VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Suositus tietoturvallisuuden vähimmäisvaatimuksista

Lautakunnat

VALTIOVARAINMINISTERIÖN JULKAISUJA – 2024:19

Valtiovarainministeriön julkaisuja 2024:19

Suositus tietoturvallisuuden vähimmäisvaatimuksista

Lautakunnat

Valtiovarainministeriö Helsinki 2024

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Valtiovarainministeriö

ISBN pdf: 978-952-367-679-4
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2024

Kuvailulehti
11.3.2024

Suositus tietoturvallisuuden vähimmäisvaatimuksista

Valtiovarainministeriön julkaisuja 2024:19		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	suomi	**Sivumäärä**	50

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää.

Tämä tiedonhallintalautakunnan suositus opastaa tiedonhallintalain asettamien tietoturvallisuuden vähimmäisvaatimusten täyttämisessä, jotka kaikkien julkishallinnon organisaatioiden tulee vähintään täyttää. Vähimmäisvaatimusten osana organisaatioiden tulee tunnistaa ja arvioida tietojenkäsittelyyn liittyvät riskit sekä toteuttaa toimenpiteet riskien pienentämiseksi hyväksyttävälle tasolle.

Suositus on tarkoitettu ensisijaisesti tiedonhallintalaissa määritetyille tiedonhallintayksiköille ja viranomaisille, mutta näiden lisäksi tätä suositusta voivat hyödyntää kaikki muutkin toimijat, jotka käsittelevät viranomaisten asiakirjoja.

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

Tiedonhallintalautakunta hyväksyi suosituksen 31.1.2024

Asiasanat	lautakunnat, tiedonhallintalautakunta, tiedonhallintalaki, julkinen hallinto, tietoturva		
ISBN PDF	978-952-367-679-4	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-679-4		

Presentationsblad
11.3.2024

Rekommendation om minimikrav på informationssäkerhet

Finansministeriets publikationer 2024:19		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	finska	**Sidantal**	50

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019) finns bestämmelser om ansvar avseende informationssäkerhetsåtgärder som gäller informationshanteringsenheter och myndigheter inom den offentliga förvaltningen samt privatpersoner, privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter till den del dessa sköter offentliga förvaltningsuppgifter.

Denna rekommendation från informationshanteringsnämnden handlar om de minimikrav på informationssäkerhet som ställs i informationshanteringslagen och som alla organisationer inom den offentliga förvaltningen åtminstone ska uppfylla. Ett av de minimikraven är att organisationerna bör identifiera och bedöma informationssäkerhetsrisker och vidta åtgärder för att minska riskerna så att de ligger på en godtagbar nivå.

I första hand riktar sig rekommendationen till informationshanteringsenheterna och myndigheterna i lagen om informationshantering, men den kan också tillämpas av andra aktörer som behandlar myndighetshandlingar

Denna rekommendation ersätter rekommendationssamlingarna om tillämpningen av vissa bestämmelser om informationssäkerhet (FM 2021:72, FM 2020:77 och FM 2020:21).

Informationshanteringsnämnden godkände rekommendationen den 31 januari 2024.

Nyckelord	nämnder, informationshanteringsnämnden, informationshanteringslagen, offentlig förvaltning, informationssäkerhet		
ISBN PDF	978-952-367-679-4	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-679-4		

Description sheet
11 March 2024

Recommendation on minimum requirements for information security

Publications of the Ministry of Finance 2024:19		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Finnish	**Pages**	50

Abstract

The Act on Information Management in Public Administration (906/2019) lays down obligations relating to information security measures that apply to information management units and public authorities as well as to private individuals or corporations or to corporations subject to public law other than those serving as authorities insofar as they perform public administrative tasks.

This recommendation of the Information Management Board provides guidance on meeting the minimum information security requirements set in the Act on Information Management in Public Administration. Every organisation in public administration must meet these minimum requirements. As part of meeting these minimum requirements, organisations must identify and assess risks relating to data processing and take measures to mitigate risks to an acceptable level.

The recommendation is primarily intended for the information management units and public authorities defined in the Act on Information Management in Public Administration. Other organisations that process official documents may also find the recommendation useful.

This recommendation replaces the Collection of recommendations on the application of certain information security regulations (versions VM 2021:65, VM 2020:61 and VM 2020:21).

The Information Management Board approved the recommendation 31 January 2024.

Keywords	board, Information Management Board, Information Management Act, public administration, information security		
ISBN PDF	978-952-367-679-4	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-679-4		

Sisältö

1 Johdanto

Tämä tiedonhallintalautakunnan suositus opastaa tiedonhallintalain tietoturvallisuuden vähimmäisvaatimusten täyttämisessä. Suositus on tarkoitettu ensisijaisesti tiedonhallintalaissa määritetyille tiedonhallintayksiköille ja viranomaisille, mutta näiden lisäksi tätä suositusta voivat hyödyntää kaikki muutkin toimijat, jotka käsittelevät viranomaisten asiakirjoja. Jäljempänä näistä tietoturvallisuussääntelyn kohteista käytetään soveltuvin osin termiä *organisaatio*.

Suosituksessa esitetään tietojen käsittelylle säädetyt tietoturvallisuusvaatimukset sekä niihin liittyviä hyviä käytäntöjä. Luvut sisältävät lain vaatimuksen, täsmennyksiä lain vaatimukseen, siihen liittyvät suositukset, käytännön esimerkkejä ja viittauksia lisätietoihin. Liitteessä 1 on kooste tiedonhallintalain tietoturvallisuutta koskevista lainkohdista.

Tämä suositus korvaa suosituskokoelman tiettyjen tietoturvallisuussäännösten soveltamisesta (versiot VM 2021:65, VM 2020:61 ja VM 2020:21). Vähimmäisvaatimussuositus muodostaa yhdessä muiden tiedonhallintalautakunnan tietoturvallisuussuositusten kanssa kokonaisuuden, jota on kuvattu luvussa 1.3.

1.1 Lainsäädännölliset perusteet

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019), jäljempänä *tiedonhallintalaki* tai *TihL*, on säädetty tietoturvallisuuteen liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä tietyin osin yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää. Tiedonhallintalakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, jollei muualla laissa toisin säädetä.

Suositus perustuu tiedonhallintalakiin. Lisäksi suosituksen laatimisessa on hyödynnetty sen perustana olevia hallituksen esitystä sekä hallintovaliokunnan mietintöjä[1].

1 HE 284/2018 ja HaVM 38/2018

Tiedonhallintalain 4 luku (pykälät 12–18) sisältävät ensisijaiset tietoturvallisuutta koskevat vaatimukset. Lisäksi suosituksessa on käsitelty seuraavia pykäliä niihin sisältyvien tietoturvallisuusvaatimusten osalta: 4 § (tiedonhallinnan järjestäminen tiedonhallintayksikössä), 5 § (tiedonhallintamalli ja muutosvaikutusten arviointi), 19 § (tietoaineistojen sähköiseen muotoon muuttaminen), 21 § (tietoaineistojen säilytystarpeen määrittäminen) sekä 28 § (kuvaus asiakirjajulkisuuden toteuttamiseksi). Suosituksessa on huomioitu myös tiedonhallintalakiin lisätty uusi 13 a § häiriötilanteista tiedottamisesta ja varautumisesta häiriötilanteisiin[2].

1.2 Vähimmäisvaatimusten merkitys

Vähimmäisvaatimukset koostuvat tiedonhallintalaissa olevista tietoturvallisuutta koskevista vaatimuksista. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Tiedonhallintalain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi sekä edistää viranomaisten tietoaineistojen turvallista ja tehokasta sekä tietojärjestelmien ja tietovarantojen yhteentoimivuutta. Suosituksessa kuvatut tiedonhallintalain mukaiset tietoturvallisuuden vähimmäisvaatimukset tukevat tätä lain tarkoitusta ja muodostavat ne vaatimukset, jotka kaikkien julkishallinnon organisaatioiden tulee vähintään täyttää. Lisäksi organisaatioiden on huomioitava myös muualla lainsäädännössä olevat tietoturvallisuusvaatimukset.

Vähimmäisvaatimuksilla tarkoitetaan yleisiä tai yksityiskohtaisia tietoturvallisuustoimenpiteitä, jotka viranomaisten ja tiedonhallintayksiköiden tulee tiedonhallintalain perusteella tehdä tietoturvallisuuden varmistamiseksi. Yleisiä toimenpiteitä ovat esimerkiksi tietoturvallisuutta koskevien vastuiden määrittely ja riskien

2 Muutoksia koskevan siirtymäsäännöksen mukaan viranomaisen on saatettava toimintansa 13 a §:n mukaiseksi 18 kuukauden kuluessa lain voimaantulosta eli 31.10.2024 mennessä.

tunnistaminen. Esimerkki yksityiskohtaisesta vaatimuksesta on vaatimus lokitietojen keräämisestä. Tämä suositus tukee sekä yleisten että yksityiskohtaisten tietoturvallisuuden vähimmäisvaatimusten tunnistamista ja täyttämistä.

Vähimmäisvaatimusten osana organisaatioiden tulee tunnistaa ja arvioida tietojenkäsittelyyn liittyvät tietoturvallisuusriskit sekä toteuttaa toimenpiteet riskien pienentämiseksi hyväksyttävälle tasolle.

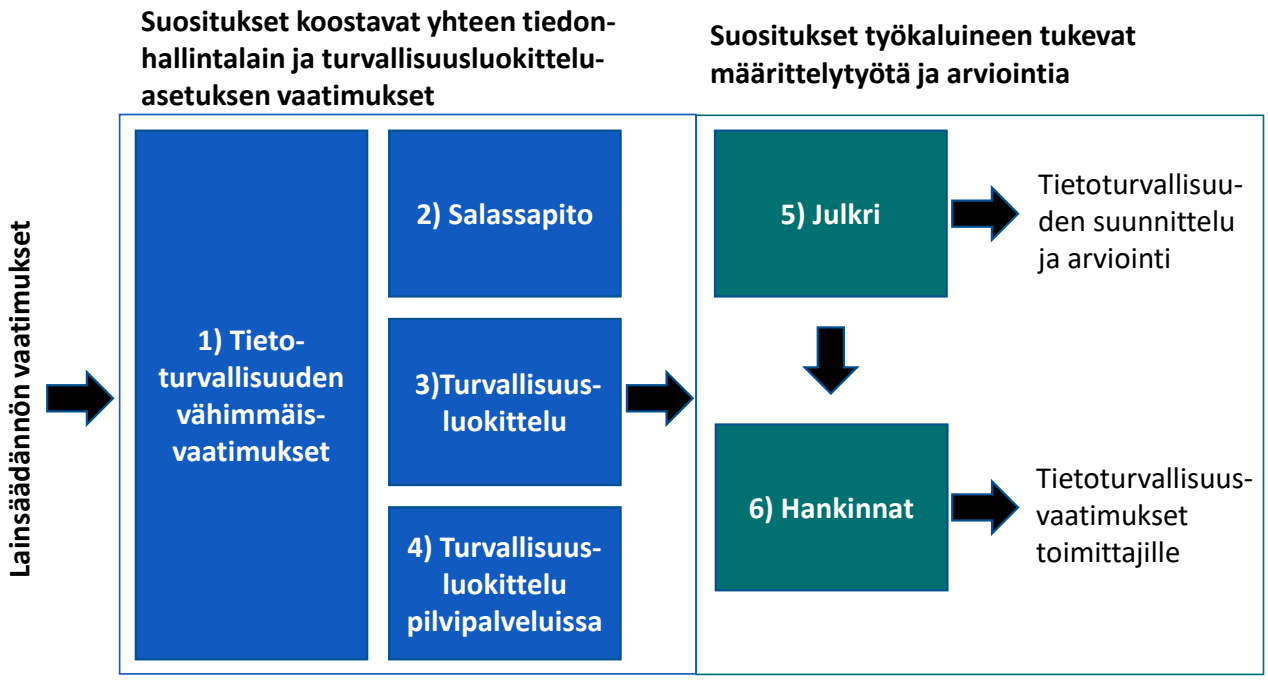
Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä, jäljempänä *Julkri*, suositellaan hyödynnettäväksi tietoturvallisuusvaatimusten täyttämisessä. Julkri sisältää erilaisia tietoturvallisuustoimenpiteitä, joita organisaatio voi toteuttaa tietoturvallisuusriskien pienentämiseksi hyväksyttävälle tasolle. Lisäksi tiedonhallintalautakunta on antanut suosituksen hankintojen tietoturvallisuudesta. Hankintasuositus pohjautuu Julkriin ja se opastaa hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyssä sekä niiden täyttymisen varmistamisessa.

