



VALTIOVARAINMINISTERIÖ  
FINANSMINISTERIET



Tiedonhallintalautakunta  
Informationshanteringsnämnden

# Suosituskoelma tiettyjen tietoturvaluussäännösten soveltamisesta

Lautakunnat

Valtiovarainministeriön julkaisu – 2020:61

VANHENTUNUT

Valtiovarainministeriön julkaisuja 2020:61

Suosituskokoelma tiettyjen  
tietoturvallisuussäännösten soveltamisesta

# VANHTENTUNNUT

Valtiovarainministeriö

ISBN PDF: 978-952-367-295-6

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2020

## Kuvailulehti

<b>Julkaisija</b>	Valtiovarainministeriö	21.9.2020
<b>Tekijät</b>	Tiedonhallintalautakunta	
<b>Julkaisun nimi</b>	Suosituskokoelma tiettyjen tietoturvaluussäännösten soveltamisesta	
<b>Julkaisusarjan nimi ja numero</b>	Valtiovarainministeriön julkaisuja 2020:61	
<b>Diaari/hankenumero</b>	-	<b>Teema</b> Lautakunnat
<b>ISBN PDF</b>	978-952-367-295-6	<b>ISSN PDF</b> 1797-9714
<b>URN-osoite</b>	<a href="http://urn.fi/URN:ISBN:978-952-367-295-6">http://urn.fi/URN:ISBN:978-952-367-295-6</a>	
<b>Sivumäärä</b>	66	<b>Kieli</b> suomi
<b>Asiasanat</b>	lautakunnat, tietoturva, julkinen hallinto, riskienhallinta, elinkaari, lokitiedostot, tiedonhallintalautakunta, tiedonhallintalaki	
<b>Tiivistelmä</b>	<p>Tämä tiedonhallintalautakunnan antama suosituskokoelma opastaa tiedonhallintalain asettamien erinäisten vaatimusten täyttämässä.</p> <p>Tiedonhallintalain luku 4 sisältää tietoturvaluutta koskevat vaatimukset, jotka kaikkien tiedonhallintalain soveltamisalaan kuuluvien viranomaisten tulee täyttää. Tietoturvaluusvaatimusten toteuttamiseksi tiedonhallintalautakunta on antanut tietoturvaluutta koskevia suosituksia.</p> <p>Tiedonhallintalautakunta hyväksyi suosituskokoelman 26.3.2020 ja täydennyksen 23.6.2020.</p> <p>Korvaa 1.4.2020 julkaistun version (<a href="#">Valtiovarainministeriön julkaisuja 2020:21</a>).</p>	
<b>Kustantaja</b>	Valtiovarainministeriö	
<b>Julkaisun jakaja/myynti</b>	Sähköinen versio: <a href="http://julkaisut.valtioneuvosto.fi">julkaisut.valtioneuvosto.fi</a> Julkaisumyynti: <a href="http://vnjulkaisumyynti.fi">vnjulkaisumyynti.fi</a>	

## Presentationsblad

<b>Utgivare</b>	Finansministeriet	21.9.2020
<b>Författare</b>	Informationshanteringsnämnden	
<b>Publikationens titel</b>	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet	
<b>Publikationsseriens namn och nummer</b>	Finansministeriets publikationer 2020:61	
<b>Diarie-/ projektnummer</b>	-	<b>Tema</b> Nämnder
<b>ISBN PDF</b>	978-952-367-295-6	<b>ISSN PDF</b> 1797-9714
<b>URN-adress</b>	<a href="http://urn.fi/URN:ISBN:978-952-367-295-6">http://urn.fi/URN:ISBN:978-952-367-295-6</a>	
<b>Sidantal</b>	66	<b>Språk</b> finska
<b>Nyckelord</b>	nämnder, informationshanteringsnämnden, lagen om informationshantering inom den offentliga förvaltningen, informationssäkerhet, den offentliga förvaltningen, riskhantering, livscykel, loggfiler	
<b>Referat</b>	<p>Denna rekommendationssamling som utfärdats av informationsförvaltningsnämnden ger vägledning när det gäller att uppfylla de krav som ställs i lagen om informationshantering inom den offentliga förvaltningen.</p> <p>Kapitel 4 i informationshanteringslagen innehåller de krav på informationssäkerhet som alla myndigheter som hör till tillämpningsområdet för lagen om informationshantering inom den offentliga förvaltningen ska uppfylla. För att se till att informationssäkerhetskraven uppfylls har informationshanteringsnämnden gett rekommendationer som gäller informationssäkerhet.</p> <p>Informationshanteringsnämnden godkände rekommendationssamlingen den 26 mars 2020 och kompletteringen den 23 juni 2020.</p> <p>Erstatter versionen som publicerades den 1 april 2020 (<a href="#">Finansministeriets publikationer 2020:21</a>).</p>	
<b>Förläggare</b>	Finansministeriet	
<b>Distribution/ beställningar</b>	Elektronisk version: <a href="http://julkaisut.valtioneuvosto.fi">julkaisut.valtioneuvosto.fi</a> Beställningar: <a href="http://vnjulkaisumyynti.fi">vnjulkaisumyynti.fi</a>	

## Description sheet

<b>Published by</b>	Ministry of Finance	21 September 2020
<b>Authors</b>	Information Management Board	
<b>Title of publication</b>	Collection of recommendations on the application of certain information security provisions	
<b>Series and publication number</b>	Publications of the Ministry of Finance 2020:61	
<b>Register number</b>	-	<b>Subject</b> Board
<b>ISBN PDF</b>	978-952-367-295-6	<b>ISSN (PDF)</b> 1797-9714
<b>Website address (URN)</b>	<a href="http://urn.fi/URN:ISBN:978-952-367-295-6">http://urn.fi/URN:ISBN:978-952-367-295-6</a>	
<b>Pages</b>	66	<b>Language</b> Finnish
<b>Keywords</b>	board, Information Management Board, Information Management Act, Boards, information security, public administration, risk management, lifecycle, log files	
<b>Abstract</b>	<p>This collection of recommendations issued by the Information Management Board provides guidance on the fulfilment of a number of requirements set out in the Information Management Act.</p> <p>Chapter 4 of the Information Management Act lists the information security requirements that must be met by all authorities covered by the Information Management Act. To ensure that the information security requirements are fulfilled, the Information Management Board has issued various recommendations on information security.</p> <p>The Information Management Board approved the collection of recommendations on 26 March 2020 and the supplement on 23 June 2020.</p> <p>Replaces the version published on 1 April 2020 (<a href="#">Publications of the Ministry of Finance 2020:21</a>).</p>	
<b>Publisher</b>	Ministry of Finance	
<b>Distributed by/ Publication sales</b>	Online version: <a href="http://julkaisut.valtioneuvosto.fi">julkaisut.valtioneuvosto.fi</a> Publication sales: <a href="http://vnjulkaisumyynti.fi">vnjulkaisumyynti.fi</a>	

VANHENTUNUT



# Sisältö

<b>1</b>	<b>Johdanto</b>	9
<b>2</b>	<b>Tietoturvallisuuden vähimmäisvaatimukset</b>	10
<b>3</b>	<b>Riskienhallinta (TiHL 13.1§)</b>	12
3.1	Tietoriskien analyysi ja hallinta	12
3.2	Jäännösriskien hallinta	14
3.3	Tietoriskien hallinnassa tarvittavat tietoaineistot	14
3.4	Yleisiä vaatimuksia	15
3.5	Säädökset ja lisätiedot	16
<b>4</b>	<b>Elinkaaren huomioiminen tietojen käsittelyssä (TiHL 13.1§)</b>	17
4.1	Tietoturvallisuus läpi tiedon elinkaaren	17
4.2	Tiedon tuottaminen ja vastaanotto	19
4.3	Tiedon säilytys	20
4.4	Tiedon käyttö	20
4.5	Tiedon jakaminen, siirtäminen ja luovuttaminen	21
4.6	Tiedon arkistointi	22
4.7	Tiedon tuhoaminen	23
4.8	Säädökset ja lisätiedot	24
4.9	Yhteenveto suosituksesta	25
<b>5</b>	<b>Elinkaaren huomioiminen tietojärjestelmissä (TiHL 13.1§)</b>	26
5.1	Tietojärjestelmä	26
5.2	Määrittely- ja suunnitteluvaihe	27
5.3	Kilpailutus- ja hankintavaihe	28
5.4	Toteutusvaihe	28
5.5	Käyttööntottovaihe	29
5.6	Ylläpitovaihe	30
5.7	Käytöstä poisto	31
5.8	Säädökset ja lisätiedot	32
5.9	Suosituksen yhteenveto	32
<b>6</b>	<b>Vahingoilta suojaaminen (TiHL 15.1§)</b>	34
6.1	Yleisiä vaatimuksia	36
6.2	Säädökset ja lisätiedot	36

<b>7</b>	<b>Lokitietojen kerääminen (TiHL 17S)</b>	37
7.1	Lähtökohdat	37
7.2	Lokitiedot	38
7.3	Lokienhallinnan suunnittelu ja ohjaus	38
7.4	Lokitietojen kerääminen	40
7.5	Lokitietojen säilyttäminen	43
7.6	Lokitietojen seuranta ja analysointi	45
7.7	Lokitietojen luovuttaminen	46
7.8	Lokitietojen suojaaminen	47
7.9	Säädökset ja lisätiedot	48
<b>8</b>	<b>Tietoturvallisuus tietojärjestelmähankinnoissa (TiHL 13 §)</b>	49
8.1	Tietoturvaluustoimenpiteiden sääntely hankinnoissa	49
8.2	Tietoturvallisuus hankintaohjeissa	51
8.3	Tietoturvallisuusvaatimukset tarjouspyynnössä	52
8.4	Tarjousten sisällön arviointi	56
8.5	Hankintasopimuksen laadinta ja täytäntöönpano	57
8.6	Hankintasopimuksen toimeenpano	58
8.7	Säädökset ja lisätiedot	59
<b>9</b>	<b>Sanasto</b>	60

# 1 Johdanto

Tämä tiedonhallintalautakunnan antama suosituskokoelma opastaa [lain julkisen hallinnon tiedonhallinnasta](#) (906/2019, jatkossa tiedonhallintalaki, TiHL) asettamien erinäisten vaatimusten täyttämässä.

Tiedonhallintalain luku 4 sisältää tietoturvallisuutta koskevat vaatimukset, jotka kaikkien tiedonhallintalain soveltamisalaan kuuluvien viranomaisten tulee täyttää. Tietoturvasuosituksien toteuttamiseksi tiedonhallintalautakunta on antanut tietoturvallisuutta koskevia suosituksia.

Yleiset huomiot suositusten sisällöstä:

- Suositukset on laadittu tiedonhallintayksikön ja viranomaisen oman toiminnan kehittämisen tueksi. Suosituksia ei ole tarkoitettu käytettäväksi auditointi- tai arviointikriteeristöinä.
- Suositukset koskevat kaikissa muodoissa olevaa tietoa, sekä analogista että sähköistä.
- Suosituksissa ei viitata mihinkään yleisiin standardeihin tai viitekehyksiin eikä anneta ohjeita teknisistä ratkaisuista, jotka voivat muuttua nopeastikin. Kunkin viranomaisen tulee tapauskohtaisen riskiarvioinnin perusteella valita kuhunkin tapaukseen sopivat, riittävän turvalliset tekniset ratkaisut.
- Suositukset kuvaavat suosituksia ja parhaita käytäntöjä, ne eivät ole velvoittavia kuten lainsäädäntö on.

Turvallisuusluokitellun tiedon käsittelyssä valtionhallinnon viranomaisten tulee huomioida sekä tiedonhallintalakia että valtioneuvoston asetusta asiakirjojen turvallisuusluokitelusta valtionhallinnossa (1101/2019) koskevat suositukset.

## 2 Tietoturvallisuuden vähimmäisvaatimukset

Julkisessa hallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset, ja niiden noudattamisesta annetut suositukset ovat seuraavat:

1. Tehtävät, joiden suorittaminen edellyttää henkilöiltä erityistä luotettavuutta on tunnistettu, 12§
2. Toimintaympäristön tietoturvaluustilaa seurataan, 13.1§
3. Tietoturvaluisuus varmistetaan tiedon elinkaaren ajan, 13.1§  
13§ Elinkaaren huomioiminen tietojen käsittelyssä, suositus kuvaa miten tietoturvaluisuus huomioidaan tiedon elinkaaren eri vaiheissa.  
13§ Elinkaaren huomioiminen tietojärjestelmissä, suositus kuvaa miten tietoturvaluisuus huomioidaan tietojärjestelmien elinkaaren eri vaiheissa.
4. Tietoriskien hallinta ja siihen perustuvat tietoturvatoimet on järjestetty, 13.1§  
13§ Riskienhallinta, suositus kuvaa miten tietoriskien hallinta voidaan toteuttaa tiedonhallintayksiköissä.
5. Tietojärjestelmien vikasetoisuus ja toiminnallinen käytettävyys on varmistettu, 13.2§
6. Julkisuus ja salassapitorakenne on huomioitu tietovarantojen tietorakenteissa, 13.3§
7. Hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvaluisuustoimenpiteet
8. Salassa pidettävät tiedot on suojattu yleisessä tietoverkossa tietoja siirrettäessä, 14.1§
9. Tietoaineistojen turvaluisuus on varmistettu, 15§  
15§ Vahingoilta suojaaminen, suositus kuvaa miten tiedot ja tietojärjestelmät voidaan suojata teknisiltä ja fyysisiltä vahingoilta.
10. Tietoaineistoa käsitellään riittävän turvaluisissa tiloissa, 15.2§

11. Käyttöoikeudet on määritelty ja hallittu tietojärjestelmissä, 16§
12. Tarpeelliset lokitiedot on kerätty tietojärjestelmien käytöstä ja luovutuksista, 17§  
17§ Lokitietojen kerääminen, suositus kuvaa mitä seikkoja lokitietojen keräämisessä tulee huomioida.
13. Turvallisuusluokiteltavista asiakirjoista ja niiden käsittelystä on huolehdittu, 18§

Viranomaisen tulee arvioida mitä suunniteltu tiedonhallintamallin muutos tarkoittaisi kunkin yllä luetellun vähimmäisvaatimuksen osalta tai mitä kunkin vähimmäisvaatimuksen osalta on huomioitava kehittämisessä.

Uusia tietojärjestelmäpalveluja hankittaessa tietoturvallisuusvaatimukset muodostuvat yllä olevista vähimmäisvaatimuksista sekä riskiarvioinnin avulla tunnistetuista muista mahdollisista vaatimuksista. Kunkin vaatimuksen toteuttamisen menettely arvioidaan riskiarviointiprosessin avulla.

## 3 Riskienhallinta (TiHL 13.1§)

*Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvittävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti.*

### 3.1 Tietoriskien analyysi ja hallinta

Tiedonhallintayksikön hyvänä käytäntönä on huolehtia tietoaineistojen, tietovarantojen ja tietojärjestelmien riskienhallinnasta (1):

- tunnistamalla ja arvioimalla olennaisia riskejä
- vähentämällä riskien todennäköisyyttä ja vaikutuksia hyväksyttävälle tasolle
- ylläpitämällä saavutettua tasoa tai
- vaihtoehtoisesti hyväksymällä jäännösriskit tai osa niistä.

Riskienhallinnalla pyritään toteuttamaan tietoturvaluustoimenpiteiden yhdistelmä, jonka avulla varmistetaan tietoaineistojen ja tietojärjestelmien riittävä tietoturvallisuuden taso ja saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Oikeasuhtainen riskienhallinnan taso voidaan saavuttaa, kun tietoihin ja tietojärjestelmiin liittyvät vaikutukset on tunnistettu vaikutusanalyysin avulla ja riskien realisoitumisen todennäköisyys on otettu huomioon. Tietojen ja tietoaineistojen laadun varmistaminen on osa riskienhallintaa, sillä virheellinen tieto voi itsessään olla iso riski.

Tietoriskien hallinta on jatkuvaa toimintaa, johon liittyvät tavoitteet, periaatteet, vastuut ja keskeiset menettelyt tiedonhallintayksikön on hyvä kuvata. Johdon vastuulla on tietoriskien hallinnan organisointi ja resursointi. Hallintaprosessi vaikuttaa tiedonhallintayksikön

toiminnan ja tavoitteiden arviointiin ja suunnitteluun. Tietoriskien hallinnassa havaitut riskit vaikuttavat tiedonhallintayksikön toimenpiteisiin koko sen toiminnan ajan.

Tietoriskien hallinnassa käytetään tiedonhallintayksikön tehtävien ja tietoaineistojen laajuuden perusteella valittuja menettelytapoja. Pienissä organisaatioissa tietoriskien koordinointi voi olla vastuutettu yhdelle henkilölle ja organisoitu tehtäväksi johdon ja muutamman henkilön yhteistyönä. Tietoriskien hallintaan vaadittavien resurssien tarpeeseen vaikuttaa organisaation koon lisäksi tehtävien ja tietoaineistojen luonne. Prosessissa voidaan hyödyntää tavanomaisia toimisto-ohjelmistoa.

Laajemmissa organisaatioissa, ja etenkin ICT-tuotannosta vastaavissa organisaatioissa, riskienhallinnassa tarvitaan sekä useiden asiantuntijoiden ja keskijohdon ja ylemmän johdon työpanosta että erityisiä riskienhallintaohjelmistoa. Kaikissa organisaatioissa johdon tulee käsitellä tietoriskit vähintään kerran vuodessa osana muuta riskienhallintaa.

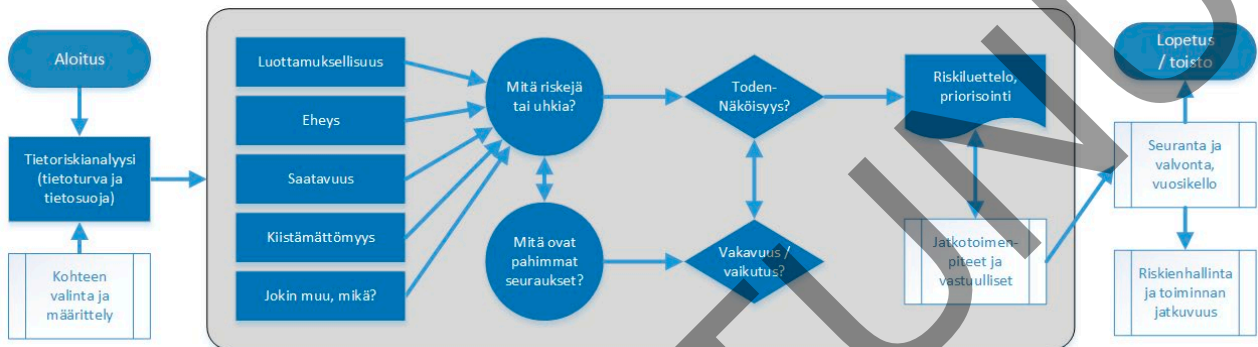
Tietoriskien käsittelyssä toimenpiteet mitoitetaan organisaation määrittämälle hyväksyttävälle tasolle. Organisaation johdolla on kokonaisvastuu riskienhallinnasta ja hyväksyttävästä riskitasosta. Jäännösriskkejä ja tehtyjä tietoturvaluustoimenpiteitä tulee seurata säännöllisesti. Tietoriskien seurannan tulee jatkua tietoaineistojen ja tietojärjestelmien koko elinkaaren ajan. Seurannassa tarkastetaan riskienkäsittelysuunnitelmien toteutumisen sekä tietoturvaluustoimenpiteiden vaikuttavuus.

