xxx ministeriön julkaisusarja 2020:xx

Suositus tietoturvallisuudesta hankinnoissa

Lautakunnat

Valtiovarainministeriön julkaisuja – 2023:

xxxministeriö Helsinki 2020

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Tuplaklikkaa ja kirjoita ministeriö

ISBN sid. VNK täyttää
ISBN pdf VNK täyttää
ISSN sid. VNK täyttää
ISSN pdf VNK täyttää

Taitto Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2020
Finland (kieliversioissa)
Paino PunaMusta Oy, 2020

Kuvailulehti
x.x.2023

Suositus

VNK täyttää, sarja ja numero		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	Suomi	**Sivumäärä**	VNK täyttää
Tiivistelmä	Tämä tiedonhallintolautakunnan antama suositus opastaa		
	Tiedonhallintalautakunta hyväksyi suosituksen xx.xx.xxxx		
Klausuuli	VNK täyttää		
Asiasanat	lautakunnat, tiedonhallintalautakunta, tiedonhallintalaki, julkinen hallinto, tietoturva, hankinta		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN nid.	VNK täyttää	**ISSN painettu**	VNK täyttää
Asianumero	Napsauta ja kirjoita	**Hankenumero**	Napsauta ja kirjoita
Julkaisun osoite	VNK täyttää		

Presentationsblad
27.2.2023

Rekommendation om

VNK täyttää, sarjanimi ja numero		**Tema**	Nämnder
Utgivare	Finansministeriet		
Författare	Napsauta ja kirjoita		
Redigerare	Napsauta ja kirjoita		
Utarbetad av	Informationshanteringsnämden		
Språk	finska	**Sidantal**	VNK täyttää

Referat

Denna rekommendationssamling som utfärdats av informationsförvaltningsnämnden ger vägledning

Informationshanteringsnämnden godkände rekommendationen den xx.xx.xxxx

Klausul	VNK täyttää		
Nyckelord	nämnder, informationshanteringsnämnden, lagen om informationshantering inom den offentliga förvaltningen, nämnder, informationssäkerhet, den offentliga förvaltningen, upphandling		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN tryckt	VNK täyttää	**ISSN tryckt**	VNK täyttää
Ärendenr.	Napsauta ja kirjoita	**Projektnr.**	Napsauta ja kirjoita
URN-adress	VNK täyttää		

Description sheet
x Month 2022

Recommendation of

VNK täyttää, sarjanimi ja numero		**Subject**	Board
Publisher	Ministry of Finance		
Authors	Napsauta ja kirjoita		
Editor	Napsauta ja kirjoita		
Group Author	Napsauta ja kirjoita		
Language	Napsauta ja kirjoita	**Pages**	VNK täyttää

Abstract

This collection of recommendations issued by the Information Management Board provides guidance on the fulfilment

The Information Management Board approved xx.xx.xxxx.

Provision	VNK täyttää		
Keywords	board, Information Management Board, Information Management Act, Boards, information security, public administration,		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN printed	VNK täyttää	**ISSN printed**	VNK täyttää
Reference no.	Napsauta ja kirjoita	**Project no.**	Napsauta ja kirjoita
URN address	VNK täyttää		

Sisältö

1 Johdanto 10
1.1 Lainsäädännölliset perusteet 10
1.2 Suhde muihin suosituksiin 12
1.3 Rajaukset 13

2 Tietoturvallisuuden varmistamisen prosessi 14
2.1 Hankinnan lähtökohtien tunnistaminen 14
2.2 Hankinnan resurssointi 15
2.3 Tietoturvallisuus hankintavaiheen aikana 15
2.4 Vaatimusten määrittely 16
2.5 Vaatimusten täyttymisen varmistaminen 17
2.6 Hyväksyntä 18
2.7 Käyttöönotto 18
2.8 Muutostenhallinta ja elinkaari 19

3 Sopimuksen tietoturvallisuusliitteet 20
3.1 Pääsopimukseen kirjattavat asiat 20
3.2 Tietoturvallisuuden vähimmäisvaatimukset 21
3.3 Tietoturvallisuusvaatimukset 22
3.3.1 Hallinnollisen turvallisuuden vaatimukset 22
3.3.2 Fyysisen turvallisuuden vaatimukset 23
3.3.3 Teknisen turvallisuuden vaatimukset 23
3.3.4 Varautumisen ja jatkuvuudenhallinnan vaatimukset 24
3.3.5 Tietoturvallisuuden lisävaatimukset 25
3.4 Tietosuojaliite ja henkilötietojen käsittelytoimien kuvaus 25

4 Hankintaehtotyökalun käyttöohje 26
4.1 Hankinnan perustiedot 26
4.2 Esiehtojen määrittely 26
4.3 Vaatimusten sisällyttäminen hankintaan 30
4.4 Vaatimusten täsmentäminen 31
4.5 Lisävaatimusten kirjaaminen 32
4.6 Vaatimusliitteiden muodostaminen 33

4.7 Toimittajan ohjeistaminen....34
4.8 Käyttötapausten määrittely....35

Sanasto....36

Liitteet....41

Lähteet....42

1 Johdanto

Tämä tiedonhallintolautakunnan suositus 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 sisältää kuvauksen hankinnan tietoturvallisuuden varmistamisen prosessista, esittelyt sopimukseen liitettävistä tietoturvallisuusvaatimuksista sekä ohjeen hankintaehtotyökalun käyttämisestä. Suosituksen liitteinä on tietoturvallisuuden vähimmäisvaatimukset ja tietoturvallisuusvaatimukset. Tietoturvavaatimuksissa on huomioitu henkilötietojen käsittelyn asettamat vaatimukset. Erilliset EU:n yleinen tietosuoja-asetuksen ((EU) 2016/679), jäljempänä *tietosuoja-asetus*, edellyttämät sopimusliitteet tulevat saataville Digi- ja väestötietoviraston Digiturvajulkaisut sivustolle kohtaan Oppaat ja hyvät käytännöt.

Suosituksen liitteenä on hankintaehtotyökalu, jonka avulla hankintayksikkö voi muodostaa hallinnollisen turvallisuuden, fyysisen turvallisuuden, teknisen turvallisuuden sekä varautumisen ja jatkuvuudenhallinnan liitteet tietoturvallisuusvaatimuksista. Hankintaehtotyökalu perustuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön, jäljempänä *Julkri*.

Suositusta on valmisteltu tiedonhallintalautakunnan kaudelle 1.1.-31.12.2022 ja 1.1.-31.12.2023 asettamassa tietoturvallisuusjaostossa. Jaoston puheenjohtajana on toiminut neuvotteleva virkamies Mika Kuronen valtiovarainministeriöstä ja jaostosihteerinä johtava asiantuntija Tuula Seppo Digi- ja väestötietovirastosta. Tiedonhallintalautakunta on nimennyt jaoston jäseniksi asiantuntijoita eri tiedonhallintayksiköistä. Lisäksi jaosto on kokouksissa, työpajoissa ja seminaareissa kuullut laajalti myös jaoston ulkopuolisia asiantuntijoita. Suositusluonnos oli avoimesti kommentoivana julkisen lausuntopalvelun kautta xx.-xx.2023 välisenä aikana.

1.1 Lainsäädännölliset perusteet

Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019), jäljempänä *tiedonhallintalaki* tai *TihL*, luvussa 4 on säädetty tietoturvallisuustoimenpiteiden toteuttamisen vähimmäisvaatimuksista. Ne kohdistuvat keskeisiltä osin tietoaineistoihin ja tietojärjestelmiin. Jotta viranomaistoiminnassa voidaan varmistua tietoturvallisuustoimenpitei-

den asianmukaisuudesta, on tietoturvallisuustoimenpiteet määriteltävä jo tietojärjestelmien ja muiden ICT-palvelujen hankintojen valmisteluvaiheessa. Hankintavaiheessa tulee myös selvittää, miten tietoturvallisuuden tilaa seurataan tietojärjestelmän käytössä sen tuotantovaiheessa ja koko tietoaineistojen ja tietojärjestelmien elinkaaren ajan.

Tietojärjestelmiin ja tietoaineistoihin liittyvät toimenpiteet on määriteltävä ja toteutettava kussakin tietojärjestelmässä käsiteltävien tietojen laadun ja luonteen näkökulmasta. Lisäksi tietoturvallisuustoimenpiteiden määrittelyyn ja toteuttamiseen vaikuttaa hankittavan tietojärjestelmän merkitys viranomaisen tehtävien hoidolle, lakisääteisten velvollisuuksien toteuttamiselle ja yhteiskunnan toiminnalle.

Tiedonhallintalain 13 §:n 4 momentin mukaan: ”Viranomaisten on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet”. Lisäksi tiedonhallintalain 13 §:n 1 momentissa on säädetty tiedonhallintayksiköille velvollisuus seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan. Tiedonhallintayksiköllä on myös velvollisuus selvittää olennaiset tietojenkäsittelyyn kohdistuvat riskit ja sen on mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Jos hankintaan sisältyy turvallisuusluokiteltavien asiakirjojen käsittelyä, on viranomaisen huomioitava hankinnassa tiedonhallintalain 18 § ja sitä täydentävä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *turvallisuusluokitteluasetus* tai *TLA*.

Hankintojen kilpailuttamisesta säädetään julkisista hankinnoista ja käyttöoikeussopimuksista annetussa laissa (1397/2016), jäljempänä *hankintalaki* sekä vesi- ja energiahuollon, liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista annetussa laissa (1398/2016) jäljempänä *erityisalojen hankintalaki*. Puolustus- ja turvallisuushankintoihin sovelletaan puolustus- ja turvallisuushankinnoista annettua lakia (1531/2011) sekä hallintolaissa (434/2003) 6 §:ssä säädettyjä periaatteita.