1.3 Suhde muihin suosituksiin

Tiedonhallintalautakunnan suositukset on laadittu tiedonhallintayksikön ja viranomaisen oman toiminnan kehittämisen tueksi. Suositus tietoturvallisuuden vähimmäisvaatimuksista muodostaa perustan organisaation tietoturvallisuudelle. Täsmentävät suositukset on laadittu salassa pidettävien ja turvallisuusluokiteltavien asiakirjojen käsittelystä. Suositus tietoturvallisuudesta hankinnoissa ja suositus julkisen hallinnon tietoturvallisuuden arvioinnista (Julkri) sisältävät työkaluja yksityiskohtaisempien tietoturvallisuusvaatimusten määrittelyyn ja niiden toteutumisen arviointiin.

Seuraavalla sivulla olevassa kuvassa on esitetty tiedonhallintalautakunnan tietoturvallisuutta koskevat suositukset ja niiden väliset suhteet.

Kuvio 1. Tietoturvallisuutta koskevat tiedonhallintalautakunnan suositukset



1) Suositus tietoturvallisuuden vähimmäisvaatimuksista (VM 2024:19)
2) Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
3) Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)
4) Turvallisuusluokiteltavaien asiakirjojen käsittely pilvipalveluissa (VM 2022:4)
5) Julkisen hallinnon tietoturvallisuuden arviointikriteeristö, Julkri (VM 2023:46)
6) Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)

Lisäksi tietoturvallisuusnäkökohtia sisältyy seuraaviin tiedonhallintalautakunnan suosituksiin:

- Suositus asiakirjajulkisuuskuvauksen laatimisesta (VM 2020:22)
- Suositus automaattisen ratkaisumenettelyn käyttöönotosta ja käytöstä (VM 2024:13)
- Suositus johdon vastuiden toteuttamisesta tiedonhallintalaissa (VM 2020:18)
- Suositus teknisistä rajapinnoista ja katseluyhteyksistä (VM 2021:21)
- Suositus tiedonhallinnan muutosvaikutusten arvioinnista (VM 2024)
- Suositus tiedonhallintamallista (VM 2024)
- Suositus tietoaineistojen säilytysajasta ja toimenpiteistä säilytysajan päätyttyä (VM 2023:77)

Tietoturvallisuutta koskevat suositukset toimivat organisaation omien vaatimusten ja toimenpiteiden suunnittelun ja toteuttamisen apuna. Tiedonhallintalautakunnan lisäksi mm. Kyberturvallisuuskeskus, Huoltovarmuuskeskus ja DVV:n Digiturvapalvelut (VAHTI-toiminta) julkaisevat tietoturvallisuuteen liittyviä ohjeita ja hyviä käytäntöjä. Kunkin viranomaisen tulee tapauskohtaisen riskiarvioinnin perusteella valita kuhunkin tapaukseen sopivat ja riittävän turvalliset ratkaisut.

1.4 Rajaukset

Tässä suosituksessa on huomioitu vain tiedonhallintalain asettamat vaatimukset. Seuraavat asiat on rajattu tarkastelun ulkopuolelle:

- toimialakohtainen erityislainsäädäntö, kuten sosiaali- ja terveydenhuollon lainsäädäntöön sisältyvät vaatimukset,
- asiankäsittelyssä ja palvelujen tuottamisessa noudatettavat menettelyt,
- salassapito ja tiedonsaantioikeus viranomaisten asiakirjoista,
- asiakirjojen arkistointi,
- henkilötietojen käsittelyä koskeva sääntely,
- laki digitaalisten palvelujen tarjoamisesta (306/2019),
- kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset sekä
- sähköisen viestinnän palveluista annettu laki (917/2014), jossa säädetään mm. sähköiseen viestintään liittyvien tietojen salassa pidosta ja käsittelystä.

Suosituksessa ei ole huomioitu tiedonhallintalain säännöksiä tietoaineistojen sähköisestä luovutustavasta teknisellä rajapinnalla ja katseluyhteydellä (22–24 §), tietoaineistojen saatavuudesta (19, 24 a ja 24 b §:ssä) eikä automaattisen ratkaisumenettelyn käyttöönotosta ja käytöstä (6 a luku).

Tietoturvallisuusvaatimusten toteuttamiseksi suosituksen hyödyntäjän tulee kuitenkin huomioida edellä mainittu lainsäädäntö.

2 Tehtävät ja vastuut

2.1 Tietoturvallisuusvastuiden määrittely

> Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on määritelty tietoturvallisuuteen liittyvät vastuut ja tehtävät.

Tiedonhallintalain 4 §:n 2 momentin 1 kohdan mukaan ”Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on määritelty tässä ja muussa laissa säädettyjen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut”. Tämä vaatimus koskee myös tietoturvallisuusvastuita.

Tiedonhallintalaissa on viranomaiselle säädetty velvollisuuksia, joiden toteuttamisesta vastuussa olevat on tiedonhallintayksikön määriteltävä. Osa velvollisuuksista kohdentuu tiedonhallintayksikölle ja osa siinä toimiville viranomaisille. Ensin mainitut ovat vaatimuksia, jotka koskevat organisaation ja siihen kuuluvien viranomaisten tiedonhallintaa yleisesti.

Tiedonhallintayksikön tulee määritellä ja dokumentoida tietoturvallisuuden hoitamisen tehtävät ja vastuut. Tehtävien ja vastuiden määrittelyssä tulee kuvata konkreettisesti, miten ja kenen vastuulla toteutetaan tiedonhallintalain edellyttämät tietoturvallisuuteen liittyvät tehtävät. Lisäksi on suositeltavaa määritellä organisaation tietojärjestelmien ja tietoaineistojen vastuut. Vastuiden määrittelyssä tulee ottaa huomioon myös palveluntuottajan vastuulla olevat tehtävät.

Vastuut tulee määritellä esimerkiksi tietoturvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä turvallisuuskokonaisuudesta (ks. Julkri HAL-osion kriteeri Tehtävät ja vastuut). Tietoturvallisuusvastuut suositellaan määrittelemään rinnakkain muiden organisaation tiedonhallintaan liittyvien vastuiden kanssa riittävällä tarkkuudella suhteessa organisaation tehtävien kriittisyyteen ja

tietoaineistoihin kohdistuviin turvallisuusvaatimuksiin. Pilvipalveluita käytettäessä on huomioitava lisäksi erilaiset palvelumallit sekä niihin liittyvät vastuujakojen erot asiakkaan ja palvelun tuottajan välillä.

Tehtävien ja vastuualueiden on oltava tarvittavilta osin eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Vastuiden määrittelyssä on huomioitava vaaralliset työyhdistelmät, jollainen on esimerkiksi se, että sama henkilö hallinnoi tietojärjestelmää sekä tietojärjestelmän seurannassa käytettäviä lokitietoja. Vaaralliset työyhdistelmät on huomioitava myös ulkoistetuissa toiminnoissa.

Lisätietoja yleisesti johdon vastuiden toteuttamisesta tiedonhallintalautakunnan suosituksesta[3].

2.2 Erityistä luotettavuutta edellyttävät tehtävät

Tiedonhallintayksikön on tunnistettava erityistä luotettavuutta edellyttävät tehtävät.

Tiedonhallintalain 12 §:n mukaan ”Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta”.

Tiedonhallintayksiköiden tulee arvioida tietoaineistojensa käsittelyyn osallistuvien henkilöiden tehtävät sekä niissä edellytettävä luotettavuus tietoturvallisuuden varmistamiseksi, ottaen huomioon myös organisaation ulkopuolella tehtävät tietojen käsittelytoimet. Erityistä luotettavuutta voivat edellyttää monet erilaiset tietoaineistojen käsittelyyn, tietojärjestelmiin, varoihin, terveydenhuoltoon tai yleiseen turvallisuuteen liittyvät tehtävät sekä pääsyoikeudet tiloihin.

3 Suositus johdon vastuiden toteuttamisesta tiedonhallintalaissa (VM 2020:18)

Turvallisuusselvityslain (726/2014) 4 luvussa[4] on määritelty millä edellytyksillä ja minkälaisissa tehtävissä toimivista voi hakea henkilöturvallisuusselvitystä. Lisäksi lain 16 §:n mukaan valtioneuvoston asetuksella voidaan säätää, että valtionhallinnon viranomaisen on hankittava henkilöturvallisuusselvitys tietyin edellytyksin. Myös valtion virkamieslain (750/1994) 8 c § sisältää asetuksenantovaltuuden, jonka mukaan asetuksella voidaan säätää henkilöturvallisuusselvitystodistusta koskevasta vaatimuksesta edellytyksenä virkaan nimittämiselle.

Työnantajan oikeudesta saada ja käyttää tehtävään valittua työnhakijaa koskevia luottotietolain (527/2007) 4 luvussa tarkoitettuja henkilöluottotietoja säädetään yksityisyyden suojasta työelämässä annetun lain (759/2004) 5 a §:ssä. Työnantajan oikeudesta käsitellä huumausainetestejä koskevia tietoja säädetään lain 3 luvussa.

Organisaatiot voivat toteuttaa seuraavia toimenpiteitä erityistä luotettavuutta edellyttävien tehtävien tunnistamiseksi:

- laatia kuvaukset tehtävistä, jotka edellyttävät erityistä luotettavuutta,
- dokumentoida perustelut, miksi tehtävässä edellytetään erityistä luotettavuutta sekä
- hakea turvallisuusselvitykset näihin tehtäviin nimettävistä henkilöistä, mikäli tähän on turvallisuusselvityslain mukaan peruste.

2.3 Tietoturvallisuus tiedonhallintamallissa

Tiedonhallintayksikön on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia muun muassa tietoturvallisuuden ylläpitämiseksi. Tiedonhallintamalli sisältää tiedot tietoturvallisuustoimenpiteistä.

