaamaan todistuksen. Rekisteröi suoritus heti, sillä koulutus ei tallenna etenemistäsi tai testin suorittamista. Jos olet töissä valtionhallinnossa, kirjaudu koulutuksen lopuksi eOppivan Moodleen. Näin suorituksesi rekisteröityy omaan profiiliisi.

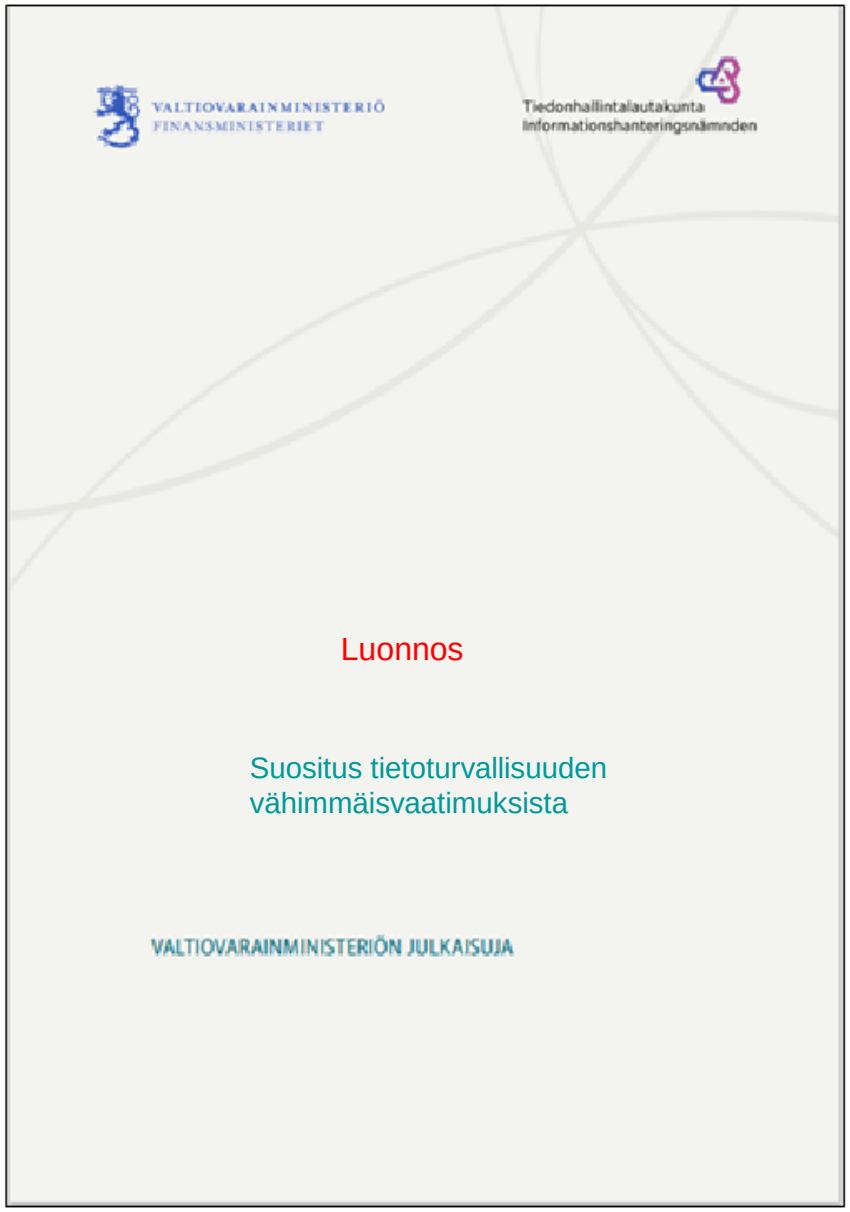
Koulutus on julkaistu 8.9.2023

eOppiva on valtionhallinnon yhteinen oppimisalusta

https://www.eoppiva.fi/

Suositus tietoturvallisuuden vähimmäisvaatimuksista

Luonnos suosituksesta tietoturvallisuuden vähimmäisvaatimuksista



- **Tämä suositus tietoturvallisuuden vähimmäisvaatimuksista korvaa suosituskokoelmat tiettyjen tietoturvallisuussäännösten soveltamisesta (versiot VM 2021:65, VM 2020:61 ja VM 2020:21).**

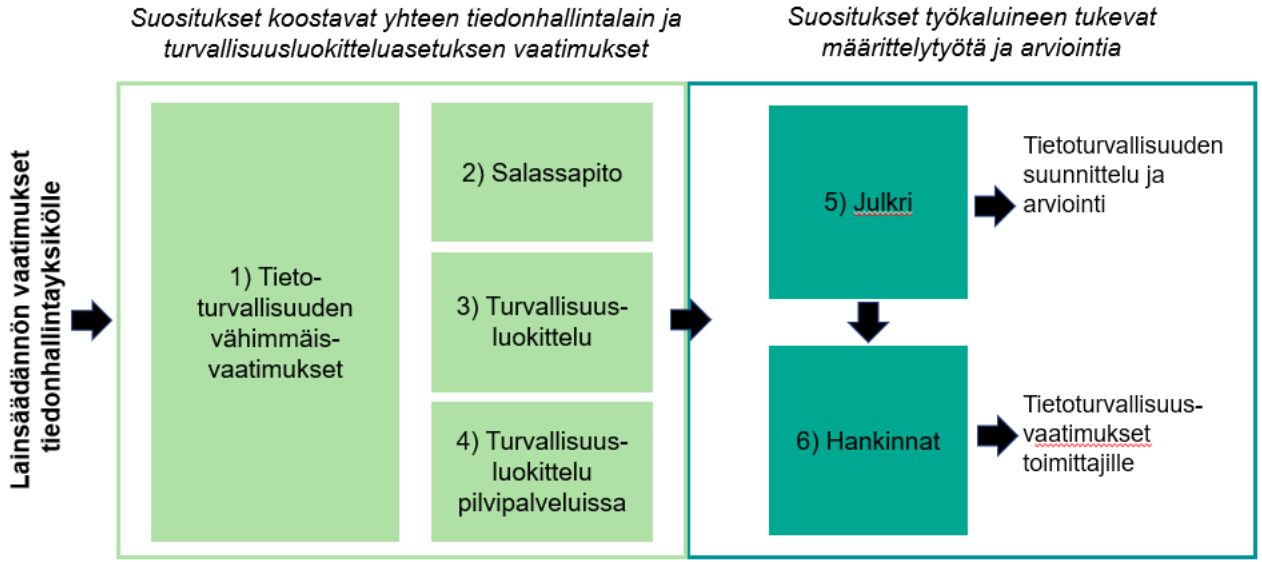
- **Suosituksessa esitetään tietojen käsittelylle säädetyt tietoturvavaatimukset sekä niihin liittyviä hyviä käytäntöjä. Jokainen luku sisältää lain vaatimuksen, siihen liittyvät suositukset, käytännön esimerkkejä ja viittauksia lisätietoihin. Liitteessä 1 on yhteenveto tiedonhallintalain tietoturvallisuutta koskevista lainkohdista.**