Mikäli hankittava tietojärjestelmä sisältää henkilötietoja on lisäksi huomioitava henkilötietojen käsittelyyn liittyvät vaatimukset. Henkilötietojen käsittelyyn liittyvät yleissäädökset ovat tietosuoja-asetus ja sekä tietosuojalaki (1050/2018). Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä säädetään henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (1054/2018).

Tietosuoja-asetuksessa on säädetty sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamisesta. Siksi hankintojen suunnitteluvaiheessa on selvitettävä ne tietosuojavaatimukset, jotka vaikuttavat hankinnassa tietoturvallisuustoimenpiteiden määrittelyyn tarjouspyyntöasiakirjoihin. Henkilötietojen käsittelystä tarkempia ohjeita antaa Tietosuojavaltuutetun toimisto.

1.2 Suhde muihin suosituksiin

Tämä suositus ja muut tiedonhallintalautakunnan suositukset muodostavat yhdessä suosituskokonaisuuden. Tässä suosituksessa on hyödynnetty erityisesti Julkria. Suositukset ja kriteeristöt, joihin on suositeltavaa perehtyä, on kuvattu alla olevassa taulukossa.

Julkaisu	**Sisältö ja miten sisältö tukee hankintaa**
Julkisen hallinnon tietoturvallisuuden arviointikriteeristö, Julkri (2022:43)	Kriteeristön käyttö tukee organisaatioita tietoturvallisuuden ja henkilötietojen suojaamisen suunnittelussa, toteuttamisessa ja arvioinnissa. Julkrin alkuperäisistä vaatimuksista on muokattu hankinnoissa sovellettavia vaatimuksia.
Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (2021:65)	Suositus sisältää julkishallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset sekä yksityiskohtaisia suosituksia tiedonhallintalain tietoturvallisuutta koskevien pykälien soveltamisesta. Suositusta voi hyödyntää hankintaan liittyvien vähimmäisvaatimusten toteuttamisessa.
Suositus salassa pidettävien asiakirjojen käsittelystä (2023:4)	Suosituksessa kuvataan salassa pidettävien asiakirjojen (tietojen) käsittelyssä sekä käsittelyä koskevien vaatimusten täyttämisessä. Suositus tulee huomioida, mikäli hankinta sisältää salassa pidettäviä asiakirjoja (tietoja).
Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) ja Suositus turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa (2022:4)	Suositukset sisältävät turvallisuusluokiteltujen asiakirjojen käsittelyä koskevia suosituksia. Nämä suositukset tulee huomioida, mikäli hankinta sisältää turvallisuusluokiteltavia asiakirjojen käsittelyä.

Suositus teknisistä rajapinnoista ja katseluyhteyksistä (2021:21)	Suositus sisältää tarkennuksia tiedonhallintalaissa säädettyjen sähköisten luovutustapojen toteuttamiseen. Mikäli hankintaan sisältyy teknisiä rajapintoja tai katseluyhteyksiä, niin nämä suositukset tulee huomioida.
Suositus tiedonhallinnan muutosvaikutusten arvioinnista (2020:53).	Suositus sisältää tiedonhallintalaissa säädetystä muutosvaikutusten arvioinnin toteuttamisesta. Tiedonhallintalaissa tarkoitettu tietojärjestelmän käyttöönotto tarkoittaa jo hankintavaiheessa tehtävää muutosvaikutusarviointia muun muassa tietoturvallisuustoimenpiteiden järjestämisen osalta.
Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille	Katakri on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Mikäli hankintaan liittyy kansainvälistä turvallisuusluokiteltavaa tietoa, tulee käyttää Katakri arviointikriteeristöä.

1.3 Rajaukset

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

- yleistä hankintoihin liittyvää sääntelyä, koska kyseessä on hankintojen tietoturvallisuuteen keskittyvä suositus,
- toimialakohtaista lainsäädäntöä, kuten sosiaali- ja terveydenhuollon lainsäädäntöön sisältyviä vaatimuksia,
- saavutettavuusvaatimuksia 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 omassa toiminnassaan ja ohjeistuksissaan. Viranomainen voi käyttää apuna esimerkiksi Digi- ja väestötietoviraston julkaisemaa Turvallisen sovelluskehityksen käsikirjaa.

2 Tietoturvallisuuden varmistamisen prosessi

2.1 Hankinnan lähtökohtien tunnistaminen

Ennen varsinaisia hankintaan liittyviä toimenpiteitä on suositeltavaa tunnistaa hankinnan tietoturvallisuuden lähtökohdat, johon sisältyy vähintään seuraavat asiat:

- hankinnan kriittisyys, eli kuinka korkeita vaatimuksia hankintaan kohdistuu tietojen luottamuksellisuuden, eheyden ja saatavuuden näkökulmista,
- hankinnan osakokonaisuudet, etenkin jos hankinnan eri osiin kohdistuu erilaisia tietoturvallisuusvaatimuksia,
- liittyykö hankintaan henkilötietojen käsittelyä sekä kuuluvatko käsiteltävät henkilötiedot tietosuoja-asetuksen mukaisiin erityisiin henkilötietoryhmiin,
- mahdollinen toimialakohtainen lainsäädäntö, joka tulee ottaa huomioon tietoturvallisuusvaatimusten määrittelyssä,
- kohdistuuko hankintaan varautumiseen, jatkuvuudenhallintaan tai poikkeusolojen valmiuteen liittyviä vaatimuksia,
- hankinnan rajaukset, eli tietoturvallisuuteen liittyvät asiat, jotka on rajattu hankinnan ulkopuolelle esimerkiksi siitä syystä, että niiden toteuttaminen on viranomaisen vastuulla tai ne hankitaan erikseen,
- viranomaisen arkkitehtuurilinjaukset, jotka tulee ottaa huomioon määriteltäessä yksityiskohtaisia tietoturvallisuusvaatimuksia,
- tiedonhallintamalli ja sen perusteella tunnistetut hankinnan riippuvuudet,
- toimittajan vastuu tietoturvallisuuteen liittyvissä tehtävissä, erityisesti sellaisissa tilanteissa, joissa palvelun tuottamiseen osallistuu useita eri osapuolia kuten esimerkiksi sovellustoimittaja sekä käyttöpalvelun toimittaja,
- edellyttääkö hankittava palvelu toimittajalta tietoturvallisuuden hallintaa sekä
- käsitelläänkö viranomaisen tietoja toimittajan vastuulla olevissa teknisissä ympäristöissä tai toimitiloissa sekä
- voidaanko aiemmissa hankinnoissa kertynyttä tietoja ja kokemusta hyödyntää.

Lähtökohtien tunnistamisen avulla saadaan selville tietoturvallisuuden näkökulmasta, kuinka vaativasta hankinnasta on kyse, mitä eri asioita hankinnan yhteydessä tulee ottaa huomioon sekä kuinka paljon tietoturvaosaamista hankintaprosessissa tarvitaan.

2.2 Hankinnan resurssointi

Yksittäiseen hankintaan tarvittava tietoturvaosaaminen vaihtelee erittäin paljon hankinnan luonteen mukaan. Vain julkista tietoa sisältävän ei-kriittisen tietojärjestelmän hankintaan riittää vähäisempi tietoturvaosaaminen kuin saatavuudeltaan kriittisen turvallisuusluokiteltuja tietoja sisältävän tietojärjestelmän hankintaan.

Tietoturvaosaamisen varmistamiseksi suositellaan, että kaikissa hankinnoissa, joissa tietoturvallisuudella on tai voi olla merkitystä, käytetään tietoturva-asiantuntijaa hankinnan lähtökohtien tunnistamisessa. Varsinaiseen hankintavaiheeseen resursoidaan riittävä tietoturva- ja tietosuojaosaaminen lähtökohtien tunnistamisen perusteella. Viranomaisen kannalta panostaminen tietoturvallisuusosaamiseen hankintavaiheessa auttaa välttämään sekä vakavia tietoturvapuutteita että tarpeetonta ja kallista ylisuojautumista.

2.3 Tietoturvallisuus hankintavaiheen aikana

Myös hankintavaiheen aikana tulee huolehtia tietojen suojaamisesta. Näitä suojattavia tietoja voivat olla esimerkiksi hankittavaa järjestelmää kuvaava dokumentaatio, testiaineistot tai korkeampien turvallisuusluokkien hankinnoissa jopa kaikki hankintaan liittyvät tiedot.

Ennen hankinnan käynnistämistä ja hankintaan liittyvien aineistojen toimittamista toimittajille, tulee tapauskohtaisen harkinnan perusteella tehdä tarpeelliset toimenpiteet hankintavaiheen turvallisuuden varmistamiseksi, joita ovat esimerkiksi:

- turvallisuusselvitykset hankintaan osallistuvista toimittajan henkilöistä,
- sopimukset toimittajien kanssa koskien hankintaan liittyvien aineistojen käsittelyä,
- hankintaan osallistuvien henkilöiden vaitiolositoumukset[1],
- ohjeet hankintaan liittyvien aineistojen käsittelystä,
- riittävän turvalliset ympäristöt kuten työtilat ja työasemat hankinta-asiakirjojen käsittelyyn sekä menettelyt aineistojen tuhoamiseksi tai palauttamiseksi hankintavaiheen jälkeen.

[1] Laki viranomaisen toiminnan julkisuudesta (621/1999) 23 §:n mukaan salassa pidettävää tietoa koskeva vaitiolovelvollisuus ja hyväksikäyttökielto ulottuvat myös henkilöön, joka toimii viranomaisen toimeksiannosta tai toimeksiantotehtävää hoitavan palveluksessa. Salassapitorikoksesta ja salassapitorikkomuksesta säädetään rikoslain (1889/39) 38 luvussa.

2.4 Vaatimusten määrittely

Hankintaan kohdistettavien tietoturvallisuusvaatimusten määrittely on yksi keskeisimmistä hankinnan turvallisuuden varmistamisen vaiheista. Vaiheen tavoitteena on määritellä riittävän tiukat vaatimukset hankinnan kohteen tietoturvallisuuden varmistamiseksi välttäen kuitenkin tarpeettoman korkeita vaatimuksia ja sitä kautta ylimääräisiä kustannuksia.