Muutosten yhteydessä on arvioitava niiden tietoturvallisuusvaikutukset.

4 Luettelot yksityiskohtaisemmista tehtävistä 19–21 §

Tiedonhallintalain 5 §:n 2 momentin 5 kohdan mukaan ”Tiedonhallintamallin on sisällettävä tiedot tietoturvallisuustoimenpiteistä”.

Tietoturvallisuuteen liittyvän kuvaamisen tavoitteena on, että viranomaiset suunnittelevat ennakkoon, millä tavoin tietoturvallisuus toteutetaan sekä mitä menettelyitä tietojenkäsittelyn, tietojärjestelmien ja tietoaineistojen turvaamiseksi on toteutettu tai aiotaan toteuttaa, ja miten ne ovat vastuutettu.

Tiedonhallintamallia laadittaessa suositellaan:

- sisällyttämään kuvaukseen, miten tiedonhallintalain edellyttämät tietoturvallisuuden vähimmäisvaatimukset, kuten esimerkiksi pääsyoikeuksien hallinta ja tietojen salaus on toteutettu,
- suunnittelemaan kokonaisuutena, miten erilaiset organisaation tietoturvallisuuteen liittyvät ratkaisut, ohjeet, prosessit ja politiikat dokumentoidaan,
- määrittelemään, mitkä tietoturvallisuuteen liittyvät kuvaukset ovat yhteisiä, eli koskevat useita tiedonhallintamallissa esitettyjä kohteita ja mitkä liittyvät yksittäisiin tiedonhallintamallin kohteisiin,
- määrittelemään tiedonhallintamallin tietoturvallisuusasiat viittauksilla erillisiin dokumentteihin sekä
- varmistamaan ylläpidon ja dokumenttienhallinnan avulla, että tiedonhallintamalli sisältää viittaukset aina ajantasaiseen tietoturvallisuutta koskevaan dokumentaatioon.

Tiedonhallintalain 5 §:n 3 momentin mukaan ”Suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa tiedonhallintalain 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja –toimenpiteisiin”.

Tiedonhallintayksikön on tehtävä tiedonhallinnan muutosvaikutusten arviointi tiedonhallintamalliin olennaisesti vaikuttavista hallinnollista uudistuksista sekä tietojärjestelmien käyttöönotoista. Muutosvaikutuksen arvioinnin tarpeellisuus tulee arvioida myös olennaisten tietojärjestelmämuutosten käyttöönottojen yhteydessä. Osana muutosvaikutusten arviointia tulee arvioida muutosten vaikutus tietoturvallisuuteen. Erityistä huomioita tulee kiinnittää tietoturvallisuuteen automatisoiduissa toimintaprosessien toteuttamisessa, koska niissä käsitellään ja tuotetaan mahdollisesti suuriakin määriä erilaisia tietoja.

Osana muutosvaikutusten arviointia tulee tehdä riskiarvio, jossa selvitetään, minkälaisia riskejä muutos voi aiheuttaa tiedonhallinnalle, tietojenkäsittelylle, tietojärjestelmille ja tietoaineistoille[5]. Riskikartoituksen perusteella tulee suunnitella toimenpiteet, joilla riskit voidaan minimoida. Ennakollisen suunnittelun tarkoituksena on varmistaa tietojen saanti ja viranomaisen toiminta lakisääteisten tehtävien hoitamiseksi ja palvelujen tuottamiseksi. Muutostarpeen arvioinnissa ja tietoturvallisuustoimenpiteiden mitoittamisessa voi hyödyntää Julkri-arviointikriteeristöä. Tarkempia tietoja tiedonhallintamallin ylläpidosta ja muutosvaikutusten arvioinnista saa tiedonhallintalautakunnan suosituksista.[6]

2.4 Luokittelu ja turvallisuusluokittelu

Organisaatioita suositellaan luokittelemaan tietoaineistot sekä tietojärjestelmät luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Luokittelu mahdollistaa tietoturvallisuustoimenpiteiden suunnittelun ja toteuttamisen sekä tukee lakisääteistä turvallisuusluokittelua.

Luokittelu

Tiedonhallintalaissa ei ole yleistä tietoaineistojen luokittelua koskevaa vaatimusta. Tietoaineistojen sekä niiden käsittelyssä käytettävien tietojärjestelmien luokittelu tukee tiedonhallintalaissa edellytettyjen tietoturvallisuustoimenpiteiden suunnittelua ja toteuttamista.

Organisaation tietojärjestelmien tietoturvallisuusvaatimusten sekä tietoturvallisuusohjeiden räätälöinti erikseen kaikille yksittäisille tietoaineistoille ei ole käytännössä mahdollista. Sen sijaan organisaatioita suositellaan määrittelemään tietoturvallisuusvaatimukset eri luokkiin kuuluville tietoaineistoille sekä hyödyntämään näitä vaatimuksia tietoturvallisuustoimenpiteiden suunnittelussa ja tietoaineistojen käsittelyssä.

5 HE 284/2018 5 § 3 mom.

6 Suositus tiedonhallintamallista (VM 2024) luku 4.4. ja Suositus tiedonhallinnan muutosvaikutusten arvioinnista (VM 2024) luku 3.4.

Tiedot suositellaan luokittelemaan luottamuksellisuuden, eheyden, saatavuuden ja niiden sisältämien henkilötietojen näkökulmista. Aineistoja luokiteltaessa suositellaan huomioimaan mahdollinen kasautumisvaikutus (Julkri HAL-osion kriteeri Suojattavat kohteet -kasautumisvaikutus).

Julkri-suosituksen luvussa Luokittelutasot, on kuvattu luokittelun eri näkökulmat sekä niihin sisältyvät luokittelutasot. Organisaatioita suositellaan täsmentämään ja ohjeistamaan omassa toiminnassa käytettävät luokittelutasot Julkrissa olevan kuvauksen pohjalta.

Turvallisuusluokittelu

Tiedonhallintalain 18 §:n 1 momentin mukaan ”Valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle”.

Lisätietoja turvallisuusluokittelusta löytyy turvallisuusluokiteltavien asiakirjojen käsittelyä koskeva suosituksesta.[7] Lisätietoja kriittisen kohteiden luokittelusta löytyy DVV:n Digiturvapalveluiden julkaisusta kriittisten kohteiden luokittelun menetelmäkuvauksesta vuodelta 2022[8].

7 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)

8 Digiturvajulkaisut | Digi- ja väestötietovirasto (dvv.fi)

2.5 Riskienhallinta

Tiedonhallintayksiköiden on selvitettävä olennaiset tietoturvallisuuteen kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Lisäksi organisaatioita suositellaan käyttämään dokumentoitua riskienhallinnan menetelmää ja ohjeistamaan sen soveltaminen tietoturvallisuusriskien hallinnassa.

Tiedonhallintalain 13 §:n 1 momentin mukaan ”Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti”. Lisäksi tiedonhallintalain 13 a §:ssä, 28 c §:ssä ja 28 f §:ssä edellytetään riskienhallintaa.

Tiedonhallintalaissa edellytetään tietoaineistojen luottamuksellisuuteen, eheyteen ja saatavuuteen sekä tietojärjestelmien käyttöön ja vikasietoisuuteen liittyvien olennaisten riskien säännöllistä arviointia koko niiden elinkaaren ajan. Olennaisilla riskeillä tarkoitetaan riskejä, jotka voivat vaikuttaa viranomaisen toimintaan tai hallinnon asiakkaan toimintaan haittaavalla tai vahingoittavalla tavalla. Lisäksi viranomaisilta edellytetään automaattisessa ratkaisumenettelyssä virheettömyyteen liittyvien riskien hallintaa.

Tiedonhallintayksiköiden tulee mitoittaa tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Tietoturvallisuustoimenpiteet on suhteutettava riskienhallinnan keinoin muun muassa uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Tietoturvallisuustoimenpiteiden suunnittelussa ja riskien arvioinnissa on suositeltavaa huomioida eri turvallisuustoimenpiteiden muodostama kokonaisuus. Esimerkiksi käsiteltäessä salassa pidettäviä tai turvallisuusluokiteltuja tietoja etäkäytössä, on käyttäjien vahva tunnistaminen perusteltu vaatimus. Jos käsittely tapahtuu turvallisissa toimitiloissa, joihin pääsy sivullisilta on estetty, voi käyttäjätunnukseen ja salasanaan perustuva tunnistaminen riittää.

Riskienhallinta on kokonaisuus, johon kuuluu riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella, jäännösriskien hyväksyminen sekä tietoturvallisuustoimenpiteiden toteuttaminen. Riskienhallinnan tulee olla jatkuvaa ja suunnitelmien toteutumista sekä toteutettujen tietoturvallisuustoimenpiteiden vaikuttavuutta tulee arvioida säännöllisesti.

Tietoturvallisuuteen liittyvien riskien hallinnassa on suositeltavaa hyödyntää dokumentoitua ja ohjeistettua riskienhallintamenetelmää, joka varmistaa yhdenmukaiset tulokset arvioijasta ja riskien tyypistä riippumatta. Esimerkki riskienhallinnan menetelmästä löytyy Riskienhallinnan käsikirjasta[9].

Organisaatiot voivat toteuttaa seuraavia toimenpiteitä laadukkaan tietoturvallisuusriskien hallinnan varmistamiseksi:

- varmistaa, että tietoturvallisuusriskien tunnistamisen lähtötietoina ovat ajantasaiset kuvaukset organisaation käsittelemistä tietoaineistoista, käsittelyprosesseista ja käsittelyssä hyödynnettävistä tietojärjestelmistä sekä niiden vastuista (ajantasainen tiedonhallintamalli voi toimia tällaisena lähtötietona)
- suunnitella loogiset kokonaisuudet, joihin riskien tunnistamista ja arviointia kohdistetaan sekä varmistaa riskienhallinnan kattavuus,
- suunnitella ja priorisoida tietoaineistojen luokittelun perusteella tietoturvallisuusriskien tunnistamiseen ja arviointiin liittyvät toimenpiteet,
- kirjata säännöllisesti toteutettavat riskienhallintatoimenpiteet vuosikelloon,
- laatia ohjeet riskien todennäköisyyden ja vaikutusten arvioinnista[10],
- määritellä tietoturvallisuusriskien hyväksymiskriteerit ja menettelyt, joiden mukaisesti jäännösriskit hyväksytään,
- viedä johdon asettamat hyväksymiskriteerit ylittävät jäännösriskit organisaation johdon päätettäväksi sekä
- seurata suunniteltujen riskienkäsittelytoimenpiteiden toteutumista ja vaikuttavuutta.

Tietoturvallisuusriskien arvioinneissa voidaan hyödyntää Julkrin HAL-osion kriteerejä Riskienhallinta.

9 Riskienhallinnan käsikirja valtionhallinnon toimijoille (VM 2023:54)

10 Ohjeen pohjana voi hyödyntää Riskienhallinnan käsikirjan luvussa ”Riskien merkityksen arviointi” olevia taulukoita, mutta niitä on suositeltavaa täydentää konkreettisilla organisaation tietoturvallisuusriskienhallintaa tukevilla esimerkeillä.

2.6 Ohjeet ja koulutus

Organisaatiolla tulee olla ajantasaiset ohjeet tietoturvallisuudesta sekä tarjolla koulutusta niiden riittävän tuntemisen varmistamiseksi.