Tietoriskien hallinnassa on tärkeää kirjata **riskirekisteriin** kaikki potentiaaliset tietoriskit ja arvioida niiden todennäköisyys ja vaikutukset. Kaikkien keskeisten henkilöiden olisi hyvä osallistua arvioitavan kohteen tietoriskien selvittämiseen ja riskiarviointiin, jotta riskirekisteristä saadaan kattava ja eri asiantuntijoiden näkemykset tulevat huomioon otetuiksi. Myös tietoriskien syyt ja mahdollisen toteutumisen seuraukset on hyvä kirjata ylös. Usein on helpompaa puuttua riskin syyhyn kuin itse tietoriskiin. Tarkempia ohjeita riskien todennäköisyyden ja vaikutusten arviointiin löytyy julkaisusta Ohje riskienhallintaan (Valtiovarainministeriön julkaisu 22/2017).

Tietoriskien selvittämisen ja arvioinnin lisäksi riskirekisteriin on hyvä kirjata jo aloitetut tai tehdyt riskienhallintatoimenpiteet sekä potentiaaliset uudet toimenpiteet. Tietoriskin omistaja päättää, mitkä hallintatoimenpiteet toteutetaan ja mitkä riskit voidaan hyväksyä ja kuka vastaa toimenpiteistä ja niiden aikatauluista. Hallintatoimenpiteet tulee suhteuttaa riskiarvioinnin perusteella tietoihin ja tietojärjestelmiin kohdistuviin uhkiin ja seuraksiin.

Riskit ja hallintatoimenpiteet tulee myös ottaa huomioon jatkuvuussuunnittelussa, jonka avulla pyritään takaamaan tietojen tai tietojärjestelmien riittävä saatavuus.

Sovittujen hallintatoimenpiteiden toteutumista ja aikataulujen pitävyyttä on hyvä seurata systemaattisesti, esimerkiksi kerran kuukaudessa tai vähintään neljä kertaa vuodessa. Tietoriskien arviointi on hyvä tehdä uudelleen, kun yksi tai useampia hallintatoimenpiteitä on tehty.



Kuvio 1. Tietoriskianalyysin prosessikaavio (2)

## 3.2 Jäännösriskien hallinta

Hallintatoimenpiteiden jälkeen voimaan jääviä riskejä, joihin ei voida tai haluta enää vaikuttaa, kutsutaan jäännösriskeiksi. Niitä syntyy esimerkiksi hallintakeinojen ollessa riskin vaikutusten suhteen liian kalliita tai raskaita. Organisaatiolla tulee olla johtoryhmätason hyväksymä menetelmä jäännösriskien käsittelemiseksi ja niiden nostamiseksi tarvittaessa myös johtoryhmän käsiteltäväksi.

## 3.3 Tietoriskien hallinnassa tarvittavat tietoaineistot

Hyvänä käytäntönä tiedonhallintayksikössä on seurata toimintaympäristön turvallisuustilannetta viranomaislähteistä, viranomaiskontaktien ja mediaseurannan avulla sekä valvomalla jatkuvasti tietojärjestelmiä ja tietovarantoja. Tämä tulee tehdä ottaen huomioon mahdollinen erityislainsäädäntö, käytännesäännöt, muu informaatio-ohjaus, tulosojaus ja taloudelliset voimavarat. Keskeisiä viranomaistietolähteitä ovat Kyberturvallisuuskeskuksen raportit sekä rikosasioissa Poliisi.



Julkisen hallinnon on hyvä ottaa omassa varautumisessaan huomioon tietoturvallisuudesta annetut VAHTI-ohjeet. Niihin kuuluu muun muassa tietoturvapoikkeamista mahdollisimman nopeasti tehty ilmoitus Kyberturvallisuuskeskukselle, jotta poikkeaman kohdeeksi joutunut viranomaisiin saa apua tilanteesta toipumiseen. Lisäksi on aina suositeltavaa tehdä rikosilmoitus Poliisille, jos rikoksen tunnusmerkit täyttyvät. Oikea-aikainen toiminta koituu sekä julkisen hallinnon että kansalaisten eduksi.

Tietoriskien hallinnassa hyödynnetään tiedonhallintayksikön ylläpitämiä, tietojärjestelmiä koskevia metatietoja sekä tiedonhallintamallista löytyviä metatietokuvauksia tietoaisteista ja -varannoista ja tietovarantojen ja -järjestelmien tärkeysluokituksista. Erityistä huomiota on kiinnitettävä siihen, missä tietojärjestelmät ja tietovarannot fyysisesti sijaitsevat ja mitä tietoriskejä siitä mahdollisesti aiheutuu, toiminta ja kyseessä olevat tietoaisteistot huomioon ottaen.

Tiedonhallintayksikkö ylläpitää riskiarvioiden tuloksista ja riskienkäsittelysuunnitelmista muodostuvaa tietoaisteistoa sekä arvioi säännöllisesti, onko se osin tai kokonaan salassa pidettävä tai turvallisuusluokiteltava. Salassapitosäännösten niin vaatiessa viranomaisen on luokiteltava tietoriskejä koskeva tietoaisteisto salassa pidettäväksi sekä turvallisuusluokitteluvaatimusten täytyessä myös turvallisuusluokiteltava se kokonaan tai osittain.

### 3.4 Yleisiä vaatimuksia

Seuraavat yleiset vaatimukset tulisi ottaa huomioon riskienhallinnassa:

- Onko viranomaisiin tunnistanut ja dokumentoinut kaiken tiedon ja kaikki tietojärjestelmät, joista se on vastuussa?
- Onko näitä ylläpitävät ja käyttävät avainhenkilöt tunnistettu?
- Onko tietoihin, tietojärjestelmiin ja avainhenkilöihin mahdollisesti kohdistuvat uhkatekijät tunnistettu?
- Onko tiedoille ja tietojärjestelmille laadittu vaikutusanalyysi, jonka perusteella on mahdollista arvioida riskienhallintatoimenpiteiden oikeasuhtaisuus?
- Ovatko riskienhallintatoimenpiteet oikeasuhtaiset riskin realisoinnin vaikutukseen ja todennäköisyyteen nähden?
- Ylläpidetäänkö riskirekisteriä ja arvioidaanko riskienhallintatoimenpiteiden toimivuutta säännöllisesti?

### 3.5 Säädökset ja lisätiedot

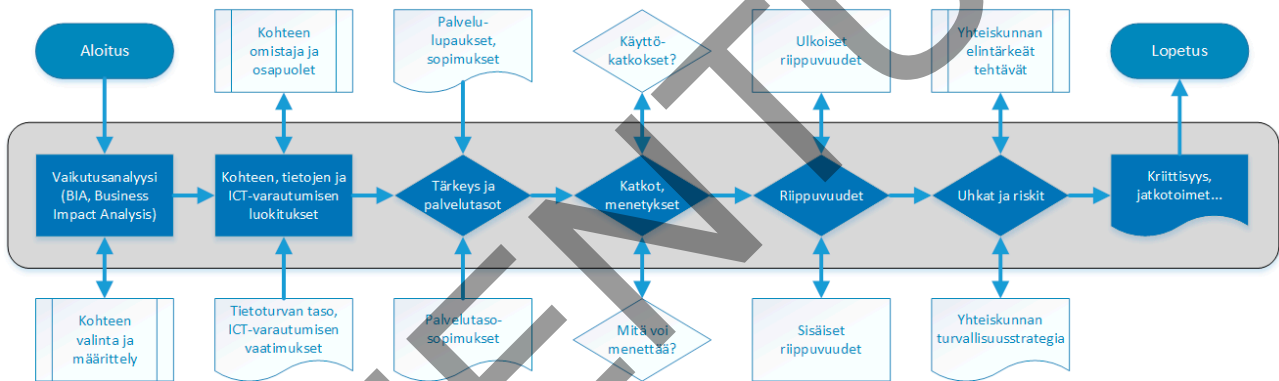
(1) ISO 31000 Riskienhallinta

(2) Ohje riskienhallintaan – Liitteet 1-6 (Valtiovarainministeriön julkaisu 22/2017)

Riskienhallinnan järjestäminen (valtiovarainministeriön sivusto)

Riskienhallintapolitiikkamalli (valtiovarainministeriön sivusto)

Ohje riskienhallintaan (Valtiovarainministeriön julkaisu 22/2017)



Kuvio 2. Vaikutusanalyysin prosessikaavio (2)

## 4 Elinkaaren huomioiminen tietojen käsittelyssä (TiHL 13.1§)

*Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.*

**Tiedon elinkaari** alkaa tiedon tuottamis- tai vastaanottovaiheessa ja päättyy tiedon pysyvään säilyttämiseen arkistossa tai tiedon tuhoamiseen. Tiedon elinkaari kattaa siis kaikki tiedon käsittelyn vaiheet, jotka ovat **tiedon tuottaminen** tai **vastaanotto, säilytys, käyttö, jakaminen, siirto** ja **arkistointi tai tuhoaminen**. Tiedon elinkaariajattelun lähtökohtana on tiedon suunnitelmallinen ja riskilähtöinen käsittely ja hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietoaineistojen tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla tietoaineistojen käsittelyyn kohdistuvat riskit ja mitoittamalla tietoturvaluustoimenpiteet tehdyn riskiarvioinnin mukaisesti. Tietoaineistojen tietoturvallisuuden on täytettävä tiedonhallintalain asettamat vähimmäisvaatimukset.

Tiedon elinkaaren osalta on tärkeää huomioida, että tietoaineistoja käsitellään useassa eri sijainnissa ja tietojärjestelmässä tai laitteistossa, joissa tiedolla voi olla oma elinkaarensa, ja että tiedon elinkaari on yleensä pidempi kuin yksittäisen tietojärjestelmän elinkaari.

### 4.1 Tietoturvallisuus läpi tiedon elinkaaren

Tietoturvallisuus tietoaineistojen elinkaareissa muodostaa kokonaisuuden, johon kuuluvat **tiedon luokittelu, riskien arviointi, tietoturvaluustoimenpiteiden suunnittelu** tunnistettujen riskien perusteella sekä **tietoturvaluustoimenpiteiden toteuttaminen**. Tiedonhallintayksikön tulee arvioida tietoaineistoihin liittyviä riskejä säännöllisesti tietoaineistojen koko elinkaaren ajan sekä huomioitava muuttuneiden riskien edellyttämät

toimenpiteet tietoturvaan koskevilla suunnitelmissa ja toteutuksissa. Ennen tiedon tuottamista tai vastaanottamista tulee huomioida tiedon määrittely, jossa arvioidaan tiedon ominaisuuksiin, turvallisuuteen ja metatietoihin liittyviä ominaispiirteitä. Tiedon määrittelyvaiheen perusteella muodostuvat tiedon käsittelyperiaatteet koko elinkaaren ajalle.

Tiedon osalta tunnistetaan ja määritellään, mihin sen käsittely perustuu ja mikä on tiedon käsittelyn tarkoitus. Lisäksi varmistetaan myös suunnitellun käsittelytarkoituksen toteutuminen läpi tiedon elinkaaren. Kaikissa elinkaaren vaiheissa varmistetaan, että tietoa käsitellään käsittelyperusteen muodostamien vaatimusten, tietoon kohdistuvien riskien ja tiedolle asetettujen tietoturva vaatimusten mukaisesti kaikissa käsittely-ympäristöissä. Tietoturvasuus on alusta alkaen osa tietoaaineistojen käsittelyyn liittyvien käytäntöjen ja käsittely-ympäristöjen suunnittelua ja toteutusta.

Tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt ja muut käsittelyyn liittyvät tekijät ovat tiedonhallintayksikön tiedossa asianmukaisen tiedonhallinnan toteuttamiseksi ja tiedon käsittelyyn liittyvien riskien arvioimiseksi. Tietoa käsitellään tehtyjen suunnitelmien mukaisesti kaikissa elinkaaren vaiheissa. Lisätietoja turvallisuusluokitellun tiedon käsittelystä löytyy mm. ulkoministeriön kansainvälisen turvallisuusluokitellun tietoaaineiston käsittelyohjeesta.

**Tiedon elinkaari** alkaa sen käsittelyn käynnistyessä tiedon tuottamis- tai vastaanottovaiheessa ja päättyy sen pysyvään säilyttämiseen arkistoinnin muodossa tai tiedon tuhoamiseen. Tiedon elinkaari kattaa siis kaikki tiedon käsittelyn vaiheet, joita tyypillisesti ovat **tiedon tuottaminen** tai **vastaanotto**, **säilytys**, **käyttö**, **jakaminen** ja **siirto** sekä **arkistointi** tai **tuhoaminen**. Tiedon elinkaariajattelun lähtökohtana on tiedon suunnitelmallinen ja riskilähtöinen käsittely ja hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietoaaineistojen tietoturvasuuden koko niiden elinkaaren ajan tunnistamalla tietoaaineistojen käsittelyyn kohdistuvat riskit ja mitoittamalla tietoturvasuus toimenpiteet tämän riskiarvioinnin mukaisesti. Tietoaaineistojen tietoturvasuuden on täytettävä tiedonhallintalain asettamat vähimmäisvaatimukset.

Tiedon elinkaaren osalta on tärkeää huomioida, että tietoaaineistoja käsitellään useassa eri sijainnissa ja tietojärjestelmässä tai laitteistossa, joissa tiedolla voi olla oma elinkaarensa ja tiedon elinkaari on yleensä pidempi kuin yksittäisen tietojärjestelmän elinkaari.

Alla on listattu keskeisiä tietoaineistojen elinkaareen liittyviä kysymyksiä:

- Onko tietoaineistojen käsittelyn peruste ja käyttötarkoitus tunnistettu ja määritetty?
- Onko tietojen käsittelyssä otettu huomioon tiedon käyttötarkoituksen mahdollinen muuttuminen?
- Onko tiedon käsittelyperusteen, kuten henkilötietojen ja erityisten henkilötietojen muodostamat vaatimukset tunnistettu?
- Onko tietoaineistoihin liittyvät riskit arvioitu koko tiedon elinkaaren ajalta? Seurataanko riskejä säännöllisesti?
- Ovatko tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät tiedonhallintayksikön tiedossa ([Tiedonhallintamalli](#), ministeriöillä lisäksi [tiedonhallintakartta](#))

## 4.2 Tiedon tuottaminen ja vastaanotto

Tietoaineistojen tuottamisella tarkoitetaan käsittelyvaihetta, jossa tuotetaan uutta tietoa tai tehdään tietoaineistoon päivityksiä. Tietoaineistojen vastaanotolla tarkoitetaan käsitteilyvaihetta, jossa tiedonhallintayksikkö vastaanottaa muualla tuotettuja tietoaaineistoja.

Tiedon tuottamisen tai vastaanoton yhteydessä tunnistetaan ja kuvataan tiedon käsittelyn perusteet ja tarkoitus. Tuotettavan ja vastaanotettavan tiedon kohdalla tunnistetaan niiden käsittelyä koskevat erityisvaatimukset, jotka voivat tulla lainsäädännöstä tai toisen organisaation tiedon käsittelylle asettamista vaatimuksista. Erityisvaatimuksia asettaa esimerkiksi henkilötietoja koskeva tietosuojalaki ja tietosuoja-asetus. Tiedon tuottamis- ja vastaanottovaiheessa määritellään tiedon alustava säilytysaika, joka voi vielä muuttua tiedon elinkaaren eri vaiheissa.

Alla on listattu tiedon tuottamiseen ja vastaanottoon liittyviä keskeisiä kysymyksiä:

- Onko tietoaineistojen käsittelyn peruste ja käyttötarkoitus tunnistettu ja määritelty?
- Onko käsiteltävää tietoaaineistoa koskevat erityisvaatimukset, kuten henkilötietoihin liittyvät vaatimukset tunnistettu?

### 4.3 Tiedon säilytys

Säilytyksen osalta määritellään ja toteutetaan tiedon riittävä suojaus sille asetettujen vaatimusten ja hallintakeinojen sekä riskitason mukaisesti. Tiedon suojauksen avulla turvataan tiedon luottamuksellisuuden ja eheyden säilyminen ja sen saatavuus. Suojaus kattaa tekniset ja hallinnolliset keinot.

Säilytyksessä varmistetaan tiedon saatavuus ja säilyminen sekä sen säilytysajan mittainen käytettävyys teknologioiden muuttuessa. Tiedon säilytyksen suunnittelussa ja toteutuksessa varaudutaan riskiarvioissa tunnistettuihin uhkatilanteisiin riskien edellyttämällä tasolla muun muassa asianmukaisen salauksen ja jatkuvuuden hallinnan avulla. Tietoaineistoille on määritelty säilytysajat, joiden päättyessä tietoaineistot joko arkistoidaan tai tuhotaan. Tietoaineistojen tuhoamiseen on dokumentoitu prosessi. Lisätietoja salauskäytännöistä löytyy mm. [Vahti-ohjeesta 2/2015](#).

Tietoaineistojen säilytykseen käytetään ainoastaan siihen hyväksytyjä ja asetettujen vaatimusten mukaisia säilytysympäristöjä, jotka noudattavat luvun 5 periaatteita.

Alla on listattu tiedon säilytykseen liittyviä keskeisiä kysymyksiä:

- Onko säilytettävä tieto luokiteltua (turvallisuusluokiteltua)? Jos on, onko säilyttämiseen liittyvät vaatimukset tunnistettu ja täytetäänkö ne? Onko tietojen luokittelussa huomioitu eri näkökulmat, kuten tietojärjestelmät, tietosuoja, tietoturva, toimintaprosessit ja tietoarkkitehtuuri?
- Säilytetäänkö tietoa siten, että vain oikeutetut tahot pääsevät siihen käsiksi?
- Onko tiedon säilytys suunniteltu siten, että sen käytettävyys ja saatavuus on taattu myös poikkeusoloissa, mikäli riskiarvio näin edellyttää?
- Onko säilytettävälle tiedolle määritetty säilytysaika, jonka päättyessä se joko arkistoidaan tai tuhotaan asianmukaisesti?

### 4.4 Tiedon käyttö

Tietoaineistojen luvallinen käyttö mahdollistetaan ja luvaton käyttö estetään henkilöiden työtehtäviin perustuvalla roolipohjaisella fyysisten ja loogisten käyttöoikeuksien ja -valtuuksien määrittelyllä ja hallinnalla. Tietoaineistojen käyttäjän identiteetti todennetaan riskeihin ja käytettävään tietoon nähden riittävällä tavalla.

Tietoaineistojen käyttöä seurataan ja valvotaan tehdyn riskiarvioinnin mukaisesti. Tietojärjestelmien kohdalla vähintään kirjautumisista ja niiden yrityksistä tulee tuottaa lokia,

mutta useissa tapauksissa myös järjestelmässä toimimisesta tulee kerätä käyttölokia. Tietoaineistojen käytön lokitus ja valvonta toteutetaan tarpeellisuusarvioinnin perusteella tiedon käyttötarkoituksen ja siihen liittyvien riskien edellyttämällä tavalla. Palvelusta vastaavan vastuulla on selvittää saako palvelusta kerätä lokitietoja.

Tietoaineistoja käyttö tapahtuu siihen hyväksytyissä ja asetettujen vaatimustenmukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä.

Alla on listattu tiedon käyttöön liittyviä keskeisiä kysymyksiä:

- Onko tietoaineiston käyttöoikeudet ja -valtuudet määritelty henkilön työtehtävien mukaisesti?
- Valvotaanko tietoaineiston käyttöä riskiarvion mukaisesti?
- Voidaanko olla varmoja siitä, että tietoaineistoa käytetään vain siihen tarkoitukseen, johon ne on (alun perin) tarkoitettu?
- Kerätäänkö tietojärjestelmien kirjautumisista lokia?
- Voidaanko olla varmoja siitä, että tietoaineistoa käsitellään vain siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä?