Tietoturvallisuuteen kohdistuvien vaatimusten määrittelyssä suositellaan noudattamaan seuraavia periaatteita:

- vaatimuksissa tulee ottaa huomioon eri näkökulmat kuten luottamuksellisuus, eheys ja saatavuus,
- vaatimuksiin tulee kirjata kaikki tietoturvallisuutta koskevat vaatimukset, eli ei pidä olettaa, että jokin vaatimus on täytetty itsestään selvyytenä,
- vaatimukset tulee kuvata riittävän yksityiskohtaisesti, mutta välttäen tarpeetonta toteutustekniikan rajausta (toteutusratkaisuja voidaan kuitenkin rajata muilla perusteilla kuten esimerkiksi teknologia-arkkitehtuurin yhdenmukaisuuden vuoksi),
- käytettäessä vaatimusten pohjana jotain yleistä vaatimusjoukkoa, tulee vaatimukset täsmentää ottaen huomioon tapauskohtaiset riskit,
- yksittäisen hankinnan tietoturvallisuusvaatimusten yhdenmukaisuus tulee varmistaa suhteessa viranomaisen tietoturva-arkkitehtuuriin sekä
- tulee sopia palvelun päättämiseen liittyvät vaatimukset, kuten tietojen hävittäminen tai siirtäminen.

Eri osapuolten vastuut vaikuttavat osaltaan hankintaan kohdistettaviin tietoturvallisuusvaatimuksiin. Tietoturvallisuusvaatimusten määrittelyn yhteydessä on syytä tunnistaa hankintaan liittyvät eri osapuolet, määritellä osapuolten roolit hankinnan tietoturvallisuuden varmistamisessa sekä asettaa vaatimukset näiden roolien mukaisesti varmistaen samalla että mitään olennaisia tietoturvallisuuteen liittyviä vaatimuksia ei jää kohdistamatta. Esimerkiksi vastuut sovellustoimittajan, käyttöpalvelutoimittajan ja viranomaisen välillä tulee olla määriteltyinä.

Joissakin tapauksissa voi olla myös perusteltua tehdä tietopyyntöjä sekä käydä vuoropuhelua toimittajien kanssa lisäymmärryksen saamiseksi vaatimusten pohjaksi. Erityisesti hankittaessa uusiin teknologioihin perustuvia palveluita voi tällainen vuoropuhelu olla perusteltua myös tietoturvallisuusvaatimusten määrittelyssä.

Yleisesti käytettyjen vaatimusluetteloiden hyödyntäminen helpottaa vaatimusten täyttymisen varmistamista. Erityisesti suurten toimittajien kannalta on helpompaa osoittaa

palvelun tietoturvallisuus auditoimalla palvelun turvallisuus yleisesti käytettyjen kriteeristöjen avulla. Vaatimusten määrittelyssä onkin suositeltavaa ottaa yhtenä näkökulmana huomioon vaatimusten täyttymisen varmistaminen ja välttää tarpeettomien organisaatiokohtaisten erillisvaatimusten käyttöä.

Riippuen hankinnan kohteen laajuudesta ja kriittisyydestä, viranomainen voi toteuttaa erilaisia menettelyitä tietoturvallisuuteen kohdistettavien vaatimusten laadun varmistamiseksi. On suositeltavaa, että hankintojen tietoturvallisuusvaatimukset katselmoidaan organisaation tietoturvallisuudesta vastaavien henkilöiden toimesta. Lisäksi kriittisemmissä hankinnoissa voidaan edellyttää vaatimusten muodollista hyväksymistä ennen hankintaprosessin etenemistä seuraaviin vaiheisiin.

2.5 Vaatimusten täyttymisen varmistaminen

Tietoturvallisuuteen kohdistuvien vaatimusten täyttyminen tulee varmistaa riittävän luotettavalla tavalla sekä ennen käyttöönottoa että kaikkien sellaisten muutosten ja päivitysten yhteydessä, jotka voivat vaikuttaa tietoturvallisuuteen.

Vaatimusten täyttymisen varmistamiseen on käytettävissä erilaisia keinoja kuten:

- tietoturvadokumentaation katselmoinnit,
- viranomaisen ja toimittajan suorittamat tietoturvatestaukset,
- ulkoiset tietoturvatestaukset,
- testaustulosten katselmoinnit,
- sopimukselliset velvoitteet sekä niihin liittyvät sanktiot,
- viranomaisen oikeus tehdä auditointeja ja tarkastuksia,
- tietoturva-arvioinnit ja -auditoinnit,
- tietosuojan vaikutustenarvioinnit,
- sertifikaatit, jotka osoittavat turvallisuusvaatimusten täyttymisen sekä
- yritysturvallisuustodistukset.

Vaatimusten täyttymisen varmistaminen yksittäisessä hankinnassa vaihtelee tapauskohtaisesti. Keinoja valittaessa tulee erityisesti pohtia niiden luotettavuutta, eli kuinka suurella varmuudella vaatimusten täyttyminen kyetään osoittamaan, sekä varmistamisen kustannuksia. Mitä korkeammat turvallisuusvaatimukset hankintaan kohdistuvat, sitä luotettavammin niiden täyttyminen tulee kyetä osoittamaan.

Hankintojen koko elinkaaren aikana tehdään tyypillisesti paljon versiopäivityksiä, jotka voivat vaikuttaa turvallisuuteen. Jos versiopäivityksiä on usein, voi niiden tietoturvallisuuden varmistaminen olla työlästä ja kallista. Siksi onkin suositeltavaa suunnitella

versiopäivitysten tietoturvallisuuden varmistaminen erityisen hyvin sekä suosia keinoja, joissa toimittajan vastuulla on osoittaa riittävillä menettelyillä tietoturvallisuusvaatimusten täyttyminen versiopäivitysten yhteydessä.

2.6 Hyväksyntä

Erityisesti kriittisissä hankinnoissa on suositeltavaa, että johto hyväksyy hankinnalle asetettavat tietoturvallisuusvaatimukset ja tekee käyttöönottopäätöksen. Hyväksymismenettely korostaa johdon vastuuta tietoturvallisuusasioissa sekä pakottaa osaltaan suorittamaan hankinnan edeltävät vaiheet riittävän huolellisesti. Hyväksymispäätöksen perusteena on tyypillisesti testaus- ja katselmointipöytäkirjat sekä niiden perusteella tehty päätösesitys. Hyväksyntään voi kohdistua myös lakisääteisiä vaatimuksia ja menettelyitä.

Mikäli hankinnan tietoturvallisuuteen liittyy puutteita ja riskejä, on hyväksymispäätöksen vieminen johdon käsittelyyn erityisen perusteltua. Tällöin päätöksenteon tueksi on tehtävä riskiarvio sekä ehdotus toimenpiteistä liian korkeiden riskien pienentämiseksi.

2.7 Käyttöönotto

Käyttöönotto on merkittävä vaihe hankinnan tietoturvallisuuden varmistamisessa. Vaiheen laajuus voi vaihdella huomattavasti hankinnan luonteesta riippuen. Erityisesti suurissa ja kriittisissä hankinnoissa käyttöönotto tulee suunnitella huolellisesti. Alla on karkean tason lista näkökohdista, joita käyttöönotossa tulee ottaa huomioon tietoturvallisuuden varmistamiseksi:

- palvelun koventaminen sisältäen mm.
    - tarpeettomien palveluiden ja protokollien poistaminen,
    - esimerkkitunnusten sekä muiden ennen käyttöönottoa käytössä olleiden tunnusten poistaminen,
    - oletussalasanojen vaihtaminen sekä
    - turvallisuusparametrien asettaminen
- tietojen eheyden varmistaminen mahdollisen konversion yhteydessä,
- palvelun tietoturvallisen käytön ohjeistaminen ja koulutus,
- toimintamalleista sopiminen tietoturvahäiriöiden yhteydessä,
- valvonta- ja lokituskäytäntöjen sopiminen,
- haavoittuvuuksien seurannasta sopiminen sekä
- ylläpitovaiheen vastuiden suunnittelu ja resursointi.

Yllä olevat näkökohdat tulee huomioida osana viranomaisen käyttöönottoprosesseja. Onkin suositeltavaa, että viranomainen määrittelee ja ohjeistaa yleisen käyttöönotto-prosessin ja sisällyttää siihen tietoturvallisuuden varmistamiseen liittyvät näkökohdat.

2.8 Muutostenhallinta ja elinkaari

Keskeinen, mutta usein liian vähälle huomiolle jäävä osa-alue on tietoturvallisuuden varmistaminen hankinnan koko elinkaaren ajan sekä muutosten yhteydessä. Muutokset voidaan jakaa karkeasti toimintaympäristön tietoturvallisuudessa tapahtuviin muutoksiin sekä muihin palvelussa tehtäviin muutoksiin ja päivityksiin. Molemmissa tapauksissa organisaation tulee varmistaa riittävällä tavalla palvelun tietoturvallisuus muutoksen jälkeen.

Tietoturvallisuuden toimintaympäristössä tapahtuvia muutoksia ovat esimerkiksi uusien haavoittuvuuksien löytyminen, uudenlaisten tietoturvauhkien tunnistaminen sekä muut sellaiset seikat, jotka saattavat heikentää hankitun palvelun tietoturvallisuutta.

Tietoturvallisuuden varmistaminen muuttuvassa toimintaympäristössä edellyttää selkeiden menettelytapojen sopimista haavoittuvuuksien seuraamiseksi sekä niihin liittyvien ohjelmistopäivitysten asentamiseksi, toimintaympäristön tietoturvallisuuden seurannan vastuuttamista sekä toimintamallia havaittujen tietoturvallisuuspuutteiden korjaamiseksi.

