



VALTIOVARAINMINISTERIÖ

# Ajankohtaista tiedonhallintalain toimeenpanossa - tietoturvallisuus

26.8.2019

Tuija Kuusisto

JulkICT



# Sisältö

- Mikä muuttuu?
- Mikä on tiedonhallintalain täytäntöönpanon tilanne?
- Miten tietoturvallisuus näkyy osana lausuntomenettelyä?
- Mitä tietoturvallisuudesta suunnitellaan kirjattavaksi tiedonhallintamallisuosituksissa?
- Mitä tiedonhallintalautakuntaa valmisteleva tietoturvallisuus-alatyöryhmä tuottaa?



# Mikä muuttuu?



## Turvallisuusluokittelu on tehtävä

”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”

## Suojaustasoista luovutaan

## Lokitiedot kerätään

Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

## Olellaiset riskit on selvitettävä

Tietoturvallisuustoimenpiteet on mitoitettava riskiarvioinnin mukaisesti

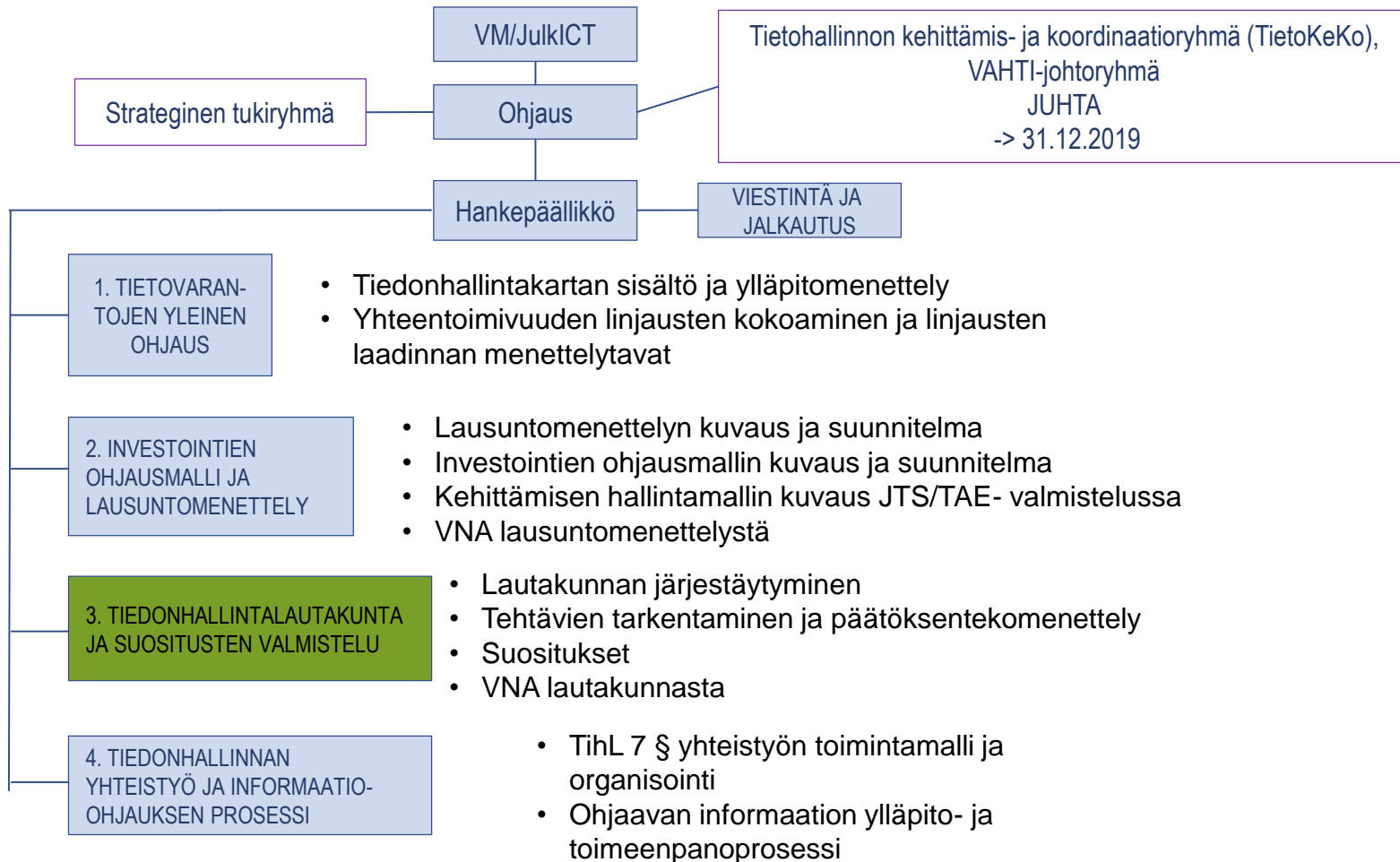
## Soveltamisala laajenee

Tätä lakia sovelletaan, kun viranomaiset käsittelevät tietoaineistoja  
Tämän lain 4 lukua ja 22–27 §:ää sovelletaan yksityisiin henkilöihin tai yhteisöihin taikka muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin siltä osin kuin ne hoitavat julkista hallintotehtävää

Laki julkisen hallinnon tiedonhallinnasta (906/2019)

<https://www.finlex.fi/fi/laki/alkup/2019/20190906>

# TihL täytäntöönpanon organisointi



# Tiedonhallintalautakunnan tehtävät

- Arvioida valtion virastojen ja laitosten sekä kuntien ja kuntayhtymien TihL säännösten toteuttamista ja noudattamista:
  - Tiedonhallinnan järjestäminen (4.2 §)
  - Tiedonhallintamalli (5 §)
  - Muutosvaikutusten arviointi (5 §)
  - Sähköiseen muotoon muuttaminen (19 §)
  - Tietojen saatavuus koneluettavassa muodossa (19 §)
  - Rajapinnat ja luovutukset (22, 24 §)
  - Katseluyhteydet (23 §)
  - Asiakirjajulkisuuskuvaus 28 §
  - Asianhallinta ja palvelujen hallinta (6 luku)
- Edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapoja ja tiedonhallintalain vaatimusten toteuttamista