## 4.5 Tiedon jakaminen, siirtäminen ja luovuttaminen

Tietoaineistojen jakamisella tarkoitetaan toimia, joiden avulla päätetään tietoaineiston vastaanottajat, varmistetaan vastaanottajien tiedontarve ja oikeus sekä kyky käsitellä jaettavaa tietoaineistoa. Tietoaineistojen siirrolla tarkoitetaan niitä toimenpiteitä, joilla tietoaineistot siirretään määritetyille tahoille tai toisiin tietojärjestelmiin. Siirto voi tapahtua esimerkiksi postin, sähköpostin, sähköisen muistivälineen, tietojärjestelmien välisen tiedonsiirron tai käsittelyoikeuksien myöntämisen avulla. Ei-julkista tai turvallisuusluokiteltua tietoa jakaessa ja siirtäessä tulee muistaa, että tavallinen sähköposti ei lähtökohtaisesti ole salattu ja turvallinen tiedonvälityskanava. Tällaista tietoa siirrettäessä tulee olla erityisen varma, että tiedonsiirrossa käytettävä menetelmä on salattu ja riittävän turvallinen. Tiedon luovuttamisella tarkoitetaan tietojen luovuttamista niitä pyytävälle taholle. Julkista tietoa luovutetaan [viranomaisten toiminnan julkisuudesta](#) annetun lain mukaisesti.

Tietoa jaettaessa, siirrettäessä ja luovutettaessa varmistetaan aina riittävän luotettavasti mahdollisen vastaanottajan identiteetistä sekä toteutetaan tiedon siirto tunnistettuihin riskeihin nähden asianmukaista salausta ja suojausta käyttäen. Näin varmistetaan, etteivät tietoon pääse käsiksi siihen oikeudettomat henkilöt ja tietoaineisto jaetaan tai luovutetaan vain henkilöille, joilla on siihen työtehtäviinsä liittyvä oikeus. Lisätietoja salausratkaisujen

turvallisuudesta on luvussa 6 sekä Kyberturvallisuuskeskuksen turvallisuusluokitellun tiedon suojaamiseen [hyväksymissä salausratkaisuissa](#), [vahvuustaulukoissa](#), sekä ohjeissa salaustuotteiden [arvioinnista](#) ja [turvallisesta kehittämisestä](#).

Kun tietoaaineistoja jaetaan tai luovutetaan viranomaisten välillä, huomioidaan (erillinen) suositus Teknisistä rajapinnoista ja katseluyhteyksistä. Alla on listattu keskeisiä tiedon jakamiseen, siirtämiseen ja luovuttamiseen liittyviä kysymyksiä:

- Voidaanko tietoaaineistoa jakaessa, siirtäessä ja luovuttaessa varmistua riittävällä tasolla vastaanottajan identiteetistä?
- Käytetäänkö tiedon siirrossa asianmukaista salausta?
- Onko tietoja luovutettaessa varmistuttu siitä, että tiedon luovuttaminen on lain mukaista ja vastaanottajalla on oikeus tietoaaineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti?

## 4.6 Tiedon arkistointi

Tietoaaineistojen arkistoinnilla tarkoitetaan niitä menettelyjä, joilla varmistetaan tiedon säilyminen muuttumattomana asetetun elinjakson ajan. Tietoaaineistot on tuhottava tai arkistoitava tietoturvalisella tavalla tiedon säilytysajan päätyttyä.

Arkistoinnissa huomioidaan tiedon säilytysaika, -paikka ja -tapa sekä varmistetaan tiedon käyttökelpoisuus ja luettavuus koko säilytysajaksi. Arkistointi perustuu sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin. Lisätietoja arkistoinnin vaatimuksesta löytyy [Kansallisarkiston ohjaussivulla](#).

Alla on listattu keskeisiä tiedon arkistointiin liittyviä kysymyksiä:

- Onko arkistoinnissa huomioitu tiedon säilytysaika, -paikka ja -tapa?
- Onko tiedon käyttökelpoisuudesta ja luettavuudesta varmistuttu koko tiedon säilytysajan?
- Perustuuko arkistointi sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin?



## 4.7 Tiedon tuhoaminen

Tietoaineistojen tuhoamisella tarkoitetaan niitä toimenpiteitä, joiden avulla tietoaineistot tuhotaan tarkoituksella niiden säilytysajan ja käyttötarpeen päättyessä tai niitä sisältävän laitteiston käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä.

Tiedon tuhoaminen tapahtuu määritellyn säilytysajan tai käyttötarpeen päättyessä tunnistettuihin riskeihin nähden riittävän luotettavalla tavalla. Tietoaineistoille määritetyt säilytysajat huomioidaan tiedon tuhoamisen suunnittelussa. Tietoaineistoista muodostetut kopiot ja luonnokset sekä väliaikaistiedostot tuhotaan niiden käyttötarpeen päättyttyä.

Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen osittain tai kokonaan. Salassa pidettävän tietoaineiston tuhoamiseen voidaan käyttää useita eri menetelmiä ja työvälineitä riippuen muun muassa tiedon olomuodosta ja saatavilla olevista erilaisista ratkaisuista. Esimerkiksi tiedon silppuamisen tai kovalevyn ylikirjoituksen sijaan tai lisäksi silppu voidaan polttaa ja kiintolevy sulattaa.

Erityisesti sähköisten aineistojen luotettavan tuhoamisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän salassa pidettävän tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys (esimerkiksi [viranomaisen hyväksymä ylikirjoitusmenettely](#)) ei ole mahdollista, salassa pidettävää tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että salassa pidettävää tietoa ei viedä huoltotoimenpiteen yhteydessä. Mikäli tiedon tuhoaminen tapahtuu palveluntarjoajan toimesta, viranomaisen tulee varmistua luotettavalla tavalla tiedon oikeellinen hävittäminen

Alla on listattu keskeisiä tiedon tuhoamiseen liittyviä kysymyksiä:

- Tapahtuuko tiedon tuhoaminen määritellyn säilytysajan tai käyttötarpeen päättyessä riittävän luotettavalla tavalla? Käytetäänkö tässä menetelmää, jolla estetään tietojen kokoaminen uudestaan tai osittain?
- Kattavatko luotettavan tuhoamisen menettelyt kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa?

## 4.8 Säädökset ja lisätiedot

EU:n yleinen tietosuoja-asetus

Arkistolaki

Kyberturvallisuuskeskuksen hyväksymät salausratkaisut

Kyberturvallisuuskeskuksen hyväksymä ylikirjoitusmenettely

Kyberturvallisuuskeskukset ohje: Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen -kansalliset suojaustasot

VANHTENTUNNUT

## 4.9 Yhteenveto suosituksesta

Taulukko 1. Yhteenveto suosituksesta.

<b>Koko elinkaari</b>	<p>Tietoaineistoihin liittyvät riskit arvioidaan säännöllisesti.</p> <p>Tunnistetaan ja määritetään tietoaineistojen käsittelyn peruste ja käyttötarkoitus.</p> <p>Varmistetaan, että tiedon käsittelyperusteen muodostamat vaatimukset, tietoon kohdistuvat riskit ja tiedolle asetetut tietoturva-vaatimukset huomioidaan tiedon käsittelyn kaikissa vaiheissa.</p> <p>Varmistetaan, että tietoon, tietoaineistoon ja niiden käsittelyyn liittyvät vaatimukset huomioidaan tietojärjestelmiä ja ympäristöä suunniteltaessa ja ratkaisujen toteuttamisessa.</p> <p>Tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät tulee olla tiedonhallintayksikön tiedossa (<i>Tiedonhallintamalli</i>, ministeriöillä lisäksi <i>tiedonhallintakartta</i>).</p>
<b>Tiedon tuottaminen ja vastaanotto</b>	<p>Tunnistetaan ja kuvataan tiedon käsittelyn perusteet ja käsittelytarkoitus.</p> <p>Tunnistetaan tiedon käsittelyä koskevat erityisvaatimukset (esim. lainsäädännöstä tai toisen organisaation vaatimuksista muodostuvat).</p>
<b>Tiedon säilytys</b>	<p>Säilytettävää tietoa suojataan sille muodostettujen vaatimusten ja hallintakeinojen sekä riskitason mukaisesti.</p> <p>Säilytettävän tiedon säilyminen ja saatavuus on turvattu.</p> <p>Säilytettävän tiedon käytettävyyden on varmistettu koko säilytysajan.</p> <p>Tietoaineistolle on määritetty säilytysaika ja sen päättyessä tieto joko arkistoidaan tai tuhoetaan.</p> <p>Tietoaineistojen säilytykseen käytetään ainoastaan siihen hyväksytyjä ja asetettujen vaatimusten mukaisia säilytysympäristöjä.</p>
<b>Tiedon käyttö</b>	<p>Käyttöoikeudet ja -valtuudet tietoaineistoihin perustuvat henkilöiden työtehtäviin.</p> <p>Tietoaineistojen käyttöä lokitetaan riskiperustaisesti.</p> <p>Tietoaineistoja käytetään siihen tarkoitukseen, joihin ne on (alun perin) tarkoitettu.</p> <p>Tietoaineistoja käyttö tapahtuu ainoastaan siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä.</p>
<b>Tiedon jakaminen, siirtäminen ja luovuttaminen</b>	<p>Tietoa jaettaessa, siirrettäessä ja luovuttaessa varmistetaan riittävällä tasolla vastaanottajan identiteetistä.</p> <p>Tiedon siirrossa käytetään asianmukaista salausta.</p> <p>Tietoa luovutettaessa varmistetaan, että tiedon luovuttaminen on lain mukaista ja vastaanottajalla on oikeus tietoaineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti.</p>
<b>Tiedon arkistointi</b>	<p>Arkistoinnissa huomioidaan tiedon säilytysaika, -paikka ja -tapa.</p> <p>Arkistoinnissa on varmistettu tiedon käyttökelpoisuus ja luettavuus koko säilytysajaksi.</p> <p>Arkistointi perustuu sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin.</p>
<b>Tiedon tuhoaminen</b>	<p>Tiedon tuhoaminen tapahtuu määritellyn säilytysajan tai käyttötarpeen päättyessä riittävän luotettavalla tavalla.</p> <p>Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.</p> <p>Sähköisten aineistojen luotettavan tuhoamisen menettelyt kattavat kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassapidettävää tietoa.</p>

## 5 Elinkaaren huomioiminen tietojärjestelmissä (TiHL 13.1§)

*Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.*

### 5.1 Tietojärjestelmä

**Tietojärjestelmällä** tarkoitetaan järjestelmää, jonka tarkoitus on tietoja käsittelemällä palvelua, helpottaa ja tehostaa jotakin toimintaa. Tietojärjestelmä koostuu ohjelmista, tietovarastoista, laitteista ja palveluista. Tietojärjestelmän elinkaari alkaa siihen liittyvästä tarvekartoituksesta ja päättyy tietojärjestelmän käytöstä poistoon. Tietojärjestelmän elinkaari kattaa kaikki tällä välillä olevat vaiheet, jotka ovat **määrittely ja suunnittelu, kilpailutus ja hankinta, toteutus ja kehitys, käyttöönotto, ylläpito** sekä **käytöstä poisto**. Tietojärjestelmien elinkaariajattelun lähtökohdiana on kussakin järjestelmässä käsiteltävien tietojen elinkaaren huomiointi ja järjestelmien suunnitelmallinen ja riskilähtöinen hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietojärjestelmien tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla niihin kohdistuvat **riskit** ja mitoittamalla tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti. Riskienarvioinnissa tunnistetaan olennaiset riskit, jotka voivat vaikuttaa tietojärjestelmien käytettävyyteen ja saatavuuteen tai niissä käsiteltävien tietoaineistojen tietoturvallisuuteen ja oikeellisuuteen.

Tietoturvallisuus tietojärjestelmien elinkaareissa muodostaa kokonaisuuden, johon kuuluvat riskien arviointi, tietoturvaluustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvaluustoimenpiteiden toteuttaminen. Tiedonhallintayksikkö arvioi tietojärjestelmiin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan sekä huomioi muuttuneiden riskien edellyttämät toimenpiteet tietoturvallisuuden suunnittelussa ja toteutuksessa. Tietojärjestelmien riskien arvioinnissa huomioidaan toimintaympäristö ja järjestelmään liittyvät tietoturva vaatimukset.

## 5.2 Määrittely- ja suunnitteluvaihe

Ennen määrittely- ja suunnitteluvaiheen aloittamista tehdään tarvekartoitus, jossa tunnistetaan ja määritellään tietojärjestelmä, sekä se mitä uuteen tai uudistettavaan tietojärjestelmään liittyy ja millaisia vaatimuksia siihen kohdistuu. Määrittely- ja suunnitteluvaiheen aikana tunnistetaan tietoturvallisuuden kannalta keskeiset asiat, jotka on huomioitava toteutuksen myöhemmissä vaiheissa. Näihin kuuluvat aina tiedonhallintalaissa asetetut tietoturvallisuuden vähimmäisvaatimukset, jotka on lueteltu luvussa 3.

Määrittely- ja suunnitteluvaiheessa tunnistetaan tietojärjestelmän liittymät muihin järjestelmiin sekä niistä muodostuvat riippuvuudet ja tietovirrat. Nämä dokumentoidaan osaksi arkkitehtuuri- ja integraatiosuunnitelmia, joiden mukaisesti toteutetaan tarvittavat integraatiot muuhun ympäristöön varmistaen myös tietoturvallisuuden toteutuminen niissä. Edellä mainitut asiat voidaan tunnistaa jo tarvekartoituksen aikana, ja ne tarkentuvat kehittämisen edetessä.

Määrittely- ja suunnitteluvaiheessa kuvataan tietojärjestelmän käyttötarkoitus sekä toimintaympäristö, kuten käyttäjät, ohjaava lainsäädäntö ja muut ulkoiset vaatimukset, järjestelmässä käsiteltävät tietoaineistot sekä liittymät muihin tietojärjestelmiin. Näiden pohjalta tehdään riskiarvio sekä määritetään tietojärjestelmään kriittisyys ja edellytetty tietoturvallisuuden taso, joiden perusteella tunnistetaan koko tietojärjestelmän elinkaaren aikana huomioitavat tietoturva-vaatimukset. Tietojärjestelmään kohdistuvat toiminnalliset vaatimukset kuvataan ja niiden pohjalta laaditaan tietojärjestelmään kohdistuvat hyväksymiskriteerit. Tämä sisältää myös tietoturvallisuutta koskevat suunnitelmat ja vaatimukset, joiden määrittelyssä käytetään tarvittavaa tietoturvaosaamista. Määrittely- ja suunnitteluvaiheessa huomioidaan luvun 6 tarkennukset hankinnan suunnitteluun ja valmisteluun.

Tietojärjestelmän tai sen osan määrittelyvaiheessa arvioidaan sekä kokonaisuuden että järjestelmän eri osien tietoturvallisen toteuttamisen riskejä. Sellaisten osakokonaisuuksien sisällyttämistä järjestelmään on vältettävä, joiden tietoturallinen toteuttaminen tai ylläpito vaativat runsaasti resursseja. Keskeistä on kiinnittää myös huomioita tietoriskien arvioinnissa koko palvelu- ja toimitusketjun kaikkien osapuolien ja heidän ympäristöjensä huomioimiseen, jotta tietojärjestelmään kohdistuvat riskit tulee kokonaisvaltaisesti hallittua. Organisaation johto sitoutuu tietoriskien hallintaan perustuvaan tietoturvallisuuden toteuttamiseen jo määrittely- ja suunnitteluvaiheesta lähtien. Johdolle on myös tarkoituksenmukaista antaa realistinen kuva tietoturvallisuuden rakentamisen ja ylläpidon vaatimista resursseista.

Lisäksi ennen hankintaa tai toteutusta suunnitteluvaiheessa laaditaan alustava suunnitelma hankinnan ja toteutuksen aikaisista tietoturvaan liittyvistä tehtävistä, vastuista ja aikataulutuksesta. Määrittely- ja suunnitteluvaiheessa on lisäksi hyvä varmistaa ja

suunnitella riittävät resurssit tietojärjestelmien tietoturvaliselle toiminnalle, kuten tietoturvapäivitysten toteuttamiselle, niiden koko elinkaaren ajalle.

### 5.3 Kilpailutus- ja hankintavaihe

Kilpailutus- ja hankintavaiheessa suunnitellaan ja toteutetaan tietojärjestelmään liittyvä hankinta luvun 6 mukaisesti.

Kilpailutus- ja hankintavaiheessa on keskeistä, että hankintavaatimuksiin, tarjouspyyntöihin ja sopimukseen sisällytetään myös tietoturvaa koskevat vaatimukset. Ne kohdistuvat sekä hankinnan kohteena olevaan tietojärjestelmään, että sen toteuttavaan ja tarjoavaan toimittajaan.

### 5.4 Toteutusvaihe

Toteutusvaiheen sisältö riippuu hankittavasta tietojärjestelmästä ja sen toteutusmallista. Kyseessä voi olla esimerkiksi täysin räätälöity järjestelmä ja siihen liittyvä laajempi kehitysprojekti tai valmisohjelmisto, johon tehdään toteutusvaiheen aikana ainoastaan tiettyjä konfigurointeja.

Toteutusvaiheessa tehdään uudelleentarkastelu määrittelyvaiheessa laadittuun riskiarviointiin sekä tehdään tarvittavat tarkentavat uhkamallinnukset ja riskiarviot tietojärjestelmään liittyvien riskien ja uhkaskenaarioiden tunnistamiseksi. Määritetyt tietoturva-vaatimukset suunnitellaan ja dokumentoidaan tietoturvakontrolleiksi, jotka toteutetaan tämän vaiheen aikana.

Tietojärjestelmät koostuvat usein lukuisista, mahdollisesti hajautetuista ja usean osapuolen tekemistä komponenteista. Tällöin on tietoriskien hallinnassa hyvä kiinnittää huomiota rajapintojen hallintaan sekä palvelujärjestelmän ja taustajärjestelmän välisen tiedonsiirron hallintaan.

Toteutuksen aikana suoritetaan suunnitellut katselmoinnit ja testaukset pohjautuen riskiarviointiin ja tarveharkintaan; mm. arkkitehtuurikatselmointi, koodikatselmointi, toiminnallisuksien testaus, väärinkäyttötapausten testaus/ tietoturvatestaus ja suorituskykytestaus.

Toteutusvaiheessa huomioidaan sille etukäteen laaditut suunnitelmat ja vaiheet. Tavoitteena on, että tarvittavat toimenpiteet tehdään riskilähtöisesti ja suunnitelmallisesti asianmukaisen tietoturvallisuuden sisään rakentamiseksi.

Toteutetut tietoturvakontrollit ja ratkaisut dokumentoidaan osaksi tietojärjestelmän turvallisuuskuvausta ja muuta laadittua dokumentaatiota.

Tietoturvallisuusvastuiden epäselvyydet toteutuksen aikana ovat tavallinen ongelma, etenkin monitoimittajaympäristössä. Tähän voidaan varautua tietoriskien jatkuvalla hallinnalla ja riskien hallintaan tähtäävien toimenpiteiden toteuttamisella, huomioiden erityisesti sopimukseen kirjatut tavoitteet ja toimenpiteet riskien hallinnan osalta. Sopimukseen liittyviä tyypillisiä riskejä ovat IPR-kysymykset, tekijänoikeudet, lisenssit ja kaikki vielä tunnistamaton immateriaalioikeuden alla oleva aineisto, omistajan vaihdokset, fuusiot ja toiminnan lopettaminen.