Muilla muutoksilla tarkoitetaan mitä tahansa palveluun kohdistuvaa muutosta, jonka taustalla on muut kuin tietoturvasta johtuvat syyt. Myös tällaiset muutokset voivat vaikuttaa palvelun tietoturvallisuuteen. Siksi palvelun toimittajan kanssa on sovittava menettelyt, joiden mukaisesti arvioidaan muutosten vaikutusten laajuus, suunnitellaan riittävä tietoturvatestaus muuttuneiden osien tietoturvallisuuden varmistamiseksi sekä sovitaan käytännön toimenpiteet ja vastuut testausten suorittamisesta.

3 Sopimuksen tietoturvallisuusliitteet

Sopimukseen sisältyvät tietoturvallisuutta koskevat sopimusehdot ja tietoturvallisuusvaatimukset dokumentoidaan ensisijaisesti sopimuksen liitteissä. Lisäksi tiettyjä keskeisimpiä tietoturvallisuutta koskevia vaatimuksia voidaan nostaa osaksi pääsopimusta.

Tietoturvallisuuden vähimmäisvaatimukset ja tietoturvallisuusvaatimukset määritellään valmiiden mallidokumenttien avulla. Hallinnollista turvallisuutta, fyysistä turvallisuutta, teknistä turvallisuutta sekä varautumista ja jatkuvuudenhallintaa koskevat liitteet määritellään Julkri-arviointikriteeristöön perustuvan hankintaehtotyökalun avulla.

Mikäli hankinnan yhteydessä tunnistetaan sellaisia tietoturvavaatimuksia, jotka eivät sisälly hankintaehtotyökaluun tai tietoturvavaatimukset liitteeseen, tulee nämä vaatimukset lisätä hankintaehtotyökalun Lisävaatimukset -välilehdelle.

Kukin yksittäinen hankintaehtotyökalun avulla muodostettava liite voidaan jättää pois niissä tilanteissa, kun kyseisen osa-alueen tietoturvallisuuden merkitys viranomaisen tietoturvallisuudelle on riskiperusteisesti arvioitu hyvin pieneksi. Esimerkiksi jos viranomaisen tietoaineistoja käsitellään ainoastaan toimittajan yksittäisissä työasemissa hyödyntäen viranomaisen tarjoamia työkaluja, voidaan teknisen osa-alueen vaatimukset koskien toimittajan ympäristöä jättää pois. Tällaisissa tapauksissa voidaan asettaa vaatimukset vain toimittajan työasemille.

Suositukseen sisältyviä tietoturvallisuusliitteitä käytettäessä on syytä muistaa, että sopimuskokonaisuuden lopullinen muoto ja sen lainmukaisuus, tarkoituksenmukaisuus sekä ristiriidattomuus ovat aina hankintayksikön vastuulla.

Seuraavissa alaluvuissa on kuvattu jokaiseen liitteeseen liittyvät yleiset ohjeet. Tarkempia ohjeita koskien yksittäisten vaatimusten käyttöä ja tarkentamista on kuvattu mallidokumenteissa sekä hankintaehtotyökalussa.

3.1 Pääsopimukseen kirjattavat asiat

Alla on suosituksia tietoturvallisuusnäkökulman huomioimiseen pääsopimuksessa:

- huolehdi siitä, että tarkastusoikeutta koskevassa luvussa tai käytettävissä yleisissä ehdoissa on oikeus tarkastaa tietoturvallisuusjärjestelyt,
- lisää tietoturvallisuuteen liittyvät vastuuhenkilöt yhteystietojen listalle,

- tarkista, että sopimuksella on riittävät sakko- ja vahingonkorvauslausekkeet myös tietoturvallisuusliitteeseen liittyvissä poikkeamissa,
- mieti, millainen purku- tai välittömän irtisanomisen ehto liittyy tietoturvallisuusliitteen velvoitteiden rikkomiseen. Esimerkkilause voisi olla:
    - *Tilaaja on oikeutettu purkamaan sopimuksen ilman irtisanomisaikaa tai Tilaajan valitsemalla 1–12 kuukauden irtisanomisajalla, mikäli Toimittaja rikkoo Liitteen X sopimusvelvoitteita olennaisesti*.
- pohdi, onko ostamassasi palvelussa perusteltua edellyttää tietojen sijaintia/käsittelyä Suomessa tai ETA-alueella,
- palvelun hankinnassa voi olla tarvetta varautua yrityskauppatilanteisiin, joissa on riskejä esimerkiksi huoltovarmuuteen, turvallisuuteen tai maanpuolustukseen liittyvästä näkökulmasta. Seuraavassa esimerkkilausekkeessa on pyritty huomioimaan yrityskauppatilanteeseen varautumisen näkökohtia suomalaisten yritysten osalta:

    Toimittaja on tietoinen ulkomaalaisten yritysostojen seurannasta annetun lain (172/2012) mukaisista velvoitteista. [Ulkomaisen omistajan on haettava työ- ja elinkeinoministeriöltä etukäteen vahvistus yritysostolle, jos yritysoston kohteena on puolustusteollisuusyritys tai yritys, joka tuottaa tai toimittaa yhteiskunnan turvallisuuden kannalta keskeisille Suomen viranomaisille niiden lakisääteisiin tehtäviin liittyviä kriittisiä tuotteita tai palveluita.] Sen lisäksi mitä sanotussa laissa säädetään yritysoston ilmoittamisesta toimivaltaiselle viranomaiselle, Toimittaja ilmoittaa Tilaajalle lain 2 §:n 1 momentin 5 kohdassa tarkoitetusta yritysostosta viipymättä yritysoston toteutumisen jälkeen ja antaa Tilaajalle tarvittavat tiedot ulkomaisesta omistajasta sekä yritysoston keskeisestä sisällöstä. Mikäli Toimittaja tuomitaan ulkomaalaisten yritysostojen seurannasta annetun lain (172/2012) 10 §:ssä säädetystä yritysostorikkomuksesta tai Toimittajan epäillään syyllistyneen sanottuun rikkomukseen, Tilaajalla on oikeus irtisanoa sopimus välittömästi, tai Tilaajan valitseman 1–12 kuukauden aikana.

3.2 Tietoturvallisuuden vähimmäisvaatimukset

Tietoturvallisuuden vähimmäisvaatimukset -liitettä voit käyttää osana sellaisia hankintoja, joissa ei käsitellä salassa pidettäviä eikä turvallisuusluokiteltuja (TLIV-TLI) tietoja, henkilötietoja eikä palveluiden eheyteen tai saatavuuteen kohdistu normaalia korkeampia vaatimuksia tai joiden tietoturvariskin olet arvioinut olevan hyvin matala. Liite sisältää tietoturvallisuuden vähimmäisvaatimukset ja kaikkien toimijoiden toimialasta riippumatta pitää pystyä sitoutumaan niihin.

Muissa tapauksissa on suositeltavaa harkinnan mukaan käyttää kattavampaa tietoturvallisuusvaatimukset liitettä, hankintaehto-työkalun avulla muodostettavia osa-aluekohtaisia tietoturvavaatimusliitteitä sekä Digi- ja väestötietoviraston Digiturvajulkaisut sivustolla kohdassa Oppaat ja hyvät käytännöt olevia tietosuojaliitteitä.

3.3 Tietoturvallisuusvaatimukset

Laajempaa tietoturvallisuusvaatimukset -liitettä voit käyttää hankintoihin, joissa käsitellään salassa pidettäviä tai turvallisuusluokiteltuja (TLIV- TLI) tietoja, henkilötietoja tai hankittavien palveluiden eheyteen tai saatavuuteen kohdistuu normaalia korkeampia vaatimuksia.

Liitteessä on kuvattu yleiset tietoturvallisuusvaatimukset, joita suositellaan täydentämään hankintaehtotyökalun avulla muodostettavilla yksityiskohtaisemmilla osa-aluekohtaisilla tietoturvavaatimuksilla. Muokkaa liite hankintaan soveltuvaksi. Käy läpi ehtojen yhteydessä olevat erilliset ohjeet ja tee tarvittavat muokkaukset niiden mukaisesti.

3.3.1 Hallinnollisen turvallisuuden vaatimukset

Hallinnollisen turvallisuusuuden vaatimukset -liite tulee sisällyttää hankinnan ehtoihin, jos toimittaja käsittelee viranomaisen salassa pidettäviä tai sitä korkeammalle luokiteltuja tietoja tai henkilötietoja. Liite voidaan jättää pois riskiarvioinnin perusteella, jos käsittely on hyvin vähäistä.

Liite sisältää vaatimuksia, joilla tietoturvallisuuden hallinta jalkautetaan osaksi koko organisaation toimintaa. Esimerkiksi suojattavien kohteiden tunnistamiseen, riskienhallintaan ja dokumentointiin liittyvät kriteerit ovat yleisiä, ja niitä tulee oletusarvoisesti hyödyntää muiden osa-alueiden kriteerien soveltamisen yhteydessä.

Tarkenna vaatimuksia tarvittaessa riskiperusteisesti hankintaan sopivaksi. Määrittele erillinen ohje tietojen käsittelystä ja säilyttämisestä, jos toimittajalle luovutetaan salassa pidettäviä tai sitä korkeammalle luokiteltuja tietoja tai henkilötietoja.

3.3.2 Fyysisen turvallisuuden vaatimukset

Fyysisen turvallisuuden vaatimukset- liite tulee sisällyttää hankinnan ehtoihin, jos toimittajan fyysisessä tietojenkäsittely-ympäristössä käsitellään tai säilytetään viranomaisen salassa pidettäviä tai sitä korkeammalle luokiteltuja tietoja tai henkilötietoja.