Tiedonhallintalain 4 §:n 2 momentin mukaan ”Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on

2) ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta;

3) tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista”.

Ohjeissa tulee huomioida seuraavat näkökohdat:

- miten tietoaineistoja käsitellään toimintaprosesseissa,
- miten tietojärjestelmiä käytetään tietoturvallisella tavalla lainmukaisiin käyttötarkoituksiin,
- miten tietojenkäsittelyoikeudet määritellään tietojärjestelmiin ja niillä operoitaviin tietovarantoihin sekä niissä oleviin tietoaineistoihin,
- millä perusteella ja kenen toimesta käyttöoikeuksia myönnetään,
- miten organisaation sisäisen tehtäväjaon mukaiset tietoturvallisuuden vastuut toteutetaan käytännössä,
- miten ja kenen vastuulla on tietopyyntöihin vastaaminen ja millä tavalla pyydetyt tiedot annetaan sekä
- varautuminen poikkeaviin tilanteisiin, kuten esimerkiksi tietoliikennehäiriöön tai tietojärjestelmässä olevan käyttökatkoon.

Koulutuksiin ja perehdytyksiin kohdistuvat seuraavat vaatimukset:

- organisaation tulee tarjota mahdollisuus koulutukseen tai muuhun perehdytykseen tietoturvallisuuteen liittyvistä menettelytavoista, määräyksistä ja ohjeista,
- koulutusten ja perehdytysten tulee sisältää tietoja sovellettavasta lainsäädännöstä, mukaan lukien asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä sekä
- koulutusta tulee järjestää henkilöstölle ja muille tiedonhallintayksikön lukuun toimiville.

Muita ohjeisiin ja koulutuksiin liittyviä suosituksia:

- laatia ohjeet kuinka eri luokkiin kuuluvia tietoja tulee käsitellä,
- varmistaa ohjeiden ymmärrettävyys henkilöillä, jotka eivät ole tietoturva-asiantuntijoita,
- jakaa ohjeet riittävän pieniin kokonaisuuksiin, joista on nopeasti löydettävissä ohjeen pääasiallinen sisältö,
- käyttää tehostekeinoja, jotka korostavat ohjeen pääasiallista sisältöä,
- varmistaa, että ohjeen otsikko ja sisältö vastaavat toisiaan,
- toteuttaa hakupalvelut, joiden avulla ohje on helposti löydettävissä,
- linkittää ohjeet niihin tilanteisiin, joissa niitä todennäköisesti tarvitaan,
- koota ajantasaiset tietoturvallisuusohjeet yhteen paikkaan, josta organisaation käyttäjien on helppo löytää ne,
- viestiä ohjeista sekä niihin tehdyistä muutoksista,
- huolehtia, että tietoturvallisuutta koskevat koulutukset ovat saatavilla myös verkon kautta ajankohdasta riippumatta sekä
- varmistaa, että ohjeisiin on tutustuttu ja keskeinen sisältö on ymmärretty.

2.7 Varautuminen häiriötilanteisiin

Tiedonhallintayksikön on selvitettävä toiminnan jatkuvuuteen kohdistuvat olennaiset riskit ja huolehdittava etukäteisvalmisteluin toiminnan mahdollisimman häiriöttömästä jatkumisesta sekä normaaliolojen häiriötilanteissa että poikkeusoloissa.

Tiedonhallintalain 13 a §:n 3 ja 4 momentin mukaan ”Tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit. Tiedonhallintayksikön on riskiarvioinnin perusteella valmiussuunnitelmin ja häiriötilanteissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava, että sen tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa.

Viranomaisten yleisestä varautumisvelvollisuudesta poikkeusoloihin sekä valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä poikkeusoloissa säädetään valmiuslaissa”.

Tiedonhallintayksikön on varauduttava toiminnassaan siihen, että tietojärjestelmät vikaantuvat tai niiden toiminta muusta syystä estyy. Tietojärjestelmien mahdollisimman häiriötön toiminta tulee pyrkiä turvaamaan kaikissa tilanteissa huomioiden tietojärjestelmien kriittisyys. Lisäksi tulee varautua turvaamaan tietojen käsittelyn ja toiminnan jatkuvuus myös niissä tilanteissa, joissa tietojärjestelmää ei voida käyttää.

Tiedonhallintayksikön on selvitettävä olennaiset toiminnan jatkuvuuteen kohdistuvat riskit. Riskejä ovat tietojärjestelmän vikaantumisen lisäksi esimerkiksi riippuvuudet muiden hallinnassa olevista tietoaineistoista ja –järjestelmistä, häiriöt sähkönsyötössä tai viestintäverkkojen ja -palvelujen toiminnassa, sekä toimitusketjujen kriittisyys ja niiden varautumisen taso. Toiminnan jatkuvuuteen liittyvät näkökohdat on huomioitava myös toimittajien kanssa tehtävissä sopimuksissa. Riskiarvioinnissa tulee ottaa huomioon tietoaineistojen ja tietojärjestelmien kriittisyys sekä jatkuvuuden turvaamisen mahdollisuudet.

Viranomaisen on suunniteltava ennalta, miten se tiedottaa muille viranomaisille häiriötilanteissa. Suunniteltaessa tulee erityisesti kiinnittää huomiota niille viranomaisille tiedottamiseen, joiden toiminta on riippuvaista viranomaisen tietojärjestelmän toiminnasta. Lisäksi viestinnän suunnittelussa on otettava huomioon digitaalisten palvelujen ja tietoaineistojen saatavuuden osalta tiedottaminen yleisölle tarjottavien palvelujen järjestelyistä.

Häiriötilanteisiin varautumiseksi suositellaan:

- tarvittaessa luokittelemaan tietojärjestelmät myös niiden kriittisyyden perusteella,
- toteuttamaan teknisiä ja rakenteellisia etukäteisvalmisteluja sekä tilojen ja kriittisten resurssien varauksia,

- varmistamaan henkilöstön osaaminen ohjeistamalla ja kouluttamalla sekä häiriötilanteiden harjoittelulla,
- suunnittelemaan sijaisjärjestelyt,
- suunnittelemaan häiriötilanteisiin liittyvät viranomaisilmoitukset,
- varautua ottamaan käyttöön vaihtoehtoisia asiointimuotoja, mikäli automatisoitua toimintaprosessia ei voida hyödyntää,
- toteuttamaan olosuhdehälytyksiä ja seurantaa, joilla varmistetaan nopea tiedonsaanti tietojärjestelmien häiriötilanteista,
- varmistamaan tehonsyöttö sekä toteuttamaan vaihtoehtoiset tietoliikenneyhteydet,
- varmistamaan tietojen saanti ulkoisista tietovarannoista, jos toiminta, esimerkiksi automaattisessa ratkaisumenettelyssä, edellyttää tietojen saantia,
- suunnittelemaan, miten häiriötilanteista palaudutaan sekä
- sopimaan menettelyt, joilla tietojärjestelmät pystyvät toimimaan tietojen saantiin liittyvissä häiriötilanteissa tai vähintään saamaan ilmoituksen niistä.

2.8 Häiriötilanteista tiedottaminen

Viranomaisen on viipymättä tiedotettava häiriötilanteista sen tietoaineistoja hyödyntäville. Viranomaisia suositellaan suunnittelemaan etukäteen, miten häiriötilanteista tiedotetaan.

Tiedonhallintalain 13 a §:n 1 momentin mukaan ”Viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden. Viranomaisen on tiedotettava häiriön tai sen uhkan arvioidusta kestosta, mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä häiriön tai uhkan päättymisestä”.

Tapa, jolla käyttökatkoista ja palvelun saatavuudesta tiedotetaan, jää viranomaisen harkintaan. Tiedottaminen on mahdollista esimerkiksi viranomaisen yleisillä verkkosivuilla tai asiayhteyteen muuten olennaisesti liittyvällä muulla verkkosivulla. Tiedottamisen tapaan vaikuttaa se, kenelle tiedotetaan. Vakiintuneille yhteistyötahoille

ja viranomaisen tietoaineistoista keskeisesti riippuvaisille tiedottaminen voi olla kohdennetumpaa kuin yleisölle suunnattu tiedottaminen. Viranomaisen on myös tiedotettava mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä kertoa häiriön arvioitu kesto.

Häiriötilanteista tiedottamiseen suositellaan:

- suunnittelemaan etukäteen, miten ja kenelle häiriötilanteissa tiedotetaan,
- määrittelemään tiedottamisen vastuut sekä
- varmistamaan tiedon nopea perillemeno ja ymmärrettävyys.

Lisäksi digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) 4 §:n 2 momentin mukaan viranomaisen on tiedotettava digitaalisten palvelujensa ja muiden tiedonsiirtomenetelmien käyttökatkoista sopivalla tavalla ennalta yleisölle. Viranomaisen on myös julkaistava käyttökatkon ajaksi ohjeet, miten jokainen saa asiansa hoidetuksi vaihtoehtoisella tavalla.

2.9 Valvonta

> Tiedonhallintayksikön johdon on huolehdittava, että yksikössä on järjestetty riittävä valvonta tietoturvallisuutta koskevien säädösten, määräysten ja ohjeiden noudattamisesta ja että henkilöstöllä on riittävä osaamistaso.

Tiedonhallintalain 4 §:n 2 momentin 5 kohdan mukaan ”Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta”.

Tiedonhallintayksikössä on oltava riittävät valvontamenettelyt, joilla varmistetaan tietoturvallisuutta koskevien laeissa säädettyjen vaatimusten sekä tiedonhallintayksikön sisäisten määräysten ja ohjeiden noudattaminen. Valvontaan sisältyy myös

henkilöstön tietoturvallisuusosaamisen riittävyyden valvonta. Valvonnan järjestäminen on osa sisäisen valvonnan järjestelyjä ja tietoturvallisuustoimenpiteiden toteuttamista.

Valvonnan toteuttamiseksi organisaatio voi toteuttaa seuraavia toimenpiteitä:

- dokumentoida, miten valvontavastuut on jaettu johdolle ja esimiehille,
- laatia valvontasuunnitelma, johon on kuvattu ja aikataulutettu valvontatoimenpiteet,
- järjestää testejä tietoturvallisuusosaamisesta ja määräysten tuntemisesta,
- toteuttaa tietojärjestelmiin automaattisia valvontakontrolleja,
- kuvata, miten valvonnan toimivuutta arvioidaan ja kehitetään sekä
- raportoida määräajoin johdolle tietoturvallisuuden valvonnan tuloksista.

3 Tietoaineistot

3.1 Tietoaineistojen tietoturvallisuus

Viranomaisten on varmistettava tarpeellisin tietoturvallisuustoimenpitein tietoaineistojen turvallisuus ottaen huomioon tiedonhallintalain 15 §:ssä eritellyt vaatimukset.

Yksittäisten tietoturvallisuustoimenpiteiden määrittely tulee tehdä riskiarvion perusteella

Tiedonhallintalain 15 §:n 1 momentin mukaan ”Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:

1. tietoaineistojen muuttumattomuus on riittävästi varmistettu;
2. tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;
3. tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;
4. tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;
5. tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;
6. tietoaineistot voidaan tarvittavilta osin arkistoida.”