## 5.5 Käyttöönottovaihe

Käyttöönottovaihetta varten laaditaan käyttöönottosuunnitelma tuotantoon viennin toteuttamiseksi. Osana tietojärjestelmän käyttöönottoa suoritetaan käyttöönottohyväksyntä, jossa varmistetaan aiemmin kuvattujen vaatimusten toteutuminen tietojärjestelmässä. Hyväksyntä edellyttää tarvittavien toiminnallisuuksien ja tietoturvakontrollien todentamista. Tietojärjestelmien, laitteiden ja sovellusten käyttöönottoasennus tehdään määritetyn prosessin ja ohjeistuksen mukaisesti huomioiden esimerkiksi organisaation laatimat arkkitehtuuriperiaatteet, yhteensopivuus muuhun ympäristöön sekä määritetyt suojausvaatimukset ja kovennukset. Näiden toteuttamiseksi on määritetty määrämuotoiset konfiguraatiot eri asetuksille ja parametreille sekä tarpeettomat palvelut poistettu käytöstä. Kovennetun, määritetyt tietoturva-asetukset sisältävän, asennuksen toteuttamisessa voidaan hyödyntää esimerkiksi ylläpidettyä luotettua levykuvaa (golden image), jonka avulla asennus tehdään. Nämä levykuvat katselmoidaan, testataan ja päivitetään säännöllisesti niiden asianmukaisuuden varmistamiseksi. Myös itse tietojärjestelmien, laitteiden ja sovellusten konfiguraatioiden säännöllinen katselmointi ja valvonta suunnitellaan osaksi ylläpitovaihetta.

Tietojärjestelmän tietoturvakuvaukseen päivitetään tarvittavien muutosten osalta käyttöönottovaiheessa.

## 5.6 Ylläpitovaihe

Osana ylläpitoa tunnistetaan käsittely-ympäristössä tai vaatimuksissa tapahtuvien muutosten vaikutus tietojärjestelmään sekä niiden edellyttämät muutokset tietoturvakontrolleihin. Tehtävissä muutoksissa noudatetaan määritettyjä muutoshallintamenettelyitä. Tietojärjestelmään kohdistetaan säännöllisiä riskiarvioita ja suojaustason asianmukaisuuden kohdistuvia arvioita, jotta varmistutaan siitä, että tietojärjestelmään kohdistuvat riskit ja vaatimukset ovat huomioitu. Arvioinneissa hyödynnetään muun muassa katselmoiteja sekä automaattisia ja manuaalisia tietoturvatestauksia. Riippuen toteutustavasta myös tietojärjestelmän palvelutoimittajaan kohdistetaan tarvittavia auditointeja ja heiltä voidaan edellyttää tietojärjestelmän turvallisuustason seuranta ja siihen liittyvää raportointia. Ylläpitovaiheen yhtenä tavoitteena on varmistaa määritettyjen tietoturvavaatimusten ja suojauskeinojen ajantasaisuus ja asianmukainen toiminta tehtyihin suunnitelmiin pohjautuen sekä näitä koskevan dokumentaation ja kuvausten ylläpito.

Tietojärjestelmien ylläpidossa noudatetaan organisaatiossa määritettyjä prosesseja ja toimintatapoja, kuten muutoshallinta, poikkeamienhallinta ja riskienhallinta, kun huolehditaan tietojärjestelmien haavoittuvuuksien hallinnasta, päivityksistä, varmuuskopioinnista, konfiguraation hallinnasta ja kovennuksista, haittaohjelmasuojauksesta sekä valvonnasta. Ylläpitovaiheessa pitää huolehtia myös toiminnan jatkuvuuden edellyttämästä tietojärjestelmän toipumissuunnitelmasta ja varmistamisesta harjoittelulla.

Osana tietojärjestelmien ylläpitoa toteutetaan tarvittava valvonta ja seuranta muun muassa tietojärjestelmän toimivuuden, suorituskyvyn ja tietoturvallisuuden seuraamiseksi ja ylläpitämiseksi. Suoritettava valvonta ja seuranta tulee kuitenkin olla suunniteltuna määrittely- ja suunnitteluvaiheen aikana.

Varmuuskopiot otetaan tehdyn suunnitelman mukaisesti huomioiden organisaation toiminnan ja käsittelyn tiedon pohjalta määritetyt varmuuskopioitavat tiedot, varmuuskopiointiin käytetyt menetelmät ja sen tiheys sekä varmuuskopioiden suojaamiseen liittyvät keinot. Varmuuskopiointi toteutetaan

- käyttäen siihen tarkoitettua ratkaisua,
- kirjaten lokiin tiedot varmuuskopioiduista tiedoista, varmuuskopioinnin ajankohdasta ja varmuuskopion kohteesta sekä merkiten varmuuskopiot asianmukaisesti,
- varmistaen varmuuskopioinnin onnistuminen ja palauttaminen esimerkiksi raportein sekä palautustestein, sekä
- suojaten varmuuskopiot vahingoilta ja väärinkäytöksiltä, kuten ylikirjoittamiselta, muuttamiselta tai tuhoutumiselta sekä niiden siirron että säilytyksen aikana.



Ohjelmistohaavoittuvuuksien hallinnassa noudatetaan määritettyä prosessia, jossa määritetään päivitystarpeen tunnistaminen ja havaitseminen, päivitysten asentamiseen liittyvät toimintamallit (huomioiden erityyppiset tietojärjestelmät ja ympäristöt sekä niiden mahdollisesti muodostamat erityistarpeet), päivitysten epäonnistumiseen ja palautumiseen liittyvät käytännöt, päivitystilanteen seurantaan ja siitä raportointiin liittyvät toimintatavat sekä vaihtoehtoiset suojaustavat ja toimenpiteet, kun haavoittuvuutta ei voida korjata päivityksellä (esimerkiksi päivitystä ei ole vielä julkaistu tai jokin sovellus ei toimi päivitetystä versiossa).

Haittaohjelmasuojaukseen liittyvät toimintamallit on määritelty kuvaten muun muassa haittaohjelmasuojaukseen käytettyjen ratkaisujen asennus ja konfigurointi sekä päivittämisen käytännöt, ratkaisujen ajantasaisuuden ylläpitäminen sekä niiden toimivuuden varmistaminen.

Ylläpitoyhteydet ja -oikeudet on toteutettu vähimpien oikeuksien periaatteen mukaisesti, jolloin ylläpitotoimiin on käytössä lievimmät mahdolliset tarvittavat oikeudet. Tietojärjestelmien ylläpitoyhteydet tehdään käyttäen salattuja yhteyksiä. Loogista ja fyysistä pääsyä rajoitetaan.

## 5.7 Käytöstä poisto

Käytöstä poistoa varten laaditaan riskiarviointi, jossa tunnistetut riskit huomioidaan poiston toteuttamisessa. Käytöstä poistolle laaditaan suunnitelma, jossa huomioidaan muun muassa säilytettävän tiedon migraatio, tuhottavien laitteiden ja muistivälineiden sanitointi sekä käytöstä poistuvan tietojärjestelmän osien tuhoaminen.

Käytöstä poiston yhteydessä tietoaineistojen tuhoamisen tulee tapahtua tunnistettuihin riskeihin nähden riittävän luotettavalla tavalla. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen osittain tai kokonaan. Tietoaineistojen elinkaaren osalta huomioidaan luvun 4 periaatteet.

Tietojärjestelmien käytöstä poistossa järjestelmien sisältämät tiedot voidaan tuhoamisen sijaan arkistoida. Arkistoinnin keskiössä on tiedon säilyvyys, käyttökelpoisuus ja luotettavuus.

## 5.8 Säädökset ja lisätiedot

JHS 166 Julkisen hallinnon IT-hankintojen yleiset sopimusehdot (JIT 2015)

Tilastoinnin yleinen prosessimalli (GSBPM)

## 5.9 Suosituksen yhteenveto

Taulukko 2. Suosituksen yhteenveto

<b>Koko elinkaari</b>	<p>Tietojärjestelmiin liittyvät riskit arvioidaan säännöllisesti.</p> <p>Suunnitellaan tiedon elinkaari kokonaisuudessaan, jotta esimerkiksi käytöstä poisto vaihe voidaan toteuttaa suunnitelmien mukaisesti.</p> <p>Suunnitelmia päivitetään kehityksen edetessä elinkaaren aikana.</p>
<b>Määrittely ja suunnittelu</b>	<p>Tunnistetaan tietojärjestelmän merkitys tiedonhallintayksikön toiminnalle ja sen jatkuvuudelle sekä siinä käsiteltävät tiedot ja niiden merkitys.</p> <p>Tunnistetaan tietojärjestelmään kohdistuvat ulkoiset vaatimukset.</p> <p>Arvioidaan tietojärjestelmään kohdistuvat riskit.</p> <p>Määritellään tietojärjestelmän kriittisyys ja tietoturvasaso.</p> <p>Määritellään ja kuvataan tietojärjestelmään ulkoisista vaatimuksista, sisäisestä luokituksesta ja tunnistetuista riskeistä muodostuvat tietoturva-vaatimukset.</p> <p>Määritellään tietojärjestelmän hyväksymiskriteerit.</p> <p>Suunnitellaan hankinnan ja toteutuksen aikaiset tietoturvaan liittyvät tehtävät ja niiden aikataulut.</p>
<b>Kilpailutus ja hankinta</b>	<p>Tietojärjestelmään liittyvä hankinta tehdään suunnitelmallisesti.</p> <p>Hankinnassa huomioidaan luvun 6 periaatteet.</p> <p>Kilpailutukseen- ja hankintaan liittyviin kuvauksiin, vaatimuksiin, tarjouspyyntöihin ja sopimuksiin sisällytetään myös tietoturva koskevat vaatimukset.</p> <p>Huomioidaan, että tietoturva-vaatimukset kohdistuvat sekä hankinnan kohteena olevaan tietojärjestelmään että sen toteuttavaan ja tarjoavaan toimittajaan.</p>
<b>Toteutus</b>	<p>Tehdään uhkamallinnus ja tunnistetaan tietojärjestelmään liittyvät riskit ja uhkaskenaariot.</p> <p>Valitaan ja dokumentoidaan tietoturvakontrollit.</p> <p>Tunnistetaan tietojärjestelmän liittymät muihin järjestelmiin sekä näihin liittyvät riippuvuudet osana kokonaisarkkitehtuuria.</p> <p>Toteutetaan valitut tietoturvakontrollit osana tietojärjestelmän kehitystä.</p> <p>Toteutetaan määritellyt katselmoinnit ja testaukset (arkkitehtuurikatselmointi, koodikatselmointi, toiminnallisuuden testaus, väärinkäyttötapausten testaus/ tietoturvatestausta, suorituskykytestaus).</p> <p>Laaditaan tietojärjestelmän turvallisuuskuvaus ja muu dokumentaatio.</p>

<b>Käyttöönotto</b>	<p>Laaditaan käyttöönottosuunnitelma.</p> <p>Toteutetaan tarvittavat integraatiot ja liittymät muuhun ympäristöön ja varmistetaan integraatioiden tietoturvallisuus.</p> <p>Suoritetaan tietojärjestelmän hyväksyntätästä.</p> <p>Tehdään hyväksyntä tietojärjestelmän käyttöönotosta.</p>
<b>Ylläpito</b>	<p>Riskejä ja suojaustason asianmukaisuutta katselmoidaan ja arvioidaan säännöllisesti.</p> <p>Tunnistetaan käsittely-ympäristössä ja vaatimuksissa tapahtuvien muutosten vaikutuksen tietojärjestelmään sekä niiden edellyttämät muutokset tietoturvakontroleihin. Muutoksissa noudatetaan määriteltyjä muutos-hallintamenettelyitä.</p> <p>Tietojärjestelmää ylläpidetään tehtyjen suunnitelmien mukaisesti. Tässä yhteydessä huolehditaan muun muassa päivityksistä, varmuuskopiointista, konfiguraation hallinnasta, kovennuksista ja haittaohjelmasuojauksesta.</p> <p>Tietojärjestelmää koskevaa dokumentaatiota ja kuvauksia päivitetään tehtyjen muutosten mukaisesti.</p> <p>Tietojärjestelmää valvotaan jatkuvasti tunnistettujen riskien mukaisesti.</p>
<b>Käytöstä poisto</b>	<p>Laaditaan ja hyväksytään käytöstä poistolle suunnitelma.</p> <p>Suunnitellaan ja toteutetaan säilytettävän tiedon migraatio.</p> <p>Sanitoidaan tuhottavat laitteet poistaen niissä olevat tiedot luotettavasti.</p> <p>Tuhotaan käytöstä poistuvan tietojärjestelmän osat.</p>

## 6 Vahingoilta suojaaminen (TiHL 15.1§)

*Viranomaisen on varmistettava tarpeellisin tietoturvaluustoimenpitein, että sen:  
2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;*

Viranomaisella tulee olla varmuus siitä, että käsiteltävä tieto tai järjestelmä on suojattu fyysisiltä vahingoilta kuten tulipalot, vesivahingot tai ilkivalta sekä sähköisiä menetelmiä käyttäen aiheutetuilta fyysisiltä vahingoilta kuten laitteiden rikkoutuminen. Tietoa tai järjestelmää tulee suojata asianmukaisin, mutta riskiarvioinnin perusteella tarkoituksenmukaisin toimin. Lisätietoja järjestelmän vaikutusten ja riskien arvioinnista on luvussa 2.

Viranomaisen tulisi määritellä kullekin tietoaineistolle hyväksytyt sijainnit, joissa sähköisessä ja paperisina olevia aineistoja ja tietovarantoja voidaan käsitellä ja myös säilyttää. Sijaintien määrittelemisessä pitää huomioida palvelujen toteuttamistapa, kuten palveluntuottajat, pilvipalvelut ja tiedon käsittelyn fyysinen sijainti.

Tyypillisesti palveluntarjoajat säilyttävät ja ylläpitävät tietojen ja tietojärjestelmien käsittelyssä tarvittavia fyysisiä tiloja ja laitteita tai näiden hankinnan sopimusta, kuten pilvipalvelut. Tällöin palveluntarjoajien kanssa on varmistettava fyysisen turvallisuuden vaatimusten toteutuminen. Viranomaisen tulee huomioida, että erilaisiin tietoaineistoihin (esim. salassa pidettävät tai henkilötiedot) kohdistuu erilaisia suojausvaatimuksia, jotka aiheuttavat lisävaatimuksia palveluntarjoajaa ja/tai viranomaista kohtaan.

Viranomaisen tulee huomioida tiedon ja tietojärjestelmien fyysisen turvallisuuteen liittyen seuraavat seikat:

- Rakenteellinen turvallisuus: Tilojen rakenteiden tulee täyttää niihin kohdistuvat vaatimukset. Lisätietoja rakenteellisista suosituksista löytyy Kansallisen auditointikriteeristön F-osiosta. Lisätietoa pysyvästi säilytettävien asiakirjallisten tietojen arkistotiloja koskevista määräyksistä ja vaatimuksista löytyy Kansallisarkiston asiakirjasta Määräys ja ohjeet arkistotiloista.
- Turvallisuusalueet: Mikäli tiloissa säilytettävään tietoon kohdistuvat vaatimukset sitä edellyttävät, tulee toimitilat olla jaettu turvallisuusalueisiin, joiden tarkoituksena on estää tai riittävästi hidastaa oikeudettomien tahojen pääsy käsiksi tietoon tai tietojärjestelmään.
- Salassapidettävien tietojen suojaaminen tapahtuu rakenteellisin, teknisin ja hallinnollisin keinoin. Hallinnollisen suojaamisen keinoja ovat esimerkiksi pääsyoikeudet salassapidettävään tietoon ja asianmukaiset salassapidettävän tiedon käsittelymenetelmät. Lisäksi kriittisiin tiloihin tai tietoihin pääsyä voidaan rajoittaa esimerkiksi turvallisuusselvitysten ja vaitiolositoumusten avulla.
- Olosuhdevalvonta: Tiloissa tulee olla säilytettävän tiedon ja tietojärjestelmä vaatimuksiin nähden riittävä olosuhdevalvonta esimerkiksi tulipalon, vesivahingon, kaasuvuodon, pölyn ja värinän varalta. Organisaatio määrittää tason riittäväälle olosuhdevalvonnalle riskienarvioinnista saatujen tuloksien avulla.
- Henkilöstöturvallisuus: Henkilöstö tulee kouluttaa tietojen käsittelyyn ja organisaation vierailijakäytäntöihin. Ne sisältävät muun muassa ohjeet siitä, mille alueille ulkopuolisia henkilöitä saa organisaation tiloissa viedä ja miten toimia, jos ulkopuolinen henkilö havaitaan väärissä tiloissa ilman saattajaa.
- Varavoima ja UPS: Tietojärjestelmillä tulisi olla käytössä UPS-ratkaisu yllättävien virtapiikkien tai sähkökatkosten varalta. Se mahdollistaa järjestelmän toiminnan siksi aikaa, kunnes se voidaan ajaa hallitusti alas ja siirtyä jatkuvuussuunnitelman mukaiseen toimintaan.

Lisätietoja toimitilaturvallisuuteen liittyvistä vaatimuksista ja ohjeistuksista löytyy VAHTI 2/2013 – Toimitilojen tietoturvaohjeesta.

Kriittiset järjestelmät tulisi kahdentaa, niin että toimintaa voidaan jatkaa toisesta konesalista tai sijainnista käsin silloin, kun toiminta ensisijaisessa ylläpitosijainnissa on estynyt. Tietoaineistojen osalta tulee huomioida tiedon turvallisuusluokittelun kautta tulevat tiedon käsittely- ja säilytysvaatimukset ja toteuttaa nämä asianmukaisesti.

## 6.1 Yleisiä vaatimuksia

Seuraavat yleiset vaatimukset tulisi huomioida vahingoilta suojaamisessa:

- Täyttääkö palveluntarjoaja tietoturvasuhteet fyysisen turvallisuuden osalta, kun on huomioitu käsiteltävän tiedon turvallisuusluokittelu tai tietojärjestelmän kriittisyys?
- Onko pääsy suojattavaan tietoon rajattu vain niihin henkilöihin, joilla on oikeus käsitellä tietoja?
- Onko kriittiset järjestelmät kahdennettu siten, että toimintaa voidaan jatkaa, mikäli ensisijainen ylläpitosijainti ei ole käytössä?
- Mikäli viranomaisella ylläpitää tietojärjestelmiä itse, onko tietojen turvallisuusluokituksista ja/tai järjestelmän kriittisyydestä johtuvat vaatimukset huomioitu ja täytetty?
  - Onko fyysiset tilat eroteltu turvallisuusvyöhykkeisiin?
  - Ovatko tilojen rakenteelliset ratkaisut riittävät?
  - Onko tiloissa olosuhdevalvonta tulipalon ja kosteusvaurioiden varalle?
  - Onko käytössä varavoimaratkaisu, joka takaa järjestelmän riittävän toiminnan hallitun alasajon ajaksi?

## 6.2 Säädökset ja lisätiedot

Kansallinen auditointikriteeristö Katakri 2015 – Tietoturvasuhteiden auditointityökalu viranomaiselle

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

VAHTI 2/2014 – Tietoturvasuhteiden arviointiohje

VAHTI 2/2013 – Toimitilojen tietoturvaohje

VAHTI 2/2012 – ICT-varautumisen vaatimukset

Kansallisarkiston Määräys ja ohjeet arkistotiloista

## 7 Lokitietojen kerääminen (TiHL 17§)

*Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.*

### 7.1 Lähtökohdat

Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen perusteella voidaan selvittää virhetilanteita ja valvoa tietojärjestelmien käyttöä muun muassa oikeusturvan toteuttamiseksi, häiriötilanteesta toipumiseksi, virkavastuun todentamiseksi sekä häiriöiden ja riskin muodostavien poikkeamien tunnistamiseksi. Lokitiedot ovat tietojärjestelmistä automaattisesti kirjautuvia tapahtumatietoja. Niitä ovat tietojärjestelmän, sovelluksen tai laitteen tuottamat tapahtumatiedot, jotka kuvaavat esimerkiksi tietojärjestelmään ulos- tai sisäänkirjautumista, tiedon käsittelyä (katselu, lisäys, muutos, poisto) tai palomuurin suorittamaa toimenpidettä.

Lokitietoja tarvitaan sekä normaali- että poikkeamatilanteissa. Normaalityötilanteissa lokien avulla toteutetaan muun muassa toiminnan häiriöttömyyden seuranta, käytönvalvontaa, tilastointia ja laskutusta. Poikkeustilanteissa lokeja käytetään muun muassa syiden selvittämiseen, tilanteen normalisointiin sekä tapahtumien ja niiden osapuolten tunnistamiseen. Lokitietojen käsittelyn yhtenä tavoitteena on siis varmistaa tapahtumien osapuolet, kulku ja tapahtumaketjun kiistämättömyys sekä kykyä havaitsemaan ja hallitsemaan tunkeutumisyrittäjiä, poikkeamia, häiriöitä ja suorituskykyongelmia. Poikkeamien ja häiriöiden tunnistamisen lisäksi lokitietoja voidaan hyödyntää myös nykytilan seuraamiseen ja visualisointiin, trendien tunnistamiseen ja tulevan ennustamiseen sekä päätöksenteon ja toiminnan tukemiseen.

Lokitiedot eivät ole välttämättä aina tietojärjestelmistä muodostuvia sähköisiä lokitietoja, sillä tietoaineistojen käsittely ja luovuttaminen voi olla myös manuaalista paperisia tietoaineistoja koskevaa käsittelyä. Tällöin suositukset on huomioitava soveltuvin osin paperiaineistojen käsittelyä koskevan seurannan suunnittelussa ja toteuttamisessa.

## 7.2 Lokitiedot

Lokitiedot kuvaavat jonkin tapahtuman toteutumista tietyinä hetkenä ja niiden on kyettävä esittämään tarvittavat tiedot tapahtumista luotettavasti kirjatun tapahtumaketjun (audit trail) muodostamiseksi. Lokitietoja kerätään erityyppisistä toimenpiteistä, kuten tietojärjestelmien käytöstä ja tiedon luovutuksista, tietojärjestelmien ylläpidosta sekä niiden teknisestä toiminnasta ja virheistä.

Lokitietojen kerääminen on sidottu tietojen tarpeellisuuteen, jota arvioidaan riskiperusteisesti. Lokitietojen kerääminen tietojärjestelmän käytöstä ja tietojen luovutuksista on tarpeellista erityisesti silloin kun tietojärjestelmässä käsitellään salassa pidettäviä tietoja. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, luovuttavassa järjestelmässä kerätään luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen peruste. Käyttölokitietojen keräämisen tarvetta arvioidaan erityisesti sillä perusteella, tarvitaanko niitä virheselvittelyjä varten tai yksilön etujen, oikeuksien ja velvollisuuksien sekä oikeusturvan toteuttamiseksi tai virkavastuun todentamiseksi. Tietojärjestelmien ylläpitotoimista kerättävät lokitiedot kuvaavat tietojärjestelmän toimintaan ja käyttöoikeuksiin tehtyjä muutoksia ja tekniset järjestelmä- ja virhelokit kuvaavat muun muassa teknisiä virheitä ja toimintahäiriöitä.

## 7.3 Lokienhallinnan suunnittelu ja ohjaus

Lokien kerääminen ja käsittely perustuvat lakiin. Lokienhallinnan toteuttamista ja lokitietojen käsittelyä organisaatiossa kuvataan ja ohjataan lokiperiaatteissa ja -suunnitelmassa, jotka ottavat kantaa lokien käsittelyyn liittyviin rooleihin ja vastuisiin, lokien käsittelyn elinkaaren vaiheisiin (miten niitä kerätään, käsitellään ja säilytetään), käsittelyn tarpeeseen ja perusteeseen sekä lokienhallinnan tekniseen toteutukseen.

Lokitietoja ei kerätä ja käsitellä summittaisesti, vaan määritellyn tarpeen pohjalta laadittujen lokiperiaatteiden ja -suunnitelman mukaisesti. Ennen tietojärjestelmän ja siihen liittyvien lokijärjestelyiden toteuttamista toteutus, käytötapa sekä kerättävien ja käsiteltävien tietojen tarpeellisuus selvitetään ja kuvataan. Lainsäädäntö asettaa myös



suojausveloitteita tietojen, erityisesti henkilötietojen, suojelemiseksi. Tämä tarkoittaa sitä, että tietojen suojaustarpeet tunnistetaan ja huomioidaan lokien käsittelyn, tieto- ja lokijärjestelmien sekä järjestelmähankintojen suunnitteluvaiheessa.

Osana lokienhallinnan suunnittelua ja sitä ohjaavan dokumentaation laatimista:

- Tunnistetaan lokitietoihin ja lokien käsittelyyn liittyvät ulkoiset vaatimukset lainsäädännöstä, määräyksistä ja mahdollisista sopimuksista
- Määritellään toimintatavat lokienhallinnalle ja käsittelylle
- Määritellään lokien käsittelyprosessi ja -tavat sekä käsittelyyn liittyvät roolit ja vastuut
- Määritellään prosessi lokienhallinnan ja käsittelyn asianmukaisuuden ja lainmukaisuuden säännölliseksi arvioimiseksi
- Tunnistetaan miksi ja mihin tarkoitukseen kutakin lokia käsitellään
- Tunnistetaan tietojärjestelmät ja laitteet, joiden tulisi tuottaa lokitietoja, kuten kriittiset tietojärjestelmät ja salassa pidettävän tiedon käsittelyyn tarkoitetut tietojärjestelmät
- Arvioidaan tallennettavien tietojen tarpeellisuus
- Tunnistetaan lokeihin tallentuvat tietotyypit, erityisesti henkilötiedot ja tunnistamistiedot.
- Tunnistetaan tallentuvien tietotyyppien suojaustarpeet.
- Määritetään suojaustarpeet ja tavat (kuten salaus, varmuuskopiointi, pääsynhallinta) lokien suojaamiseksi
- Varmistetaan, että tietojen suojaustarve toteutuu järjestelmän toteutuksessa ja tietojen käsittelyssä.
- Huomioidaan tarve lain yksityisyyden suojasta työelämässä mukaiselle yhteistoimintamenettelylle, mikäli kyseessä on tekninen valvonta.
- Huomioidaan yhteistoimintamenettelyn lisäksi muu käyttäjien, rekisteröityjen tai muiden tahojen informointi.
- Huomioidaan henkilötietojen käsittelyä koskevat lainsäädännön (kuten tietosuoja-asetus ja tietosuojalaki) asettamat vaatimukset, jos lokit sisältävät henkilötietoja.
- Suunnitellaan ja dokumentoida säilytystarve ja varmistaa sen toteutuminen käytännössä.
- Määritellään lokien keräämiseen liittyvät konfiguraatiot tietojärjestelmille ja laitteille

Lokeihin liittyvät vaatimukset määritellään ja edellytetään toteutettavaksi myös järjestelmäkehityksen, hankinnan tai ulkoistuksen yhteydessä lisäämällä ne osaksi näitä koskevia vaatimusmäärittelyitä, suunnitelmia ja sopimuksia. Toimittajilta edellytetään kuvausta omalla vastuullaan olevien järjestelmien tai toimintojen lokien keräämiseen, tallennukseen ja analysointiin liittyvistä asioista. Sopimuksen teon yhteydessä määritellään myös lokien käsittelyyn liittyvät vaatimukset ja käytännöt, lokitiedot omistava organisaatio ja omistajan mahdollisuudet saada lokitietoja käyttöönsä tarpeen vaatiessa. Organisaatio voi kerätä lokitietoja myös käyttämistään, palveluntarjoajien omistamista tietojärjestelmistä ja palveluista.

Lokitietojen käsittelyyn sekä etenkin keräämiseen, säilyttämiseen ja säilytysaikoihin voi kohdistua vaatimuksia erityislainsäädännöstä sekä määräyksistä ja standardeista. Nämä on tunnistettava ja huomioitava osana lokienhallintaa.

## 7.4 Lokitietojen kerääminen

Lokitietoja tuotetaan ja kerätään tietojärjestelmän käytöstä ja tietojen luovutuksista, mutta missä laajuudessa ja mitä lokitietoja, perustuu tiedonhallintalain mukaiseen tarpeellisuusarviointiin. Siihen pohjautuvat lokitietojen keräämisen peruste ja laajuus (mitä lokitietoja kerätään) sekä lokitietojen käyttötarkoitus ja käsittelyn laajuus (miten ja kenen toimesta niitä käsitellään). Tarpeellisuusarviointiin vaikuttaa myös yleisessä tietosuojalainsäädäntöön säädetty vaatimukset teknisten ja organisatoristen toimenpiteiden toteuttamiseksi henkilötietojen suojaamiseksi. Tarpeellisuusarvioinnin tekee tietojärjestelmästä vastuussa oleva viranomaisena.

Lokitietojen käyttötarve määrittelee sen, mitä tietoja lokitietoina kerätään tietystä tietojärjestelmästä. Jokaisen kerättävän lokitiedon tulee sisältää – tarpeellisuusarvioinnin mukaisesti – riittävät tiedot tarvittavan luotettavan tapahtumaketjun muodostamiseksi sekä tapahtumien valvomiseksi ja analysoimiseksi. Lokin käyttökelpoisuus riippuu siihen kerättävien tietojen riittävydestä lokin käsittelytarkoitusta varten. Lokitiedot kuvaavat lokeille aina riittävässä laajuudessa jokaisen tapahtuman osalta sen, milloin, missä, kuka ja mitä:

- Milloin (milloin tapahtuma oli?)
  - Lokitiedon aikaleima eli päivämäärä ja kellonaika
  - Tapahtuman aikaleima päivämäärä ja kellonaika (lokitiedon ja tapahtuman aikaleima voivat joskus myös erota toisistaan)
  - Tapahtuman tunniste

- Missä (mihin tietoon ja/tai järjestelmään tapahtuma ja toiminta kohdistuivat?)
  - Tapahtuman kohteen (tietojärjestelmän, laitteen, sovelluksen) tunnistetiedot, kuten nimi, kohdeosoite, laitteen identiteetti ja tunnistetiedot, yhteystapa, käytetty protokolla sekä sijainti
  - Tapahtuman kohdetta kuvaavat tiedot, kuten missä tietojärjestelmän, sovelluksen tai palvelun osassa ja mihin elementtiin tai tietoon tapahtuma on kohdistunut
- Kuka (toimija eli kuka tai mikä teki ja mikä oli tapahtuman lähde?)
  - Tapahtuman lähteen (ihmis- tai laitekäyttäjän) tunnistetiedot, kuten nimi, lähteosoite, henkilön tai laitteen identiteetti ja tunnistetiedot, sijainti
  - Millä oikeuksilla ja valtuuksilla tapahtuma tehtiin
- Mitä (mitä tapahtui ja onnistuiko tapahtuma?)
  - Tapahtuman tyyppi, kuten objektin luominen, objektin muuttaminen, kirjautuminen tai järjestelmän kaatuminen
  - Tapahtuman tila (onnistuiko vai epäonnistuiko tapahtuma ja miksi se mahdollisesti epäonnistui)
  - Tapahtuman merkitys tai prioriteetti
  - Tapahtuman kuvaus

Lokiin ei lähtökohtaisesti tule kerätä seuraavan kaltaisia tietoja:

- henkilötunnuksia
- erityisiä henkilötietoja (ns. arkaluonteiset henkilötiedot)
- luottokorttinumeroita
- salasanoja (ei edes tiivistemuotoisia)
- järjestelmien välisiä käyttöavaimia ja salaisuuksia
- valtuutustietoja
- henkilöiden välisen viestiliikenteen sisältöä
- lähdekoodia
- lokienhallintajärjestelmää korkeampaa turvallisuuden tasoa edellyttäviä tietoja

Lokilähteet ovat tietojärjestelmiä, sovelluksia tai laitteita, jotka tuottavat lokitietoja. Lokia tuottavina lokilähteinä voivat toimia muun muassa:

- sovellukset
- käyttöjärjestelmät
- palvelimet
- päätelaitteet
- verkkolaitteet
- palomuurit
- pääsynhallinta
- tunkeutumisenestojärjestelmä (IPS)
- tunkeutumisenhavaitsemisjärjestelmä (IDS)
- virustorjuntaohjelmat

Mikäli käytössä on useita lokeja, niin niiden helposti tapahtuva yhdistely analysointitarpeita varten on hyvä mahdollistaa. Lokia tuottavien lokilähteiden kellojen synkronoinnilla varmistetaan, että eri järjestelmien tuottamat lokitiedot ovat keskenään yhtenäisiä ja jotta niistä voidaan muodostaa yhtenäinen tapahtumaketju. Erityisesti lokilähteiden aikaleimojen on tarve olla samassa ajassa. Eri lokeja tuottavien järjestelmien aika on mahdollista synkronoida NTP:n (Network Time Protocol) avulla. Myös lokien aikavyöhyketiedot on hyvä tallentaa. Suositeltavaa on käyttää UTC-aikaa kaikissa lähteissä.

Käyttö- ja luovutuslokien tietosisällön suunnittelu on yleensä järkevää tehdä koko järjestelmän tietosisällön ja käyttötapauksien määrittelyn yhteydessä, kuitenkin niin, että lokitapahtumien lisääminen ja poistaminen on helppoa järjestelmän elinkaaren kaikissa vaiheissa. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokien tiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen perusteensa. Jos tietoaineistojen luovutus tapahtuu tietojärjestelmien ulkopuolella, paperimuodossa, on luovutuslokien kirjaaminen suunniteltava myös tämän osalta.

Käyttöä, muutoksia ja luovutuksia koskevien lokitietojen keräämistä määriteltäessä arvioidaan muun muassa seuraaventyyppisten tietojen tarpeellisuutta:

- tiedot tietojen tallentamisesta, muuttamisesta, poistamisesta, katselusta tai muusta tietoihin kohdistuvasta toimenpiteestä sisältäen tiedot mm.
- tietosisällön lisäyksistä ja poistoista (voidaan kutsua myös muutoslokiksi),
- tietosisällön muutoksista ja epäonnistuneista kirjauksista (voidaan kutsua myös muutoslokiksi),
- tietokannan lukutapahtumista ja kyselytiedoista hakuehtoineen,
- tulostuksesta ja
- tietojen luovutuksista
- tiedot sisään- ja uloskirjautumisista käyttäjä-, ryhmä- ja sovellustietotasolla (voidaan kutsua myös pääsynvalvontalokiksi)

Teknisen lokin tietosisältö on tyypillisesti vähemmän tarkasti määritelty kuin käyttölokien, mutta erityistä huomiota on kiinnitettävä siihen, ettei tekniseen lokiin kerry sellaista salassa pidettävää tietoa, joka ei ole välttämätöntä järjestelmän käytön selvittämisen kannalta. Tällaisia voivat olla esimerkiksi tarkemmat kuvaukset käsittelystä tietosisällöstä tai erityisiä henkilötietoryhmiä, kuten terveyttä, koskevat tiedot. Tietojärjestelmien ylläpito- toimia ja teknisiä järjestelmä- ja virhetietoja koskevien lokitietojen keräämistä määriteltäessä arvioidaan muun muassa seuraavan tyyppisten tietojen tarpeellisuutta:

- tiedot käyttöoikeuksien muutoksista, poistoista ja lisäyksistä,
- tiedot järjestelmään tehdyistä muutoksista,
- tiedot järjestelmien järjestelmäparametrien ja asetustiedostojen muutoksista.

- tiedot seurattavassa tietojärjestelmässä tai tapahtumassa havaituista virheistä,
- tiedot käyttöön liittyvien virhetilanteiden hallinnasta ja
- tiedot havaituista virheistä ja epäjatkuvuuksista.

Tietojärjestelmän käyttöä koskevien lokitietojen ja keräämisen ja seurannan merkitys korostuu erityisesti, kun tietojärjestelmässä käsitellään salassa pidettäviä tietoja. Lokitietojen tarkoituksena on myös dokumentoida tietojärjestelmistä tehtävät luovutukset ja samalla osaltaan varmistaa, että luovutuksille on ollut olemassa lainmukainen peruste. Tämä korostuu erityisesti silloin, jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja.

Samaan järjestelmään liittyvät erilaiset lokit on hyvä toteuttaa niin, että niiden tietoja voidaan yhdistää ja erotella. Mikäli erilaiset lokitiedot on kerätty yhteen lokiin, on tietojen suositeltavaa olla sellaisessa muodossa, että kiinnostavia käyttötapauksia pystytään seuraamaan niin, ettei esimerkiksi teknisen lokiaineiston runsaus hankaloita näiden seuraamista.

Lokitiedot ovat osa viranomaisten tietojärjestelmien tietoturvajärjestelyjä, joten ne ovat salassa pidettäviä julkisuuslain 24 §:n 1 momentin 7 kohdan perusteella, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista.

## 7.5 Lokitietojen säilyttäminen

Lokitietojen säilyttämisen suunnittelussa määritellään lokien säilytysaika ja -paikka. Säilytysaika johdetaan aina niiden käyttötarkoituksesta. Viranomaisen on hyvä tunnistaa ne lokitiedot, joiden säilytysaika on tyypillisesti vähintään viisi vuotta rikosoikeudellisten vanhentumisaikojen vuoksi. Erityislainsäädännössä voi olla säädetty erikseen lokitietojen säilytysajoista etenkin, jos lokitietoja säilytetään pitempiä aikoja kuin on tarpeen viranomaisella olevien velvollisuuksien toteuttamiseksi. On tärkeää varmistaa, että lokitiedot säilyvät ja ovat käytettävissä koko määritellyn säilytysajan, jonka jälkeen ne on poistettava.

Teknisten lokien säilytysajan tulee olla riittävän pitkä, jotta niitä voidaan käyttää erilaisen järjestelmän toimivuuteen liittyvien ongelmien selvittämiseen. Tietoturvaan liittyvät tapahtumat (kuten erilaiset väärinkäytökset tai tietojen luvaton käyttö), voivat olla sellaisia tapahtumia, jotka havaitaan vasta kauan tapahtuman jälkeen. Tämä huomioidaan lokien säilytyksessä siten, että esimerkiksi teknisiä lokeja, joissa on ainoastaan teknisiä ongelmia koskevia tietoja, suositellaan säilytettäväksi vähintään 6 kuukautta, mutta tietomurtotapausten selvittelyyn edellä mainittu 6 kuukauden säilytysaika on useimmiten sen sijaan riittämätön. Myös käyttö- ja luovutuslokin muuttumattomuudesta voi olla mahdotonta varmistua, mikäli keskeiset tekniset lokit eivät ole käyttölokeja vastaavan säilytysajan piirissä.

Edellä mainittujen tarpeiden täyttämiseksi keskeisille teknisille lokeille suositellaan yleisesti vähintään 5 vuoden säilytysaikaa.

Lokien säilyttämistarve voi edellyttää pidempiä säilytysaikoja, kuin mitä esimerkiksi lokia tuottava sovellus tai tietojärjestelmä ja tallennuskapasiteetti tukevat, jolloin syntyy tarve lokien arkistoinnille. Lokien pitkäaikaissäilytyksellä tarkoitetaan lokien säilyttämistä pidennetyn ajan. Lokit voidaan siirtää pidempiaikaiseen säilytykseen esimerkiksi erilliselle lokipalvelimelle tai tähän tarkoitettuun muulle laitteelle, jottei lokia tuhoeta normaalin lokikierroksen mukaan säilytysaikaa lyhemmissä ajassa. Lähtökohtaisesti on kuitenkin aina suositeltua toteuttaa keskitetty lokienhallinta, jossa lokit siirretään lähdejärjestelmästä erilliseen keskitettyyn lokienhallintajärjestelmään, mikä mahdollistaa myös tehokkaamman lokien seurannan ja analysoinnin.

Lokien keräämistä varten on suunniteltu tarvittavat toimintamallit ja infrastruktuuri, jotta lokeille on varattu riittävästi säilytystilaa suhteessa kerättävien lokien määrän ja niiden säilytysaikaan. Säilytystilan suunnittelussa ja toteutuksessa on huomioitu myös se, ettei lokien kerääminen pysähdy lokin tai lokitilan täytyessä. Lokien säilytyskapasiteettia seurataan ja siihen liittyvistä ongelmista on tärkeä luoda hälytyksiä.

Kun lokitietojen käsittelylle ei ole enää tarvetta ja niiden säilytysaika on umpeutunut, ne joko poistetaan tai anonymisoidaan. Lokitietojen tyhjentäminen on automatisoitu poistamaan alkuperäisestä lokista kaikki lokitiedot, jotka ylittävät määritetyn säilytysajan. Tässä yhteydessä tulee huomata, että lokeja on tyypillisesti myös tallennettu varmistusnauhoille tai muille vastaaville tallennus- ja arkistointivälineille, joista tiedot tulee tarvittaessa myös poistaa. Tietojen poistamisessa tulee huomioida, onko tietojen poistaminen mahdollista vaarantamatta tiedon eheyden säilymistä. Varmistusnauhoille tai muille vastaaville tallennus- tai arkistointivälineille tallennettujen tietojen poistamisessa tulee huomioida varmistusten eheyden säilyminen.

## 7.6 Lokitietojen seuranta ja analysointi

Tarvittavan havainnointikyvykkyyden luomiseksi ja ylläpitämiseksi lokitietoja on seurattava ja analysoitava säännöllisesti. Lokeja koskevan seurannan, analysoinnin ja hälytysten tuottamisen tarkoituksena on luoda etenkin kriittisten kohteiden ja tietojen kohdalla mahdollisimman reaaliaikainen havainnointikyvykkyys, jotta tarvittaviin toimenpiteisiin on mahdollista ryhtyä nopeasti.

Lokitietojen seuranta ja valvonta palvelevat myös tiedonhallintalain 13.1§ edellytettyä tietoturvallisuuden tilan seurantaa.

Lokien analysoinnissa ja ymmärtämisessä on tärkeää ymmärtää jokaisen lokia tuottavan järjestelmän ja sitä käyttävän käyttäjän normaali, tyypillinen toiminta. Tavoitteena on saada käsitys normaaleista lokitietoja muodostavista tapahtumista, jotta saadaan vertailukohta epätavallisille lokitapahtumille. Ajan kuluessa opitaan tunnistamaan järjestelmän normaalitoiminta ja kyetään erottamaan siitä eroavat epätavalliset lokitapahtumat.

Lokitietojen seurannan ja analysoinnin osalta on määritetty:

- kuinka usein ja mitä lokitietoja seurataan ja analysoidaan
- kenellä on pääsy lokitietoihin ja millaista lokitietoa tuotetaan itse lokitietojen käsittelystä
- miten toimitaan, kun havaitaan lokitiedoissa reagointia vaativia poikkeamia (lokienhallinnan liityntä esimerkiksi poikkeamienhallintaprosessiin)
- miten lokitietoja ja niiden pohjalta muodostettua informaatiota hyödynnetään toiminnassa sekä sen johtamisessa ja kehittämisessä tai tietojärjestelmien ylläpidossa
- miten ennaltaehkäistään luottamuksellisen tiedon, kuten salasanojen, arkaluonteisen henkilötiedon ja viestinnän sisällön paljastumista sekä kuinka käsitellään tällaisen tiedon tahaton paljastuminen.

Koska laajoja ympäristöjä koskevien lokitietojen manuaalinen analysointi on työlästä ja jopa mahdotonta, pyritään lokienhallintaan liittyvillä työkaluilla ja ratkaisuilla automatisoimaan lokitietojen seurantaa ja analysointia. Normaalikäytöstä poikkeavat tapahtumat pyritään automaattisesti tunnistamaan ja suodattamaan, jotta niihin voidaan reagoida hälytyksin ja manuaalisin toimin sekä automaattisin tietoturvakontrollein. Suodattaminen mahdollistaa myös manuaalisen analysoinnin priorisointia, kun siinä voidaan keskittyä tehokkaasti ja helposti ainoastaan merkitykselliseksi tunnistettuihin lokitapahtumiin.

Tehokkaamman lokitietojen seurannan, analysoinnin ja suojauksen toteuttamiseksi hyödynnetään keskitettyjä lokienhallintaratkaisuja, jotka tukevat poikkeamien tunnistamista ja suodattamista normaaleista tapahtumista, tietoturvaloukkausten havaitsemista, epäselvän ja harhaanjohtavan datan hallintaa sekä tehokasta reagoimista. Käytetyt ratkaisut

hyödyntävät lokitietojen ja tapahtumien analysoinnissa valmiiksi määritettyjä sääntöjä ja raja-arvoja sekä normaalikäytöstä ja ihmisten ja tietojärjestelmien toiminnasta muodostettuja käyttäytymismalleja verran näitä tapahtumista ja toimista muodostettuihin lokitietoihin tunnistuen anomaliaita eli poikkeamia ja epätavallisuutta normaalista.

Hälytysten muodostamiseksi ja analysoinnin priorisoimiseksi on määritetty malli lokitietojen suodattamiselle ja priorisoinnille, joka huomioi muun muassa:

- lokimerkinnän tyyppin, kuten tapahtumaa kuvaavan luokan
- lokimerkinnän harvinaisuuden tai poikkeuksellisuuden (täysin uuden tyyppinen lokimerkintä)
- lokimerkinnän kohteen (esim. kriittinen tietojärjestelmä tai tieto)
- tapahtuman poikkeuksellisuuden (esim. tapahtuman normaalista poikkeava ajankohta tai ilmaantumistiheys)

Jotta lokitietojen seuraamiseksi ja analysoimiseksi sekä poikkeaviin tilanteisiin reagoimiseksi on tarvittava kyvykkyys, organisaatio on varannut riittävät ja osaavat resurssit toimenpiteiden suorittamiseksi. Lokien seurantaan ja analysointiin ja poikkeamienhallintaan voidaan käyttää sekä sisäisiä että palveluna hankittuja resursseja. Lokien seuranta ja analysointi on liitetty organisaation muihin prosesseihin, kuten poikkeamienhallintaprosessiin, joka käynnistyy esimerkiksi tietoturvapoikkeaman havaitsemisesta lokienhallinnan avulla.

## 7.7 Lokitietojen luovuttaminen

Lokitietoja voidaan luovuttaa muun muassa muille viranomaisille tietoturvapoikkeamien ja rikosten selvittelyä varten. Lokitietojen tiedonsaantioikeudet ratkaistaan julkisuuslain tai erityislakien perusteella. Erityislainsäädäntö voi tietyillä toimialoilla mahdollistaa henkilöille muun muassa lokipyyntöjen ja tarkastuspyyntöjen tekemisen, jolloin organisaatiolla on oltava prosessi ja toimintamallit pyyntöihin reagoimiseksi.

Organisaation on varmistettava lokitietojen kerääminen ja saatavuus sopimuksellisesti, jos tietojärjestelmä on toteutettu ostopalveluna ja palvelutoimittaja huolehtii lokitietojen keräämisestä ja hallinnoinnista. Tällöin luovutusoikeus perustuu sopimukseen ja luovutuksen osapuolten asemaan lokitietojen tosiasiallisena omistajana.



## 7.8 Lokitietojen suojaaminen

Lokeihin muodostuu erilaisia tietoja, joilla on omat suojaustarpeensa. Tämä tietojen ja lokeihin kohdistuvien riskien muodostama suojaustarve sekä lokeihin kohdistuvat ulkoiset vaatimukset on tunnistettu lokien asianmukaisen suojaamisen toteuttamiseksi koko lokienhallintaympäristöön. Jotta lokitietoihin voidaan luottaa, on niiden eheys eli muuttumattomuus kyettävä turvaamaan estämällä lokitietojen oikeudeton muuttaminen tai tuhoaminen niiden säilytyksen ja siirron aikana. Lisäksi lokien luottamuksellisuus varmistetaan muun muassa asianmukaisen pääsynhallinnan avulla. Lokitietojen saatavuuden turvaamiseksi varmistetaan muun muassa niiden säilyminen ja käytettävyys koko lokien säilytysajan.

Lokit muodostavat yhden tietojärjestelmään kuuluvan tietoaineiston ja niiden turvallisuus on suositeltavaa varmistaa vähintään samalla tavoin kuin järjestelmän muiden tietoaineistojen turvallisuus. Tämä voidaan toteuttaa esimerkiksi siirtämällä lokitiedot toiseen, suojattuun järjestelmään, joka on eriytetty lokitiedot luoneesta tietojärjestelmästä. Hyvin toteutettu lokiympäristö onkin muista tietojärjestelmistä erillään oleva tietokanta, jonka eheys on varmistettu estäen lokien muokkauksen.

Lokien käsittelyn suunnittelussa ja toteuttamisessa on varmistettu, että lokien kirjoitusoikeus on vain sillä prosessilla, joka lokia tuottaa. Muilla prosesseilla, tietojärjestelmän käyttäjillä ja ylläpitäjillä ei tule ole kirjoitusoikeuksia lokitietoihin. Lokien käyttöoikeudet poikkeavat tietojärjestelmän varsinaisen tietosisällön käyttöoikeuksista. Lokeja koskevat käyttöoikeudet ja pääsynhallinta on määritelty ja sen noudattamista valvotaan samalla periaatteella kuin järjestelmän muun tietosisällön käyttöoikeuksia. Lokitiedon kohdalla on huomioitava erityisesti vaaralliset työyhdistelmät niin, että järjestelmän käyttäjällä tai ylläpitäjällä ei ole oikeuksia käsitellä omaa käyttölokiaan. Tyypillisesti tämä edellyttää käyttöoikeuksien rajaamista sekä hallinnollisella että teknisellä tasolla. Tämä tarkoittaa muun muassa vaarallisten työyhdistelmien tunnistamista ja määrittämistä ja näiden huomioista rooleja ja käyttöoikeuksia myöntäessä. Vaarallisten työyhdistelmien erottaminen on hyvä saada toteutettua myös teknisesti pakottamalla rajaten vaarallisia työyhdistelmiä muodostavien roolien myöntäminen samalle käyttäjälle.

## 7.9 Säädökset ja lisätiedot

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) 14 §

EU yleinen tietosuojasetus

Tietosuojalaki (1050/2018)

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018

VAHTI lokiohje (3/2009)

Kyberturvallisuuskeskus: Näin keräät ja käytät lokitietoja

Viestintäviraston ohje 04/2016, Lokien keräys ja käyttö

Katakri, osio I10

## 8 Tietoturvallisuus tietojärjestelmä-hankinnoissa (TiHL 13 §)

*Viranomaisten on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvaluustoimenpiteet. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.*

### 8.1 Tietoturvaluustoimenpiteiden sääntely hankinnoissa

Tiedonhallintalain 4 luvussa on säädetty tietoturvaluustoimenpiteiden toteuttamisen vähimmäisvaatimuksista. Ne kohdistuvat keskeisiltä osin tietoaineistoihin ja tietojärjestelmiin. Jotta viranomaistoiminnassa voidaan varmistua tietoturvaluustoimenpiteiden asianmukaisuudesta, on tietoturvaluustoimenpiteet määriteltävä jo tietojärjestelmien ja muiden ICT-palvelujen hankintojen valmisteluvaiheessa.

Tiedonhallintalain 13.4 § velvoittaa hankinnasta vastaavan viranomaisen varmistamaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvaluustoimenpiteet.

Laissa ei ole säädetty varsinaisesti tietojärjestelmiin tai tietoaineistoihin liittyvistä konkreettisista toimenpiteistä, vaan ne on määriteltävä ja toteutettava kussakin tietojärjestelmässä käsiteltävien tietojen laadun ja luonteen näkökulmasta. Lisäksi tietoturvaluustoimenpiteiden määrittelyyn ja toteuttamiseen vaikuttaa hankittavan tietojärjestelmän merkitys viranomaisen tehtävien hoidolle, lakisäateisten velvollisuuksien toteuttamiselle ja yhteiskunnan toiminnalle.

Tiedonhallintalain 13.1 §:ssä on säädetty tiedonhallintayksiköille velvollisuus seurata toimintaympäristönsä tietoturvaluuden tilaa ja varmistaa tietoaineistojen ja tietojärjestelmien tietoturvaluus koko niiden elinkaaren ajan.

Tiedonhallintalain 13.1 §:ssä on myös säädetty tiedonhallintayksikölle velvollisuus selvittää olennaiset tietojenkäsittelyyn kohdistuvat riskit, joiden perusteella tietoturvallisuus-toimenpiteet mitoitetaan ja suhteutetaan niihin vaatimuksiin, joita tiedonhallintalaissa tietoturvallisuus-toimenpiteille on säädetty. Hankintavaiheessa tulisi myös selvittää, miten tietoturvallisuuden tilaa seurataan tietojärjestelmän käytössä sen tuotantovaiheessa.

Euroopan unionin yleisessä tietosuoja-asetuksessa (EU) 2016/679 on säädetty sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamisesta. Tietosuoja-asetuksen resitaalin 78 mukaan sisäänrakennettu ja oletusarvoinen tietosuoja on otettava huomioon julkisten tarjouskilpailujen yhteydessä. Siksi hankintojen suunnitteluvaiheessa on selvittettävä ne tietosuoja-vaatimukset, jotka vaikuttavat hankinnassa tietoturvallisuus-toimenpiteiden määrittelyyn tarjouspyyntöasiakirjoihin.

Tietosuoja-asetuksen 25 (2) artiklan perusteella rekisterinpitäjän on suunniteltava ja toteutettava henkilötietojen käsittelyyn asianmukaiset tietoturvallisuus-toimenpiteet (tekniset ja organisatoriset toimenpiteet), joilla varmistetaan tietosuoja-asetuksessa säädettyjen tietosuojaperiaatteiden toteutuminen henkilötietojen käsittelyssä. Tietoturvallisuus-toimenpiteet on toteutettava siten, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

Tietojärjestelmän hankinnasta johtuvat tietoturvallisuusjärjestelyjen muutosten arviointi kuuluu tiedonhallintalain 5.3 §:ssä tarkoitetun tiedonhallinnan muutosvaikutusarvioinnin piiriin. Säännöksen mukaan suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa muun muassa tiedonhallintalain 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja -toimenpiteisiin. Säännöksessä tietojärjestelmän käyttöönotolla tarkoitetaan joko uuden tietojärjestelmän hankkimista tai käytössä olevan tietojärjestelmän uudistamista siten, että uudistuksella on vaikutusta tiedonhallintamallin sisältöön. Tiedonhallintalaissa tarkoitettu tietojärjestelmän käyttöönotto tarkoittaa jo hankintavaiheessa tehtävää muutosvaikutusarviointia muun muassa tietoturvallisuus-toimenpiteiden järjestämisen osalta. Muutosvaikutusarvioinnissa arvioidaan toimintaympäristöön kohdistuvat riskit ja suunnitellaan tarvittavat tietoturvallisuus-toimenpiteet suhteessa säädettyihin tietoturvallisuusvaatimuksiin.

Koska tiedonhallintalaissa on säädetty tiedonhallintayksikölle velvollisuus varmistaa sekä tietojärjestelmähankintojen toteuttamisessa että tietojärjestelmän elinkaaren ajan tietoturvallisuus-toimenpiteiden asianmukaisuus, on tiedonhallintayksikön suunniteltava sekä hankintamenettelylle, tietojärjestelmän käyttöönoton eri vaiheille että tietojärjestelmän

tuotantokäytölle riittävät kontrollit. Hankinnan ja toteutusprojektin turvallisuustoimenpiteiden ja -kontrollien on myös oltava toteutettavan järjestelmän turvallisuusvaatimusten mukaisia.

Tietoturvaluustoimenpiteiden suunnittelu ja dokumentointi tietojärjestelmähankinnoissa voidaan jakaa osiin:

- Hankintaohjeet
- Tarjouspyyntö
- Tarjousten sisältöjen arviointi
- Hankintasopimuksen laadinta
- Hankintasopimuksen toimeenpano.

## 8.2 Tietoturvaluus hankintaohjeissa

Tiedonhallintayksiköillä voi olla useita eri asiakirjoja, joilla ohjataan hankintojen toteuttamista. Tällaisia voivat olla esimerkiksi hankintasäännöt, taloussäännöt, hankintaohjeet, hankintastrategiat sekä tietojärjestelmien arkkitehtuurilinjaukset. Hankintojen toteuttamista ohjaaviin asiakirjoihin tulisi tarkentaa, miten hankintamenettelyssä toteutetaan tiedonhallintalaissa säädetyt vaatimukset hankinta-asiakirjojen tietoturvaluusasta käsittelystä. Hankinnan kohteen tietoturvaluustoimenpiteiden suunnitteluun vaikuttavat hankintojen toteutuksen yhteiset periaatteet kuuluvat myös asianmukaiseen hankintoja ohjaavaan dokumentaatioon. Tiedonhallintayksikössä noudatettavat tietoturvaluusperiaatteet voivat olla määriteltynä tiedonhallintamallissa, joten nekin vaikuttavat hankintojen suunnitteluun.

Hankintoja ohjaaviin asiakirjoihin tulisi sisällyttää:

- hankinta-asiakirjojen käsittelyä koskevat ohjeet, joista ilmenee, mitä tietoturvaluustoimenpiteitä hankinta-asiakirjojen käsittelyssä on noudatettava tiedonhallintayksikössä
- tarjouspyynnön mallipohja, joka sisältää tiedot tiedonhallintayksikössä noudatettavista yleisistä tietoturvaluustoimenpiteistä riippumatta hankintakohteesta
- sopimusmallin, jonka perusteella hankintakohdekohtaisesti hankintaan suunnittelevan vastuuhenkilön on kuvattava asianmukaiset tietoturvaluusvaatimukset ja -toimenpiteet tarvittavilta osin niin henkilö-, tietoliikenne-, tietojärjestelmä-, tietoaineisto- kuin toimintaturvaluisuuden osalta.

Julkisia hankintoja toteutettaessa on myös eri toimijoiden roolien oltava selkeät. Tiedonhallintayksiköstä on säädetty tiedonhallintalaissa. Se on viranomaisorganisaatio, kuten valtion virasto tai kunta. Tiedonhallintayksikkö voi koostua useammasta viranomaisesta, joista kukin voi olla hankintalaissa tarkoitettu hankintayksikkö. Tässä suosituksessa käytetään tiedonhallintayksikön käsitettä, koska tiedonhallintayksikkö toimii pääsääntöisesti viime kädessä hankintasopimuksen sopimusosapuolena, kuten kunta oikeushenkilönä, jota voi edustaa hankinnan tehnyt kunnallinen viranomaisen hankintayksikkönä.

### 8.3 Tietoturvaluusvaatimukset tarjouspyynnössä

Tiedonhallintayksikössä tarjouspyyntöasiakirjoihin sisällytettäviä tietoturvaluusvaatimuksia ja -toimenpiteitä määriteltäessä on hankinnan kohteesta riippuen otettava huomioon julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain (1397/2016) 3 §:ssä, julkisista puolustus- ja turvallisuushankinnoista annetun lain (1531/2011) 2 §:ssä sekä hallintolain (434/2003) 6 §:ssä säädetyt periaatteet. Tietoturvaluusvaatimukset ja niitä toteuttavat toimenpidevaatimukset on suhteutettava hankittavan tietojärjestelmän tietosisältöihin ja tietojärjestelmän merkitykseen viranomaisen toiminnan kannalta. Määriteltäessä tietoturvaluusvaatimuksia tarjouspyyntöön on huolehdittava siitä, että vaatimukset liittyvät hankinnan kohteena olevaan tietojärjestelmään sekä siihen liittyviin hankittaviin muihin palveluihin. Tietoturvaluusvaatimuksissakin on huomioitava edellä mainituista laeista johtuvat vaatimukset tarjoajien tasapuolisesta ja syrjimättömästä kohtelusta. Lisäksi lainsäädäntö edellyttää vaatimusten olevan kohtuullisia suhteessa hankittavaan tietojärjestelmään.

Tarjouspyynnön laadinnassa on suositeltavaa käyttää erilaisia valmiita tietoturvaluusustoimenpiteiden toteuttamisen vaatimuslistoja tai -kriteeristöjä, mutta niiden sisältö on sovitettava yhteen hankittavan tietojärjestelmän ja siinä käsiteltävien tietojen kanssa. Tiedonhallintalain asettamien vähimmäisvaatimusten ylittäviä vaatimuksia määriteltäessä on arvioitava niiden soveltuvuus ja suhteutettava ne hankinnan kohteeseen, koska ylimitoitettut ja turhat vaatimukset voivat aiheuttaa lisäkustannuksia sekä vaikuttaa hankinnan kohteen käytettävyyteen ja tehokkuuteen. Vaatimusten on oltava perusteltuja ja asianmukaisesti määriteltyjä.

Tarjouspyynnössä on myös selkeästi erotettava, mitkä ovat tietojärjestelmän tietoturvaluudelle määriteltäviä ehdottomia vaatimuksia ja mitkä tietoturvaluusustoimenpiteitä sisältävät määritykset ovat tietojärjestelmän laatuun liittyviä kriteereitä, joita käytetään mahdollisesti tarjousvertailussa. Tarjoajille määriteltävät vaatimukset ja tarjousvertailussa käytetyt kriteerit on erotettava selkeästi toisistaan. Epäselvä tarjouspyyntö voi johtaa siihen, että tarjouskilpailu joudutaan toteuttamaan uudestaan.

Tietoturvaluusvaatimusten on oltava niin selkeitä ja ymmärrettäviä, että alalla ammattimaisesti toimiva ja kohtuullisen valistunut tarjoaja saa niistä selon. Vaatimuksia sisältävät tarjouspyyntöasiakirjat on laadittava tavalla, joka mahdollistaa tarjoajille antaa selkeitä ja yksiselitteiset vastaukset niin tarjottavan tietojärjestelmän vaatimusten täyttämistä, kuin tarjousvertailussa käytettävistä kriteereistä. Epäselvät tarjouspyyntö ja sen liitteenä olevat, täytettävät lomakkeet voivat johtaa siihen, ettei tiedonhallintayksikkö ei saa vertailukelpoisia tarjouksia. Tarjouksien käsittelyllä tiedonhallintayksikön on pystyttävä todentamaan tarjouksista, että tarjouspyynnössä tietojärjestelmälle määritellyt vaatimukset täyttyvät.

Tietoturvaluusvaatimusten täyttymisen todentaminen tarjouksista on tärkeää myös tietosuoja toteuttamisen näkökulmasta, koska tietosuoja-asetuksen 28 (1) artiklan mukaan rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytöntöönpanemiseksi niin, että käsittely täyttää asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojele. Tietojärjestelmän hankkivan tiedonhallintayksikön on siis varmistettava, että tietojärjestelmän toimittaja (esimerkiksi henkilötietojen käsittelijänä) täyttää ne vaatimukset, jotka henkilötietojen suojaamiseksi tarjouspyynnössä on määriteltä osana tietoturvaluusustoimenpiteitä. Tiedonhallintayksikkö ei voi valita tietojärjestelmän toimittajaksi sellaista tarjoajaa, joka ei varmuudella voi täyttää tietoturvaluusustoimenpiteille määriteltä vaatimuksia.

Tarjouspyynnön laadinnassa on tärkeää ottaa huomioon, että tiedonhallintalaissa on säädetty tiettyjä pakollisia tietojärjestelmien tietoturvaluusjärjestelyihin liittyviä vaatimuksia:

1. salassa pidettävien tietojen siirtäminen yleisessä tietoverkossa on toteutettava salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä.
2. tietojärjestelmän käyttöoikeudet on pystyttävä määrittelemään käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja käyttöoikeuksien myöntämistä koskevien toiminnallisuuksien on tuettava käyttäjä- ja käyttöoikeushallinnan ajantasaisena pitämistä.
3. tietojärjestelmän käytöstä ja tietoluovutuksista on pystyttävä keräämään tiedonhallintalain 17 §:n mukaiset tarpeelliset lokitiedot.
4. tietojärjestelmien rajapinnat on toteutettava tavalla, joka täyttää tiedonhallintalain 22 §:ssä säädetty vaatimukset ja katseluyhteydet tavalla, joka täyttää tiedonhallintalain 23 §:ssä säädetty vaatimukset.

Valtionhallinnossa tietojärjestelmän tarjouspyynnössä esitettäviin tietoturvaluusustoimenpiteitä koskeviin vaatimuksiin voi sisältyä myös asiakirjojen turvallisuusluokittelusta annetun asetuksen (1101/2019) mukaisia vaatimuksia. Tarjouspyyntö voi myös sisältää

turvallisuusluokiteltavia tietoja, jolloin tarjouspyynnön käsittelyssä on otettava huomioon edellä mainitussa asetuksessa säädetyt vaatimukset turvallisuusluokiteltujen asiakirjojen käsittelystä.

Suositus tarjouspyynnön sisällöstä:

- Tarjouspyynnössä esitetään ne tietoturvaluusvaatimukset, jotka tietojärjestelmään on toteutettava. Vaatimuksiin voi sisällyttää myös kuvaukset toteutettavista toimenpiteistä, kuten teknisistä ratkaisuista, tai antaa tarjoajille mahdollisuus tarjota tietoturvaluusustoimenpiteitä tietoturvaluusvaatimusten täyttämiseksi. Tällöin tarjoajan on pystyttävä osoittamaan, että esitetty tietoturvaluusustoimenpide täyttää kiistatta määritellyn tietoturvaluusvaatimuksen. Jos ei haluta vertailla tai arvioida erilaisia teknisiä tietoturvaluusustoimenpiteitä, kannattaa vaatimukset täyttävät tietoturvaluusustoimenpiteet kuvata tarjouspyyntöön. Tietoturvaluusustoimenpiteiden kuvaamisella ei saa edellyttää jonkin tietyn tuotemerkin käyttöä.
- Tietoturvaluusvaatimuksissa on myös suositeltavaa kertoa, jos tiedonhallintayksikkö teetättää palvelun toimittajasta ja sen alaisuudessa toimivista, nimetyistä henkilöistä turvallisuus selvityksen.
- Tietoturvaluusvaatimukseen voidaan kytkeä mahdolliset toimittajan tietoturvaluuden tietoturvasertifikaatit tai jokin muu tapa (esim. riippumattoman tietoturva-auditoijan auditointi), jolla toimittaja voi antaa vahvistuksen organisaationsa tietoturvaluusustasosta.
- Tietoturvaluusvaatimukseen sisältyy myös palvelutasoa koskevat vaatimukset, jotka tulisi kuvata selkeästi tarjouspyyntöön, koska palvelutasolla on vaikutus myös tietojärjestelmän hankintahintaan ja palvelun soveltuvuuteen. Palvelutaso voi vaihdella merkittävästikin eri tietojärjestelmien välillä riippuen tietojärjestelmän käyttötarkoituksesta ja merkityksestä viranomaisen toiminnalle.
- Tarjouspyyntöön on suositeltavaa sisällyttää myös tietoturvaluusvaatimusten toteutumista mittaavia kriteerejä tietojärjestelmän palvelutuotannon aikana sekä vaatimukset vikasetoisuuden varmistamisesta säännöllisesti ainakin viranomaisen toimintaan olennaisesti vaikuttavan tietojärjestelmän osalta, koska tiedonhallintalain 13.2 § tätä edellyttää.



- Tarjouspyynnössä tulisi myös kuvata, miten tietojärjestelmän tuotantokäyttö turvataan poikkeusoloissa, mikäli tietojärjestelmä on olennainen viranomaisen tehtävien hoidon tai yhteiskunnan toiminnan kannalta katsottuna.
- Tarjouspyyntöön tulisi myös kuvata, millä menettelyillä muun muassa erilaisista poikkeamista ja havaituista tietoturvaloukkauksista raportoidaan tiedonhallintayksikölle, sekä miten ja kuinka nopeasti tällaisissa poikkeavissa tilanteissa toimitaan.
- Tarjouspyynnössä tulisi esittää myös kuvaukset muutoksenhallinnalle riippumatta siitä, koskevatko muutokset tietoturvaluustoimenpiteiden ajan tasalla pitämistä vai jotain muuta ylläpitoa.
- Tarjouspyynnöstä tulisi myös ilmetä sanktiomenettelyt, jos tietojärjestelmän toimittaja ei ole noudattanut määriteltyjä tietoturvaluusvaatimuksia.
- Tarjouspyynnössä tulisi esittää myös ehdot ja menettelyt sille, että tiedonhallintayksiköllä on oikeus auditoinneilla varmistaa tietoturvaluusustoimenpiteiden vaatimustenmukaisuus tietojärjestelmän toiminnassa ja tuotannossa. Auditointien osalta tulee kuvata kustannusten jakautumisen periaatteet sekä aika, jonka kuluessa ilmoituksesta auditointi voidaan tehdä. Varmistamiseen liittyvät tarkistuspisteet tulisi kiinnittää käytettävään tietojärjestelmän kehittämis- tai käyttöönottomalliin.
- Tarjouspyyntöön tulisi myös sisällyttää vahingonkorvausperiaatteet, jos tiedonhallintayksikölle aiheutuu vahinkoa toimittajan laiminlyönneistä tietoturvaluusustoimenpiteiden toteuttamisessa. Erityisen merkityksellistä vahingonkorvausperiaatteiden sisällyttämiselle on sellaisiin tarjouspyyntöihin, joissa hankinnan kohteena on henkilötietojen käsittelyyn tarkoitettu tietojärjestelmä. Tietosuoja-asetuksessa ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (1054/2018) on säädetty vahingonkorvausvastuut rekisterinpitäjälle, jolloin tiedonhallintayksikön on suositeltavaa varmistaa, että tietojärjestelmän toimittajan toiminnassa henkilötietojen käsittelyn takia aiheutuvat vahingonkorvausvastuut voidaan viime kädessä kohdentaa toimittajalle.
- Tarjouspyyntö voi sisältää myös tietoturvaluuteen liittyviä laatukriteerejä, joita käytetään tarjousvertailussa. Tällaisten kriteerien

asettaminen edellyttää tiedonhallintayksiköltä kuitenkin riittävää osaamista erilaisten tarjottujen tietoturvallisuusratkaisujen arvioimiseksi ja niiden vertailemiseksi. Tästä syystä tietoturvallisuustoimenpiteitä vertailuperusteina tulee harkita aina erikseen ja siihen vaikuttaa myös hankittavassa tietojärjestelmässä käsiteltävien tietojen luonne sekä teknologinen kehitys. Tavoiteltu tietoturvallisuuden minimitaso tulisi kuitenkin olla aina määritelty ehdottomana vaatimuksena.

- Tarjouspyynnössä tai sen liitteenä olevissa sopimus pohjissa tulisi esittää myös menettelyt ja vaatimukset sille, miten hankittavan tietojärjestelmän elinkaaren loppuvaiheessa turvataan tiedonhallintayksikön toiminta sekä tietojärjestelmässä olevien tietojen siirto (mukaan lukien lokitiedot) uuteen järjestelmään tai uudelle asiakkaalle. Lisäksi tulisi esittää myös menettelyt, jolla varmistetaan, että käytöstä poistetussa järjestelmässä ei enää ole käsiteltävissä sen käytöstä muodostuneita tietoaaineistoja.
- Ennen tarjouspyynnön tekemistä tulee arvioida tietojärjestelmään liittyvät immateriaalioikeustarpeet (omistus-, muutos- ja luovutus oikeudet) ottaen huomioon tietojärjestelmän turvallisuusvaatimukset ja elinkaaren aikaiset kehitystarpeet. Nämä immateriaalioikeustarpeet kirjataan tarvittaessa tarjouspyyntöön vaatimuksina.

Tarjouspyynnössä esitetyt tietoturvallisuusvaatimukset ovat osa hankintasopimusta. Tarjouspyyntöön on suositeltavaa sisällyttää jo valmiiksi sopimusluonnos liitteineen, jolla varmistetaan niin tiedonhallintalaissa kuin tietosuoja-asetuksessa säädettyjen vaatimusten täytyminen niin valitun toimittajan toiminnassa kuin hankitussa tietojärjestelmässä. Sopimusluonnoksessa tietoturvallisuusvaatimusten ensisijaisuus tulee varmistaa sopimusliitteiden pätemisjärjestyksessä.

## 8.4 Tarjousten sisällön arviointi

Tarjousten vastaanottamisen jälkeen tarjouksista on tarkastettava, täyttävätkö ne tarjouspyynnössä esitetyt vaatimukset. Hankintalain (74.1 §, 104.2 §) mukaan tarjoajan tulee tarjouksessaan osoittaa tarjoamansa tavaran, palvelun tai rakennusurakan olevan tarjouspyynnössä ja muissa hankinta-asiakirjoissa esitettyjen vaatimusten mukainen. Hankintayksikön on suljettava tarjouspyyntöä tai tarjousmenettelyn ehtoja vastaamattomat tarjoukset tarjouskilpailusta. Sellaiset tarjoukset, joissa on esitetty puutteellisia tietoja tarjouspyynnössä määritellyistä tietoturvallisuusvaatimuksista, on hankintalain nojalla suljettava tarjousvertailun ulkopuolelle.

Kuitenkin, jos puute on teknisluonteinen, esimerkiksi vaatimuslistassa olevan rastin puuttuminen, voi tiedonhallintayksikkö pyytää tarjoajaa täydentämään tarjousta. Tällöin täydennys voi olla vain havaitun puutteen teknisluonteinen täydentäminen ilman, että tarjous muuten sisällöllisesti muuttuu. Hankintalain (74.2 §, 104.2 §) mukaan hankintayksikkö voi pyytää tarjoajaa tai ehdokasta toimittamaan, lisäämään, selventämään tai täydentämään tarjouksensa tai osallistumisilmoituksensa tietoja tai asiakirjoja hankintayksikön asettamassa määräajassa. Täydentämisessä on kuitenkin otettava huomioon erityisesti tarjoajien tasapuolisen ja syrjimättömän kohtelun vaatimus.

Tarjousten käsittelyssä on suositeltavaa:

- varata riittävät ja asiantuntevat resurssit varmistamaan tarjouksissa esitettyjen tietoturvaluustoimenpiteiden vastaavuus tarjouspyynnössä määriteltyihin tietojärjestelmän ja sen toimituksen tietoturvaluusvaatimuksiin.
- käyttää useampaa tietoturva-asiantuntijaa arvioimaan tarjouksissa esitettyjä tietoturvaluustoimenpiteisiin liittyviä ratkaisuja, jos niitä käytetään tarjousvertailuperusteina. Useamman asiantuntijan käyttö luo perustan asianmukaiselle tarjousten arvioinnille tasapuolisen ja syrjimättömän kohtelun varmistamiseksi. Arvioinnissa on käytettävä ennalta tarjouspyynnössä määriteltyjä kriteereitä ja asteikkoja, jotta tietoturvaluustoimenpiteitä koskevien ratkaisujen arviointi ei muodosta rajoittamatonta harkintamarginaalia tarjousten arvioimiselle.

## 8.5 Hankintasopimuksen laadinta ja täytäntöönpano

Hankintamenettely on kumulatiivinen prosessi. Tarjouspyyntö, hankintailmoitus ja saatu tarjous ovat osa hankintasopimuskokonaisuutta. Jos tarjouspyynnössä on esitetty hankintasopimuksen ja sen liitteiden pohjat, voidaan niitä täydentää vain siltä osin kuin ne on jätetty tarjouspyyntövaiheessa avoimeksi tai niiden sisällössä on saatuun tarjoukseen liittyviä muuttujia. Sopimuksesta tai sen liitteistä on ilmentävä ne vaatimukset, jotka tarjouspyynnössäkin on esitetty tietoturvaluusvaatimuksiksi. Koska tarjous on osa hankintasopimusta, on tarjouksessa esitetyt tietoturvaluusvaatimuksia vastaavat valitun toimittajan esittämät tietoturvaluustoimenpiteet toimittajaa sitovia. Hankintasopimukseen voidaan liittää tarvittaessa erikseen turvallisuussopimus, mutta sen on pitänyt joko olla mukana tarjouspyynnössä tai vastaavat vaatimukset on pitänyt esittää tarjouspyynnössä. Turvallisuuksopimuksen sisällöllä voi olla vaikutuksia tietojärjestelmän toimittamiseen ja sen hinnoitteluun, jolloin turvallisuussopimusta ei voida pitää hankintamenettelystä irrallisena asiakirjana. Turvallisuuksopimuksissa on suositeltavaa käyttää turvallisuussopimusmalleja,

mutta niiden tarkoituksenmukaisuus ja sopivuus suhteessa hankittavaan kohteeseen on arvioitava jo tarjouspyynnön laatimisvaiheessa.

Tietojärjestelmähankinnoissa ja asiantuntijapalveluhankinnoissa käytetään tyypillisesti tiedonhallintayksikköjen laatimia vaitiolositoumuksia. Vaitiolositoumukset eivät ole merkityksellisiä muuta kuin sopimusoikeudellisesti määriteltäessä esimerkiksi salassapitovelvollisuuden rikkomisen perusteella sopimussakkoa tai sopimuksen purkuperusteita. Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 23 §:ssä on säädetty vaitiolovelvollisuudesta ja hyväksikäyttökiellosta. Mainitun lainkohdan mukaan vaitiolovelvollisuus ja hyväksikäyttökielto koskevat myös sitä, joka toimii viranomaisen toimeksiannosta tai hoitaa toimeksiantotehtävää. Säännöksellä tarkoitetaan, että esimerkiksi tietojärjestelmän toimittavan toimittajan palveluksessa olevat ja mahdolliset alihankkijat ovat vaitiolovelvollisia suoraan laissa säädetyn velvollisuuden velvoittamina. Jos laissa säädettyä vaitiolovelvollisuutta on rikottu, kuuluu se rikosvastuun piiriin. Jos vaitiolositoumuksia tehdään, on suositeltavaa sitoa ne osaksi varsinaista hankintasopimusta.

Ennen hankintasopimuksen tekemistä tiedonhallintayksikön tulisi vielä varmistaa, että hankintasopimuksessa tai sen liitteissä ovat kaikki ne kuvaukset ja vaatimukset tietoturvalisuustoimenpiteiden toteuttamiseksi, joita tarjouspyyntöasiakirjoissa ja tarjouksessa on esitetty.

## 8.6 Hankintasopimuksen toimeenpano

Hankinnan kohteena olevan tietojärjestelmän tai tuotteen toteutusvaiheen sekä palveluun liittyvän projekti- ja käynnistysvaiheen aikana varmistetaan prosessin eteneminen ja tulosten laatu. Tietojärjestelmän kehittämisprosessin tai käyttöönottoprosessin eri vaiheissa tulisi olla tarkistuspisteitä, joissa arvioidaan muun muassa tietojärjestelmän tietoturvalisuustoimenpiteiden vaatimuksenmukaisuutta.

Jos toimintaympäristön tietoturvallisuuden tilassa tapahtuu muutoksia kehittämistyön aikana, tulisi ne ottaa huomioon tarvittaessa muutospyyntöinä toimittajalle, asianmukaisen ja riittävän tietoturvallisuuden varmistamiseksi ennen varsinaista tuotantokäyttöönottoa.

Ennen käyttöönottoa vielä hyväksymistestausvaiheessa tulisi tehdä systemaattinen tietoturvalisuustestaus tarjouspyynnössä esitettyjen tietoturvalisuusvaatimusten täyttämisen varmistamiseksi, sekä suorittaa vielä erikseen eri testausvaiheiden katselmointi sen varmistamiseksi, että tietoturvalisuusvaatimukset on otettu huomioon kaikissa tarpeellisissa testauksen vaiheissa.

Tiedonhallintayksikön ja siinä toimivien viranomaisten toimintaan olennaisesti vaikuttavien tietojärjestelmien osalta on otettava huomioon, että tiedonhallintalain 13.2 §:n mukaan tällaisten tietojärjestelmien vikasietoisuutta ja toiminnallista käytettävyyttä on testattava säännöllisesti. Käytännössä tämä tarkoittaa sitä, että tiedonhallintayksikön ja tietojärjestelmän toimittajan on luotava laadunvarmistusprosessi tuotantokäytössä olevan tietojärjestelmän vikasietoisuuden varmistamiseksi testauksen avulla. Tietojärjestelmien toiminnallinen käytettävyys tulisi varmistaa jo tietojärjestelmän kehittämis- ja käyttöönottovaiheissa sekä tehtäessä tietojärjestelmän toiminnallisuuksiin ja käyttöliittymään olennaisia, tietojärjestelmän käyttäjän toimintaan vaikuttavia päivityksiä. Toiminnallisen käytettävyyden varmistamisessa on suositeltavaa käyttää niin teknisiä käytettävyydestestauksia kuin käyttäjillä suoritettavia käytettävyydestestejä tai heuristisia asiantuntija-arviointeja.

## 8.7 Säädökset ja lisätiedot

Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)

Laki julkisista puolustus- ja turvallisuushankinnoista (1531/2011)

Hallintolaki (434/2003)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

ENISA, Security Guide for ICT Procurement

Ohje turvallisuuskriittisiin hankintoihin, Valtiovarainministeriön julkaisuja 2019:7

ISO/IEC 27036

ISO/IEC 28000

ISO/IEC 27001 ja 27002

## 9 Sanasto

Kyberturvallisuuden sanasto (Turvallisuuskomitea)

Kokonaisturvallisuuden sanasto (Sanastokeskus TSK ry)

VAHTI-ohjeen 2/2014, Tietoturvallisuuden arviointiohje, käsitteistö

Valtionhallinnon tietoturvasanasto (VAHTI 8/2008, valtiovarainministeriö)

**Aikaleima** on tapahtumatietoon tai viestiin liitetty tieto lähetyks-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista. Aikaleimalla saadaan aikaan viestin lähettämisen tai vastaanottamisen kiistämättömyys.

**Alusta** on ohjelmiston tai tietojärjestelmän tekninen toimintaympäristö. Alustalla tarkoitetaan yksinkertaisimmillaan laitteistoa ja sen varusohjelmistoa. Yleisemmässä tapauksessa alustalla saatetaan tarkoittaa tiettyä laajempaa sovellusten ajoympäristöä erilaisine tukiohjelmistoineen, tietokantoineen, tietoliikennevalmiuksineen.

**Anonymisointi** tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei enää voida tunnistaa niistä. Tiedot voidaan esimerkiksi karkeistaa yleiselle tasolle (agregoida) tai muuttaa tilastolliseen muotoon siten, etteivät yksittäistä henkilöä koskevat tiedot ole enää tunnistettavassa muodossa. Tunnistamisen täytyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi.

**Arviointi** on sen selvittäminen, täyttääkö tietty kohde eri osiltaan sille asetetun tavoitetilän (vaatimukset, suositukset ja parhaat käytännöt). Arviointiprosessi on usein hyväksyntäprosessin osaprosessi.

**Auditointi** on riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määrääjain tapahtuva tutkiminen sen selvittämiseksi, vastaako kohde siihen kohdistuvia vaatimuksia.

**Haavoittuvuudet** ovat alttiuksia turvallisuutta uhkaaville tekijöille, puutteita ja heikkouksia turvatoimissa sekä suojauksissa. Tietoturva haavoittuvuudet ovat tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan. Haavoittuvuus voi olla seurausta ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturva-haavoittuvuuksia.

**Haittaohjelma** on ohjelma, joka tarkoituksellisesti aiheuttaa tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat esimerkiksi virukset, madot ja troijalaiset sekä näiden yhdistelmät. Kiristys-haittaohjelma on haittaohjelma, joka salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta.

**Haavoittuvuusskannaus** on tietoverkossa kohdejärjestelmän palveluissa olevien tunnettujen haavoittuvuuksien automaattinen haku, esimerkiksi murtokokeilla tai tutkimalla palvelimen ohjelmistoversiota.

**Havaitseva kontrolli** pyrkii havaitsemaan suojaavan kerroksen läpi päässeeseen jäännösriskin aiheuttamat vaikutukset. Valvonta ei enää estä vahinkoa tapahtumasta, vaan ainoastaan saattaa sen näkyväksi.

**Hyväksymistarkastus** kattaa toimet, joilla todetaan, täyttääkö tuote tai työn tulos asetetut vaatimukset.

**Häiriö** on tilanne tai tapahtuma, jonka vuoksi järjestelmä ei toimi normaalisti tai toiminnan jonkin osatekijän haitallinen vaihtelu, jonka puitteissa toiminta voi silti pääosin jatkua.

**Immateriaalioikeudet** ovat aineettomia oikeuksia, mm. tekijänoikeus, patentti-, malli-, tavaramerkki ja toiminimi oikeus.

**IPR-kysymykset** (Intellectual Property Rights) eli immateriaalioikeuksiin liittyvät kysymykset koskevat tekijänoikeuksia, tavaramerkkejä, patenteja, toiminimiä ja liikesalaisuuksia.

**Katselmointi** on kohteen tilan arviointi, jonka tarkoituksena on tunnistaa eroavuudet tavoitetilaan ja tuottaa kehitysehdotuksia.

**Komponentti** on itsenäinen ohjelmistoyksikkö, joka tarjoaa palveluja hyvin määritellyn rajapinnan kautta.

**Kontrolli** on riskien hallinnan tavoite, keino tai menetelmä, suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan (tieto)

turvaloukkauksia tai haitallisia tapahtumia vastaan. Kontrollit ovat ehkäiseviä, havaitsevia (ilmaisevia) tai korjaavia.

**Kriteeri** on arviointiperuste, jolla todetaan tavoitteen täyttyminen.

**Levykuva** eli image on massamuistilaitteen koko sisällöstä ja rakenteesta tehty tiedosto.

**Loki** on tiedosto, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista. Loki kerätään yleensä automaattisesti ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki, laskutusloki, turvaloki.

**Lokitieto** on tietojärjestelmästä automaattisesti kirjautuva tapahtumatieto. Lokitieto voi sisältää erilaisia tunnistamistietoja ja koskea muun muassa sitä, kuka järjestelmää on käyttänyt tai miten ja milloin järjestelmää on käytetty samoin kuin tietoa erilaisista virhetilanteista.

**Lokitietojen käsittelyllä** tarkoitetaan lokin koko elinkaaren liittyviä toimenpiteitä lokien keräämisestä niiden säilyttämiseen ja arkistointiin sekä lokien valvonnasta ja analysoinnista niiden luovuttamiseen ja poistamiseen.

**Lähdekoodi** on tietokoneohjelma ohjelmoijien kirjoittamassa ja ylläpitokelpoisessa muodossa.

**Muistivälineiden sanitointi** tarkoittaa muistivälineiden tyhjentämistä tai puhdistamista halutusta tiedosta tai materiaalista.

**Osapuolen todentaminen** on menetelmä tai prosessi, jolla todennetaan viestinnän osapuoli.

**Palveluelementti** on palvelujärjestelmän toiminto tai tieto, jonka käyttöä halutaan erikseen valvoa.

**Palvelujärjestelmä** on tietojärjestelmä, joka tarjoaa käyttäjille sovelluspalveluja.

**Penetraatiotestaus** tarkoittaa tietojärjestelmien testaamista tietoturvariskien varalta. Penetraatiotestausta käytetään tietojärjestelmien suojausmekanismien heikkouksien ja haavoittuvuuksien havaitsemiseen.

**Protokolla** eli käytäntö on yleisesti sovittu menettely kahdenvälisestä yhteydenpitoa varten sekä tietoliikenteessä säännöstö, jota lähettävän ja vastaanottavan laitteen tulee noudattaa, jotta datansiirto onnistuisi tarkoitetulla tavalla. Yhteyskäytäntö on säännöstö, joka



määrittelee datayhteydellä käytettävät yhteydenpitotavat, koodin sekä siirto-, ohjaus- ja toipumismenettelyt.

**Pääsynhallinta** käsittää ne menettelyt, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti.

**Pääsynvalvonta** kattaa ne tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palveluelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille.

**Rajapinta** on yhtymäkohta, joka mahdollistaa tiedon siirron laitteiden, ohjelmien tai käyttäjien välillä.

**Riskirekisteriin** tallennetaan tunnistetut riskit ja niiden arvioinnit sekä suunnitellut hallintatoimenpiteet.

**Salakirjoittaa** eli käyttää menetelmää tiedon esityksen muuttamiseksi sellaiseksi, että tiedon alkuperäinen sisältö on mahdollista saada selville vain samaa tai soveltuvaa käänteistä menetelmää käyttäen. Salakirjoittaminen tapahtuu salausavainta käyttäen tietyn salausalgoritmin mukaisesti.

**Salattu yhteys** on salausmenetelmällä ulkopuolisilta suojattu tietojärjestelmien välinen yhteys.

**Salaus** on tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittelyä niin, että ulkopuolinen ei saisi haltuunsa tietoa tai viestiä tai sen sisältämää informaatiota. Salaus tarkoittaa myös salakirjoitusta eli salakirjoittamista tai sen tulosta.

**Salausmenetelmä** on salaukseen ja salauksen purkamiseen käytettävä menetelmä.

**Suojattava kohde** on organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta. Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema.

**Suojattavien kohteiden tunnistamisella ja dokumentoinnilla** tarkoitetaan kaiken tiedonhallintayksikön hallinnassa olevan tiedon ja järjestelmien sekä muiden suojattavien kohteiden, kuten avainhenkilöiden tunnistamista.

**Suojauksella** tarkoitetaan haitallisen ulkopuolisen vaikutuksen torjumista tai ennalta ehkäisyä.

**Tapahtumaketju**, kirjausketju ja jäljitysketju tarkoittavat alkutositteiden, syöttötietojen ja tulosteiden aukotonta ketjua, jonka avulla on mahdollista jäljittää yksittäisen tiedon käsittelyvaiheet.

**Taustajärjestelmä** käsittää ne järjestelmät, jotka tukevat varsinaisen järjestelmän toimintaa.

**Testaus** on järjestelmän toimivuuden, käytettävyyden, suorituskyvyn, määritysten mukaisuuden tai muun ominaisuuden selvittämiseksi tehtävä toimenpidesarja.

**Tiedonhallintayksiköitä** ovat esimerkiksi valtion ja kuntien organisaatiot, kuten valtiovarainministeriö, Valtion tieto- ja viestintätekniikkakeskus Valtori, Maanmittauslaitos ja Helsingin kaupunki.

**Tiedon migraatio** on tiedon siirtämistä toiseen järjestelmään aitouden, eheyden, luotettavuuden ja käytettävyyden varmistamiseksi.

**Tietojärjestelmä** on ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi sekä abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt.

**Tietoriskillä** tarkoitetaan tietoon kohdistuvaa tai tiedosta aiheutuvaa, jonkinlaisen haitan tai vaurion todennäköisyyttä ja sen seurauksia. Tietoriski ilmaistaan tavallisesti riskin lähteiden ja mahdollisten tapahtumien sekä niiden seurausten ja todennäköisyyden yhdistelmänä.

Tietoriskit voivat aiheutua esimerkiksi inhimillisistä virheistä, annettujen ohjeiden puutteista tai noudattamatta jättämisestä, varkauksista tai ilkeistä, laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä, haittaohjelmien leviämisestä, tietoaaineistojen tuhoutumisesta tai alihankkijan tai kumppanuuksien verkostoon kuuluvan toimijan virheistä tai laiminlyönneistä.

**Tietoturva-vaavoittuvuudet** ovat tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan. Vaavoittuvuus voi olla seurausta ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturva-vaavoittuvuuksia.

**Tietoturvaloukkauksen tutkinta** tarkoittaa toimenpiteitä, jotka käynnistetään tietoturvaloukkauksen paljastuttua loukkauksen selvittämiseksi. Tietoturvaloukkauksen tutkinta voi käsittää muun muassa todistusaineiston turvaamista, forensiikkaa, haittaohjelma-analyysia, lokianalyysia tai yleisesti tietoturvaloukkauksen vaikutusten ja laajuuden selvittämistä

**Tietoturvaloukkaus** on oikeudeton puuttuminen tietoon tai tietojärjestelmään. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

**Tietoturvapoikkeama** on yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. Tietoturvapoikkeamat ovat haitallisia tapahtumia, tahallisia tai tahattomia tapahtumia tai olotiloja, joiden seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyytensä on tai saattaa olla vaarantunut.

**Tietoturvapoikkeaman hallinta** sisältää toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

**Tietoturvatapahtuma** tai tietoturvallisuustapahtuma on tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan. Tietoturvatapahtumia voidaan havaita esimerkiksi tunnistamalla muutoksia tai poikkeamia (engl. anomalies) datassa tai tietojärjestelmän toiminnassa. Muutoksia ja poikkeamia havaitaan pääasiassa teknisiä työkaluja hyödyntävillä seuloilla.

**Tietoturvauhalla** tarkoitetaan tietoa-ineistoihin ja tietojärjestelmiin liittyvää sellaista tahatonta tai tahallista tekijää, joka vaarantaa tietoa-ineistojen luottamuksellisuutta, eheyttä tai käytettävyyttä tai tietojärjestelmien käyttöä tai vikasetoisuutta.

Tietoturvauhat voivat aiheutua esimerkiksi inhimillisistä virheistä, annettujen ohjeiden puutteista tai noudattamatta jättämisestä, varkauksista tai ilkivallasta, laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä, haittaohjelmien leviämisestä, tietoa-ineistojen tuhoutumisesta tai organisaation oman työntekijän, alihankkijan, palveluntarjoajan tai kumppanuusverkostoon kuuluvan toimijan virheistä tai laiminlyönneistä.

**Tietoverkkohyökkäys** tai verkkohyökkäys on tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön. Tietoverkkohyökkäys voidaan tehdä esimerkiksi palvelunestohyökkäyksenä tai haittaohjelman avulla.

**Tietoverkkovalvonta** tai verkkovalvonta on toimintaa, jossa seurataan ja analysoidaan omissa tietoverkoissa tapahtuvaa tietoliikennettä. Organisaatiot voivat seurata ja analysoida oman tietoverkkonsa tietoliikennettä esimerkiksi teknisen vian tai virheen havaitsemiseksi tai tietoturvasta huolehtimiseksi.

**Toipuminen** kuvastaa toimintakyvyn palautumista kriisin, erityistilanteen, häiriötilan tai poikkeusolojen jälkeen tai elpymistä kriisistä tai katastrofista.

**Toipumissuunnittelua** on toipumissuunnitelman laatiminen ja ylläpito. Toipumissuunnitelma on jatkuvuussuunnitelman tai varautumissuunnitelman osa, joka sisältää ohjeet katastrofista toipumiseen, toiminnan jatkamisesta ja paluusta normaaliin toimintaan. Määrittelee tärkeille tietojärjestelmille varajärjestelyvaatimukset, vastuut ja toimet valmiuden luomiseksi sekä antaa ohjeet toiminnasta poikkeustilanteissa. Suunnitelma ei sisällä vain vaatimuksia vaan konkreettisia sovittuja toimenpiteitä, menettelytapoja ja teknisiä vararatkaisuja.

**Turvallisuuskuvaus** on kuvaus esimerkiksi järjestelmän turvallisuudesta ja sen toteuttamisesta.

**Vaatus** on kohteelle asetettu yksittäinen tavoite, joka kohteen tulee pystyä toteuttamaan.

**Vaikutusanalyysillä** tarkoitetaan toiminnan keskeyttävien tai jatkuvuutta häiritsevien uhkien sekä toimintaan liittyvien riippuvuuksien tunnistamista. Tieto- ja kyberturvallisuuden näkökulmasta tulee vaikutusanalyysissä, erityisesti valtionhallinnon tai muun julkisen hallinnon organisaation toiminnan kannalta, tarkastella muun muassa:

- vaikutuksia omaan operatiiviseen toimintakykyyn
- vaikutuksia säädösperusteisten tehtävien hoitamiseen (vrt. myös yhteiskunnan elintärkeät tehtävät)
- vaikutuksia yhteiskunnalle
- riippuvuussuhteita ja niiden vaikutuksia:
  - oman organisaation riippuvuutta toisesta osapuolesta tai palvelusta tai toisista organisaatioista tai palveluista
  - toisen organisaation tai palvelun riippuvuutta oman organisaation tuottamasta palvelusta tai toiminnasta.

**Viranomaisen** tulee kyetä tunnistamaan kaikki tiedot ja tietojärjestelmät, jotka ovat sen vastuulla sekä ottamaan huomioon niitä ylläpitävät ja käyttävät avainhenkilöt. Jokaiseen tunnistettuun kohteeseen liittyvät riskit ja niiden mahdolliset vaikutukset tulee arvioida ja kirjata organisaation itsensä ylläpitämään riskirekisteriin.

VANHENTUNUT



VALTIOVARAINMINISTERIÖ  
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ  
Snellmaninkatu 1 A  
PL 28, 00023 VALTIONEUVOSTO  
Puhelin 0295 160 01  
[vm.fi](http://vm.fi)

ISSN 1797-9714 (pdf)  
ISBN 978-952-367-295-6 (pdf)

Syyskuu 2020