# Tiedonhallintalautakunnan sihteeristö ja jaostot

- Sihteeristö
  - Pääsihteeri
  - Arviointisihteeri
  - Tietoturvallisuusasioiden sihteeri
  - Tiedonhallinnan suunnittelun ja kuvausten sihteeri
  - Yhteentoimivuusasioiden sihteeri
  - Tietoaineistojen hallinnan sihteeri
- Tiedonhallintalautakunta voi asettaa väliaikaisia jaostoja
  - Jaostoihin voi kuulua tiedonhallintayksikköjen asiantuntijoita
  - Lautakunnan sihteerit toimivat jaostojen puheenjohtajina.
- VRK tuottaa tiedonhallintalautakunnalle asiantuntijapalveluja tiedonhallinnan ja tietoturvallisuuden menettelyjen kehittämiseksi



# Tiedonhallintalautakuntaa valmisteleva työryhmä, asetettu 10.6.2019

- neuvotteleva virkamies Tomi Voutilainen, valtiovarainministeriö, puheenjohtaja
- tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö, varapuheenjohtaja
- tietohallintoneuvos Timo Saastamoinen, valtiovarainministeriö
- neuvotteleva virkamies Suvi Remes, valtiovarainministeriö
- suunnittelija Lotta Sjöblom, valtiovarainministeriö
- tietovirta-asiantuntija Suvi Metsärinta-Lehmusvaara, valtiovarainministeriö
- neuvotteleva virkamies Päivi Tommila, työ- ja elinkeinoministeriö
- asianhallintajohtaja Janne Mykrä, Pääesikunta
- johtava asiantuntija Minna Romppanen, Maanmittauslaitos
- ICT-arkkitehti Markus Virolainen, Verohallinto
- kehityspäällikkö Anu Ylä-Pietilä, Liikenne- ja viestintävirasto
- asianhallintapäällikkö Sanna-Leena Eskola, Oulun kaupunki
- hallinnon erityisasiantuntija Jaana Immonen, Järvenpään kaupunki
- tietoturvapäällikkö Matti Parviainen, Espoon kaupunki
- projektipäällikkö Birgit Paajanen, Helsingin ja Uudenmaan sairaanhoitopiiri



# Työryhmän tehtävät

- Koordinoida suositusten sisältöjä valmistelevien alatyöryhmien toimintaa
- Suunnitella tiedonhallintalautakunnan toimintamalli
- Osallistua tiedonhallintalautakunnan toimintaa koskevan asetuksen valmisteluun