Edellä oleva pykälä sisältää luettelon pakollisista vaatimuksista tietoaineistojen tietoturvallisuustoimenpiteiden toteuttamiseksi.

Viranomaisten on varmistettava tietoaineistojen muuttumattomuus tarvittavassa laajuudessa. Tietoaineistojen muuttumattomuus on osassa tietoaineistoja tärkeää niiden todistusvoimaisuuden kannalta. Muuttumattomuus tulee varmistaa erityisesti tietoaineistoissa, joilla määritellään yksilöiden ja yhteisöjen etuja, oikeuksia ja velvollisuuksia. Viranomainen voi harkita, miten muuttumattomuus varmistetaan.

Tietoaineistot tulee suojata teknisiltä ja fyysisiltä vahingoilta. Vaatimus koskee muun muassa tietojärjestelmien ja niihin liittyvien palvelimien säilytystiloja sekä paperimuotoisten tietoaineistojen säilytyspaikkoja.

Tietojen alkuperäisyys, ajantasaisuus ja virheettömyys ovat tärkeitä viranomaistoiminnan asianmukaisuuden sekä hallinnossa työskentelevien ja hallinnon asiakkaiden oikeusturvan varmistamiseksi.

Viranomaisten toiminta on tietointensiivistä ja riippuvaista viranomaisten tietovarannoissa olevista tietoaineistoista. Asianmukaisen viranomaistoiminnan varmistamiseksi on varmistettava, että tiedot ovat saatavissa käyttökelpoisessa muodossa.

Pääsyä julkisiin tietoaineistoihin ei tule rajoittaa tarpeettomasti. Pääsyn rajoittaminen henkilötietoihin ja salassa pidettäviin tietoihin perustuu lakiin.

Tietoaineistot on voitava arkistoida tarpeellisilta osin. Arkistoituihin tietoaineistoihin sovelletaan tiedonhallintalain tietoturvallisuussäännöksiä, ellei muualla ole toisin säädetty. Arkistoinnista on säädetty erikseen arkistointia koskevissa säädöksissä, joista keskeisimpiä ovat arkistolaki (831/1994), EU:n yleinen tietosuoja-asetus ((EU) 2016/679), jäljempänä *tietosuoja-asetus*, sekä tietosuojalaki (1050/2018).

Lisäksi suositellaan, että organisaatiot määrittelevät riskiarvion perusteella tietoaineistoihin, niiden käsittelyssä käytettäviin tietojärjestelmiin sekä tietoaineistojen käsittelyprosesseihin kohdistuvat yksityiskohtaiset tietoturvallisuustoimenpiteet, kuten tämän suosituksen luvuissa 2.5 Riskienhallinta ja 4.1 Tietojärjestelmien tietoturvallisuus on kuvattu. Yksittäisten tietoturvallisuustoimenpiteiden suunnittelussa ja niiden vaatimuksenmukaisuuden arvioinnissa voi hyödyntää Julkri-arviointikriteeristöä.

Organisaatio voi toteuttaa tietoaineistojen tietoturvallisuuden varmistamiseksi esimerkiksi seuraavia toimenpiteitä:

- varmistaa tietoaineistojen muuttumattomuus digitaalisilla varmenteilla,
- sijoittaa laitteistot fyysisen turvallisuuden standardit täyttäviin auditoituihin konesaleihin,
- varmistaa dokumenttien alkuperäisyys sähköisin allekirjoituksin,
- dokumentoida etukäteen perusteet, joilla tietojen saatavuutta voi rajoittaa sekä
- ottaa huomioon tietojen arkistointivaatimukset tietojen elinkaaren alussa.

3.2 Toimitilaturvallisuus

Tietoaineistoja on käsiteltävä ja säilytettävä niiden eheyden, saatavuuden ja luottamuksellisuuden kannalta riittävän turvallisissa toimitiloissa. Turvallisuuden varmistamiseksi suositellaan toteuttamaan riskiperusteisesti ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä.

Tiedonhallintalain 15 §:n 2 momentissa todetaan, että ”Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia”.

Säännös korostaa sitä, että tietoaineistojen säilyttämisessä käytettävissä toimitiloissa on huomioitava kaikki tietoaineistojen säilytystä koskevat tietoturvallisuusvaatimukset. Toimitilaturvallisuuden varmistamiseksi suositellaan toteutettavaksi ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä turvallisuutta vaarantavien tekojen ennalta ehkäisemiseksi, havaitsemiseksi, jäljittämiseksi sekä turvallisuustason palauttamiseksi.

Toimitilaturvallisuus perustuu riskien arviointiin ja monitasoiseen suojaukseen. Siten joissakin tilanteissa voidaan riskien arviointiin perustuen joko hyväksyä puutteita yksittäisissä suojaustoimenpiteissä tai edellyttää normaalia korkeampia toimenpiteitä.

Osana toimitilaturvallisuuden suunnittelua on suositeltavaa määritellä, ohjeistaa ja kouluttaa henkilöstöä, millä edellytyksillä eri tietoaineistoja voi käsitellä ja säilyttää etätöissä tai yhteiskäyttöisissä toimitiloissa.

Toimitilojen suojaamisessa on suositeltavaa hyödyntää Julkri-kriteeristöä sekä siellä määriteltyjä turvallisuusalueita ja fyysisen turvallisuuden kriteereitä.

Toimitilaturvallisuuden varmistamiseksi organisaatio voi toteuttaa esimerkiksi seuraavia toimenpiteitä:

- huolehtia tilojen lukituksista sekä pääsyoikeuksien ja avainten hallinnasta,
- edellyttää henkilöstöltä kuvallisten henkilökorttien käyttöä,

- ottaa käyttöön kulunvalvontajärjestelmä,
- jakaa toimitilat tarvittaessa erillisiin turvallisuusalueisiin ja toteuttaa ylimääräisiä tietoturvallisuustoimenpiteitä alueilla, joissa käsitellään tietoja, joihin kohdistuu korkeampia turvallisuusvaatimuksia,
- sijoittaa työpisteet siten, että salakatselu ei ole mahdollista sekä hankkia salakatselun estäviä suojia,
- huolehtia tilojen äänieristyksistä siten, että salassa pidettävistä tiedoista on mahdollista keskustella turvallisesti sekä
- huolehtia, että vierailijoilla on saattajat.

3.3 Tietoaineistojen sähköiseen muotoon muuttaminen

Viranomaisten tulee varmistaa sähköiseen muotoon muutetun asiakirjan eheys ja luotettavuus.

Tiedonhallintalain 19 §:n 1 momentin mukaan ”Jos asiakirja saapuu viranomaiselle muussa kuin sähköisessä muodossa, on se muutettava sähköiseen muotoon, jos asiakirja on säädetty pysyvästi säilytettäväksi taikka lailla tai lain nojalla arkistoitavaksi. Viranomainen vastaa siitä, että sähköiseen muotoon muutetun asiakirjan luotettavuus ja eheys varmistetaan. Viranomaisen laatimat asiakirjat säilytetään sähköisesti. Sähköiseen muotoon muuttamisesta ja säilyttämisestä voidaan poiketa, jos se on välttämätöntä turvallisuusluokiteltavien asiakirjojen käsittelyä koskevien vaatimusten, muiden tietoturvallisuusvaatimusten tai muun asiakirjan luonteeseen liittyvän välttämättömän syyn vuoksi”.

Viranomaisen tulee lähtökohtaisesti säilyttää laatimiaan ja saapuneita asiakirjoja vain sähköisessä muodossa. Jos asiakirja saapuu viranomaiselle muussa kuin sähköisessä muodossa ja se on säädetty pysyvästi säilytettäväksi tai arkistoitavaksi, on se muutettava sähköiseen muotoon.

Viranomaisen harkintaan jää, milloin saapunut asiakirja muutetaan sähköiseen muotoon. Sähköiseen muotoon muuttamisesta ja säilyttämisestä voi poiketa, jos se on välttämätöntä turvallisuusluokiteltavien asiakirjojen käsittelyä koskevien vaatimusten, muiden tietoturvallisuusvaatimusten tai muun asiakirjan luonteeseen liittyvän välttämättömän syyn vuoksi.

Viranomaisen on huolehdittava sähköiseen muotoon muutetun asiakirjan todistusvoimaisuudesta siten, että sähköiseen muotoon muutetun asiakirjan luotettavuus ja eheys voidaan varmistaa. Käytettävän tekniikan on varmennettava, että viranomainen on tarkastanut ja varmistanut muunnetun asiakirjan tietosisällön. Varmennuksen on oltava sellainen, että jälkikäteen voidaan todentaa, jos asiakirjaan on tehty muutoksia.

Organisaatio voi toteuttaa sähköiseen muotoon muutettujen asiakirjojen eheyden ja luotettavuuden varmistamiseksi esimerkiksi seuraavia toimenpiteitä:

- varmentaa muunnetut asiakirjat esimerkiksi sähköisellä allekirjoituksella sen henkilön toimesta, joka muuntamisen on tehnyt,
- säilyttää tiedot sekä alkuperäisessä muodossa että arkistointikelpoisessa PDF/A-formaatissa sekä
- seurata Kansallisarkiston määräyksiä ja ohjeita koskien tietojen pitkäaikaissäilytystä.

3.4 Tietoturvallinen arkistointi ja tuhoaminen

Tiedonhallintayksikön on huolehdittava tietoaineistojen arkistoinnista tai tuhoamisesta tietoturvallisella tavalla.

Tiedonhallintalain 21 §:n 2 momentin mukaan ”Säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla”.

Arkistointi tai tietoaineistojen tuhoaminen on tehtävä tietoturvallisella tavalla siten, että tietoaineisto ei ole sivullisten saatavilla ja että tietoaineistoa ei enää käsitellä alkuperäiseen käyttötarkoitukseensa. Arkistoinnin edellytyksistä ja arvon määrityksestä saa lisätietoja Kansallisarkistosta[11].

11 Arkistoinnin ohjaus | Kansallisarkisto

Tietoaineistojen tuhoamisella tarkoitetaan sitä, että tietoaineisto on poistettava käytöstä siten, ettei sitä enää voida palauttaa uudelleen käyttöön. Tuhoaminen voidaan tehdä erilaisilla teknisillä toimilla, kuten esimerkiksi kovalevyjen päällekirjoittamisella tai fyysisellä murskaamisella tai sulattamalla. Paperiaineistojen tuhoaminen tapahtuu puolestaan esimerkiksi polttamalla tai silppuamalla. Säännöksellä korostetaan sitä, että aineistot on tuhottava tosiasiallisesti, kun säilyttämiselle ei ole perusteita tai ellei tietoaineistoa siirretä arkistoon säädöksen tai Kansallisarkiston määräyksen perusteella.

Tietoaineistojen tietoturvallisen arkistoinnin tai tuhoamisen varmistamiseksi organisaatio voi toteuttaa seuraavia toimenpiteitä:

- suunnitella arkistointiratkaisun tietoturvallisuustoimenpiteet ottaen huomioon arkistoitavien tietojen luottamuksellisuuteen kohdistuvat riskit,
- huomioida tuhoamismenettelyn valinnassa tietoaineiston luottamuksellisuus,
- ohjeistaa tuhoaminen osana laitteiden elinkaaren hallintaa mukaan lukien oheislaitteet ja muistivälineet,
- sisällyttää laitteistojen osien (kuten kiintolevyt, muistit ja muistikortit) sisältämän tiedon luotettava tuhoaminen osaksi käytöstä poiston, huoltoon lähetyksen ja uusiokäytön prosesseja sekä
- ohjeistaa ja varmistaa tietojen tosiasiallinen tuhoaminen tietoaineistojen elinkaaren päättyessä.

Sähköisessä muodossa olevien tietojen tuhoamisen menetelmiä on kuvattu Julkrin TEK-osion kriteerissä Sähköisessä muodossa olevien tietojen tuhoaminen ja sen alikriteereissä. Tietojen fyysisen tuhoamisen menetelmiä on kuvattu tarkemmin Julkrin FYY-osion kriteerissä Tietojen fyysinen tuhoaminen ja sen alikriteereissä. Suosituksia säilytysajoista ja toimenpiteistä säilytysajan päätyttyä saa tiedonhallintalautakunnan suosituksesta[12].

12 Suositus tietoaineistojen säilytysajasta ja toimenpiteistä säilytysajan päätyttyä (VM 2023:77)

4 Tietojärjestelmät

4.1 Tietojärjestelmien tietoturvallisuus

Tiedonhallintayksikön on seurattava toimintaympäristön tietoturvallisuutta ja varmistettava tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan riskien arviointiin perustuvilla tietoturvallisuustoimenpiteillä.

Yksittäisten tietoturvallisuustoimenpiteiden tunnistamisessa ja valinnassa suositellaan hyödyntämään Julkri-suositusta.

Tiedonhallintalain 13 §:n 1 momentin mukaan ”Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti”.

Tiedonhallintalain 4 §:n 2 momentin 4 kohdan mukaan ”Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on: 4) asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi;”

Tietojärjestelmä voi olla laaja kokonaisuus, johon voi tapauskohtaisesti kuulua laaja joukko erilaisia tietojenkäsittelyyn liittyviä ratkaisuja ja palveluita sekä organisaation sisällä että sen ulkopuolella. Esimerkiksi ulkoistettu pilvipalvelu voi olla tietojärjestelmä tai sen osa, jonka tietoturvallisuus tulee varmistaa. Tarkastelussa tulee huomioida koko palvelun toimitusketju sisältäen myös mahdolliset toimittajan alihankkijoiden vastuulla olevat palvelut.

Tietoturvallisuuden varmistamiseksi suositellaan:

– suunnittelemaan ja kohdistamaan seuranta toiminnan luonteen ja kriittisyyden mukaan,

- varmistamaan, että työvälineet, kuten päätelaitteet, palvelimet ja ohjelmistot ovat tehtävien edellyttämällä tavalla ajantasaisia ja riittävän suojattuja,
- sisällyttämään seurantaan myös organisaation ulkoinen toimintaympäristö,
- seuraamaan ulkoisen ja sisäisen toimintaympäristön välistä tietoliikennettä,
- seuraamaan kriittisten tietojärjestelmien kuormitusta ja käyttöhäiriöitä,
- seuraamaan korkeaa luottamuksellisuutta vaativien tietojen käyttöä ja siinä havaittavia poikkeavuuksia,
- seuraamaan haavoittuvuuksia ja huolehtia niiden nopeasta korjaamisesta sekä
- muodostamaan tilannekuvaa tietoturvallisuudesta.

Lisätietoja seurannan toteutuksesta eri turvallisuuden tasoilla löytyy Julkrin TEK-osion kriteereistä Turvallisuuteen liittyvien tapahtumien jäljitettävyys, Poikkeamien havainnointikyky ja toipuminen sekä niiden alikriteereistä.

Tietoturvallisuustoimenpiteet voivat vaihdella hyvinkin paljon tietojärjestelmän ja siinä käsiteltävien tietojen luonteen perusteella. Tiedonhallintalaissa on määritelty vaatimuksia tietoturvallisuustoimenpiteille esimerkiksi käyttöoikeuksien hallinnan ja tietojen siirtämisen osalta. Tällaisia vaatimuksia on käsitelty myöhemmin tässä luvussa.

Pääosa tietojärjestelmiin kohdistuvista tietoturvallisuustoimenpiteistä tulee määritellä riskiarvioinnin perusteella. Erilaisia tietoturvallisuustoimenpiteitä on paljon ja niiden yksityiskohdat vaihtelevat käsiteltävien tietojen luonteen mukaan. Tämä suositus ei ota kantaa yksittäisiin tietoturvallisuustoimenpiteisiin, mutta niiden tunnistamisessa voi hyödyntää Julkria, joka sisältää työkaluja sekä tarvittavien tietoturvallisuustoimenpiteiden tunnistamiseen että niiden asettamiseen sopivalle vaatimustasolle. Tietoturvallisuustoimenpiteiden määrittelyn perusteena olevaa riskienhallintaa on käsitelty tämän suosituksen luvussa 2.5.

Tietojärjestelmien koko elinkaaren ajan kestävä tietoturvallisuuden varmistaminen edellyttää toimenpiteitä tietojärjestelmien hankinnasta niiden käytöstä luopumiseen asti. Tämä edellyttää, että tietoturvallisuuden tilan seuranta, tietojärjestelmiin kohdistuva riskien arviointi sekä niiden perusteella tehtävä tietoturvallisuustoimenpiteiden ylläpito on suunnitelmallista ja jatkuvaa toimintaa.

4.2 Tietojärjestelmien hankinnat

Hankinnoissa on varmistettava, että tietojärjestelmä täyttää käsiteltävien tietoaineistojen mukaiset tietoturvallisuusvaatimukset ja on käyttökelpoinen viranomaisen tehtävien hoitamiseksi.

Tiedonhallintalain 13 §:n 4 momentin mukaan ”Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet”.

Viranomaisten tietojenkäsittely tapahtuu pääsääntöisesti tietojärjestelmissä. Hankinnoissa on varmistettava, että hankittava tietojärjestelmä täyttää käsiteltävien tietoaineistojen mukaiset tietoturvallisuusvaatimukset ja että tietojärjestelmä on käyttökelpoinen viranomaisen tehtävien hoitamiseksi tuloksekkaasti ja tehokkaasti.

Tiedonhallintalautakunnan suositus tietoturvallisuudesta hankinnoissa[13] sisältää ohjeita tietoturvallisuuden varmistamiseksi tietojärjestelmähankinnoissa sekä liitteitä, joita voi hyödyntää tarjouspyynnöissä ja sopimuksissa. Suosituksessa kuvattu prosessi kattaa vaiheet, joiden avulla suunnitellaan ja varmistetaan hankinnan tietoturvallisuus sekä huolehditaan tietoturvallisuuden säilymisestä koko elinkaaren ajan.

13 Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)

4.3 Vikasietoisuuden ja toiminnallisen käytettävyyden testaus

Viranomaisen tulee testata säännöllisesti olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys.

Tiedonhallintalain 13 §:n 2 momentin mukaan ”Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti”.

Testaus on tarpeellista toiminnan jatkuvuuden varmistamiseksi ja tietoturvallisuustoimenpiteiden ajan tasalla pitämiseksi. Olennaisilla tietojärjestelmillä tarkoitetaan tietojärjestelmiä, jotka ovat kriittisiä viranomaisen lakisääteisten tehtävien toteuttamisen kannalta erityisesti hallinnon asiakkaille palveluja tuotettaessa.

Tietojärjestelmien toiminnallinen käytettävyys tulee varmistaa hankintavaiheessa sekä merkittävien ylläpitotoimien yhteydessä. Toiminnallisella käytettävyydellä tarkoitetaan, että tietojärjestelmä on helposti opittava, sen toimintalogiikka on helposti muistettava, sen toiminta tukee niitä työtehtäviä, joita käyttäjän pitää tehdä tietojärjestelmällä ja tietojärjestelmä edistää sen käytön virheettömyyttä.

Vikasietoisuuden ja toiminnallisen käytettävyyden varmistamiseksi suositellaan seuraavia toimenpiteitä:

- luokittelemaan tietojärjestelmät niiden toiminnallisen kriittisyyden mukaan,
- laatimaan suunnitelma vikasietoisuuden ja toiminnallisen käytettävyyden säännöllisestä testaamisesta,
- parantamaan olennaisten tietojärjestelmien vikasietoisuutta erilaisin keinoin kuten kahdentamalla, hajauttamalla tai varajärjestelmillä,
- ottamaan varmistuksia tiedoista riittävän usein,
- testaamaan, että tietojen palautus varmuuskopioista onnistuu,
- testaamaan toiminnallinen käytettävyys yhdessä järjestelmän varsinaisten käyttäjien kanssa sekä
- suunnittelemaan tietojärjestelmään virheentarkastusmenettelyt sekä käyttäjien syöttämille että ulkopuolisista lähteistä siirrettäville tiedoille.

4.4 Salassa pidettävien tietojen siirtäminen yleisissä tietoverkoissa

Viranomaisen on suojattava salassa pidettävien tietojen siirto yleisissä tietoverkoissa. Lisäksi tietojen vastaanottaja on varmistettava riittävän tietoturvallisella tavalla ennen pääsyä salassa pidettäviin tietoihin.

Tiedonhallintalain 14 §:n 1 momentin mukaan ”Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja”.

Käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa[14].

Viranomainen voi harkita, miten salassa pidettävien tietojen suojaaminen yleisessä tietoverkossa toteutetaan. Yhteys voi olla suojattu esimerkiksi salauksella tai tiedot voidaan siirtää ilman tietoliikenneyhteyden suojaustakin, jos tiedot ovat salattuna siirrettävässä tiedostossa ja salaus voidaan purkaa vain riittävän vahvalla salausavaimella. Lisätietoja löytyy tiedonhallintalautakunnan suosituksesta salassa pidettävien asiakirjojen käsittelystä sekä Julkrin TEK-osion kriteeristä Tiedon salaaminen.

Vaatimus salassa pidettävien tietojen suojaamisesta yleisessä tietoverkossa koskee sekä viranomaisten välistä tietoliikennettä että yleisölle tarjottavia digitaalisia palveluita. Viranomaisen velvollisuudesta tarjota tietoturvallista tiedonsiirtomenetelmää sekä velvollisuudesta tunnistaa digitaalisen palvelun käyttäjä säädetään lisäksi digitaalisten palvelujen tarjoamisesta annetun lain 5 ja 6 §:ssä. Tiedonhallintalaki edellyttää suojaamaan siirrettävät tiedot vain yleisissä tietoverkoissa, koska viranomaisen sisäisessä tietoverkossa tietojen siirtoon liittyvät riskit eivät ole vastaavia kuin yleisessä tietoverkossa.

14 Laki digitaalisten palvelujen tarjoamisesta (306/2019)

Riskiarvion perusteella vaatimusta voi soveltaa myös sellaisissa viranomaisen sisäisissä tietoverkoissa, joissa tietoliikennettä ei ole suojattu salauksella tilanteissa, joissa tietoa siirretään viranomaisen hallinnoimien fyysisten turvallisuusalueiden ulkopuolella tai tuntemattoman tietoverkon kautta.

Vastaanottajan varmistaminen tietojärjestelmien välillä voidaan toteuttaa esimerkiksi palvelinvarmenteita käyttämällä. Jos salassa pidettävien tietojen vastaanottaja on luonnollinen henkilö, tulee hänet tunnistaa jollakin luotettavalla menetelmällä, kuten vahvaa sähköistä tunnistusmenetelmää käyttämällä.

Vaatimus salassa pidettävien tietojen vastaanottajan tunnistamisesta ja varmistamisesta koskee esimerkiksi viranomaisten välistä viestintää sähköpostin avulla sekä viranomaisten tietojärjestelmien välistä viestintää rajapintojen avulla.

4.5 Käyttöoikeuksien hallinta

> Viranomaisen tulee varmistaa, että tietojärjestelmiin pääsevät vain ne henkilöt, joilla on oikeus käsitellä tietoaineistoja tietojärjestelmässä ja vain siltä osin kuin heidän tehtäviinsä perustuvat tietoaineistojen käyttötarpeet sitä edellyttävät. Käyttöoikeudet tulee pitää jatkuvasti ajan tasalla.

Tiedonhallintalain 16 §:n mukaan ”Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina”.

Käyttöoikeudet on määriteltävä ennalta kullekin tietojärjestelmän käyttäjälle käyttäjän tyypillisten työtehtävien mukaisesti. Käyttöoikeudet on pidettävä ajantasaisena, jotta tarpeellinen tietoihin pääsy voidaan varmistaa ja toisaalta estää vanhentuneiden käyttöoikeuksien perusteella tiedonsaanti laajemmin kuin käyttäjän tehtävät edellyttävät.

Käyttöoikeuksien hallinnan vastuut tulee määritellä osana tiedonhallintamallia siten, että tiedetään, kenen vastuulle käyttöoikeuksien määrittely ja ylläpito kuuluvat. Tietojärjestelmästä vastuussa oleva viranomainen ei välttämättä ylläpidä käyttöoikeuksia, vaan tietojärjestelmää käyttävä viranomainen voi olla vastuussa käyttöoikeuksien ajan tasalla pitämisestä. Esimerkiksi palvelukeskus voi määritellä käyttöoikeudet tietojärjestelmän vastuuviranomaisena, mutta tietojärjestelmää käyttävät viranomaiset huolehtivat käyttöoikeuksien ajantasaisuudesta.

Käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiseksi organisaatio voi:

- määritellä prosessit, jonka mukaisesti käyttöoikeudet eri tietojärjestelmiin hyväksytään ja ylläpidetään,
- määritellä kunkin tietojärjestelmän käyttöoikeuksien hallinnan vastuut,
- uudelleenarvioida ja päivittää käyttöoikeudet työntekijöiden tehtävämuutosten yhteydessä,
- sisällyttää käyttöoikeuksien poistamisen työsuhteiden ja palvelusopimusten päättymisprosesseihin,
- varmistaa käyttöoikeuksien ajantasaisuuden määräajoin tehtävillä tarkastuksilla,
- välttää yhteiskäyttötunnuksien käyttöä ilman pakottavaa perusteltua syytä,
- käyttää kertakirjautumista mahdollisimman laajasti,
- ottaa käyttöön monivaiheisen tunnistautumisen erityisesti kirjauduttaessa palveluihin suojatun ympäristön ulkopuolelta sekä
- huomioida käyttöoikeuksissa tietojen luokittelusta ja sopimuksista johtuvat vaatimukset.

Lisätietoja käyttöoikeuksien hallintaan löytyy Julkrin HAL-osion kriteeristä Käyttö- ja käsittelyoikeudet sekä TEK-osion kriteereistä Hallintayhteydet, Pääsyoikeuksien hallinnointi sekä Tietojenkäsittely-ympäristön toimijoiden tunnistaminen.

4.6 Lokitietojen kerääminen

Viranomaisen tulee kerätä tarpeelliset lokitiedot tietojärjestelmän käytöstä ja tietojen luovutuksista erityisesti, jos tietojärjestelmässä käsitellään salassa pidettäviä tietoja tai henkilötietoja.

Tiedonhallintalain 17 §:n mukaan ”Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista”.

Lokitietojen keräämisen tarkoituksena ja perusteena on toteuttaa viranomaisten tietojärjestelmien tietoturvallisuutta siten, että lokitietojen perusteella voidaan selvittää virhetilanteita ja valvoa tietojärjestelmien käyttöä muun muassa oikeusturvan toteuttamiseksi ja virkavastuun todentamiseksi.

Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen peruste.

Käyttölokitietoja kerätään tietojen tallentamisesta, muuttamisesta, poistamisesta, katselusta ja muista tietoihin kohdistuvista toimenpiteistä. Käyttölokitiedot tulee kerätä esimerkiksi tietojärjestelmistä, joissa käsitellään salassa pidettäviä tietoja ja henkilötietoja. Muissa tapauksissa käyttölokitietojen tarpeellisuus tulee arvioida sillä perusteella, onko niillä merkitystä virheiden selvittelyn, yksilön oikeusturvan, virkavastuun todentamisen tai henkilötietojen suojaamisen näkökulmista.

Viranomaisen tulee määritellä lokitietojen säilytysajat tarpeellisuuden perusteella. Yleisesti lokitietojen säilytysaika on vähintään viisi vuotta viranomaistoiminnassa rikosoikeudellisten vanhentumisaikojen vuoksi, mutta lainsäädännön perusteella voi olla pidempiäkin säilytysaikoja. Lisäksi lokitiedot voivat sisältää henkilötietoja, joiden käsittelyssä tulee huomioida tietosuoja-asetuksen vaatimukset.

Lokitietojen keräämisen lainmukaisuuden ja tehokkuuden varmistamiseksi suositellaan:

- määrittelemään tarpeelliset lokitiedot tietojärjestelmittäin ja laatimaan tarvittaessa lokisuunnitelmat,
- määrittelemään sekä koko organisaation lokitietojen hallinnan että kunkin yksittäisen tietojärjestelmän lokitietojen vastuut,
- suunnittelemaan ja ohjeistamaan lokitietojen keruu ja käsittely sekä niissä noudatettavat tietoturvamenettelyt,
- ottamaan käyttöön keskitetty lokienhallintajärjestelmä, jos organisaatiossa kerätään paljon lokitietoja,
- suunnittelemaan ja toteuttamaan lokitietoihin perustuva tietojen luovutusten ja käytön seuranta sekä
- ottamaan käyttöön määrämuotoinen lokitietojen poistamisprosessi.

Lisätietoja lokitietojen keruusta ja käytöstä löytyy Julkrin TEK-osion kriteeristä Turvallisuuteen liittyvien tapahtumien jäljitettävyys sekä HAL-osion kriteeristä Seuranta ja valvonta. Lisäksi lokien käytöstä saa lisäohjeita Traficomin ohjeesta[15] ja suosituksia säilytysajoista ja toimenpiteistä säilytysajan päätyttyä tiedonhallintalautakunnan suosituksesta[16].

4.7 Tietojärjestelmien suunnittelu asiakirjajulkisuuden toteuttamiseksi

> Viranomaisten tulee suunnitella tietojärjestelmänsä siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa vaarantamatta salassa pidettävien tietojen luottamuksellisuutta.

Tiedonhallintalain 13 §:n 3 momentin mukaan ”Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa”.

15 Näin keräät ja käytät lokitietoja

16 Suositus tietoaineistojen säilytysajasta ja toimenpiteistä säilytysajan päätyttyä, liite 5 Tiedonhallinta (VM 2023:77)

Vaatimuksen tavoitteena on tietojen saatavuuden varmistaminen viranomaisten tehtävien hoitamiseksi ja viranomaisen toiminnan julkisuuden toteuttamiseksi siten, että salassa pidettävien tietojen salassapito ei vaarannu. Vaatimus kohdistuu tietojärjestelmien, tietovarantojen tietorakenteiden ja niihin liittyvän tietojen käsittelyn suunnitteluun.

Tietojärjestelmät ja niissä käsiteltävät tiedot tulee suunnitella siten, että tietojärjestelmien hakutoiminnot mahdollistavat asiakirjajulkisuuden toteuttamisen ja tietojen saamisen viranomaisen tehtävien hoitamiseksi.

Asiakirjojen julkisuuden mahdollistamiseksi viranomaiset voivat toteuttaa seuraavia toimenpiteitä:

- selvittää eri tietovarantoihin kohdistuvat tiedonsaantivaatimukset sekä viranomaisen toiminnan julkisuuden että eri viranomaisten tehtävien hoitamisen osalta,
- tunnistaa tietovarantoihin sisältyvät julkiset ja salassa pidettävät tiedot,
- suunnitella miten tietovarannon tietoihin kohdistuvat erilaiset saatavuustarpeet voidaan täyttää vaarantamatta salassapitoa,
- suunnitella tietojärjestelmien hakutoiminnot ottaen huomioon salassapitovaatimukset,
- varmistaa tietojen saatavuus myös hankittaessa valmisjärjestelmiä sekä
- dokumentoida tietojärjestelmät ja tietovarannot siten, että tiedonhallintalain 28 §:ssä edellytetty kuvaus asiakirjajulkisuuden toteuttamiseksi voidaan laatia.

Tiedonhallintalautakunta on antanut erillisen suosituksen asiakirjajulkisuuskuvaksen laatimisesta.[17]

17 Suositus asiakirjajulkisuuskuvauksen laatimisesta (VM 2020:22)

SANASTO

Termi	Määritelmä	Lähde
alkuperäisyys; aitous	ominaisuus, joka ilmentää tiedon eheyttä ja sitä, että tiedon alkuperäinen lähde on se, joka sen väitetään olevan	Tiivis tietoturva-sanasto (TSK 31, 2004)
asiakirjan käsittely	asiakirjan vastaanottamista, laatimista, tallentamista, katselua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä ja arkistointia sekä muita asiakirjaan kohdistuvia toimenpiteitä	TLA 2 §
eheys; muuttumattomuus	tiedon ominaisuus, joka ilmentää sitä, että tietoa ei ole muutettu luvatta, ettei se ole tahattomasti muuttunut ja että mahdolliset muutokset voidaan todentaa ja jäljittää	Tietotermit (2018)
	Eheydellä viitaan myös tiedon oikeellisuuteen ja kattavuuteen.	ISO/IEC 27000
hallinnollinen alue	viranomaisen normaaliin työskentelyyn tarkoitettu alue tai tila, jonka osalta aluetta tai tilaa hallitseva toimija varmistaa, että siihen on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamilla henkilöillä	Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
	Hallinnollinen alue tai tila voi olla esimerkiksi toimistotila, useista eri toimistotiloista muodostuva kokonaisuus, palvelintila, konesali tai jonkin yrityksen tai muun yhteisön tila.	
	Turvallisuusluokitusasetuksessa hallinnollinen alue on turvallisuusluokiteltujen asiakirjojen suojaamiseksi määritelty alue, jolla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa.	TLA 9 § 1 kohta

Termi	Määritelmä	Lähde
jäännösriski	riskin käsittelyn jälkeen jäljellä oleva riski	Digi- ja väestötietovirasto.Sanastot.suomi.fi: Hakusana: jäännösriski. VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön. Yhteentoimivuusalusta (suomi.fi) http://uri.suomi.fi/terminology/digiriski/concept-3
käyttökelpoisuus	tiedon ominaisuus, joka ilmentää tiedon laatua sekä sitä, että tieto on käsiteltävissä yleisesti käytössä olevalla tietojärjestelmällä	perustuu HE 284/2018 sisältöön
luokittelu	tietojen ja tietojärjestelmien ryhmittely luokkiin niiden luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvien vaatimusten perusteella	Suositus tietoturvallisuuden vähimmäisvaatimuksista (VM 2024:19)
luottamuksellisuus	tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu muille	Tietotermit (2018)
muuttumattomuus	ks. eheys	
riskiperusteisuus	riskien suuruuden ja niiden hyväksyttävyyden arviointia sekä riskien suuruuden suhteuttamista riskien pienentämisen kustannuksiin osana tietoturvallisuuteen liittyvää päätöksentekoa	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)
saatavuus	tiedon ominaisuus, joka ilmentää sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla	Tietotermit (2018)
tiedonhallintayksikkö	viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti	TihL 2 § 1 mom. kohta 5
tietoaineisto	asiakirjoista ja muista vastaavista tiedoista muodostuva, tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus	TihL 2 § 1 mom kohta 5

Termi	Määritelmä	Lähde
tietojärjestelmä	tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuva kokonaisjärjestely Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja ohjelmistojen käsittelyyn käytettävät päätelaitteet.	TihL 2 § 1 mom. kohta 3
tietoturvallisuustoimenpiteet	tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistaminen hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä	TihL 2 § 1 mom. kohta 8
tietoturva; tietoturvallisuus	järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus	Kyberturvallisuuden sanasto (TSK 52, 2018)
toimintaympäristö	fyysinen tai digitaalinen ympäristö, jossa organisaation tai henkilön toiminta tapahtuu	Sisäisen turvallisuuden sanasto (Sisäministeriö, 29.6.2023)
turva-alue	alue, joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle	TLA 9 § 2 kohta
turvallisuusalue	käsite, joka sisältää hallinnolliset alueet ja turva-alueet	TLA 9 §
turvallisuusluokiteltu asiakirja	asiakirja, johon valtionhallinnon viranomaisen toimesta on tehty turvallisuusluokkaa koskeva merkintä Asiakirja on turvallisuusluokiteltava, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.	TihL 18 § JulkL 24 §

Termi	Määritelmä	Lähde
varautuminen	toiminta, jolla varmistetaan tehtävien mahdollisimman an häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa	Kokonaisturvallisuuden sanasto (TSK 50, 2017)
viranomainen	viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:n 1 momentissa tarkoitettu viranomainen	TihL 2 § 1 mom. kohta 1

Liite 1: Kooste tiedonhallintalain tietoturvallisuusvaatimuksista

Liitteeseen on koottu tiedonhallintalain tietoturvallisuutta koskevat sisällöt. Laista poimittua sisältöä on muokattu ja tiivistetty luettavampaan muotoon pyrkien säilyttämään lain vaatimuksen. Lisäksi luettelon eri kohtien perään on lisätty viittaus suosituksen lukuun, jossa asiaa on käsitelty laajemmin.

1. Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on: TihL 4 § 2 mom (suosituksen luvut 2.1, 2.6, 2.9 ja 4.1)

    1) määritelty tietoturvallisuuden vastuut,
    2) ajantasaiset ohjeet tietoturvallisuustoimenpiteistä,
    3) tarjolla koulutusta tietoturvallisuudesta,
    4) asianmukaiset ja riittävän suojatut työvälineet,
    5) riittävä tietoturvallisuuden valvonta.

2. Tiedonhallintayksikössä ylläpidettävän tiedonhallintamallin on sisällettävä tiedot tietoturvallisuustoimenpiteistä. Lisäksi on arvioitava näihin kohdistuvat muutokset olennaisten muutosten yhteydessä. (TihL 5 § 2 mom (suosituksen luku 2.3)
3. Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. TihL 12 § (suosituksen luku 2.2)
4. Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. TihL 13 § 1 mom (suosituksen luvut 2.5 ja 4.1)
5. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. TihL 13 § 1 mom (suosituksen luvut 2.5 ja 4.1)
6. Viranomaisen on varmistettava tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen

käytettävyys riittävällä testauksella säännöllisesti. TihL 13 § 2 mom (suosituksen luku 4.3)

7. Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa. TihL 13 § 3 mom (suosituksen luku 4.7)
8. Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. TihL 13 § 4 mom (suosituksen luku 4.2)
9. Viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden. TihL 13 a § 1 mom (suosituksen luku 2.8)
10. Tiedonhallintayksikön on selvitettävä tietojen käsittelyyn kohdistuvat olennaiset riskit sekä riskiarvioinnin perusteella huolehdittava, että tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä poikkeusoloissa. TihL 13 a § 3 mom (suosituksen luvut 2.5 ja 2.7)
11. Viranomaisen on toteutettava salassa pidettävien tietojen siirto yleisessä tietoverkossa salattuna tai muuten suojattuna sekä varmistettava vastaanottaja riittävän tietoturvallisella tavalla. TihL 14 § 1 mom (suosituksen luku 4.4)
12. Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein tietoaineistojen: TihL 15 § 1 mom (suosituksen luku 3.1)

    1) muuttumattomuus;
    2) suojaus teknisiltä ja fyysisiltä vahingoilta;
    3) alkuperäisyys, ajantasaisuus ja virheettömyys;
    4) saatavuus ja käyttökelpoisuus;
    5) saatavuuden rajoittaminen vain, jos laissa on erikseen rajoitettu;
    6) arkistoitavuus.

13. Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia. TihL 15 § 2 mom (suosituksen luku 3.2)
14. Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet käyttäjän tehtäviin liittyvien

käyttötarpeiden mukaan ja pidettävä ne ajantasaisina. TihL 16 § (suosituksen luku 4.5)

15. Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. TihL 17 § (suosituksen luku 4.6)
16. Valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. TihL 18 § (suosituksen luku 2.4)
17. Viranomaisten tulee muuttaa pysyvästi säilytettävät ja arkistoitavat saapuvat asiakirjat sähköiseen muotoon sekä varmistaa niiden eheys ja luotettavuus. TihL 19 § 1 mom (suosituksen luku 3.3)
18. Säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla TihL 21 § 2 mom (suosituksen luku 3.4)

LÄHTEET

Säädökset

Arkistolaki (831/1994). https://www.finlex.fi/fi/laki/ajantasa/1994/19940831.

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

Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi (HE 284/2018 vp). https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_284+2018.pdf.

Hallintovaliokunnan mietintö koskien hallituksen esitystä eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi. (HaVM 38/2018 vp). HaVM 38/2018 vp (eduskunta.fi)

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

Laki julkisen hallinnon tiedonhallinnasta (906/2019). Laki julkisen hallinnon tiedonhallinnasta 906/2019 - Ajantasainen lainsäädäntö - FINLEX ®.

Laki sähköisen viestinnän palveluista (917/2014). Laki sähköisen viestinnän palveluista 917/2014 - Ajantasainen lainsäädäntö - FINLEX ®.

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

Laki yksityisyyden suojasta työelämässä (759/2004). Laki yksityisyyden suojasta työelämässä 759/2004 - Ajantasainen lainsäädäntö - FINLEX ®.

Luottotietolaki (527/2007). Luottotietolaki 527/2007 - Ajantasainen lainsäädäntö - FINLEX ®

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

Turvallisuusselvityslaki (726/2014). Turvallisuusselvityslaki 726/2014 - Ajantasainen lainsäädäntö - FINLEX ®.

Valmiuslaki (1552/2011). Valmiuslaki 1552/2011 - Ajantasainen lainsäädäntö - FINLEX ®

Valtion virkamieslaki (750/1994). Valtion virkamieslaki 750/1994 - Ajantasainen lainsäädäntö - FINLEX ®.

Tiedonhallintalautakunnan suositukset

Tiedonhallintalautakunta 2023. Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö. Valtiovarainministeriön julkaisuja 2023:46. http://urn.fi/URN:ISBN:978-952-367-458-5.

Tiedonhallintalautakunta 2020. Suositus asiakirjajulkisuuskuvauksen laatimisesta. Valtiovarainministeriön julkaisuja 2020:22. http://urn.fi/URN:ISBN:978-952-367-304-5.

Tiedonhallintalautakunta 2024. Suositus automaattisen ratkaisumenettelyn käyttöönotosta ja käytöstä. Valtiovarainministeriön julkaisuja 2024:13. http://urn.fi/URN:ISBN:978-952-367-655-8

Tiedonhallintalautakunta 2020. Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa. Valtiovarainministeriön julkaisuja 2020:18. http://urn.fi/URN:ISBN:978-952-367-288-8.

Tiedonhallintalautakunta 2023. Suositus salassa pidettävien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2023:4. http://urn.fi/URN:ISBN:978-952-367-241-3.

Tiedonhallintalautakunta 2024. Suositus tiedonhallinnan muutosvaikutusten arvioinnista. Valtiovarainministeriön julkaisuja 2024. https://vm.fi/tiedonhallintalautakunta

Suositus tiedonhallintamallista. Valtiovarainmisteriön julkaisuja 2024. https://vm.fi/tiedonhallintalautakunta

Tiedonhallintalautakunta 2023. Suositus tietoaineistojen säilytysajasta ja toimenpiteistä säilytysajan päätyttyä. Valtiovarainministeriön julkaisuja 2023:77. http://urn.fi/URN:ISBN:978-952-367-483-7.

Tiedonhallintalautakunta 2023. Suositus tietoturvallisuudesta hankinnoissa. Valtiovarainministeriön julkaisuja 2023:57. http://urn.fi/URN:ISBN:978-952-367-645-9.

Tiedonhallintalautakunta 2021. Suositus teknisistä rajapinnoista ja katseluyhteyksistä. Valtiovarainministeriön julkaisuja 2021:21. http://urn.fi/URN:ISBN:978-952-367-489-9.

Tiedonhallintalautakunta 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2021:5. http://urn.fi/URN:ISBN:978-952-367-500-1.

Tiedonhallintalautakunta 2022. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. Valtiovarainministeriön julkaisuja 2022:4. http://urn.fi/URN:ISBN:978-952-367-906-1.

Ohjeet ja muut materiaalit

Kansallisarkisto. Arkistoinnin ohjaus. Verkkosivusto. Arkistoinnin ohjaus | Kansallisarkisto Viitattu 2.2.2024

Digi- ja väestötietovirasto (2022). Kriittisten kohteiden luokittelu. (11.3.2022). Haku: vuosi 2022 Oppaat ja hyvät käytännöt Kriittisten kohteiden luokittelun menetelmäkuvaus. Digiturvajulkaisut | Digi- ja väestötietovirasto (dvv.fi). Viitattu 2.2.2024

Liikenne- ja viestintävirasto. Traficom. Näin keräät ja käytät lokitietoja. Verkkosivusto. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja?toggle=Lokeja%20eri%20tarkoituksiin. Viitattu 2.2.2024

Valtiovarainministeriö (2023). Riskienhallinnan käsikirja valtionhallinnon toimijoille (2023:54). http://urn.fi/URN:ISBN:978-952-367-633-6. Viitattu 2.2.2024.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-679-4 (pdf)

Maaliskuu 2024