- **Vähimmäisvaatimussuositus muodostaa yhdessä muiden tiedonhallintalautakunnan tietoturvallisuussuositusten kanssa kokonaisuuden.**

- **Vähimmäisvaatimuksia arvioitaessa on huomioitu:**
  - **hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyvistä laista (HE 284/2018),**
  - **hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (HE 145/2022 vp),**
  - **hallintovaliokunnan mietintö (HaVM 39/2022 vp) koskien hallituksen esitystä eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi,**
  - **hallintovaliokunnan mietintö (HaVM 38/2018 vp) koskien hallituksen esitystä eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.**

Tiedonhallintalautakunnan tietoturvallisuutta koskevat suositukset

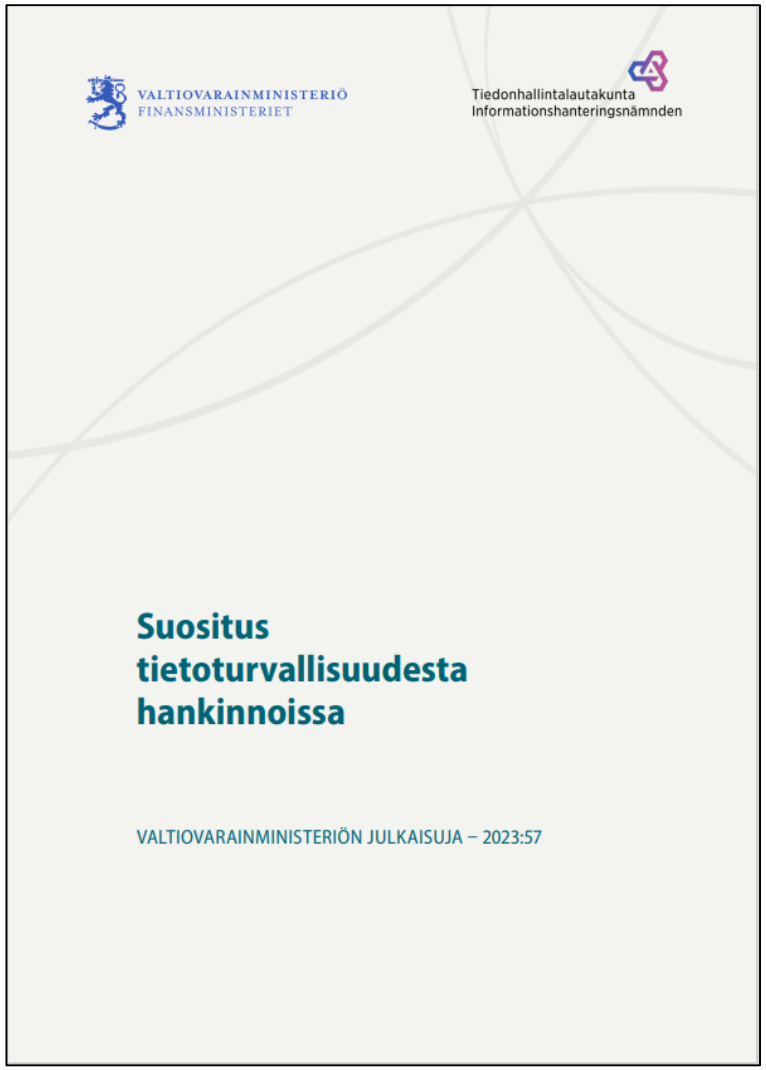
1) Suositus tietoturvallisuuden vähimmäisvaatimuksista (VM 2024: XX)
2) Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
3) Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)
4) Turvallisuusluokiteltavaien asiakirjojen käsittely pilvipalveluissa (VM 2022:4)
5) Julkisen hallinnon tietoturvallisuuden arviointikriteeristö, Julkri (VM 2023:46)
6) Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)



Kysymykset tai palaute?

Suositus tietoturvallisuudesta hankinnoissa

Suositus tietoturvallisuudesta hankinnoissa julkaistu 4.8.2023



Julkaisun pysyvä osoite on
http://urn.fi/URN:ISBN:978-952-367-645-9

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää. Lain 13 §:n 4 momentin mukaan viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Tämä tiedonhallintolautakunnan antama suositus opastaa viranomaisia ja erityisesti hankintayksiköitä tietojärjestelmien ja soveltuvin osin muiden palveluiden hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyssä sekä niiden täyttymisen varmistamisessa.

Suositus sisältää kuvauksen hankinnan tietoturvallisuuden varmistamisen prosessista, esittelyt sopimukseen liitettävistä tietoturvallisuusvaatimuksista sekä ohjeen hankintaehtotyökalun käyttämisestä. Suosituksen liitteinä ovat tietoturvallisuusvaatimukset (suppea ja laaja) sekä hankintaehtotyökalu, jonka avulla hankintayksikkö voi muodostaa hallinnollisen turvallisuuden, fyysisen turvallisuuden, teknisen turvallisuuden sekä varautumisen ja jatkuvuudenhallinnan liitteet. Hankintaehtotyökalu perustuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön Julkriin.

Tiedonhallintalautakunta hyväksyi suosituksen 13.6.2023.

Hankintojen tietoturvavaatimuksia koskevan suositustyön tavoitteena on ollut…

- Määrittää tiedonhallintalakiin perustuvat suositeltavat hankintojen tietoturvallisuusvaatimukset
- Työssä on hyödynnetty Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä (Julkri)
- Päivittää hankintoja koskevat turvallisuusehdot sekä niihin liittyvä ohjeistus
- Päivittää tiettyjen tietoturvallisuussäännösten suosituskokoelman hankintoja koskeva luku (8) tähän hankintojen tietoturvallisuutta koskevaan suositukseen
- Hyödyntää ja päivittää vanhentuneissa VAHTI -suosituksissa kuvattua turvallisuussopimusmallia (edelleen laajalti käytetty/hyväksi koettu) tässä työssä ja tuoda siihen mukaan tiedonhallintalain asettamat vaatimukset
- Tarkistaa ja tehdä hankinnoissa tarvittavat tietosuojavaatimuksia koskevat sopimusliitteet yhteistyössä VAHTI-tietosuojaverkoston kanssa.
- Suositusta ja siihen liittyviä liitteitä työsti lukuisa määrä tietoturvallisuuden, tietosuojan ja hankinnan asiantuntijoita mukaan lukien Hansel ja Valtori.

Kenelle suositus on tarkoitettu?

- Suosituksen tarkoituksena opastaa viranomaisia ja erityisesti hankintayksiköitä hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyssä sekä niiden täyttymisen varmistamisessa.
- Suosituksen liitteissä on esitetty hankintoihin suositeltavia tietoturvallisuusvaatimuksia, joita viranomaiset voivat hyödyntää hankintasopimusten liitteinä.