Tarvittaessa viranomainen tarkentaa fyysisen turvallisuuden vaatimuksia riskiperusteisesti kyseiseen hankintaan sopivaksi. Tällainen tarkennus voi koskea esimerkiksi tilanteita, joissa toimittajan tiloissa käsitellään tietoa, mutta mahdollinen tietoaineiston säilytys tapahtuu muualla. Hankintayksikkö määrittelee lisäksi hyväksyttävän jäännösriskitason, joka voidaan hyväksyä, kun toimittajan fyysiseen tietojenkäsittely-ympäristöön luovutetaan salassa pidettäviä tai sitä korkeammalle luokiteltuja tietoja tai henkilötietoja.

Liitteessä kuvatulla hallinnollisella alueella[2] tarkoitetaan normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotiloja tai useista eri toimistotiloista muodostuvaa kokonaisuutta. Liitteessä kuvatulla turva-alueella[3] tarkoitetaan työskentelyyn tarkoitettuja, hallinnollisia alueita paremmin suojattuja alueita ja tiloja, joissa käsitellään ja säilytetään turvallisuusluokiteltuja tietoja. Tarvittaessa hankintayksikkö täsmentää alueille asetettuja vaatimuksia siellä käsiteltävän ja/tai säilytettävän tiedon luottamuksellisuuden ja kriittisyyden perusteella. Hankintayksikkö voi lisäksi rajata vaatimukset koskemaan esimerkiksi vain turvallisuusluokiteltavia tietoja ja tarvittaessa täsmentää tietoaineistoon perustuen, mitä vaatimuksia sovelletaan.

3.3.3 Teknisen turvallisuuden vaatimukset

Teknisen turvallisuuden vaatimukset -liite tulee sisällyttää hankinnan ehtoihin, jos toimittajan teknisessä ympäristössä käsitellään viranomaisen salassa pidettäviä tai sitä korkeammalle luokiteltuja tietoja, henkilötietoja tai sieltä käsin hallinnoidaan viranomaiselle tuotettavia palveluita.

Hankinnoissa, joissa ei käytetä toimittajan teknistä ympäristöä lukuun ottamatta yksittäisiä työasemia, voidaan teknisen turvallisuuden ehtojen sijaan määritellä työasemalle asetettavat turvallisuusvaatimukset. Hankintaehtotyökalu ei sisällä näitä vaatimuksia, vaan hankintayksikön tulee määritellä ne esimerkiksi soveltamalla organisaation omia työasemavaatimuksia.

[2] TLA 9 §
[3] TLA 9 §

Monet tekniseen turvallisuuteen liittyvät hankintaehtotyökalussa olevat vaatimukset edellyttävät täsmennyksiä hankintayksiköltä, koska sellaisenaan käytettynä vaatimukset jättävät liian suuren liikkumavaran toimittajille. Täsmennystä edellyttävät vaatimukset on eritelty kunkin vaatimuksen kohdalla olevassa vaatimuskohtaisessa soveltamisohjeessa. Vaatimusten täsmentämisessä hankintayksikkö voi hyödyntää Julkri-kriteeristössä olevia vaatimuskohtaisia toteutusesimerkkejä.

Olennaista on täsmentää vaatimusta sille tasolle, että vaatimus on kyseisen hankinnan riskien näkökulmasta tarkasteltuna riittävällä tasolla. Riskitason lisäksi tekniseen turvallisuuteen liittyvien vaatimusten täsmentämisessä tulee ottaa huomioon viranomaisen teknologiavalinnat sekä muut tekniseen arkkitehtuuriin liittyvät näkökohdat, jotta hankittava palvelu on yhteensopiva viranomaisen muiden teknisten ratkaisujen kanssa.

Toisaalta teknisen osa-alueen sopimusehdoissa tulee välttää liian yksityiskohtaisia toteutusteknisiä vaatimuksia, jotka perusteettomasti rajoittavat toimittajan vaihtoehtoja vaatimuksen toteuttamiseen.

3.3.4 Varautumisen ja jatkuvuudenhallinnan vaatimukset

Varautumisen ja jatkuvuudenhallinnan vaatimukset - liite tulee sisällyttää hankinnan ehtoihin, jos palvelun toimitusvarmuus on hankintayksikölle tärkeää. Hankintayksikön tulee arvioida hankinnan kriittisyys, eli kuinka korkeita saatavuusvaatimuksia hankintaan kohdistuu.

Varautuminen ja jatkuvuudenhallinta hankinnoissa edellyttävät, että hankintayksiköt pohtivat jatkuvuudenhallintaa ja varautumiseen kohdistuvia vaatimuksia sekä niitä riskejä, joita hankittavaan palveluun tai tuotteeseen saattaa liittyä.

Hankintaehdot suositus sisältää normaaliolojen varautumista ja jatkuvuudenhallintaa koskevia kriteereitä. Kriteerit perustuvat tiedonhallintalakiin (muun muassa 4 §:n 2 mom 2 k, 13 §:n 1, 2 ja 4 mom sekä 15 §) sekä standardissa ISO/IEC 27002 kuvattuihin tietoturvallisuuden jatkuvuutta kuvaaviin hallintakeinoihin.

3.3.5 Tietoturvallisuuden lisävaatimukset

Voit lisätä sellaisia tietoturvallisuuteen kohdistuvia lisävaatimuksia, jotka eivät sisälly muihin liitteisiin, hankintaehtotyökalun Lisävaatimukset -välilehden avulla.

3.4 Tietosuojaliite ja henkilötietojen käsittelytoimien kuvaus

Henkilötietojen käsittely vaikuttaa osaltaan myös muihin hankinnan tietoturvallisuusvaatimuksiin. Nämä vaatimukset otetaan huomioon hankintaehtotyökalun ehdottamissa vaatimuksissa, jos hankintayksikkö on valinnut kohdassa *Esiehdot/ Henkilötiedot hankinnan kohteessa*, joko vaihtoehdon *Henkilötietoja* tai *Erityisiin henkilötietoryhmiin kuuluvia tietoja*.

Erilliset tietosuoja-asetuksen edellyttämät tietosuojaliitteet koskien henkilötietojen käsittelijöiden kanssa laadittavia sopimuksia tulee saataville Digi- ja väestötietoviraston Digiturvajulkaisut sivustolle kohtaan Oppaat ja hyvät käytännöt.

4 Hankintaehtotyökalun käyttöohje

Hankintaehtotyökalun avulla hankintayksikkö voi muodostaa liitteet hallinnolliseen turvallisuuteen, fyysiseen turvallisuuteen, tekniseen turvallisuuteen sekä varautumiseen ja jatkuvuudenhallintaan kohdistuvista tietoturvallisuusvaatimuksista.

Liitteiden muodostaminen etenee vaiheittain. Aluksi tulee määritellä esiehdot, joiden perusteella hankintaehtotyökalu ehdottaa hankinnassa käytettäviä tietoturvavaatimuksia. Ehdotusten sekä tapauskohtaisen riskiarvion perusteella tulee tehdä päätökset hankintaan sisällytettävistä vaatimuksista sekä täsmentää niitä tarvittaessa. Lopuksi tulee nimetä ja numeroida liitteet osaksi tarjouspyyntöä.

Seuraavissa luvuissa on kuvattu yksityiskohtaisemmin, miten hankintaehtotyökalun käytön eri vaiheet tehdään.

4.1 Hankinnan perustiedot

Hankinnan perustiedot-välilehdellä voi kirjata seuraavat hankintaa koskevat tiedot.

- *Organisaatio*: Hankintaa tekevän viranomaisen nimi. Esimerkiksi ”Valtiovarainministeriö.”
- *Yksikkö*: Hankintaa tekevää viranomaista kuvaava tarkenne. Esimerkiksi ”Julkisen hallinnon tieto- ja viestintätekninen osasto”.
- *Ajankohta*: Hankinnan ajankohta.
- *Hankinnan kohde*: Hankintaa kuvaava nimi, esimerkiksi ”Sovelluksen x ylläpitopalvelu”.
- *Hankinnan yhteyshenkilö*: Henkilö, jolta saa tarvittaessa lisätietoja hankinnasta.
- *Yhteystiedot*: Hankintayksikön ja yhteyshenkilön yhteystiedot.
- *Lisätiedot*: Kenttä muita hankintaa koskevia lisätietoja varten, joka voi sisältää esimerkiksi yleiskuvauksen hankinnasta ja sen taustoista.

4.2 Esiehtojen määrittely

Hankintayksikön tulee määritellä hankinnan kohteelta vaadittavat turvallisuuden tasot sekä sopimukseen sisällytettävät turvallisuusliitteet hankintaehtotyökalun *Esiehdot*-

välilehdellä. Ennen esiehtojen määrittelyä on suositeltavaa tunnistaa hankinnan lähtökohdat tämän suosituksen luvussa 2.1 Hankinnan lähtökohtien tunnistaminen kuvatulla tavalla. Seuraavassa kuvassa näkyvät esiehdot välilehdellä annettavat tiedot. Kuvion jälkeen on kuvattu yksityiskohtaisemmin kunkin esiehdon sisältö ja vaihtoehdot.

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

Kuvio 1. Esiehdot-välilehti.

Turvallisuustasot ja henkilötiedot

Turvallisuustasot tulee määritellä erikseen luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Lisäksi tulee määritellä, sisältyykö hankinnan kohteeseen henkilötietoja sekä kuuluvatko henkilötiedot tietosuoja-asetuksen mukaisiin erityisiin henkilötietoryhmiin.

Turvallisuustasoja ja henkilötietoja koskevat valinnat tehdään alasvetovalikoiden avulla, jotka saa näkyviin kunkin kentän oikealla puolella olevasta nuolesta. Nuoli tulee näkyviin, kun valitset kentän.

Vaadittava luottamuksellisuuden taso:

- *Julkinen*: Viranomaisen asiakirjat ovat julkisia, jollei laissa erikseen toisin säädetä. (JulkL 1 §).
- *Salassa pidettävä*: Viranomaisen asiakirja on pidettävä salassa, jos se laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. (JulkL 22 § ja 24 §).