# Tietoturvallisuus -alatyöryhmä



Nimi	Organisaatio	Rooli
<b>Tuija Kuusisto</b>	valtiovarainministeriö	vastuuhenkilö
<b>Eeva Lantto</b>	valtiovarainministeriö	jäsen
<b>Petri Puhakainen</b>	valtioneuvoston kanslia	jäsen
<b>Minna Romppanen</b>	Maanmittauslaitos	jäsen
<b>Sonja Marjamäki, Mika Raappana</b>	Valtori	jäsen varajäsen
<b>Matti Parviainen</b>	Espoon kaupunki	jäsen
<b>Tomi Kelo</b>	Traficom	jäsen
<b>Kirsi Janhunen Erja Kinnunen</b>	Väestörekisterikeskus	asiantuntija asiantuntija

Tiedonhallintalautakunnan perustamista valmistelevan työryhmän puheenjohtaja Tomi Voutilainen osallistuu työryhmän kokouksiin tilanteen mukaan.

# Tietoturvallisuus –alatyöryhmän tavoite

Valmistella suositusluonnokset keskeisten tietoturvallisuustoimenpiteiden toteuttamisesta tiedonhallintalautakunnan käsiteltäväksi vuoden 2020 alussa

Tiedonhallintalautakunnan perustamista valmistelevan työryhmän asettamispäätöksestä,  
10.6.2019



## LÄHTÖKOHTA TIETOTURVALLISUUSSUOSITUKSILLE

# Digipalveluissa huomioitavat tietoturvallisuusvaatimukset

Toimintaympäristön tietoturvallisuustilan seuranta

Tietoturvallisuuden varmistaminen tiedon elinkaaren ajan

Tietoriskien hallinnan järjestäminen ja siihen perustuvat tietoturvatoimet

Vikasietoisuuden ja toiminnallisen käytettävyyden varmistaminen

Hyvän julkisuus ja salassapitorakenteen huomioiminen tietovarantojen tietorakenteissa

Salassa pidettävien tietojen suojaaminen yleisessä tietoverkossa tietoja siirrettäessä

Tietoaineistojen turvallisuuden varmistaminen

Käyttöoikeuksien määrittely ja hallinta tietojärjestelmiin

Tarpeellisten lokitietojen kerääminen

Turvallisuusluokiteltavat asiakirjat + niiden käsittely (asetus)