Suositus tietoturvallisuudesta hankinnoissa – taustaa?

Hankintojen tietoturvallisuusvaatimuksien määrittäminen?

- **Tiedonhallintalautakunta on julkaissut julkishallinnon käyttöön suosituksen koskien hankintojen tietoturvallisuusvaatimuksia.**
- Suositus ei sisällä yleisiä hankintoihin liittyviä vaatimuksia, vaan näkökulma on tietoturvallisuus ja miten se tulee huomioida hankinnan kohteen vaatimuksissa ja miten tietoturvallisuuden säilymisestä huolehditaan koko hankinnan elinkaaren ajan.
- Suosituksen sisältyvien liitteiden avulla on mahdollista muodostaa tietoturvallisuusvaatimukset toimittajille, esimerkiksi osana hankintadokumentaatiota.
- Suositus sisältää pääsopimukseen kirjattavat asiat sekä liitteinä suppeat ja laajat tietoturvallisuusvaatimukset, hankintaehtotyökalun yksityiskohtaisempien tietoturvallisuusvaatimusten määrittelyyn ja erillisenä VAHTI-toiminnassa julkaistut tietosuojaliitteet.

Suosituksen sisältö

Sisältö

Suosituksen liitteet

Liite 1 a Tietoturvallisuusvaatimukset (suppea)
Liite 1 b Tietoturvallisuusvaatimukset (laaja)
Liite 2 a Hankintaehtotyökalu (Uudet Excel-versiot)
Liite 2 b Hankintaehtotyökalu (Vanhat Excel-versiot)

Lisäksi VAHTI-toiminnassa on julkaisu erilliset tietosuojaliite ja henkilötietojen käsittelytoimien kuvaus.

Liitteet löytyvät Digi- ja väestötietoviraston Digiturvajulkaisut sivustolla kohdassa Työkalut ja mallipohjat.

Suosituksen taustaa ja perusteita…

VAHTI-ohjeisiin perustuvat tietoturvallisuussopimusmallit:

- Hankkeen tietoturvaohje (Vahti-ohje 9/2008)
- Valtion ICT-hankintojen tietoturvaohje (Vahti-ohje 3/2011)
- ICT-hankintojen tietoturvallisuussopimus (Vahti-ohje 5/2016)
- ICT-hankintojen tietoturvallisuussopimus (Vahti-ohje 12/2018)
- Ohje turvallisuuskriittisiin hankintoihin (VM 7/2019)

Lisäksi mm. seuraavia malleja:

- Hansel turvallisuussopimusmalli 6/2018
- Kiinteistöpalvelujen turvallisuussopimusmalli (Vahti-ohje) 2/2013 liite 7.3) → VAHTI 2/2013 Toimitilojen tietoturvaohje

Näiden mallien perusteella:

- Ministeriöiden tekemät ministeriötä ja/tai koko hallinnonalaa koskevat turvallisuussopimusmallit
- Virastojen tekemät virastokohtaiset turvallisuussopimusmallit
- Turvallisuussopimuksen tietoturvallisuusvaatimuksina on käytetty Vahti-tietoturvatasovaatimuksia/Katakri vaatimuksia
- **Kuntapuolella ei ole juurikaan käytetty turvallisuussopimusmalleja**

VAHTI-ohjeet ovat olleet malleja – niitä ei ole tullut käyttää sellaisenaan - organisaation on tullut mukauttaa malli/vaatimukset aina jokaista käyttötapausta (hankintaa) varten erikseen.

Vahti-mallin mukainen turvallisuussopimus (ICT-hankinta):

SISÄLLYSLUETTELO

Tiedonhallintayksiköissä tätä mallia mukautettu ja täydennetty mm.

- Lisäämällä uuden lainsäädännön viittaukset (tiedonhallintalaki/turvallisuusluokitteluasetus
- Lisäämällä tietosuojavaatimukset (yleisesti)
- Tekemällä tästä eri tasoisia turvallisuussopimusmalleja (suppea, normaali ja laaja)
- Tekemällä erilaisia vaitiolositoumusliitteitä
- Tekemällä tästä yleisen kaikkea hankintaa koskevan sopimuspohjan
- Tarkentamalla jatkuvuudenhallinnan ja varautumisen vaatimuksia
- Lisäämällä tietoturvavaatimukset: Vahti/Katakri

Ei ole ollut mallia tiedonhallintalain huomioivista hankintojen tietoturvallisuusvaatimuksista.

Aikaisemman VAHTI-mallin mukainen esimerkkilistaus hankinnan tietoturvavaatimuksista:

Tietoturvavaatimukset **Tiedonhallinnan ja digiturvallisuuden asiantuntijapalvelut 2021-2026 (DPS)**

Toimittaja sitoutuu tuottamaan tähän dynaamiseen hankintajärjestelmään perustuvat palvelut noudattaen vähintään tämän liitteen mukaisia tietoturvavaatimuksia. Asiakas voi dynaamisen hankintajärjestelmän sisäisessä kilpailutuksessa täsmentää jäljempänä esitettyjä tietoturvavaatimuksia sekä asettaa muita tietoturvaan ja turvallisuuteen liittyviä vaatimuksia, joita Toimittajan tulee noudattaa. Hanselilla ja asiakkaalla on oikeus tarkastaa näiden vaatimusten täyttyminen itse tai kolmannen osapuolen toimesta.

Selvyyden vuoksi todetaan, että Toimittajan järjestelmille asetettuja vaatimuksia tulee noudattaa siinä tapauksessa, että Toimittaja käsittelee Asiakkaan aineistoja ja tietoja muissa kuin Asiakkaan järjestelmissä.