- *TL IV*: Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **lievää vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle. (maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle)
- *TL III*: Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.
- *TL II*: Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **merkittävää vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.
- *TL I*: Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **erityisen suurta vahinkoa** tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.

Vaadittava eheyden taso:

- *Vähäinen*: Tiedon häviämisestä tai muuttumisesta ei aiheudu olennaista haittaa.
- *Normaali*: Tiedon häviäminen tai muuttuminen aiheuttaa kohtuullista haittaa, mutta se voidaan havaita ja siitä voidaan toipua.
- *Tärkeä*: Tiedon häviäminen tai muuttuminen aiheuttaa merkittävää haittaa tai mainevahinkoa ja sen havaitseminen voi olla vaikeaa.
- *Kriittinen*: Tiedon häviäminen tai muuttumista ei voida hyväksyä missään tilanteessa.

Vaadittava saatavuuden taso:

- *Vähäinen*: Tiedon saatavuuden osalta pystytään hyväksymään useiden viikkojen mittaisia häiriöitä.
- *Normaali*: Tiedon saatavuuden osalta pystytään hyväksymään enintään päivien mittaisia häiriöitä.
- *Tärkeä*: Tiedon saatavuuden osalta pystytään hyväksymään enintään tuntien mittaisia häiriöitä.
- *Kriittinen*: Tiedon saatavuuden osalta pystytään hyväksymään enintään minuuttien mittaisia häiriöitä.

Henkilötiedot hankinnan kohteessa:

- *Henkilötietoja*: Hankinnan kohde sisältää henkilötietojen käsittelyä, mutta käsiteltävät henkilötiedot eivät sisällä erityisiin henkilötietoryhmiin kuuluvia henkilötietoja.
- *Erityisiin henkilötietoryhmiin kuuluvia henkilötietoja*: Hankinnan kohde sisältää tietosuoja-asetuksen 9 artiklan mukaisia erityisiin henkilötietoryhmiin kuuluvien henkilötietojen, eli ns. arkaluontoisten henkilötietojen käsittelyä.
- *Ei henkilötietoja*: Hankinnan kohde ei sisällä henkilötietojen käsittelyä.

Huom.! Henkilötiedot hankinnan kohteessa valinta vaikuttaa yhdessä turvallisuustasojen kanssa siihen, mitkä hallinnollista turvallisuutta, fyysistä turvallisuutta, teknistä turvallisuutta sekä varautumista ja jatkuvuudenhallintaa koskevat vaatimukset valikoituvat ehdotettaviin hankinnan ehtoihin.

Erilliset tietosuoja-asetuksen edellyttämät henkilötietojen käsittelyä koskevat sopimuksen tietosuojaliitteet tulevat saataville Digi- ja väestötietoviraston Digiturvajulkaisut sivustolle kohtaan Oppaat ja hyvät käytännöt, eikä niitä muodosteta hankintaehtotyökalun avulla.

Sopimukseen sisällytettävät turvallisuusliitteet

- *Kyllä*: Liite sisältyy hankintaan
- *Ei*: Liite ei sisälly hankintaan

Huom.! Kun jätät sopimusliitteen pois, hankintaehtotyökalu ehdottaa kaikille kyseisen sopimusliitteen vaatimuksille vaihtoehtoa *Ei ehdoteta hankintaan*. Myöhemmin tässä luvussa kuvataan, miten nämä sopimusliitteet poistetaan toimittajalle lähetettävästä vaatimusluettelosta.

Käyttötapaus

Valintalistalta voi valita hankinnassa hyödynnettävän käyttötapauksen. Mikäli hankinnassa ei hyödynnetä käyttötapausta, voi kentän jättää tyhjäksi. Valittavina ovat hankintaehtotyökaluun ennalta määritellyt neljä käyttötapausta sekä organisaation itsensä määrittelemät käyttötapaukset.

Tarkemmat ohjeet organisaatiokohtaisten käyttötapausten määrittelystä löytyvät luvusta Käyttötapausten määrittely.

4.3 Vaatimusten sisällyttäminen hankintaan

Hankintayksikön tulee tehdä vaatimuksen olennaisuuden sekä tapauskohtaisen harkinnan ja riskiarvion perusteella päätös kunkin kriteerin sisällyttämisestä hankintaan välilehdellä *Hankintaehtojen määrittely*.

Esiehdoissa tehtyjen valintojen perusteella hankintaehtotyökalu määrittelee kunkin vaatimuksen olennaisuuden, joka ohjaa päätöksiä seuraavasti:

- *Olennainen*: Vaatimus suositellaan sisällytettäväksi hankintaan.
- *Valinnainen*: Vaatimuksen sisällyttäminen hankintaan tulee päättää tapauskohtaisen harkinnan ja riskiarvion perusteella.
- *Ei ehdoteta hankintaan*: Vaatimusta ei suositella sisällyttämään hankintaan.

Päätökset kirjataan Päätös soveltamisesta -sarakkeessa alasvetovalikon avulla. Valikon saa näkyviin kunkin kentän oikealla puolella olevasta nuolesta, joka tulee näkyviin, kun valitset kentän. Vaihtoehtoja ovat:

- *Sisältyy*: Vaatimus sisältyy hankintaan
- *Ei sisälly*: Vaatimus ei sisälly hankintaan

Olennaisuus	Päätös soveltamisesta	Perustelut
Olennainen	Sisältyy	
Valinnainen	Sisältyy	
Valinnainen	Ei sisälly	
Olennainen	Ei sisälly	Erillisen riskiarvion #127 perusteella, vaatimus voidaan jättää soveltamatta.
Ei ehdoteta hankintaan	Ei sisälly	

Kuvio 2. Esimerkki soveltamispäätösten ja niiden perusteluiden kirjaamisesta.

Koska hankinnan turvallisuuteen voivat vaikuttaa myös monet seikat, joita hankintaehtotyökalu ei pysty ottamaan huomioon, hankintayksikkö voi perustelluista syistä tai riskiarvion perusteella poiketa työkalun antamasta ohjauksesta. Tällöin on hyvä kirjata syy Perustelut-sarakkeeseen.

Vinkki! Hankintayksikkö voi tehostaa päätösten kirjaamista suodattamalla näkyviin olennaisuuden perusteella samaan ryhmään kuuluvat vaatimukset ja käsittelemällä ne kokonaisuuksina. Suodatusvalikko avautuu sarakkeen otsikkokentässä olevasta alaspäin osoittavasta nuolesta.

Jos esimerkiksi haluaa sisällyttää kaikki olennaiset vaatimukset hankintaan, on nopeinta suodattaa näkyviin kaikki olennaiset vaatimukset, kirjata ensimmäiselle vaatimukselle soveltamispäätös *Sisältyy* ja kopioida tämä päätös kaikille muille näkyvissä oleville riveille. Vastaavalla tavalla voi kirjata *Ei sisälly* päätökset niille vaatimuksille, joita työkalu ei ehdota hankintaan. Eniten aikaa on suositeltavaa käyttää niiden vaatimusten soveltamispäätösten harkintaan, jotka hankintaehtotyökalu on määritellyt valinnaisiksi.

4.4 Vaatimusten täsmentäminen

Hankintayksikön tulee tarvittaessa täsmentää hankintaan sisältyviä vaatimuksia. Täsmennykset tehdään välilehdellä *Hankintaehtojen määrittely* sarakkeessa *Vaatimuksen täsmennys toimittajalle*. Vaatimusten täsmentäminen voi olla tarpeen esimerkiksi yleisellä tasolla olevien vaatimusten tarkentamiseksi tai toteutuksen yhteensovittamiseksi tilaajan muiden ratkaisujen kanssa.

Vaatimuksen täsmennys toimittajalle -sarakkeeseen on laadittu etukäteen täsmennyksiä, joilla alun perin julkishallinnolle tarkoitettuja arviointikriteereitä on muokattu soveltumaan paremmin hankinnan turvallisuusvaatimuksiksi. Hankintayksikön tulee käydä läpi kaikki vaatimukset ja niiden täsmennykset, sekä tehdä niihin tarvittavat muutokset. Sarakkeessa *Ohje hankintayksikölle* on vaatimuskohtaisia ohjeita, jotka tulee ottaa huomioon vaatimuksia täsmennettäessä.

Esimerkki: Hankintayksiköllä on erikseen dokumentoituja ohjeita salassa pidettävien tietojen käsittelystä. Toimittajan velvollisuus näiden erillisten ohjeiden noudattamiseen voidaan kirjata vaatimuksen täsmennykseen kohdassa HAL-12.

Alla olevassa kuviossa on näkymä vaatimusten täsmennysten kirjaamisesta. Tähän kohtaan hankintayksikkö voi esimerkiksi määritellä viittauksen noudatettaviin ohjeisiin alkuperäisen täsmennyksen tilalle.

Tunniste	Nimi	Vaatimus	Vaatimuksen täsmennys toimittajalle	Ohje hankintayksikölle
HAL-12, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto	Ohjeet	Organisaatiossa on ajantasaiset ja kattavat ohjeet tietoturvallisuuden varmistamiseksi.	Toimittajan ohjeiden tulee olla riittävät tilaajan asettamien tietoturvavaatimusten täyttämiseksi. Toimittaja on velvollinen pyydettäessä selvittämään kuinka toimittajan ohjeet täyttävät tilaajan asettamat tietoturvavaatimukset.	Hankintayksikkö voi tarvittaessa pyytää selvitystä toimittajan tietoturvaohjeista ja niiden riittävyydestä.

Kuvio 3. Vaatimusten täsmentäminen Hankintaehtojen määrittely -välilehdellä.

Toimittajalle lähetettävässä vaatimusliitteessä näytetään yhdistetty vaatimus, joka koostuu alkuperäisestä vaatimuksesta sekä siihen tehdystä täsmennyksestä. Ennen tarjouspyynnön lähettämistä tulee vielä tarkastaa toimittajalle lähetettävien vaatimusten sisällöt.