# Tietoturvallisuus-alatyöryhmän tehtävät ja aikataulu

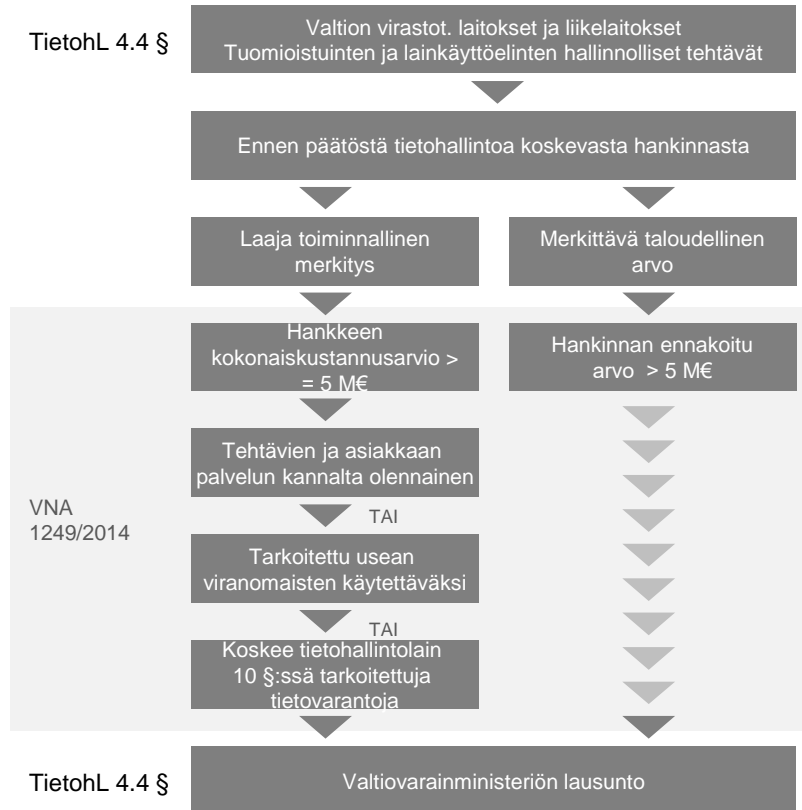


- Valmistella keskeisten tietoturvaluustoimenpiteiden suositukset
  - TiIL luku 4, VRK/JUDO-hanke Vahti-korttiluonnosten pohjalta
  - TihL Sähköinen tiedonantotapa (§22-23)
  - Turvallisuusluokitteluasetus, VRK/JUDO-hanke
- Valmistella tietoturvaluustoimenpiteiden suositusten liitokset/käyttäminen
  - TihL-mukaista lausuntomenettelyä varten tietoturvaluusta koskevassa arviointikriteeristössä
  - Tiedonhallintamallisuositukseen sisältyvissä tietoturvaluusjärjestelyjä koskevissa osioissa
- Valmisteluasiakirjojen lausuntomenettelyn aikataulu
  - Suositus- ja ohjeluonnokset lausuntoversioina 21.10 mennessä, ja lausuntokierrokset päättyvät viimeistään 11.11.
  - Suositukset ja ohjeet valmiit 23.12. mennessä

# Lausuntomenettely

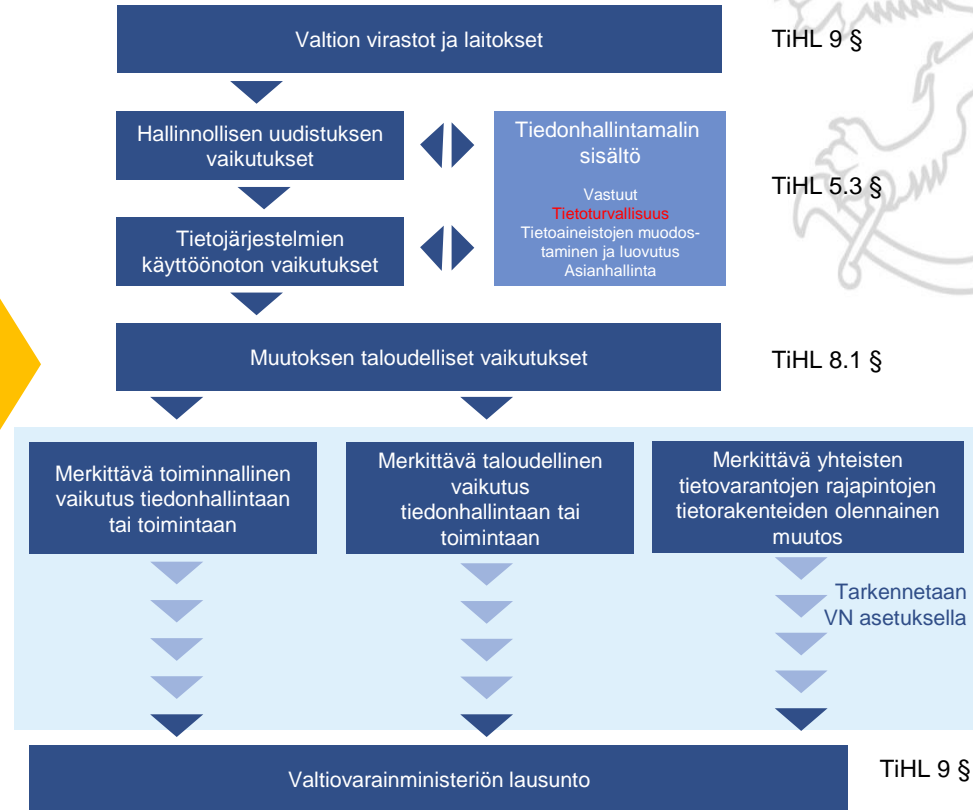
**- 31.12.2019**

## Tietohallintolaki (634/2011)



**1.1.2020 -**

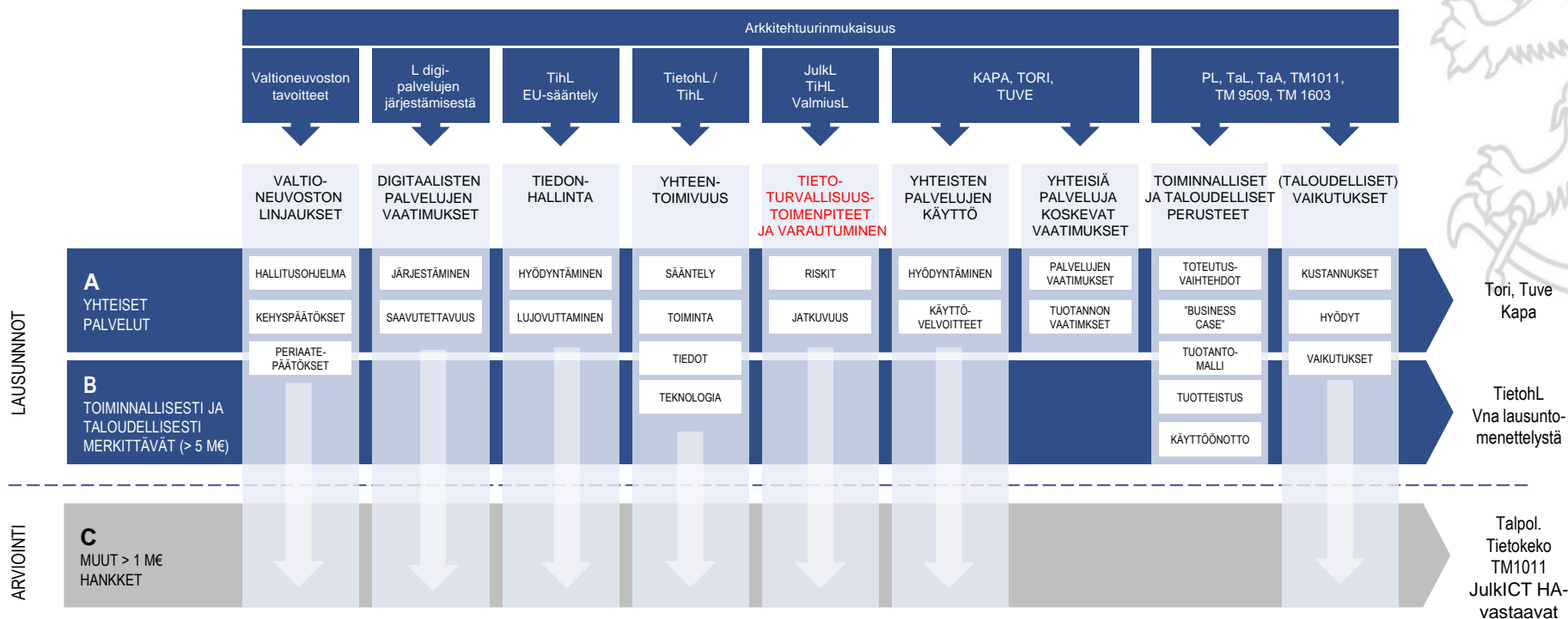
## Tiedonhallintalaki (HE 284/2018 vp, HaVM 38/2018 vp)



# Lausuntopyynnön tietosisältö – laaja näkökulma

Keskitytään TihL sisältöön

LUONNOS



- Yhteiset palvelut: arviointi tulosohjaukseen linkittyvänä lausuntomenettelynä (?)
- Toiminnallisesti ja taloudellisesti merkittävät: arviointi lausuntomenettelynä
- Muut < 1 M€ hankkeet: näkökulmien ja kriteerien arviointi tehdään hankesalkun analysoinnin kautta

# Tiedonhallintamallia koskevat suositukset – tietoturvallisuusjärjestelyt 1/3

- Tiedonhallintamallissa kuvataan tiedonhallintaan liittyvät tietoturvamennettelyt ja –toimenpiteet.
  - Kuvauksen tavoitteena on, että viranomaiset suunnittelevat ennakkoon, millä tavoin tietoturvallisuus toteutetaan ja
  - mitä menettelyitä tietojenkäsittelyn, tietojärjestelmien ja tietoaaineistojen turvaamiseksi on toteutettu tai aiotaan toteuttaa.
- Tiedonhallinnassa tulee noudattaa tiedonhallintalain 4 luvussa määriteltyjä tietoturvallisuuden perustason vaatimuksia.
- Henkilötietojen käsittelyn osalta tulee lisäksi noudattaa yleisen tietosuoja-asetuksen (GDPR) vaatimuksia.
- Tiedonhallintamallin kuvaukseen tietoturvajärjestelyistä yhdistetään arvio siitä, miltä osin tietoturvallisuusvaatimukset toteutuvat eri kokonaisuuksien osalta. *Miten?*



# Tiedonhallintamalli koskevat suositukset – tietoturvallisuusjärjestelyt 2/3



- Tietovarannoista, joihin kohdistuu henkilötietojen käsittelytoimia tai ne sisältävät henkilötietoja, ei tarvitse laatia erillistä kuvausta
  - Yleisen tietosuoja-asetuksen (GDPR) 30 artiklan 1 mukaan laadittu seloste käsittelytoimista voidaan sisällyttää tiedonhallintamalliin.
    - Yleisen tietosuoja-asetuksen (GDPR) 30 artiklan mukaan käsittelytoimia koskevassa selosteessa on mahdollisuuksien mukaan kuvattava tekniset ja organisatoriset turvatoimet
- Tietovarantojen, joihin ei kohdistu henkilötietojen käsittelytoimia eikä henkilötietoja, kuvauksiin tulee sisältyä
  - Tietoaineistoryhmien käsittelyn tietoturvavaatimukset
    - Sisältääkö tietoaineisto: salassa pidettäviä tietoja/ turvaluokiteltavia tietoja?
  - Tiedonsaannin oikeudet ja rajoitukset
    - Kenelle ja millä perusteella tietoa saadaan luovuttaa?
- Tietojärjestelmien kuvauksen tavoitteisiin sisältyy tietoturvallisuuteen liittyvien velvoitteiden sekä julkisuusperiaatteen toteuttamisen edistäminen.



# Tiedonhallintamalli koskevat suositukset – tietoturvallisuusjärjestelyt 3/3

- Muutosvaikutusten arvioinnilla suhteessa muualla tiedonhallintalaissa säädettyihin asiakirjojen julkisuuteen, salassapitoon, suojaan ja tiedonsaantioikeuksiin tarkoitetaan, että tietojen julkisuus ja salassapito toteutuvat muutostenkin jälkeen lainsäädännössä edellytetyllä tavalla.
  - Niin ikään arvioinnissa tulee ottaa huomioon muualla lainsäädännössä asetetut vaatimukset tietojen suojaamiseksi.
- Tiedonhallinnan muutosten arvioinnin yhteydessä on arvioitava vaikutukset suhteessa TihL:n 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja –toimenpiteisiin
  - Tällä tarkoitetaan riskiarviota: minkälaisia riskejä muutos voi aiheuttaa tiedonhallinnalle, tietojenkäsittelylle, tietojärjestelmille ja tietoaineistoille
  - Riskikartoituksen perusteella tiedonhallintamalliin suunniteltaisiin toimenpiteet, joilla riskit voidaan minimoida
  - Ennakollisen suunnittelun tarkoituksena on varmistaa tietojen saanti ja viranomaisen toiminta lakisääteisten tehtävien hoitamiseksi ja palvelujen tuottamiseksi



# Tietoturvallisuustoimenpiteitä koskevat keskeisiksi priorisoidut suositukset



- 13.2§ riskienhallinta
- 17 § lokitietojen kerääminen,
- 15.1 §, 2 kohta: Vahingoilta suojaaminen
- 13.1 § elinkaaren huomioiminen tietojärjestelmissä, tietojenkäsittelyssä
- 13.4 § tietoturvallisuus hankinnoissa
- Turvallisuusluokitteluasetus
  - Tarkentuu kun lausunto-aika päättyy 30.8.2019

# Suosituksen sisältö

Mitä tiedonhallintayksikön on vähintään tehtävä, jotta lain vaatimus täyttyy?

Mitkä ovat hyvät käytänteet tehtävän toteuttamiseksi?

Liiteaineisto

Vahti-jaostojen  
tukea tarvitaan



# Esimerkki - riskienhallinta

13§ Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti.

Tiedonhallintayksikön on seurattava toimintaympäristönsä turvallisuustilannetta ja hallittava tietoaineistoihin ja tietojärjestelmiin liittyviä riskejä.

Riskienhallinnan tehtävät ovat riskien arviointi, tietoturvaluustoimenpiteiden suunnittelu tunnistettujen riskien perusteella, tietoturvaluustoimenpiteiden toteuttaminen sekä suunnitelmien toteutumisen ja toteutettujen tietoturvaluustoimenpiteiden vaikuttavuuden arviointi.

Riskiarvioinnissa on tunnistettava olennaiset riskit, jotka voisivat vaikuttaa tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden vaarantumiseen taikka tietojärjestelmien käyttöön ja vikasietoisuuteen.

Olennaisilla riskeillä tarkoitetaan riskejä, joita voivat vaikuttaa viranomaisen toimintaan tai hallinnon asiakkaan toimintaan haittaavalla tai vahingoittavalla tavalla.

Riskienhallinta on jatkuvaa toimintaa, johon liittyvät tavoitteet, periaatteet, vastuut ja keskeiset menettelyt tiedonhallintayksikön tulee kuvata.

Riskien arvioinnin tulee vaikuttaa organisaation toiminnan ja tavoitteiden arviointiin ja suunnitteluun.





VALTIOVARAINMINISTERIÖ

Tuija Kuusisto  
Tietohallintoneuvos