Nro	Vaatimus	Tarkennus/esimerkki soveltamisesta
	Johtaminen ja hallinnollinen tietoturva	
1	Toimittajalla on kirjallinen tietoturvamenettely, jota Toimittaja noudattaa käsitellessään hankinnan kohteeseen liittyvää tietoa.	Tietoturvamenettelyssä tulee huomioida tietojen luottamuksellisuus ja turvallisuusluokittelu (mikäli palvelussa käsitellään turvallisuusluokiteltua materiaalia).
2	Toimittaja määrittelee hankinnan kohteen tietoturvallisuuteen, jatkuvuuteen ja tietosuojaan liittyvät tehtävät ja nimeää niihin vastuu- ja varahenkilöt. Henkilölistan tulee olla ajantasainen koko sopimuskauden ajan.	Resursointi tulee suunnitella siten, että Toimittaja pystyy täyttämään mm. henkilötietojen tietoturvaloukkauksiin liittyvät velvoitteet.
3	Toimittaja reagoi hankinnan kohteeseen liittyviin tietoturvapoikkeamiin viivytyksettä, ryhtyy niiden johdosta asianmukaisiin toimenpiteisiin, pitää niistä kirjaa ja raportoi ne Asiakkaalle.	Henkilötietoihin liittyvissä tietoturvapoikkeamissa tulee huomioida henkilötietojen käsittelyä koskevissa ehdoissa määritellyt vaatimukset.
4	Toimittaja raportoi Asiakkaalle sovittujen, hankinnan kohteeseen liittyvien tietoturvallisuuden ja jatkuvuudenhallinnan kehittämistoimenpiteiden edistymisestä normaalin raportoinnin osana.	Kehittämistoimenpiteillä tarkoitetaan tässä esimerkiksi auditoinnin yhteydesssä tai tietoturvapoikkeaman havaitsemisen yhteydessä Asiakkaan kanssa sovittuihin toimenpiteisiin joilla varmistetaan, että tietoturva vastaa sopimuksen vaatimuksia.
5	Toimittaja seuraa tietoturvallisuudesta annettujen vaatimusten ja Asiakkaan kirjallisesti antamien ohjeiden noudattamista ja puuttuu havaitsemiinsa poikkeamiin.	Toimittaja pitää kirjaa havaituista poikkeamista ja niihin liittyvistä korjaustoimenpiteistä.
6	Toimittaja varmistaa ja kehittää omia tietoturvallisuuteen liittyviä prosesseja ja järjestelmiä säännöllisesti suoritettavan riskiarvioinnin perusteella.	

- Hankintojen tietoturvallisuusvaatimukset suositus ei enää sisällä vakiomuotoista ”kiinteää” vaatimustaulukkoa.
- Tietoturva-vaatimukset muodostetaan suosituksen liitteenä olevalla Excel-työkalulla.

Suosituksen osa-alueiden esittely ja rajaukset

Miten tietoturvallisuus varmistetaan hankinnoissa?

- Tietoturvallisuusvaatimusten määrittely on yksi keskeisimmistä vaiheista hankinnan turvallisuuden varmistamisessa.
- Tietoturvallisuusvaatimukset tulee määritellä riskilähtöisesti riittävän tiukoiksi välttäen tarpeettoman korkeita vaatimuksia ja niihin liittyviä ylimääräisiä kustannuksia.
- Suosituksessa on kuvattu tietoturvallisuuden varmistamisen prosessi:
  - Se sisältää ne vaiheet, joiden avulla voi suunnitella ja varmistaa hankinnan tietoturvallisuuden sekä huolehtia, että tietoturvallisuus säilyy koko hankinnan elinkaaren ajan.
  - Valmistelu- ja määrittelyvaiheessa korostuu lähtökohtien tunnistaminen, tarvittavien osaamisten ja resurssien varaaminen sekä vaatimusten määrittely.
  - Toteutus- ja varmistusvaiheessa tulee huolehtia vaatimusten täyttymisestä, johdon hyväksynnästä sekä käyttöönotosta.
  - Käyttöönotto tulee suunnitella huolellisesti varsinkin suurissa ja kriittisissä hankinnoissa. Lopuksi on tärkeä huolehtia muutostenhallinnasta, joka pitää sisällään ylläpidon ja palvelun käytön päättämiseen liittyviä näkökulmia.

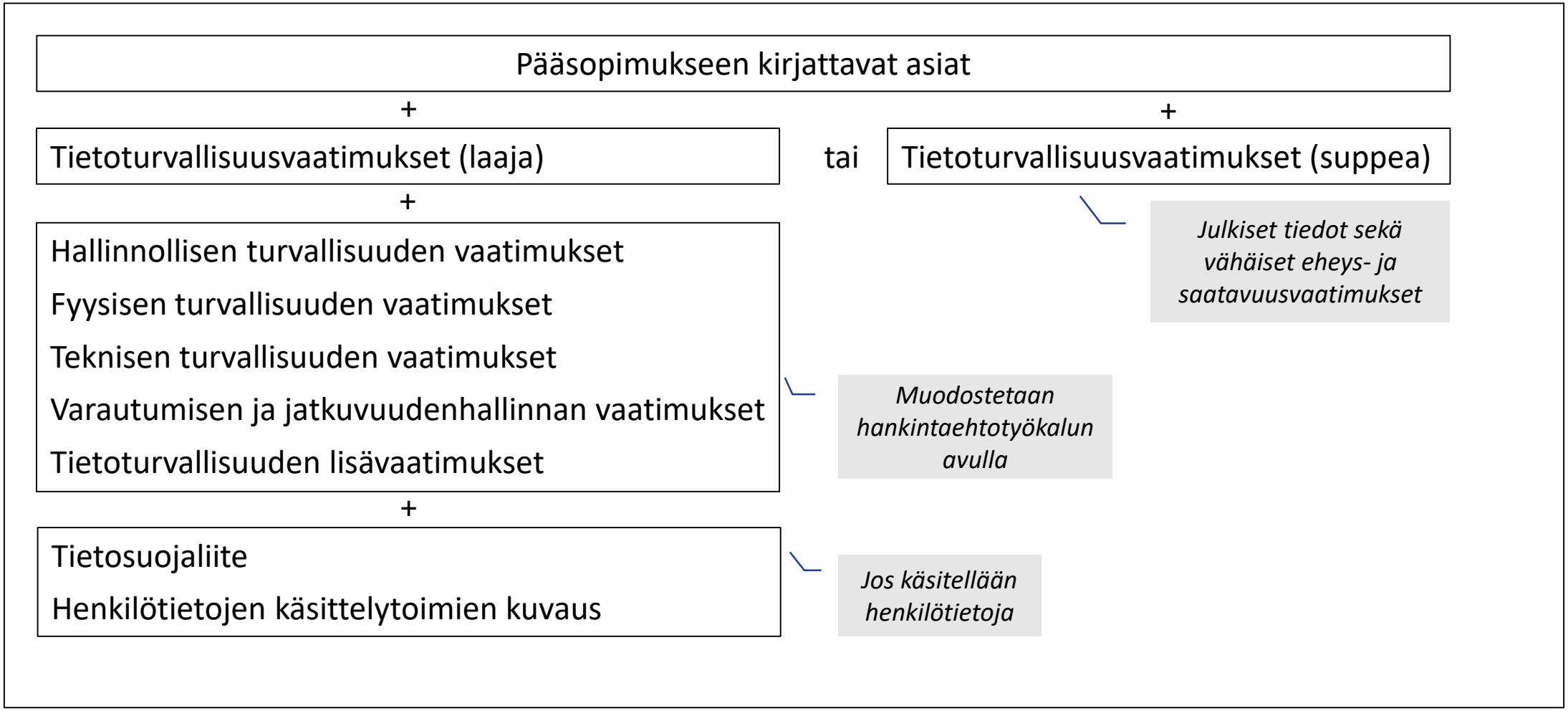
Rajaukset

Tämä suositus koskee tiedonhallintalain tietoturvallisuusvaatimusten soveltamista hankinnoissa. Tässä suosituksessa ei ole huomioitu:

- yleistä hankintoihin liittyvää sääntelyä,
- toimialakohtaista sääntelyä, kuten sosiaali- ja terveydenhuollon lainsäädäntöön sisältyviä vaatimuksia,
- tietosuoja-asetuksen 28 artiklan mukaisia sopimusvaatimuksia,
- henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) mukaisia vaatimuksia,
- digitaalisten palvelujen tarjoamista koskevan lain (306/2019) mukaisia saavutettavuusvaatimuksia,
- valmiuslain (1552/2011) piiriin kuuluvia toiminnan jatkuvuutta poikkeusoloissa koskevia toimenpiteitä,
- EU:n turvallisuusluokiteltujen tietojen suojaamista koskevia sääntöjä (2013/488/EU) eikä
- kansainvälisistä tietoturvallisuusvelvoitteista johtuvia vaatimuksia.

Suositus ei ota kantaa kaikkiin yksityiskohtaisiin järjestelmien tietoturvavaatimuksiin. Vaikka suositus ei sisällä edellä mainittuja vaatimuksia, niin organisaation tulee kuitenkin tunnistaa ja ottaa huomioon nämä vaatimukset hankinnoissaan.

Hankinnan kohteen tietoturvallisuusvaatimuksien muodostaminen?



Suositukseen sisältyvät liitteet ja niiden käyttötarkoitukset

Pääsopimuksessa olisi hyvä huomioida, että seuraavat tietoturvallisuusnäkökulman asiat ovat mukana:

- Oikeus tarkastaa kohteen kannalta riittävät tietoturvallisuusjärjestelyt
- Tietoturvallisuuden vastuuhenkilöt yhteystiedoissa
- Sopimuksen ja liitteiden soveltamisjärjestyksen huomiointi (erityisesti tietoturva- ja tietosuojaliitteet)
- Riittävät sakko- ja vahingonkorvauslausekkeet (myös tietoturvallisuus- ja tietosuojavaatimuksiin liittyvissä poikkeamissa)
- Millainen purku- tai välittömän irtisanomisen ehto liittyy tietoturvallisuusliitteen velvoitteiden rikkomiseen
- Tietojen sijainti tai käsittely Suomessa tai ETA-alueella
- Mahdollisten yrityskauppatilanteiden huomiointi.

Suppeat tietoturvallisuusvaatimukset –liite 1a

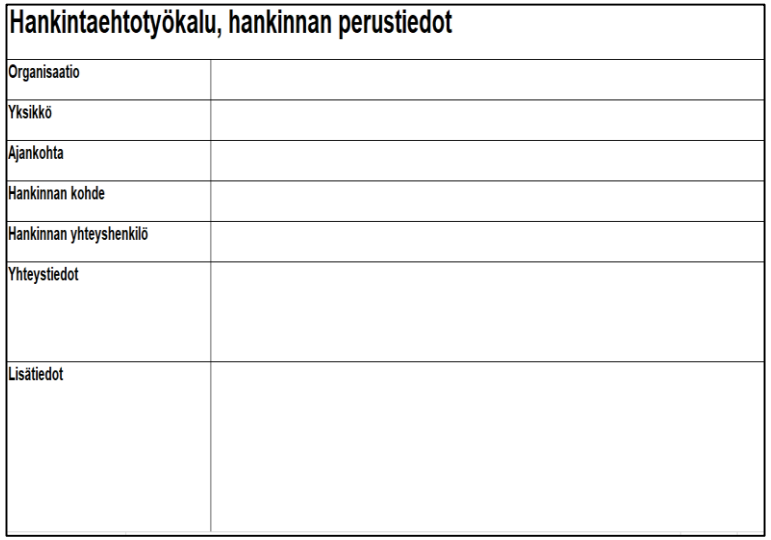
- Suppeita tietoturvallisuusvaatimuksia voi käyttää osana sellaisia hankintoja, joissa käsitellään vain julkista tietoa ja tiedon eheyteen sekä saatavuuteen ei kohdistu normaalia korkeampia vaatimuksia.
- Näitä vaatimuksia voidaan käyttää myös tilanteissa, joissa käsitellään vain vähäisessä määrin muita kuin julkisia tietoja ja joiden paljastumisen aiheuttama vahinko on vähäinen.

Laajat tietoturvallisuusvaatimukset –liite 1b

- Laajoja tietoturvallisuusvaatimuksia suositellaan käyttämään hankintoihin, joissa käsitellään salassa pidettäviä tietoja, turvallisuusluokiteltuja tietoja tai henkilötietoja.
- Lisäksi liite on tarkoitettu käytettäväksi sellaisissa tilanteissa, joissa palvelujen eheyteen tai saatavuuteen kohdistuu normaalia korkeampia vaatimuksia. Liitettä suositellaan käytettäväksi yhdessä hankintaehtotyökalun avulla muodostettavien osa-aluekohtaisten liitteiden sekä tietosuojaliitteiden kanssa.

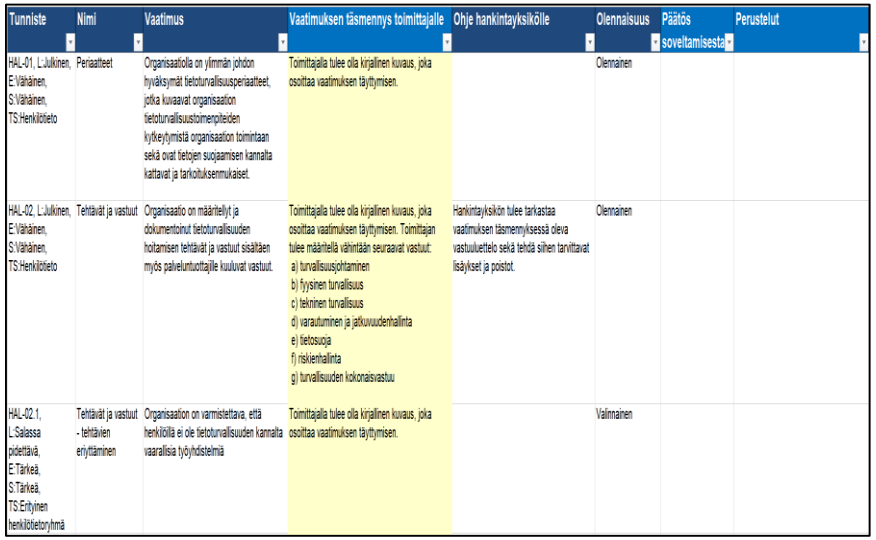
Hankintaehtotyökalu – liite 2

- Laajan tietoturvallisuusvaatimusliitteen kanssa suositellaan käyttämään Excel-pohjaista hankintaehtotyökalua.
- Työkalu helpottaa riskilähtöistä vaatimusten määrittelyä.
- Se pohjautuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön, Julkriin. Julkrin arviointikriteerit on muokattu toimittajaa koskeviksi vaatimuskriteereiksi. Vaatimukset voidaan muodostaa eri osa-alueille, joita ovat hallinnollinen, fyysinen ja tekninen turvallisuus sekä varautuminen ja jatkuvuudenhallinta. Hankintayksikkö voi täsmentää ennalta määriteltyjä vaatimuksia sekä määritellä lisävaatimuksia.



Hankintaehtotyökalu, hankinnan perustiedot	
Organisaatio	
Yksikkö	
Ajankohta	
Hankinnan kohde	
Hankinnan yhteyshenkilö	
Yhteystiedot	
Lisätiedot	

Esiehdot:	Hankintayksikön valinnat
Turvallisuustasot hankinnan kohteessa	
Vaadittava luottamuksellisuuden taso	Julkinen
Vaadittava eheyden taso	Vähäinen
Vaadittava saatavuuden taso	Vähäinen
Henkilötiedot hankinnan kohteessa	Ei henkilötietoja
Sopimukseen sisällytettävät turvallisuusliiteet	
Hallinnollinen turvallisuus	Kyllä
Fyysinen turvallisuus	Kyllä
Tekninen turvallisuus	Kyllä
Varautuminen ja jatkuvuudenhallinta	Kyllä
Käyttötapaus	



Tunniste	Nimi	Vaatimus	Vaatimuksen täsmennys toimittajalle	Ohje hankintayksiköllle	Olennaisuus	Päätös soveltamisesta	Perustelut
HAL-01, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto	Periaatteet	Organisaatiolla on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan sekä ovat tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset.	Toimittajalla tulee olla kirjallinen kuvaus, joka osoittaa vaatimuksen täyttymisen.		Olennainen		
HAL-02, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto	Tehtävät ja vastuut	Organisaatio on määritellyt ja dokumentoinut tietoturvallisuuden hoitamisen tehtävät ja vastuut sisältäen myös palveluntuottajille kuuluvat vastuut.	Toimittajalla tulee olla kirjallinen kuvaus, joka osoittaa vaatimuksen täyttymisen. Toimittajan tulee määritellä vähintään seuraavat vastuut: a) turvallisuusjohtaminen b) fyysinen turvallisuus c) tekninen turvallisuus d) varautuminen ja jatkuvuudenhallinta e) tietosuoja f) riskienhallinta g) turvallisuuden kokonaisvastuu	Hankintayksikön tulee tarkastaa vaatimuksen täsmennyksessä oleva vastuuluettelo sekä tehdä siihen tarvittavat lisäykset ja poistot.	Olennainen		
HAL-02.1, L:Salassa pidettävä, E:Tärkeä, S:Tärkeä, TS:Erityinen henkilötietoryhmä	Tehtävät ja vastuut - tehtävien eriyttäminen	Organisaation on varmistettava, että henkilöillä ei ole tietoturvallisuuden kannalta vaarallisia työyhdistelmiä	Toimittajalla tulee olla kirjallinen kuvaus, joka osoittaa vaatimuksen täyttymisen.		Valinnainen		

Ohje | Hankinnan perustiedot | Esiehdot | Hankintaehtojen määrittely | Kriteeristö | Hallinnollinen turvallisuus | Fyysinen turvallisuus | Tekninen turvallisuus | Varautuminen ja jatkuvuudenhall | Lisävaatimukset | Käyttötapauskuvaukset | Käyttötapauskriteerit

Tietosuojaliitteet

- Myös henkilötietojen käsittely on huomioitava hankinnan tietoturvallisuusvaatimusten määrittelyssä. Henkilötietojen käsittelyyn liittyvät vaatimukset voi huomioida hankintaehtotyökalun esiehdoissa valitsemalla, että kohde sisältää henkilötietoja tai erityisiin henkilötietoryhmiin kuuluvia tietoja.
  - Esiehtojen valinnalla hankintaehtotyökalu huomioi henkilötietoihin kohdistuvat tietoturvavaatimukset osana vaatimusmäärittelyä.
- Lisäksi VAHTI-toiminnassa on julkaisu erilliset tietosuojaliite ja henkilötietojen käsittelytoimien kuvaus.
  - Liitteet löytyvät Digi- ja väestötietoviraston Digiturvajulkaisut sivustolla kohdassa Työkalut ja mallipohjat.
  - Tietosuojaliite on tarkoitettu malliasiakirjaksi hankintoihin, joissa toimittaja tulee käsittelemään tilaajan henkilötietoja tilaajan lukuun. Henkilötietojen käsittelytoimien kuvaus on tarkoitettu malliasiakirjaksi, siihen mitä tilaajan (rekisterinpitäjän) henkilötietoja toimittaja (käsittelijä) tai sen alihankkija käsittelee tuottaessaan sopimuksen mukaista palvelua.

Lausuntopalautteet?

Suositus ja sen liitteet olivat lausuntopalvelussa kommentoitavana 31.3. asti:

- Palautteita tuli lausuntopalveluun 27 kappaletta
- Lisäksi palautteita tuli sähköpostiin ja VM:n kirjaamoon 5
- Palautteita on käyty läpi tietoturvajaostossa 3.4.- 5.6.2023

Lausunnonantajat

1. Finnish Information Security Cluster (FISC)- Kyberala ry
2. Oikeusministeriö
3. Verohallinto
4. Valtion talous- ja henkilöstöhallinnon palvelukeskus
5. Vantaan ja Keravan hyvinvointialue
6. Dolk Lars
7. Ilmatieteen laitos
8. Tulli.fi
9. PTCServices Oy
10. Valtiokonttori
11. Maanmittauslaitos
12. Museovirasto
13. HUS-Yhtymä
14. Työ- ja elinkeinoministeriö
15. Elinkeinoelämän keskusliitto EK
16. Raahen kaupunki
17. Suomen kuntaliitto ry
18. Valtori
19. Turun kaupunki
20. Sosiaali- ja terveysministeriö
21. Helsingin kaupunki
22. Puolustusvoimat
23. Valtioneuvoston kanslia
24. Mikkelin kaupunki
25. Valtiovarainministeriö
26. Nurmijärven kunta
27. Metropolia Ammattikorkeakoulu Oy
28. Hansel
29. Liikenne- ja viestintävirasto
30. Poliisihallitus
31. Sisäministeriö
32. Rajavartiolaitos

Poimintoja annetuista lausuntopalautteista:

Suosituksen osalta:

Nähty hyvänä…

- Hyvä yleinen tietoturvallisuuden kypsyyden kehittämisenä
- Yhdenmukaistaa hankintoja ja sopimusmalleja

Yleistä kehitettävää?

- Ylätason suositus, vaatii organisaation omaa ohjeistusta
- Tietoturvallisuus vai turvallisuus? Käsitteiden selkeyttämistä
- Pilvipalveluiden osalta suositus toimii heikosti ja pilvipalveluiden käytön mahdollistamiseen osalta suositusta olisi syytä tarkastella uudestaan

Suhde muihin suosituksiin?

- Mikä on suhde JYSE ja JIT?
- Turvallisuussopimus, Hanselin sopimusehdot, näiden suhde suositukseen?
- Suosituksessa pitää selventää laajalti käytetyn turvallisuussopimuksen ja liitteinä olevien turvallisuusvaatimusten keskinäinen suhde

Suhde muuhun lainsäädäntöön?

- Sisältää ristiriitoja hankintalain ja erityisalojen hankintalain säädösten ja periaatteiden kanssa

Tietosuoja?

- Tietosuojan toteutumiseen hankinnoissa tulisi kiinnittää tässä suosituksessa enemmän huomiota

Turvallisuusliitteiden osalta:

- Suosituksessa pitää selventää laajalti käytetyn turvallisuussopimuksen ja liitteinä olevien turvallisuusvaatimusten keskinäinen suhde
- Liitteiden käyttö voi vaatia suurta tapauskohtaista muokkausta?
- Työkalun ja materiaalin toteutuksessa edelleen kehittämistä, Excelin työkalun käyttö on nähty jossain määrin hankalaksi
- Vaihtoehtoisena ratkaisuna on verkkopohjainen työkalu (julkaistu).

Huomioitua lausuntopalautta:

Johdanto (muutokset)

- Suositus **opastaa viranomaisia ja erityisesti hankintayksiköitä** tietojärjestelmien ja soveltuvin osin muiden palveluiden hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyssä
- **Tietoturvallisuustoimenpiteet määriteltävä jo hankintojen valmisteluvaiheessa** (poistettu tietojärjestelmien ja muiden ICT-palvelujen) Pidetään hankintojen valmisteluvaihe ei tarjouspyyntövaihe
  - **Lisätty:** tietojärjestelmän määritelmä
  - **Lisätty tarkennus:** Hankintaehtotyökalusta on kaksi versiota. Uudempia Office 365-ympäristöissä toimivia Excel-versioita edellyttävä liite 2 a ja vanhempia Excel-versioita tukeva liite 2 b.

1.1 Lainsäädännölliset perusteet (lisäykset/ tarkennukset)

- Hankintojen tietoturvallisuusvaatimukset **tulee määritellä riskilähtöisesti**. Riskienarviointi on yksi keskeisimmistä tietoturvallisuusvaatimusten asettamisen vaiheista.
- Suosituksen tulisi ohjata sijoittamaan tietoturvallisuusvaatimusten määrittely ja hallinta organisaatioiden ja niiden hanketoiminnan vaatimustenhallinnan sisään ja kehottaa välttämään rinnakkaisten ja aihealueittain pirstaloituvien prosessien tuottamista.
  - **Lisätty mm:** viittaukset julkisuuslakiin ja hallintolakiin ja huomautus, että tietosuoja-asetus on otettu huomioon hankintaehtotyökalussa
  - **Poistettu:** viittaukset hankintalakiin, erityisalojen hankintalakiin, puolustus- ja turvallisuushankintalakiin, tietosuoja-asetukseen, tietosuojalakiin, henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettuun lakiin
  - **Ei lisätty:** NIS2, CER

1.2 Suhde muihin suosituksiin (tarkennukset)

- **Lisätty:** Viittaukset PiTuKriin ja Pilvipalveluiden soveltamisohjeeseen. Ei ole kuitenkaan avattu tämän suosituksen suhdetta turvallisuussopimukseen eikä Hanselin sopimusmalleihin.

1.3 Rajaukset

- **Lisätty:** yleinen hankintoihin liittyvä sääntely, tietosuoja-asetuksen 28 artiklan mukaiset sopimusvaatimukset, henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain mukaisia vaatimuksia, valmiuslaki ja EU:n turvallisuusluokiteltujen tietojen suojaamista koskevia sääntöjä

Lukujen 2 (Tietoturvallisuuden varmistamisen prosessi), 2.1 (Hankinnan lähtökohtien tunnistaminen), 2.3 (Tietoturvallisuus hankintavaiheen aikana), 2.4 (Riskilähtöinen vaatimusten määrittely)

Muutoksia tai tarkennuksia kuten:

- **Lisätty:** Täsmennys kasautumisvaikutuksesta
- **Lisätty:** Kohta uhkien ja riskien tunnistamisesta ja riskilähtöisestä vaatimusten määrittelystä
- **Lisätty:** Kohta hankintaketjuihin kohdistuvien riskien tunnistamisesta
- **Täydennetty:** Etätyöhön liittyvää kohtaa viittauksella vaatimukseen FYY-03
- **Siirretty:** Salassapito- ja vaitiolositoumukset luettelon ensimmäiseksi kohdaksi
- **Lisätty:** Turvallisuusselvitykset hankintaan osallistuvista henkilöistä
- **Lisätty maininta:** Toimittajien luottamuksellisista aineistoista
- **Lisätty:** Kappale vaatimustenmäärittelyn tarpeellisuudesta riippumatta siitä hankitaanko tietojärjestelmä palveluna vai omaan ympäristöön asennettavana
- **Lisätty huomioitaviin asioihin:** elinkaari, vaatimusten ulottaminen alihankkijoihin, muutostenhallinta sekä ns. TORI-hankinnat
- **Lisätty:** kappale markkinakartoituksista.

Huomioitua lausuntopalautetta:

Luku 2.5 (Vaatimusten täyttymisen varmistaminen) ja luku 2.6 (Hyväksyntä) ja 2.7 (Käyttöönotto)

Muutoksia tai tarkennuksia kuten:

- **Lisätty:** käyttöönottoon palvelun tai järjestelmän kriittisyysluokittelun varmistaminen sekä käyttöönoton- ja ylläpitovaiheen vastuiden suunnittelu ja resursointi mukaan lukien toimittajan vastuut
- **Lisätty teksti:** Käyttöönottoon ja ylläpitoon liittyvät tehtävät ja vastuut on suositeltavaa huomioida jo hankinnan kohteen määrittelyssä (ennen hankinnan käynnistämistä) niin, että ne tulevat huomioiduksi itse kilpailutuksessa.

Luku 2.8 (Muutostenhallinta ja elinkaari)

Muutoksia tai tarkennuksia kuten:

- **Lisätty:** Osa-alue on tietoturvallisuuden varmistaminen hankinnan kohteen koko elinkaaren ajan sekä muutosten yhteydessä mukaan lukien palvelun käytön päättäminen.
- **Lisätty:** Muilla muutoksilla tarkoitetaan mitä tahansa palveluun kohdistuvaa muutosta, jonka taustalla on muut kuin tietoturvasta johtuvat syyt, kuten esimerkiksi säädösperustaan ja sen tulkintaan kohdistuvat muutokset.

Luku 3 alkuosa (Sopimuksen tietoturvallisuusliitteet)

Muutoksia tai tarkennuksia kuten:

- **Lisätty huomio:** Vaatimusten kohdistamisen laajuudesta toimittajan organisaatiossa ja tilaajan mahdollisuudesta täsmentää sitä
- **Lisätty huomio:** Yleisten täsmennysten lisäämisestä osaksi tarjouspyyntöä (ei erikseen jokaiseen erillisen vaatimukseen).
- **Lisätty kuva:** Kuvio 2. Sopimuksen tietoturvallisuusliitteet.

Luku 3.2 ja luku 3.3. ja 3.3.1 (Tietoturvallisuusvaatimukset suppea/laaja/hallinnollisen tietoturvan vaatimukset

- **Muutettu:** liitteen 1a nimi Tietoturvallisuusvaatimukset (suppea)
- **Muutettu:** liitteen 1b nimi Tietoturvallisuusvaatimukset (laaja)

Luku 4 (Hankintaehtotyökalun käyttöohje)

Muutoksia tai tarkennuksia kuten:

- **Luku 4:** Lisätty täsmennys vaatimusten kohdistamisesta hankinnan eri osiin
- **Luku 4.7:** Lisätty täsmennys luottamuksellisten vastausten merkitsemisestä
- **Luku 4.7:** Täsmennetty miten hankintayksikön tulee ohjeistaa eri tasoisten vaatimusten soveltamista eri tiedoille
- **Luku 4.8:** Täsmennetty, mistä saa tarkemmat tiedot kunkin käyttötapauskriteerin taustalla olevasta vaatimuksesta
- **Täsmennetty:** Käyttötapauskriteerien olennaisuuden vaikutusta hankinnan vaatimuksiin.

Huomioitua lausuntopalautetta:

Liite 1a (Suppeat tietoturvallisuusvaatimukset)

Muutoksia tai tarkennuksia kuten:

Muutettu liitteen 1a nimi: Tietoturvallisuusvaatimukset (suppea)

- **Muutettu teksti:** Näitä vaatimuksia voi käyttää osana sellaisia hankintoja, joissa käsitellään vain julkista tietoa ja tiedon eheyteen sekä saatavuuteen ei kohdistu normaalia korkeampia vaatimuksia. Vaatimuksia voidaan käyttää myös niissä tilanteissa, joissa käsitellään vain vähäisessä määrin muita kuin julkisia tietoja, joiden paljastuminen ei aiheuta riskiä
- **Muutettu teksti:** Muissa tapauksissa on suositeltavaa käyttää kattavampaa liitettä 1b tietoturvallisuusvaatimukset (laaja) sekä harkinnan mukaan hankintaehto-työkalun avulla muodostettavia osa-aluekohtaisia liitteitä ja tietosuojaliitettä.
- **Muutettu sopimus määritelmää nimen mukaisesti kohta 1.3:** Sopimus tarkoittaa Tilaajan ja Toimittajan välistä sopimusta, jonka liitteenä tämä Tietoturvallisuusvaatimukset – dokumentti on.
- **Lisätty kohta 7.3:** Toimittaja toimittaa Tilaajan pyynnöstä selvityksen tämän liitteen mukaisten velvollisuuksien täyttämisestä.

Liite 1b huomioidut palautteet (Tietoturvallisuusvaatimukset (laaja)

Muutoksia tai tarkennuksia kuten:

Muutettu liitteen 1b nimi: Tietoturvallisuusvaatimukset (laaja)

- **Selvennetty säädösten nimiä kohta 1.12:** Tiedonhallintalain (906/2019) 18 §:ssä ja Turvallisuusluokitteluasetuksessa (1101/2019) tarkoitettua turvallisuusluokiteltua asiakirjaa sekä tietoa, jotka asiakirjaan merkittyinä olisivat turvallisuusluokiteltavia
- **Selvennetty kohtaa 2.3.:** Sopijapuolet tiedostavat, että Palvelussa voidaan käsitellä tietoa, joka on lain mukaan pidettävä salassa. Tällä liitteellä Sopijapuolet sopivat menettelyistä, joilla varmistetaan, että Palvelussa käsiteltävät salassa pidettävät tiedot on suojattu asianmukaisesti.
- **Täsmennetty kohta 3.4.:** Tilaajalla on oikeus saada selvitys Toimittajan Alihankkijoidensa kanssa tekemistä turvallisuutta koskevista sopimuksista ja muista järjestelyistä siltä osin kuin ne koskevat Suojattavia aineistoja tai pääsyä Tiloihin.

Lopputekstin osalta korjattu kirjoitus- ja kielioppivirheitä ja tehty tarkennuksia kuten;

- **Lisätty kohta 8.1. Soveltamisjärjestys:** Soveltamisjärjestys Liitteitä sovelletaan niiden numerojärjestyksessä pienimmästä suurimpaan.
- **Lisätty ensisijaisuus Liite X.7 Tietosuojaliite** (ensisijainen käsiteltäessä henkilötietoja)
- **Lisätty käsiteltäessä henkilötietoja.** Liite X.7.1 Henkilötietojen käsittelytoimien kuvaus (käsiteltäessä henkilötietoja)
- **Lisätty ohje tekstiä kohta 8.1.:** [Ohje: Liitteet X.1-X.6 koskevat kaikkia tietoja. Liitteet X.7-X.7.1 koskevat vain henkilötietojen käsittelyä. Poista tarpeettomat liitteet ja numeroi liitteet uudestaan. Muokkaa numeroinnit myös sopimusliitteisiin. Siirrä tarvittaessa liiteluettelo ja soveltamisjärjestys pääsopimukseen.]

Huomioitua lausuntopalautetta:

Hankintaehtotyökalu – liite 2

Muutoksia tai tarkennuksia kuten:

- **Muokattu lausuntopalautteen johdosta seuraavien vaatimusten täsmennyksiä ja ohjeita:** TEK-05, TEK-07.1, TEK-10.1, TEK-12.1, TEK-17.1, TEK-18.3
- Osa liitteeseen 2 kohdistuneista palautteista huomioitiin tekemällä muutoksia suosituksessa oleviin ohjeisiin
- Muokattu Kriteeristö-välilehteä siten, että siitä on helpompi katsoa vaatimusta tarkentavia tietoja (yleiskuvaus, toteutusesimerkki, viitteet)
- **Lisätty täsmennys:** Hankintaehtotyökalusta on kaksi versiota. Uudempia Office 365-ympäristöissä toimivia Excel-versioita edellyttävä liite 2 a ja vanhempia Excel-versioita tukeva liite 2 b.

Kysymykset tai palaute?

Tiedonhallintalautakunta
Informationshanteringsnämnden

Lisätietoja

mika.kuronen@gov.fi
tuula.seppo@dvv.fi
martti.setala@gov.fi