Tunniste	Nimi	Vaatimus	Kuvaus vaatimuksen täyttämisestä
HAL-12, L:Julkinen, E:Vähäinen, S:Vähäinen, TS:Henkilötieto	Ohjeet	Organisaatiossa on ajantasaiset ja kattavat ohjeet tietoturvallisuuden varmistamiseksi. Toimittajan ohjeiden tulee olla riittävät tilaajan asettamien tietoturvavaatimusten täyttämiseksi. Toimittaja on velvollinen pyydettäessä selvittämään kuinka toimittajan ohjeet täyttävät tilaajan asettamat tietoturvavaatimukset.	

Kuvio 4. Täsmennetty vaatimus toimittajalle näytettävässä muodossa.

4.5 Lisävaatimusten kirjaaminen

Jos tunnistat hankinnan yhteydessä sellaisia tietoturvallisuusvaatimuksia, jotka eivät sisälly vakiomuotoisiin tietoturvallisuusliitteisiin tai hankintaehtotyökalun ehdottamiin vaatimuksiin, voit määritellä ne hankintaehtotyökalun välilehdellä "Lisävaatimukset".

Määrittele kunkin lisävaatimuksen:

- Tunniste: Vaatimuksen yksilöivä tunniste, esim. LIS-1, LIS-2 jne.
- Nimi: Vaatimusta kuvaava lyhyt nimi.
- Vaatimus: Täsmällinen kuvaus vaatimuksesta.

4.6 Vaatimusliitteiden muodostaminen

Hankintaehtotyökalu muodostaa liitteet *Hallinnollisen turvallisuuden*, *Fyysisen turvallisuuden*, *Teknisen turvallisuuden* sekä *Varautumisen ja jatkuvuudenhallinnan* vaatimuksista käyttäjän tekemien soveltamispäätösten perusteella. Liitteisiin valikoituvat vain ne vaatimukset, jotka käyttäjä on sisällyttänyt hankintaan.

Kukin liite on eri välilehdellä. Mikäli liite ei sisälly hankintaan, eli sillä ei ole yhtään vaatimusta, voi kyseisen välilehden poistaa tarpeettomana. (osoita hiirellä poistettavan välilehden nimeä / paina hiiren oikeaa painiketta / paina "Poista" hiiren vasemmalla painikkeella)

Kunkin liitteen ensimmäisellä rivillä on liitteen nimi ja paikka liitteen numerolle. Muokkaa tarvittaessa liitteen numeroa kunkin liitteen kentässä A1.

Hankintaehtotyökalun avulla laaditut sopimusehdot voi liittää toimittajalle lähetettävään tarjouspyyntöön joko erillisinä PDF-liitteinä tai Excel-tiedostona.

PDF-liitteet muodostetaan tallentamalla kukin vaatimusliite erilliseen PDF-tiedostoon Excelin tallennustoiminnon avulla (Tiedosto/Tallenna nimellä). Sekä nimeämällä tiedosto liitteen nimen mukaisesti ja valitsemalla tallennusmuodoksi PDF (*.pdf).

Excel-liitteiden yhteydessä on suositeltavaa tehdä seuraavat toimenpiteet ennen tiedoston toimittamista tarjouspyynnön liitteenä.

- Välilehdeltä *Hankintaehtojen määrittely* sarakkeessa *Perustelut* olevat tiedot tulee poistaa, mikäli perustelut sisältävät sellaista organisaation turvallisuuteen liittyvää tietoa, jota toimittajan ei tarvitse tietää.
- Tarpeettomat hankintaehtotyökalun välilehdet on suositeltavaa piilottaa toimittajalle lähetettävästä tiedostosta. Tarpeettomia välilehtiä ovat kaikki muut välilehdet paitsi toimittajalle lähetettävät vaatimusliitteet sekä *Hankinnan perustiedot*. Piilottaminen onnistuu klikkaamalla hiiren oikealla painikkeella Excelin alareunassa olevaa välilehden nimeä ja valitsemalla *Piilota***.**
- Näin muokattu Excel-tiedosto tulee tallentaa nimellä, josta käy ilmi mitkä vaatimusliitteet tiedosto sisältää. Esimerkiksi: Tietoturvavaatimukset liitteet 3–5.

4.7 Toimittajan ohjeistaminen

Toimittajalle tulee antaa tarjouspyynnön yhteydessä riittävät ohjeet, jotta varmistetaan sekä asetettujen tietoturvallisuusvaatimusten oikeanlainen tulkinta että riittävän kattavat ja vertailukelpoiset vastaukset.

Vaaditun dokumentaation ohjeistaminen

Hankintayksikön tulee määritellä ja ohjeistaa minkälaista dokumentaatiota edellytetään tietoturvallisuusvaatimusten täyttymisen osoittamiseksi ja miten se tulee toimittaa. Hankinnan luonteesta riippuen vaaditun dokumentaation voi kuvata joko tarjouspyynnössä, yksittäisten vaatimusten yhteydessä tai molemmissa.

Vastausten perusteluiden ohjeistaminen

Toimittajan vastauksissa on *Kuvaus vaatimuksen täyttämisestä* -sarake, jossa toimittaja voi kuvata miten vaatimus on täytetty.

Vastausten perusteluiden ohjeistamisessa kannattaa kiinnittää huomiota erityisesti siihen, että saatujen vastausten perusteella on helppo varmistaa vaatimuksen täyttyminen. Esimerkiksi jos toimittaja viittaa perusteluissa laajempaan dokumentaatioon, on hyvä pyytää tarkentamaan, mikä dokumentin kohta osoittaa vaatimuksen täyttymisen.

Vaatimusten soveltamisen ohjeistaminen

Hankintaehtotyökalun ehdottamat vaatimukset on luokiteltu sen mukaan, mistä luokasta alkaen vaatimusta sovelletaan. Esimerkiksi salassa pidettäviä tietoja koskevaa vaatimusta sovelletaan kaikkiin salassa pidettäviin sekä korkeammille tasoille tasolle luokiteltuihin tietoihin (TLIV – TLI).

Hankinnan yhteydessä on mahdollista edellyttää riskilähtöisesti myös ylemmän tason vaatimusten soveltamista. Esimerkiksi salassa pidettävien tietojen käsittelyssä voidaan edellyttää TLIV tason vaatimuksen soveltamista.

Toisaalta joissakin hankinnoissa voi olla tarkoituksenmukaisinta edellyttää kaikkien vaatimusten soveltamista kaikkien tilaajan tietojen käsittelyyn.

Edellä olevasta johtuen hankintayksikön tulee täsmentää toimittajalle, miten vaatimuksia sovelletaan eri tilanteissa. Esimerkkejä vaihtoehtoisista tavoista ovat:

- Kaikkia vaatimuksia sovelletaan kaikkien tilaajan tietojen käsittelyyn. Yksinkertaisin tapa, jolloin vaatimusten luokittelulla ei ole merkitystä toimittajan kannalta.
- Pääsääntöisesti vaatimuksia sovelletaan eri tietoihin vaatimusten luokittelun mukaisesti. Lisäksi vaatimusliitteissä olevia TL IV -tason vaatimuksia sovelletaan tilaajan salassa pidettävien tietojen käsittelyyn. Hankintayksikkö on tässä tilanteessa täydentänyt riskiperusteisesti salassa pidettävien tietojen käsittelyn vaatimuksia tietyillä TL IV -tason vaatimuksilla. Tämä tulee ohjeistaa, jotta toimittaja tietää, että vaatimukset kohdistuvat myös salassa pidettävien tietojen käsittelyyn.

Hankintayksikön tulee päättää, miten eri tasoisia vaatimuksia sovelletaan sekä ohjeistaa valittu tapa selkeästi toimittajalle. Mikäli tästä soveltamistavasta poiketaan yksittäisten vaatimusten kohdalla, tulee nämä poikkeukset täsmentää vaatimuskohtaisesti.

4.8 Käyttötapausten määrittely

Hankintaehtotyökalussa käyttötapausten määrittely tapahtuu yhdenmukaisesti Julkri-suosituksen sisältyvän Julkri-työkalun käyttötapausten määrittelyn kanssa. Seuraavassa on lyhyt ohje käyttötapausten määrittelystä hankintaehtotyökalussa. Kattavampi kuvaus käyttötapauksista sekä niiden vaikutuksesta vaatimusten/kriteerien olennaisuuteen löytyy Julkri-suosituksen liitteestä 3.

Käyttötapauksen nimi sekä lyhyt yleiskuvaus käyttötapauksen sisällöstä kirjataan välilehdelle *Käyttötapauskuvaukset*. Käyttötapauksen yleiskuvauksessa kuvataan, millaisiin hankintoihin käyttötapaus soveltuu. Koska käyttötapauksen soveltamiseen liittyy useita eri näkökohtia, on suositeltavaa laatia käyttötapauksesta myös erillinen yksityiskohtaisempi kuvaus.

Käyttötapauksessa sovellettavat vaatimukset määritellään välilehdellä *Käyttötapauskriteerit*. Välilehden ylimmälle riville on linkitetty Käyttötapauskuvaukset välilehdellä määriteltyjen käyttötapausten nimet. Kukin vaatimus määritellään käyttötapauksen kohdalla olevaan sarakkeeseen seuraavasti:

- Olennainen vaatimus: 1
- Valinnainen vaatimus: 2
- Vaatimusta ei ehdoteta hankintaan: 0

Sanasto

Termi	Määritelmä	Lähde
arkkitehtuuri	yleistermi kuvauksesta, joka sisältää järjestelmän tai muun kuvattavan kohteen osat, osien keskinäiset suhteet, osien suhteet ympäristöön sekä periaatteet, jotka ohjaavat järjestelmän suunnittelua ja evoluutiota	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
auditointi	järjestelmällinen, riippumaton dokumentoitu prosessi sen määrittämiseksi, onko toiminta ja siihen liittyvät tulokset suunniteltujen järjestelyiden mukaiset, onko nämä järjestelyt toteutettu tehokkaasti ja ovatko ne sopivia tavoitteiden saavuttamisen kannalta	Tieteen termipankki (2022)
arviointi	tarkastelun kohdetta koskevan tiedon analysointi ja tulkitseminen ja niiden pohjalta tehtävä kohteen arvottaminen	Suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (VM 2022:43). Opetus- ja koulutussanasto (OKM 2021:10).
eheys	tiedon ominaisuus, joka ilmentää sitä, että tietoa ei ole muutettu luvatta, ettei se ole tahattomasti muuttunut ja että mahdolliset muutokset voidaan todentaa ja jäljittää	Tietotermit (2018)
erityisiin henkilötietoryhmiin kuuluva henkilötieto	sellainen henkilötieto, josta ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettinen tai biometrinen tieto, terveyttä koskeva tieto tai luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskeva tieto	Tietosuoja-asetus 9 art.
haavoittuvuus	puute, vika tai toimintatapa, joka altistaa turvallisuuteen kohdistuville uhkille	VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään; 9.6.2022 (Digi- ja väestötietovirasto)
hallinnollinen alue	viranomaisen normaaliin työskentelyyn tarkoitettu alue tai tila, jonka osalta aluetta tai tilaa	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)

	hallitseva toimija varmistaa, että siihen on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamilla henkilöillä Hallinnollinen alue tai tila voi olla esimerkiksi toimistotila, useista eri toimistotiloista muodostuva kokonaisuus, palvelintila, konesali tai jonkin yrityksen tai muun yhteisön tila. Turvallisuusluokitusasetuksessa hallinnollinen alue on turvallisuusluokiteltujen asiakirjojen suojaamiseksi määritelty alue, jolla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa.	Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4) TLA 9 § 1 kohta
hankintaehtotyökalu	julkisen hallinnon tietoturvallisuuden arviointikriteeristöön (Julkri) perustuva työkalu, joka tukee tietoturvavaatimusten valintaa ja muokkaamista	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
hankintayksikkö	julkishallinnon yksikkö, joka suorittaa hankintaa Hankintayksiköitä ovat: 1) valtion, kuntien ja kuntayhtymien viranomaiset; 2) evankelisluterilainen kirkko ja ortodoksinen kirkko sekä niiden seurakunnat ja muut viranomaiset; 3) valtion liikelaitokset; 4) julkisoikeudelliset laitokset; 5) mikä tahansa hankinnan tekijä silloin, kun se on saanut hankinnan tekemistä varten tukea yli puolet hankinnan arvosta 1—4 kohdassa tarkoitetulta hankintayksiköltä.	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX) Hankintalaki 5 §
henkilötieto	tieto, jonka perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.	Tietosuoja-asetus 4 art. 1 kohta Rikosasioiden tietosuojalaki 3 § 1 mom 1 kohta
henkilötietojen käsittelijä	luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muuta elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun	Tietosuoja-asetus 4 art. 8 kohta

jatkuvuudenhallinta	organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa	Kyberturvallisuuden sanasto (TSK 52, 2018)
jäännösriski	riskin käsittelyn jälkeen jäljellä oleva riski	VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään; 9.6.2022 (Digi- ja väestötietovirasto)
kriittisyys	välttämättömyys tavoitteiden saavuttamiseksi tai erityisen haitallisten seurausten välttämiseksi Kriittisyys liittyy kolmeen eri asiaan: 1. korkein saatavuuden vaatimustaso 2. korkein eheyden vaatimustaso 3. yleistermi, jolla viitataan hankinnan kohteen kaikkien turvallisuusvaatimusten tasoon	VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään; 9.6.2022 (Digi- ja väestötietovirasto) Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
käyttötapaus	etukäteen valikoitua vaatimusten joukkoa, joka soveltuu tietyn tyyppisiin hankintoihin	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
luottamuksellisuus	tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu muille	Tietotermit (2018)
olennaisuus	hankintaehtotyökalun tekemää ehdotusta vaatimuksen soveltuvuudesta hankinnan kohteeseen hankintayksikön antamien esiehtojen perusteella Jos vaatimus on olennainen, se on lähtö-kohtaisesti tarkoitettu sisällytettäväksi hankinnan vaatimuksiin.	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
rekisterinpitäjä	luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muuta elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot	Tietosuoja-asetus 4 art. 7 kohta

riskiperusteisuus	riskien suuruuden ja niiden hyväksyttävyyden arviointia sekä riskien suuruuden suhteuttamista riskien pienentämisen kustannusiin osana tietoturvallisuuteen liittyvää päätöksentekoa	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
saatavuus	tiedon ominaisuus, joka ilmentää sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla	Tietotermit (2018)
saavutettavuus	periaatteet ja tekniikat, joita on noudatettava digitaalisten palvelujen suunnittelussa, kehittämisessä, ylläpidossa ja päivittämisessä, jotta ne olisivat paremmin käyttäjien, erityisesti vammaisten henkilöiden, saavutettavissa	Laki digitaalisten palvelujen tarjoamisesta 2 §
sertifikaatti	vaatimusten täyttymistä osoittava todistus	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX
tietoaineisto	asiakirjoista ja muista vastaavista tiedoista muodostuva, tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus	TihL 2 §
tietojärjestelmä	tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuva kokonaisjärjestely Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja ohjelmistojen käsittelyyn käytettävät päätelaitteet.	TihL 2 §
tietosuoja	järjestelyt, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen	Kyberturvallisuuden sanasto (TSK 52, 2018)
tietoturva; tietoturvallisuus	järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus	Kyberturvallisuuden sanasto (TSK 52, 2018)
tilaaja	osapuoli, joka asettaa hankinnan vaatimukset ja hyväksyy niiden täyttymisen Tilaaja -termiä on käytetty hankintayksikön sijasta toimittajalle lähetettävissä vaatimusliitteissä.	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:XX)
toimittaja	luonnollinen henkilö, oikeushenkilö tai julkinen taho taikka edellä tarkoitettujen tahojen ryhmit-	Hankintalaki 4 §

	tymä, joka tarjoaa markkinoilla tavaroita tai palveluja taikka rakennustyötä tai rakennusurakoita	
turva-alue	alue, joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle	TLA 9 § 2 kohta
turvallisuusalue	käsite, joka sisältää hallinnolliset alueet ja turva-alueet	TLA 9 §
turvallisuusluokiteltu asiakirja	asiakirja, johon valtion viranomaisen toimesta on tehty turvallisuusluokkaa koskeva merkintä Asiakirja on turvallisuusluokiteltava, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.	TihL 18 § JulkL 24 §
varautuminen	toiminta, jolla varmistetaan tehtävien mahdollisimman an häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa	Kokonaisturvallisuuden sanasto (TSK 50, 2017)

Liitteet

Liite 1 a Tietoturvallisuuden vähimmäisvaatimukset
Liite 1 b Tietoturvallisuusvaatimukset
Liite 2 Hankintaehtotyökalu (Excel)

Lähteet

Säädökset

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI.

Hallintolaki (434/2003). Hallintolaki 434/2003 - Ajantasainen lainsäädäntö - FINLEX ®.

Laki digitaalisten palvelujen tarjoamisesta (306/2019). Laki digitaalisten palvelujen tarjoamisesta 306/2019 - Ajantasainen lainsäädäntö - FINLEX ®

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181054.

Laki julkisen hallinnon tiedonhallinnasta (906/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190906.

Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016). Laki julkisista hankinnoista ja… 1397/2016 - Ajantasainen lainsäädäntö - FINLEX ®

Laki julkisista puolustus- ja turvallisuushankinnoista (1531/2011). Laki julkisista puolustus- ja… 1531/2011 - Ajantasainen lainsäädäntö - FINLEX ®

Laki ulkomaalaisten yritysostojen seurannasta (172/2012). Laki ulkomaalaisten yritysostojen seurannasta 172/2012 - Ajantasainen lainsäädäntö - FINLEX ®

Laki vesi- ja energiahuollon, liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista ja käyttöoikeussopimuksista (1398/2016). Laki vesi- ja energiahuollon, liikenteen ja… 1398/2016 - Ajantasainen lainsäädäntö - FINLEX ®

Laki viranomaisten toiminnan julkisuudesta (621/1999). https://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

Tietosuojalaki (1050/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=tietosuojalaki.

Rikoslaki (1889/39). Rikoslaki 39/1889 - Ajantasainen lainsäädäntö - FINLEX ®.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Valtioneuvoston asetus asiakirjojen… 1101/2019 - Ajantasainen lainsäädäntö - FINLEX ®

Tiedonhallintalautakunnan suositukset

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2022:43). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö. http://urn.fi/URN:ISBN:978-952-367-275-8

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2023:4). Suositus salassa pidettävien asiakirjojen käsittelystä. http://urn.fi/URN:ISBN:978-952-367-241-3

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2021:65). Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. http://urn.fi/URN:ISBN:978-952-367-897-2

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2021:21). Suositus teknisistä rajapinnoista ja katseluyhteyksistä. http://urn.fi/URN:ISBN:978-952-367-489-9

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2020:53). Suositus tiedonhallinnan muutosvaikutusten arvioinnista. http://urn.fi/URN:ISBN:978-952-367-318-2

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2021:5). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. http://urn.fi/URN:ISBN:978-952-367-500-1

Tiedonhallintalautakunnan suositus – Valtiovarainministeriö (2022:4). Suositus turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. http://urn.fi/URN:ISBN:978-952-367-906-1

Ohjeet ja muut materiaalit

Digi- ja väestötietovirasto (2020). Turvallisen sovelluskehityksen käsikirja. Turvallisen sovelluskehityksen käsikirja | Suomidigi

Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille