VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Suositus salassa pidettävien asiakirjojen käsittelystä

Lautakunnat

Valtiovarainministeriön julkaisuja – 2023:4

Valtiovarainministeriön julkaisuja 2023:4

Suositus salassa pidettävien asiakirjojen käsittelystä

Valtiovarainministeriö Helsinki 2023

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

ISBN pdf: 978-952-367-241-3
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2023

Kuvailulehti
19.1.2023

Suositus salassa pidettävien asiakirjojen käsittelystä

Valtiovarainministeriön julkaisuja 2023:4		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	suomi	**Sivumäärä**	52

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.

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

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

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

Tiedonhallintalautakunta hyväksyi suosituksen 15.12.2022.

Asiasanat	tietoturva, lautakunnat, tietosuoja, tiedonhallintalautakunta, varautuminen, toimitilat, tiedonhallintalaki, julkinen hallinto, salassa pidettävä asiakirja, salassa pidettävä tieto

ISBN PDF	978-952-367-241-3	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-241-3		

Presentationsblad
19.1.2023

Rekommendation om behandling av sekretessbelagda handlingar

Finansministeriets publikationer 2023:4		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	finska	**Sidantal**	52

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019) finns bestämmelser om ansvar i fråga om 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 av informationshanteringsnämnden redogör för behandlingen av sekretessbelagda handlingar (uppgifter) och uppfyllandet av de krav som gäller behandlingen. Publikationen innehåller de krav som ställs i lagstiftningen, rekommendationer och praktiska exempel som gäller behandlingen av sekretessbelagda handlingar. Bilaga 1 är en sammanställning av rekommendationerna och den rättsliga grund som hänför sig till dem.

Informationshanteringsnämndens tidigare rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet (FM 2021:72) fastställer de minimikrav på informationssäkerhet som ska iakttas inom den offentliga förvaltningen. Det rekommenderas att dessa minimikrav också ska tillämpas på behandlingen av sekretessbelagda handlingar.

Rekommendationen är i första hand avsedd för myndigheter, men utöver dem kan även aktörer inom näringslivet och andra som behandlar handlingar som myndigheterna klassat som sekretessbelagda ha nytta av rekommendationen.

Informationshanteringsnämnden godkände rekommendationen den 15 december 2022.

Nyckelord datasäkerhet, nämnder, datasekretess, informationshanteringsnämnden, beredskap, lokaler, informationshanteringslagen, offentlig förvaltning, sekretessbelagda handlingar, sekretessbelagda uppgifter

ISBN PDF	978-952-367-241-3	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-241-3		

Description sheet
19 January 2023

Recommendation for the processing of non-disclosable documents

Publications of the Ministry of Finance 2023:4		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Finnish	**Pages**	52

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 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 issued by the Information Management Board describes the recommendations and practices to be applied when processing non-disclosable documents (data) and fulfilling the requirements for processing. The recommendation includes legislative requirements, recommendations and practical examples of the processing of non-disclosable documents. The recommendation in the documents and the related legal grounds have been compiled in Appendix 1.

The previously published Collection of recommendations on the application of certain security regulations (VM 2021:65) includes the minimum data security requirements to be complied with in public administration. These minimum requirements are also recommended to be applied to the processing of non-disclosable documents.

The recommendation is primarily intended for authorities, but can also be used by business and industry and any other parties that process documents that have been classified as non-disclosable by the authorities.

The Information Management Board approved the recommendation on 15 December 2022

Keywords data security, board, data privacy, Information Management Board, precautionary measures, business premises, Act on Information Management in Public Administration, public administration, non-disclosable document, non-disclosable information

ISBN PDF	978-952-367-241-3	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-241-3		

Sisältö

1 Johdanto

Julkisen hallinnon tiedonhallintalautakunnan, jäljempänä *tiedonhallintalautakunta*, salassa pidettävien asiakirjojen käsittelyä koskevan suosituksen tarkoituksena on auttaa ja opastaa tiedonhallintayksiköitä ja viranomaisia salassa pidettävien asiakirjojen (tietojen) käsittelyä koskevien vaatimusten toteuttamisessa. Suosituksessa on esitetty tietojen käsittelylle säädettyjä vaatimuksia sekä hyviä käytäntöjä, joita viranomaiset voivat hyödyntää tietojen käsittelyä koskevien toimenpiteiden toteuttamisessa sekä käsittelyä koskevissa ohjeissaan.

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999), jäljempänä *julkisuuslaki* tai *JulkL*, 22 §:n 1 momentin mukaan: ”Viranomaisen asiakirja on pidettävä salassa, jos se tässä tai muussa laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus”.

Salassapito tarkoittaa julkisuuslain 22 §:n 2 momentin mukaan sitä, että salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi. Tavoitteena on suojata salassa pidettävä tieto riippumatta siitä, missä tai miten se esitetään. Salassa pidettävää tietoa koskevasta vaitiolovelvollisuudesta ja hyväksikäyttökiellosta säädetään julkisuuslain 23 §:ssä.

Suositus on tarkoitettu ensisijaisesti viranomaisille, mutta niiden lisäksi tätä suositusta voivat hyödyntää elinkeinoelämän toimijat ja kaikki muutkin, jotka käsittelevät viranomaisten salassa pidettäväksi määrittelemiä asiakirjoja. Jäljempänä näistä tietoturvallisuussääntelyn kohteista käytetään termiä *organisaatio*.

Suosituksen lisäksi organisaatioissa tarvitaan edelleen omaa käsittelyohjeistusta ja koulutusta sekä vastuuhenkilöille että koko henkilöstölle. Tätä varten on julkisen hallinnon tiedonhallinnasta annetun lain (906/2019), jäljempänä *tiedonhallintalaki* tai *TihL*, 4 §:n 2 momentin 2 kohdan mukaan oltava käytössä omaa tarkentavaa materiaalia salassa pidettävien tietojen käsittelyyn liittyvistä käytännön toimenpiteistä.

Suositusta on valmisteltu tiedonhallintalautakunnan kaudelle 1.1.-31.12.2022 asettamassa tietoturvallisuusjaostossa. Jaoston puheenjohtajana on toiminut neuvotteleva virkamies Mika Kuronen valtiovarainministeriöstä ja jaostosihteerinä johtava asiantuntija Tuula Seppo Digi- ja väestötietovirastosta. Tiedonhallintalautakunta on nimennyt jaoston jäseniksi asiantuntijoita eri tiedonhallintayksiköistä. Lisäksi jaosto on kokouksissa, työpajoissa ja seminaareissa kuullut laajalti myös jaoston ulkopuolisia asiantuntijoita. Suositusluonnos oli avoimesti kommentoivana julkisen lausuntopalvelun kautta 30.8.-21.9.2022 välisenä aikana.

1.1 Lainsäädännölliset perusteet

Tiedonhallintalain 10 §:ssä säädetään julkisen hallinnon tiedonhallintalautakunnan tehtävästä edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalainlain vaatimusten toteuttamista. Edistämistehtävän toteuttamiseksi tiedonhallintalautakunta ylläpitää suosituksia, joiden tarkoituksena on ohjata tiedonhallintayksikköjä ja viranomaisia toteuttamaan hyviin käytäntöihin pohjautuen tiedonhallintalaissa säädetyt vaatimukset.

Tiedonhallintalain 4.2 §:ssä säädetään tiedonhallintayksiköiden johdon velvollisuudesta huolehtia, että sillä on ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta. Kyseisen momentin mukaan tiedonhallintayksikön johdon vastuulla on myös huolehtia koulutuksesta, 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. Salassa pidettävien tietojen käsittelyä koskevat ohjeet liittyvät olennaisesti tiedonhallintalaissa tiedonhallintayksikön johdolle säädettyjen vastuiden toteuttamiseen.

Salassa pidettävien tietojen käsittelyä koskevat vaatimukset ovat olennainen arviointikohde tiedonhallintayksikön selvittäessä tiedonhallintalain 13.1 §:n mukaisesti olennaisia sen tietojenkäsittelyyn kohdistuvia riskejä ja sen mitoittaessa tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Riskiarvioinnin perusteella tiedonhallintayksiköt ja niissä toimivat viranomaiset voivat varmistaa tarpeellisin tietoturvallisuustoimenpitein salassa pidettäviä tietoja sisältävien tietoaineistojen turvallisuuden (tiedonhallintalaki 15 §) sekä tietojen käsittelyn edellyttämät käyttöoikeudet tietojärjestelmiin (tiedonhallintalaki 16 §). Lisäksi tiedonhallintalain 14 §:ssä säädetään vaatimuksista salassa pidettävien tietojen siirtämiselle tietoverkoissa.

Salassa pidettävien tietojen käsittelyssä tiedonhallintayksiköt ja viranomaiset soveltavat tiedonhallintalain lisäksi muun muassa julkisuuslakia Tämän vuoksi suosituksessa on esitetty myös julkisuuslaissa säädettyjä vaatimuksia tiedonhallintalaissa säädettyjen vaatimusten yhteydessä ja rinnalla. Esitystavalla on pyritty muodostamaan suosituksen soveltajalle riittävä kuva tietojen käsittelyyn olennaisesti vaikuttavasta yleislainsäädännöstä.

Tiedonhallintalain 18 §:ssä ja sitä täydentävässä valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *turvallisuusluokitteluasetus tai TLA*, säädetään turvallisuusluokittelusta, luokittelumerkinnöistä sekä turvallisuusluokiteltavien asiakirjojen käsittelystä.

Organisaation salassa pidettävät tiedot saattavat sisältää henkilötietoja, joiden käsittelyssä tulee lisäksi ottaa huomioon henkilötietojen käsittelyyn liittyvät vaatimukset. Henkilötietojen käsittelyyn liittyvät yleissäädökset ovat EU:n yleinen tietosuoja-asetus ((EU) 2016/679), jäljempänä *tietosuoja-asetus*, sekä tietosuojalaki (1050/2018). Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä säädetään henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (1054/2018). Henkilötietojen käsittelystä tarkempia ohjeita antaa Tietosuojavaltuutetun toimisto.

1.2 Suhde muihin suosituksiin

Tämä suositus ja muut tiedonhallintalautakunnan suositukset muodostavat yhdessä suosituskokonaisuuden, jonka avulla voidaan suunnitella salassa pidettävien tietojen käsittelyn edellyttämiä toimenpiteitä, muun muassa tietojen suojaamisen osalta. Suositusta laadittaessa on pyritty välttämään päällekkäisyyttä muiden suositusten kanssa. Kooste tähän dokumenttiin sisältyvistä suosituksista ja niiden lakiperustasta on liitteessä 1. Tiedonhallintalautakunnan suositukset, joihin on suositeltavaa perehtyä, on kuvattu alla olevassa taulukossa.

Taulukko 1. Suositeltavia tiedonhallintalautakunnan suosituksia.

Julkaisu	Sisältö
Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (2021:65)	Suositus sisältää julkishallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset sekä yksityiskohtaisia suosituksia tiedonhallintalain tietoturvallisuutta koskevien pykälien soveltamisesta. Näitä suosituksia tulee lähtökohtaisesti soveltaa myös salassa pidettävien tietojen käsittelyssä.
Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) ja Suositus turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa (2022:4)	Suositukset sisältävät turvallisuusluokiteltujen asiakirjojen käsittelyä koskevia suosituksia, joita suositellaan sovellettavaksi riskilähtöisesti ja tilannekohtaista harkintaa käyttäen myös salassa pidettävien tietojen käsittelyssä.
Julkisen hallinnon tietoturvallisuuden arviointikriteeristö, Julkri (2022:43)	Kriteeristön käyttö tukee organisaatioita tietoturvallisuuden ja henkilötietojen suojaamisen suunnittelussa, toteuttamisessa ja arvioinnissa. Sitä voi hyödyntää lainmukaisuuden arvioinnissa ja osana tietosuoja-asetuksen mukaista osoitusvelvollisuutta.
Suositus asiankäsittelyn metatiedoista (2021:33) ja Suositus viranomaisten asiakirjojen metatiedoista palveluja tuotettaessa (2022:42)	Suositukset sisältävät suosituksia rekisteröinnistä ja suositeltavista metatiedoista asiankäsittelyssä ja palveluja tuotettaessa.
Suositus teknisistä rajapinnoista ja katseluyhteyksistä (2021:21)	Suositus sisältää tarkennuksia tiedonhallintalaissa säädettyjen sähköisten luovutustapojen toteuttamiseen.
Suositus tiedonhallintamallista (2020:29)	Suositus sisältää ohjeita ja hyviä käytäntöjä tiedonhallintayksiköiden toimintaympäristön tiedonhallintaa määrittävän ja kuvaavan tiedonhallintamallin laatimiseksi, muun muassa tietoturvallisuustoimenpiteiden osalta.
Suositus tiedonhallinnan muutosvaikutusten arvioinnista (2020:53)	Suositus sisältää ohjeita ja hyviä käytäntöjä tiedonhallintalain 5.3 §:ssä säädetyn muutosvaikutusten arvioinnin toteuttamiselle, muun muassa suhteessa tiedonhallintalain 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja -toimenpiteisiin.

1.3 Rajaukset

Tämä suositus koskee tiedonhallintalain soveltamista salassa pidettävän tiedon käsittelyyn. Tässä suosituksessa ei ole huomioitu:

- turvallisuusluokiteltaviin tietoihin liittyviä käsittelyvaatimuksia,
- toimialakohtaista lainsäädäntöä, kuten sosiaali- ja terveydenhuollon lainsäädäntöön sisältyviä vaatimuksia salassa pidettäville tiedoille,
- henkilötietojen käsittelyä koskevaa sääntelyä,
- kansainvälisistä tietoturvallisuusvelvoitteista johtuvia vaatimuksia eikä ole erikseen otettu huomioon sähköisen viestinnän palveluista annettua lakia (914/2014), jossa säädetään mm. sähköiseen viestintään liittyvien tietojen salassa pidosta ja käsittelystä.

Vaikka suositus ei sisällä edellä mainittuja vaatimuksia, niin organisaation tulee kuitenkin tunnistaa ja ottaa huomioon nämä vaatimukset omassa toiminnassaan ja ohjeistuksissaan.

2 Salassa pidettävien asiakirjojen käsittelyn perusteet

2.1 Salassa pidettävät viranomaisen asiakirjat

Organisaation on tunnistettava, milloin se käsittelee salassa pidettäviä tietoja.

Viranomaisen tiedot jaetaan pääsääntöisesti julkisiin tai salassa pidettäviin tietoihin. Jos nämä tiedot sisältävät henkilötietoja, on huomioitava myös niiden käsittelyyn liittyvä sääntely ja ohjeistus. Salassa pidettävät tiedot voivat myös sisältää turvallisuusluokiteltavia[1] tietoja, jotka on jaettu eri turvallisuusluokkiin. Tietojen luovuttamisen näkökulmasta osa tiedoista, jotka eivät ole salassa pidettäviä, voivat olla harkinnanvaraisesti[2] annettavia.

Julkisuuslain 22 §:ssä[3] säädetään asiakirjasalaisuudesta. Julkisuuslain 24 §:n 1 momentissa on 32 kohtaa, joissa on eritelty viranomaisen salassa pidettävät asiakirjat, joita ovat muun muassa:

> 17) asiakirjat, jotka sisältävät tietoja valtion, hyvinvointialueen, kunnan tai muun julkisyhteisön tai (julkisuuslain) 4 §:n 2 momentissa tarkoitetun yhteisön, laitoksen tai säätiön liikesalaisuudesta,
>
> 20) asiakirjat, jotka sisältävät tietoja yksityisestä liikesalaisuudesta, samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja muusta vastaavasta yksityisen elinkeinotoimintaa koskevasta seikasta,
>
> 25) asiakirjat, jotka sisältävät tietoja sosiaalihuollon asiakkaasta tai työhallinnon henkilöasiakkaasta sekä tämän saamasta etuudesta tai tukitoimesta taikka sosiaalihuollon palvelusta tai työhallinnon henkilöasiakkaan palvelusta taikka tietoja henkilön terveydentilasta tai vammaisuudesta taikka hänen saamastaan terveydenhuollon ja kuntoutuksen palvelusta taikka tietoja henkilön seksuaalisesta käyttäytymisestä ja suuntautumisesta;

1 TihL 18 § ”Turvallisuusluokiteltavat asiakirjat valtionhallinnossa” sekä Turvallisuusluokitteluasetus 3 § ”Turvallisuusluokittelu ja turvallisuusluokan merkitseminen”.

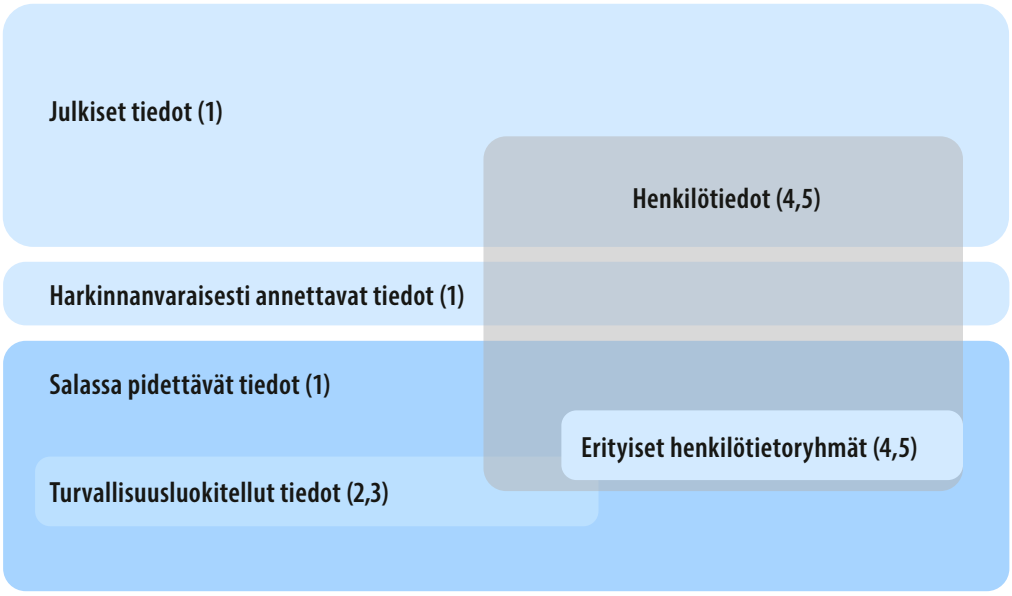
2 JulkL 16 a § ”Muuhun kuin salassa pidettävään asiakirjaan tehtävät merkinnät”, 9 § ”Tiedonsaanti julkisesta asiakirjasta”, sekä 17 § ”Tiedonsaantioikeuksien huomioon ottaminen päätöksenteossa”.

3 JulkL 22 § ”Asiakirjasalaisuus”.

Salassapidosta on säädetty myös muussa lainsäädännössä, mutta näitä salassapidon perusteita ei ole erikseen huomioitu tässä suosituksessa.

Alla olevassa suuntaa antavassa kuviossa on selvennetty julkisten, salassa pidettävien ja turvallisuusluokiteltavien tietojen sekä henkilötietojen ja erityisiin henkilötietoryhmiin kuuluvien tietojen suhdetta toisiinsa. Harkinnanvaraisesti annettavat tiedot on sijoitettu julkisten ja salassa pidettävien tietojen väliin. Harkinnanvaraisesti annettavia tietoja käsitellään tarkemmin luvussa 2.8.

Kuvio 1. Erilaisten tietojen suhde toisiinsa



1) Julkisuuslaki 621/1999
2) Tiedonhallintalaki 906/2019
3) Turvallisuusluokitteluasetus 1011/2019
4) EU:n yleinen tietosuoja-asetus (EU) 2016/679
5) Tietosuojalaki 1050/2018

Henkilötiedot eivät ole salassa pidettäviä, ellei niitä laissa tai asetuksessa ole erikseen säädetty salassa pidettäväksi. On kuitenkin huomioitava, että tietosuojasääntelystä tulee lisävaatimuksia henkilötietojen suojaamisen osalta. Osa erityisiin henkilötietoryhmiin kuuluvista tiedoista on julkisuuslain mukaan 24 § 1 momentin mukaan salassa pidettäviä.

Organisaation tuleekin tunnistaa, mitä tietoja se käsittelee ja mitkä säädökset kyseisiä tietoja koskevat. Tietojen tunnistamisella ja luokittelulla voidaan helpottaa tietoturvaan liittyvien investointien priorisointia. Salassa pidettävät tiedot vaativat lisäsuojaustoimia verrattuna julkisiin tietoihin.

2.2 Vähimmäisvaatimukset ja niiden riskilähtöinen täydentäminen

Organisaation tulee täyttää salassa pidettävän tiedon käsittelyä koskevat lainsäädäntöön pohjautuvat vähimmäisvaatimukset. Lisäksi suositellaan, että organisaatiot täydentävät vähimmäisvaatimuksia soveltamalla riskilähtöisesti tätä ylemmän tason tietoturvallisuusvaatimuksia.

Tiedonhallintalaki ei sisällä kovin yksityiskohtaisia vaatimuksia salassa pidettävien tietojen tietoturvallisuustoimenpiteistä. Tiedonhallintalain 13 §:n 1 momenttiin sisältyvä velvoite ”Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti” toimii perusteena sille, että tarvittavat toimenpiteet voidaan useissa tapauksissa määritellä tapauskohtaisen riskienarvioinnin perusteella. Esimerkiksi salassa pidettävien tietojen määrä sekä oikeudettomasta paljastumisesta aiheutuvat seuraukset vaikuttavat toimenpiteiden valintaan.

Täytyy kuitenkin muistaa, että mitään salassa pidettävää tietoa ei tule joutua vääriin käsiin. Kaikki salassa pidettävä tieto on suojattava erittäin hyvin.

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2021:65) sisältää julkisessa hallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset. Suositusta suositellaan sovellettavaksi myös salassa pidettävien tietojen käsittelyssä. Lisäksi suositellaan, että salassa pidettäviä tietoja käsittelevät organisaatiot täydentävät salassa pidettävien tietojen käsittelyn tietoturvallisuustoimenpiteitä soveltamalla riskilähtöisesti ylemmän turvallisuustason tietojen käsittelyä koskevia suosituksia sekä tietoturvallisuusstandardeissa kuvattuja toimenpiteitä[4] tarpeellisessa laajuudessa. Riskien arvioinnin tulos vaikuttaa siihen, mitkä turvatoimet tulee valita, jotta niiden tavoitteet saavutetaan. Jos riski arvioidaan vähäiseksi esimerkiksi suojatun edun ja mahdollisen vahingon rajallisuuden ja vahingon toteutumisen epätodennäköisyyden perusteella, turvatoimet voivat olla kevyempiä kuin niissä tilanteissa, joissa suojattava etu ja mahdollinen vahinko ovat merkittäviä ja riski vahingon toteutumiseen vähäistä suurempi.

Riskilähtöisessä tietoturvallisuustoimenpiteiden valinnassa tulee ottaa huomioon sekä tietojen luvattoman paljastumisen riskien potentiaaliset seuraukset että niiden pienentämisen kustannukset. Oikean tason löytäminen edellyttää systemaattista riskien arviointia.

4 esimerkiksi SFS-ISO/IEC 27002:2022. Tietoturvallisuuden hallintakeinojen menettelyohjeet.

Edellä olevan perusteella suositellaan, että organisaatiot ottavat käyttöön tietoturvariskien arviointiin soveltuvan riskienarviointimenetelmän[5] sekä soveltavat sitä systemaattisesti salassa pidettävien tietojen käsittelyn tietoturvallisuuden toteuttamisen suunnittelussa. Tämä voidaan toteuttaa esimerkiksi Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä, jäljempänä *Julkri-kriteeristö*, hyödyntämällä siten, että organisaatiot arvioivat, mitkä turvallisuusluokan TL IV tasolle luokiteltujen tietojen tietoturvallisuustoimenpiteistä ovat tarpeellisia myös organisaation salassa pidettäville tiedoille. Tietyissä tapauksissa, kuten esimerkiksi paljon salassa pidettävää tietoa sisältävien tietokasaumien yhteydessä, voi harkita myös turvallisuusluokka TL III tason toimenpiteiden soveltamista.

Kasautumisvaikutus on ilmiö, jossa suuri määrä tietoa voi lisätä riskejä ja muodostaa yksittäisiä tietoja merkittävämmän asiakokonaisuuden. Kasautumisvaikutukseen ei ole yleistä, kaikkiin tilanteisiin sopivaa määrittelyä. Kasautumisvaikutuksen voi aiheuttaa sekä tiedon suuri määrä tai tietolähteiden yhdistäminen. Mahdollinen kasautumisvaikutus pitää huomioida tiedon suojaamisessa ja mahdollisesti luokittelussa.

Esimerkki toimenpiteestä, joita organisaatio voi toteuttaa:

- esimerkiksi organisaation asianhallintarekisteri ja hyvinvointialueen potilastietorekisteri voivat sisältää suuria määriä salassa pidettävää tietoa, minkä johdosta niiden suojaamisessa on riskilähtöisesti harkittava myös turvallisuusluokiteltavien tietojen suojaamisessa käytettäviä hallintakeinoja.

5 esimerkiksi: SFS-ISO/IEC:27001:2022. Tietoturvallisuuden hallintajärjestelmä Luku 6 tai SFS-ISO 31000:2018 Riskienhallinta ja SFS-ISO/IEC:27005:2018 Tietoturvariskien hallinta.

2.3 Tiedon elinkaari ja salassapito

Organisaation tulee tunnistaa salassa pidettävän tiedon käsittelyyn liittyvät prosessit ja tietojärjestelmät sekä varmistaa riskilähtöisesti, että ne ovat riittävän tietoturvallisia koko tiedon elinkaaren ajan.

Tiedonhallintalain 13 §:n 1 momentin mukaan: ”Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan”. Lisäksi lain 13 §:n 4 momentin mukaan: ”Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet”. Tiedonhallintalautakunnan suosituksessa (VM 2021:65) luvussa 8 käsitellään laajasti tietoturvallisuutta tietojärjestelmähankinnoissa.

Näiden perusteella suositellaan, että salassa pidettävän tiedon käsittelyn tietoturvallisuuden varmistamiseksi organisaatio toteuttaa seuraavat toimenpiteet:

- tunnistaa kaikki sen vastuulle kuuluvat salassa pidettävät tiedot ja käsittelijät sekä käsittelyssä käytettävät tietojärjestelmät koko tiedon elinkaaren ajalta,
- määrittelee käsittelyssä käytettävien tietojärjestelmien ja palveluiden tietoturvavaatimukset ottaen huomioon salassa pidettävien tietojen käsittelyyn liittyvät riskit,
- varmistaa tietojärjestelmien ja palveluiden tietoturvavaatimusten täyttymisen hankinnan yhteydessä sekä säännöllisesti koko järjestelmän elinkaaren ajan soveltamalla systemaattisesti muutoshallinnan menettelyitä,
- suunnittelee ja ohjeistaa salassa pidettävän tiedon käsittelyprosessit siten, että käsittely on riittävän turvallista,
- varmistaa riittävällä seurannalla, että edellä kuvatut suositukset täyttyvät sekä ylläpitää tiedonhallintamallia tietoturvallisuuden hallitsemiseksi.

Edellä lueteltujen suositusten toteuttamisen varmistamiseksi organisaatio voi ottaa käyttöön tietoturvallisuuden johtamis- ja hallintajärjestelmän tarkoituksenmukaisessa laajuudessa.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- määritellä ja ohjeistaa salassa pidettävien tietojen käsittelyyn sallitut järjestelmät,
- määritellä järjestelmien tietoturvavaatimukset siten, että ne ovat riittävän turvallisia salassa pidettävien tietojen käsittelyyn ja huolehtia vaatimusten ajantasaisuudesta,
- käsitellä ja säilyttää tietoaineistoja toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia,
- varmistaa vaatimusten toteutumisen sekä
- käyttää ohjelmistoja, joiden turvallisuus on osoitettu ulkopuolisen tarkastuslaitoksen suorittamalla tarkastuksella.

2.4 Salassa pidettävien tietojen merkintä

Organisaatioita suositellaan suunnittelemaan ja toteuttamaan salassa pidettävien tietojen merkitseminen siten, että kaikki henkilöt, jotka käsittelevät tai joille luovutetaan salassa pidettäviä tietoja, ovat tietoisia salassapitovaatimuksesta.

Salassa pidettävien tietojen luottamuksellisuuden varmistamiseksi suositellaan, että organisaatio selvittää systemaattisesti missä eri tilanteissa ja millä eri tietojärjestelmillä käsitellään salassa pidettäviä tietoja sekä suunnittelee näihin menettelyt, joiden avulla varmistetaan, että salassa pidettäviä tietoja käsittelevät henkilöt saavat kaikissa tilanteissa tiedon salassapidosta.

Julkisuuslain 25 §:n 1 momentin mukaan ”Viranomaisen asiakirjaan, jonka viranomainen antaa asianosaiselle ja joka on salassa pidettävä toisen tai yleisen edun vuoksi, on tehtävä merkintä sen salassa pitämisestä. Asianosaiselle on annettava tieto hänen salassapitovelvollisuudestaan myös silloin, kun salassa pidettäviä tietoja annetaan suullisesti.”

Julkisuuslain 25 §:n 2 momentin ensimmäisen virkkeen mukaan merkintä voidaan tehdä muihinkin kuin 1 momentissa tarkoitettuihin asiakirjoihin – eli merkintä voidaan tehdä muulloinkin kuin silloin kun viranomainen antaa asiakirjan asianosaiselle.

Yleinen periaate on, että tiedon laatija määrittelee salassa pidettävän tiedon ja tekee tarvittavat merkinnät. Merkinnästä on käytävä ilmi, miltä osin tieto on salassa pidettävä sekä se, mihin salassa pitäminen perustuu.

Salassapito merkitään asiakirjoihin suomeksi ”SALASSA PIDETTÄVÄ”, ruotsiksi ”SEKRETESSBELAGD”. Salassapitomerkinnöistä ei ole annettu tarkempaa yhtenäistä suositusta, mutta seuraava havainnekuva ilmentää asiakirjoihin tehtävää salassapitomerkintää. Merkintää voidaan käyttää sekä manuaalisissa että sähköisissä asiakirjoissa.

Kuvio 2. Havainnekuva salassapitomerkinnästä.

Tieto salassapidosta voidaan merkitä asiakirjoihin esimerkiksi kappale- tai lukukohtaisesti käyttäen kappaleen tai luvun edessä lyhenteitä (J), joka tarkoittaa julkista tai (SALPID), joka tarkoittaa salassa pidettävää. Jos salassapito perustuu säännökseen, jossa on vahinkoedellytyslauseke, merkintä voidaan tehdä kuitenkin niin, että siitä ilmenee vain se säännös, johon salassapito perustuu.

Tieto salassapidosta voidaan merkitä tietojärjestelmiin metatiedoilla, joita ovat esimerkiksi tieto salassapidon perusteesta sekä salassapitoaika.[6] Lisäksi tulee huomioida, että mikäli metatiedot näkyvät muille, kuin niille, joilla on oikeus käsitellä salassa pidettävää tietoa, niin metatietoihin ei saa kirjata salassa pidettävää tietoa. Tarkempia tietoja metatiedoista ja rekisteröinnistä löytyy tiedonhallintalautakunnan suosituksista asiankäsittelyn ja palvelujen metatiedoista.[7]

Esimerkkejä toimenpiteistä, joilla voidaan varmistaa luottamuksellisuus:

- salassa pidettävien asiakirjojen laatijat ohjeistetaan tekemään merkintä salassapidosta heti asiakirjan laatimisen yhteydessä,
- metatietojen kirjaaminen ohjeistetaan siten, että metatiedot eivät sisällä salassa pidettävää tietoa tai henkilöiden yksilöintiä,
- tietojen luovuttajat ohjeistetaan informoimaan salassa pidosta, myös mikäli tietoja luovutetaan suullisesti,
- salassa pidettäviä tietoja sisältävät tietojärjestelmät toteutetaan niin, että tietojen laatijat ohjataan ottamaan kantaa tietojen salassapitoon heti tiedon laatimisen yhteydessä,
- tietojärjestelmiin toteutetaan visualisointeja tai varoituksia, jotka näytetään käyttäjälle, kun hän aloittaa salassa pidettävien tietojen käsittelyn,
- salassa pidettävien tietojen tulostaminen ja kopioiminen eri tavoin ohjeistetaan siten, että tieto salassa pidosta välittyy käsittelijälle myös niissä tilanteissa, kun käsitellään kopiota sekä
- salassapidon toteutumista seurataan ja arvioidaan määräajoin.

6 JulkL 25 §

7 Suositus asiankäsittelyn metatiedoista VM 2021:33, Suositus viranomaisten asiakirjojen metatiedoista palveluja tuotettaessa VM 2022:42

2.5 Salassapidon voimassaolo ja päättyminen

Organisaatioita suositellaan suunnittelemaan ja ohjeistamaan, että kaikki ne henkilöt, jotka käsittelevät tai luovuttavat salassa pidettäviä tietoja, tarkistavat salassapidon voimassaolon siten, että tietoja ei pidetä salassa perusteettomasti ja että salassapitoa koskevat merkinnät ovat ajan tasalla.

Julkisuuslain 25 §:n 2 momentin mukaan ”Salassa pitämisen perusteen päättymisen jälkeen merkinnän poistamisesta tai muuttamisesta on tehtävä merkintä samaan asiakirjaan, johon alkuperäinen merkintä on tehty. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa”. Salassapitoaika voi olla umpeutunut tai tietosisältö ei välttämättä ole enää tiedonantamisajankohtana salassa pidettävä. Asiakirjan luokittelua muutettaessa tehdään seuraavat toimenpiteet:

- mikäli asiakirjaa on käsitelty paperimuodossa, yliviivataan salassapitoa osoittava leima,
- leiman alle kirjoitetaan ”salassapito päättynyt”, päivämäärä ja toimivaltaisen virkamiehen allekirjoitus,
- tieto asiakirjan julkiseksi tulosta tehdään myös asiarekisteriin,
- sähköisiin asiakirjoihin merkintä tehdään metatietoja muuttamalla,
- tietopyyntöjen kohteena olevat asiakirjat varustetaan erillisellä saatteella, jossa kerrotaan salassapidon päättymisaika sekä
- metatietojen muuttaminen tallennetaan asiakirjan lokitietoihin.

Julkisuuslain 31 §:n 1 momentin mukaan: ”Viranomaisen asiakirjaa ei saa pitää salassa, kun salassapidolle laissa säädetty tai lain nojalla määrätty aika on kulunut tai kun asiakirjan salassa pidettäväksi määrännyt viranomainen on peruuttanut salassapitoa koskevan määräyksen.”

2.6 Salassapito- ja vaitiolovelvollisuus

Organisaation tulee varmistaa riittävällä ohjeistuksella, viestinnällä ja seurannalla, että kaikilla salassa pidettäviä tietoja käsittelevillä henkilöillä on tietoisuus salassa pidettävien asiakirjojen salassapitovelvollisuudesta, vaitiolovelvollisuudesta sekä hyväksikäyttökiellosta.

Julkisuuslain 22 §:n 1 momentin mukaan viranomaisen asiakirja on pidettävä salassa, jos se on julkisuuslaissa tai muussa laissa säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus.

Julkisuuslain 23 §:n mukaan viranomaisen palveluksessa olevat sekä muilla perusteilla salassa pidettäviä tietoja käsittelevät henkilöt ovat vaitiolovelvollisia eivätkä saa käyttää salassa pidettäviä tietoja omaksi tai toisen hyödyksi.

Tiedonhallintalain 4 § 2 momentin 2, 3 ja 5 kohdan mukaisesti tiedonhallintayksikön johdon on huolehdittava ajantasaisista ohjeista, tarjottava koulutusta tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista sekä järjestettävä riittävä valvonta niiden noudattamisesta.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- ohjeistaa selkeästi salassapitovelvollisuuteen, vaitiolovelvollisuuteen ja hyväksikäyttökieltoon liittyvät asiat,
- huolehtia viestinnän, perehdytysten ja koulutusten avulla riittävästä tietoisuudesta salassapitoon ja vaitiolovelvollisuuteen sekä hyväksikäyttökieltoon liittyvissä asioissa,
- informoida salassa pidettäviä tietoja käsitteleviä henkilöitä salassapitovelvollisuuden ja vaitiolovelvollisuuden sekä hyväksikäyttökiellon rikkomisen rangaistavuudesta,
- seurata aktiivisesti vaitiolovelvollisuuden toteutumista organisaatiossa sekä
- varmistaa työ- ja palvelusuhteiden sekä harjoitteluajan päättymisen yhteydessä, että lähtijä on tietoinen vaitiolovelvollisuuden jatkumisesta myös työ- ja palvelusuhteen sekä harjoitteluajan päättymisen jälkeen.

2.7 Salassa pidettävien tietojen luovuttaminen

Organisaatioita suositellaan määrittelemään ja ohjeistamaan selkeästi, missä tilanteissa, millä perusteilla sekä miten salassa pidettävää tietoa voidaan luovuttaa.

Viranomaisten asiakirjoja koskevan julkisuusperiaatteen toteutumisen sekä salassa pidettävien tietojen luottamuksellisuuden säilymisen varmistamiseksi organisaatioita suositellaan tunnistamaan ja ohjeistamaan[8] ne tilanteet, joissa luovutetaan salassa pidettävää tietoa.

Julkisuuslain 26–32 §:ssä on säädetty yleisistä perusteista salassa pidettävän tiedon antamiselle eli salassapidosta poikkeamiselle sekä salassa pidon lakkaamiselle. Julkisuuslain 17–21 §:ssä on kuvattu viranomaisten velvollisuutta edistää tiedonsaantia, johon sisältyy myös salassa pidettävien tietojen luovuttamiseen liittyviä täsmennyksiä.[9] Ohjeissa tulee ottaa huomioon nämä sekä mahdollinen erityislainsäädäntö.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- käydä läpi toimintaansa liittyvät yleiset sekä erityislainsäädäntöön liittyvät tietojen luovuttamisen perusteet,
- ohjeistaa niihin perustuen, miten ja millä perusteilla salassa pidettäviä tietoja voi luovuttaa,
- määritellä salassa pidettävien tietojen luovuttamisen vastuut ja päätösmenettelyt,
- ohjeistaa tarkastamaan salassapidon voimassaolo muun muassa sen varmistamiseksi, ettei luovutettavissa asiakirjoissa ole aiheettomia salassapitomerkintöjä sekä
- huolehtia siitä, että luovutuksensaaja on tietoinen salassapito- ja vaitiolovelvollisuudesta sekä hyväksikäyttökiellosta.

8 TihL 4 § 2 mom 2 k

9 Yleisöltä salassa pidettäviä asiakirjoja voidaan esimerkiksi luovuttaa ennalta määritellylle tiedonsaajalle julkisuus- tai salassapito-olettaman sisältävän säännöksen osoittamissa rajoissa (JulkL 17 §:n 2 ja 3 mom sekä 23 §:n 2 mom).

2.8 Harkinnanvaraisesti annettavat tiedot

Organisaatioita suositellaan tunnistamaan harkinnanvaraisesti annettavat tiedot, merkitsemään ne tarvittavassa laajuudessa sekä suojaamaan ne hyödyntäen riskilähtöisesti salassa pidettävien tietojen suojaamisessa käytettyjä hallintakeinoja.

Julkisuuslain 16 a §:n 1 momentin mukaan asiakirjaan voidaan tehdä merkintä ”HARKINNANVARAISESTI ANNETTAVA”, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Harkinnanvaraisesti annettavia tietoja voivat olla esimerkiksi sellaisia asioita koskevat tiedot, joiden valmistelu on vielä kesken ja jotka eivät ole vielä julkisia.[10] Alla oleva havainnekuvio ilmentää harkinnanvaraisesti annettaviin asiakirjoihin tehtävää merkintää. Merkintää voidaan käyttää sekä manuaalisissa että sähköisissä asiakirjoissa.

Kuvio 3. Havainnekuvio harkinnanvaraisesti annettavasta merkinnästä.

Merkinnän tarkoituksena on ilmaista asiakirjan käsittelijälle, että asiakirjaan sisältyy tietoja, joiden luovuttamiseen kohdistuu erityisiä edellytyksiä, joko sen vuoksi, ettei asiakirja ole vielä julkinen tai sen vuoksi että sitä voidaan sen julkisuudesta huolimatta luovuttaa vain tietyin edellytyksin. Julkisuuslain 16 §:n 3 momentin mukaan: ”Viranomaisen henkilörekisteristä saa antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja. Henkilötietoja saa kuitenkin luovuttaa suoramarkkinointia ja mielipide- tai markkinatutkimusta varten vain, jos niin erikseen säädetään tai jos rekisteröity on antanut siihen suostumuksensa”.

10 JulkL 6 §, 7 §, 9 § 2 mom

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- ohjeistaa valtuudet, menettelyt ja periaatteet, joiden mukaisesti harkinnanvaraisesti annettavia tietoja luovutetaan,
- suojata harkinnanvaraisesti annettavat tiedot hyödyntämällä riskilähtöisesti salassa pidettävien tietojen käsittelyssä käytettäviä tietoturvallisuuden hallintakeinoja sekä
- varmistaa että harkinnanvaraisesti luovutettavien henkilötietojen käsittelyssä on otettu huomioon tietosuojaa koskeva sääntely.

3 Suosituksia salassa pidettävien tietojen suojaamiseksi

3.1 Käsittely ja ohjeistaminen

3.1.1 Tietojen suojaaminen sivullisilta

Organisaation tulee järjestää salassa pidettävien tietojen käsittely siten, että tiedot eivät vahingossa tai tahallisesti tule sivullisten tietoon.

Organisaatioita suositellaan varmistamaan tietojen suojaaminen sivullisilta käyttämällä salassa pidettävien tietojen käsittelyyn riittävän turvallisia tiloja ja toteuttamalla muita toimenpiteitä, jotka pienentävät riskiä salassa pidettävien tietojen tulemisesta sivullisen tietoon.[11]

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- sijoittaa salassa pidettäviä tietoja sisältävät tietojärjestelmät ja tietovarannot riittävällä tavalla suojatulle alueelle. Arviointiin voi hyödyntää turvallisuusluokitteluasetuksessa kuvattuja turvallisuusalueita koskevia vaatimuksia,[12]
- ohjeistaa käyttämään salassa pidettävistä tiedoista keskusteltaessa tiloja, joissa on riittävä äänieristys,
- hankkia sivustakatsomisen estäviä suojia sekä järjestää työpisteet siten, että käsiteltävät tiedot eivät vahingossa voi näkyä sivullisille,
- ohjeistaa salassa pidettävien tietojen käsittelyn erityisesti tilanteissa, joissa salassa pidettäviä tietoja joudutaan käsittelemään tai kuljettamaan turvallisten tilojen ulkopuolella sekä
- varmistaa, että salassa pidettävät tiedot tuhotaan riittävän turvallisella tavalla.

11 TihL 13 § 1 mom, 15 § 2 mom, JulkL 22 §

12 TLA 9 § 1 k ja Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä VM 2021:5

3.1.2 Tilaturvallisuus

> Organisaatioiden tulee käsitellä ja säilyttää tietoaineistoja toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.[13]

Tilaturvallisuuden varmistamiseksi suositellaan toteutettavaksi ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä turvallisuustason palauttamiseksi.

Fyysisten turvatoimien arviointi perustuu riskien arviointiin ja monitasoiseen suojauksen kokonaisuuteen. Siten joissakin tilanteissa voidaan riskien arviointiin perustuen joko hyväksyä puutteita yksittäisissä suojaustoimenpiteissä tai edellyttää normaalia tavoitetasoa korkeampia turvatoimia. Monitasoista suojausperiaatetta soveltaen voidaan määritellä asianmukainen ja riskiarviointiin nähden riittävä turvatoimien yhdistelmä, joka muodostuu hallinnollisista, toiminnallisista ja fyysistä keinoista.

Salassa pidettävien asiakirjojen fyysisessä suojaamisessa suositellaan soveltamaan turvallisuusluokitteluasetuksessa[14] määriteltyjä käsitteitä eri tasoista turvallisuusalueista sekä hyödyntämään Julkri-kriteeristöä yksityiskohtaisten fyysisten suojausten (FYY-05, FYY-06 ja FYY-07) määrittelyssä.

Salassa pidettäviä tietoja ja asiakirjoja sisältävät tietovarannot sekä niiden käsittelyyn käytetyt tietojärjestelmät tulisi sijoittaa viranomaisen tähän tarkoitukseen määrittelemälle alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa kuvattu hallinnollinen alue tai tieto pitää suojata riskiperusteisesti muilla turvakontrolleilla.

Kyseiset turvallisuusluokitteluasetuksessa määritellyt alueet ovat:

1. ”hallinnolliset alueet, joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa;
2. *turva-alueet*, 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.”

13 TihL 15 § 2 mom

14 TLA 9 §

Käytettäessä yhteiskäyttöisiä toimitiloja, tulee etukäteen varmistaa tilojen turvallisuusratkaisujen riittävyys salassa pidettävien tietojen käsittelyn kannalta. Lisäksi tulee ottaa huomioon, että tiloissa voi työskennellä myös muiden organisaatioiden työntekijöitä.

Lisätietoja tilaturvallisuuteen liittyvistä asioita löytyy tiedonhallintalautakunnan suosituksesta (VM 2021:65).[15] Kansallisarkisto antaa tarkempaa ohjausta arkistotilojen vaatimuksista.[16]

Esimerkkejä tilaturvallisuutta parantavista toimenpiteistä:

- huolehtia tilojen lukituksista ja avaintenhallinnasta,
- sijoittaa työpisteet siten, että salakatselu ei ole mahdollista,
- huolehtia pääsyoikeuksien hallinnasta,
- huolehtia, että vierailijoilla on saattajat sekä
- ottaa käyttöön kulunvalvontajärjestelmä.

15 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, VM 2021:65, luku 12.

16 Kansallisarkisto Määräys ja ohjeet arkistotiloista. AL/19699/07.01.01.00/2012

3.1.3 Sallitut tietojenkäsittely-ympäristöt

Organisaation suositellaan määrittelemään ja ohjeistamaan selkeästi missä järjestelmissä, palveluissa, säilytysratkaisuissa sekä päätelaitteissa saa käsitellä ja säilyttää salassa pidettäviä tietoja[17]

Tietojärjestelmien suojaamisen lisäksi pitää käyttäjien tietää, missä ympäristöissä mitäkin tietoja voi käsitellä, minkä johdosta sallitut käsittely-ympäristöt on ohjeistettava.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- ohjeistaa missä järjestelmissä saa käsitellä ja säilyttää salassa pidettävää tietoa mukaan lukien ryhmätyövälineet,
- ohjeistaa myös missä järjestelmissä ei saa käsitellä tai säilyttää salassa pidettävää tietoa,
- ohjeistaa paperiasiakirjojen ja muiden ei-sähköisten salassa pidettävien tietojen säilytysratkaisut,
- kieltää salassa pidettävän tiedon käsittely sosiaalisen median palveluissa,
- ohjeistaa, miten salassa pidettävää tietoa voi käsitellä mobiililaitteissa,
- täsmentää järjestelmäkohtaisesti rajaukset sekä muut mahdolliset vaatimukset, jotka tulee ottaa huomioon käsiteltäessä salassa pidettävää tietoa kyseisen järjestelmän avulla sekä
- valvoa että salassa pidettävien tietojen käsittelyyn käytetään vain sallittuja järjestelmiä.

17 TihL 4 § 2 mom 2 kohta

3.1.4 Tietojen käsittely pilvipalveluissa

Yleinen lähtökohta suunniteltaessa salassa pidettävien tietojen käsittelyä pilvipalveluissa on turvallisuuden varmistaminen kattavasti ja riskilähtöisesti kuten muillakin teknologioilla tuotetuissa palveluissa.

Pilvipalveluiden käyttöä suunniteltaessa sekä siihen liittyviä riskejä arvioitaessa tulee lisäksi ottaa huomioon pilvipalveluiden ominaispiirteet, kuten palveluiden erilaiset toteutusmallit, turvallisuusvastuiden jakautuminen asiakkaan ja toimittajan välillä, tietojen fyysiseen sijaintiin liittyvät näkökohdat sekä pilvipalveluiden nopea tekninen kehitys ja siihen liittyvät muutoshallinnan haasteet.

Lähtökohtaisesti salassa pidettävien tietojen käsittelylle pilvipalveluissa ei ole lainsäädännöllisiä esteitä. Pilvipalveluiden soveltuvuutta arvioitaessa organisaation on kuitenkin selvitettävä pilvipalvelun turvallisuuteen liittyvät riskit sekä palvelun soveltuvuus suunniteltuun käyttötarkoitukseen ottaen huomioon erityisesti seuraavia näkökohtia:

- tietoaineistojen siirtämiseen tietoverkossa liittyvä turvallisuus ja riskit, [18]
- pilvipalvelun käyttöön ja hallintaan liittyvät riskit,
- organisaation sisäinen kyvykkyys hyödyntää pilvipalveluja,
- lainsäädäntöjohdannaiset ja määräysvaltaan liittyvät riskit,
- voidaanko tietojen saatavuus varmistaa riittävällä tavalla myös vakavissa häiriötilanteissa sekä mahdollisesti myös poikkeusoloissa sekä
- tietojen fyysiseen sijaintiin liittyvät riskit.

Tässä suosituksessa ei analysoida ja ohjeisteta tarkemmin pilvipalveluiden käyttöön liittyviä asioita, mutta suositellaan hyödyntämään seuraavia pilvipalveluiden käyttöön liittyviä suosituksia:

- julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) sekä siihen sisältyvä käyttötapaus ”SaaS-pilvipalvelun arviointi”[19],
- suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa (VM 2022:4) sekä
- pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri).

18 TihL 14 §

19 Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), liite 3, luku 2.1.2 SaaS-pilvipalvelun arviointi

3.1.5 Etäkäyttö

Organisaatioita suositellaan määrittelemään ja ohjeistamaan salassa pidettävien tietojen käsittelyyn liittyvät menettelyt, kun työskennellään organisaation määrittelemien turvallisuusalueiden ulkopuolella. [20]

Lainsäädäntö ei estä salassa pidettävien tietojen käsittelyä turvallisuusalueiden [21] ulkopuolella kuten julkisissa tiloissa tai etätöissä [22]. Käsiteltäessä salassa pidettäviä tietoja tällaisissa tiloissa, käsittelyyn liittyy erilaisia riskejä, jotka tulee ottaa huomioon käsittelyä suunniteltaessa. Tästä johtuen suositellaan, että organisaatiot arvioivat näitä riskejä sekä määrittelevät siltä pohjalta missä ja millä tavalla salassa pidettäviä tietoja saa käsitellä.[23]

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- ohjeistaa, missä laajuudessa salassa pidettäviä tietoja saa käsitellä turvallisuusalueiden ulkopuolella,
- listata tietojärjestelmät ja tiedonsiirtotavat, joita saa käyttää salassa pidettävien tietojen etäkäsittelyyn,
- määritellä vaatimukset tiedon käsittelyyn käytettäville päätelaitteille,
- laatia ohjeet salakatselun ja salakuuntelun estämiseksi,
- laatia ohjeet tietojen ja tietovälineiden säilyttämisestä eri muodoissa turvallisuusalueiden ulkopuolella,
- ohjeistaa hyvät käytännöt käsittelyn turvallisuuden parantamiseksi ei-turvallisessa ympäristössä sekä
- laatia ohjeet koskien salassa pidettävien tietojen käsittelystä ulkomailla.

20 TihL 4 § 2 mom
21 Kts. luku 3.1.2 Tilaturvallisuus
22 TLA 10 §
23 TihL 13 § 1 mom

3.1.6 Ohjeistaminen

Organisaatioita suositellaan ohjeistamaan salassa pidettävien tietojen käsittelyyn liittyvät asiat mahdollisimman helppokäyttöisellä tavalla.

Tiedonhallintalain 4 §:n 2 momentin 2 kohdan mukaan organisaatiolla ”tulee olla ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta”. Sen lisäksi, että ohjeet ovat kattavia, oikeita, ristiriidattomia ja ajantasaisia organisaatioiden kannattaa kiinnittää erityistä huomiota ohjeiden helppokäyttöisyyteen ja saatavuuteen.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- varmistaa ohjeiden ymmärrettävyyden 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 voimassa olevat tietoturvaohjeet yhteen paikkaan, josta organisaation käyttäjien on helppo löytää ne sekä
- viestiä ohjeista sekä niihin tehdyistä muutoksista.

3.2 Prosessit

3.2.1 Hankintojen ja järjestelmien turvallisuus

> Organisaatioiden tulee sisällyttää salassa pidettävien tietojen käsittelyyn liittyvien tietojärjestelmien ja palveluiden hankinta- ja ylläpitoprosesseihin tietoturvavaatimusten määrittelyt ja niiden täyttymisen varmistaminen.

Tiedonhallintalain 13 § 4 momentin mukaan ”Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet”. Lakisääteisen vaatimuksen täyttämiseksi suositellaan, että salassa pidettävien tietojen käsittelyyn liittyvien tietojärjestelmien ja palveluiden hankintaprosesseihin on sisällytetty vaiheet, joissa määritellään hankinnan tietoturvavaatimukset sekä varmistetaan niiden täyttyminen.

Osana palveluun kohdistettavien tietoturvavaatimusten määrittelyä suositellaan, että arvioidaan myös palveluntuottajan toimintaan kohdistuvien tietoturvavaatimusten tarpeellisuus ja laajuus. Lisäksi suositellaan arvioimaan hankinnan yhteydessä lainsäädäntöjohdannaiset[24] riskit ja huomioimaan ne palvelun tuottajaan ja tietojen fyysiseen sijaintiin liittyvissä vaatimuksissa.

Ylläpitoprosessit suositellaan suunnittelemaan siten, että niiden yhteydessä varmistetaan riittävän säännöllisesti tietoturvavaatimusten ajantasaisuus, asetettujen tietoturvavaatimusten täyttyminen versiopäivitysten yhteydessä sekä yleisesti tunnistettuihin haavoittuvuuksiin liittyvät korjaukset.

Hankintoja ja niiden turvallisuutta on käsitelty tiedonhallintalautakunnan suosituksen ”Suosituskokoelma tiettyjen tietoturvallisuus säännösten soveltamisesta (VM 2021:65)” luvussa 8 sekä Julkri-kriteeristön kriteerissä Hankintojen turvallisuus (HAL-16).

Valtion virastojen ja laitosten on tiettyjä poikkeuksia lukuun ottamatta käytettävä yhteisiä perustietotekniikka- ja tietojärjestelmäpalveluja[25]. Näiden palveluiden tuottamisesta

24 Lainsäädäntöjohdannaisella riskillä tarkoitetaan tässä yhteydessä esimerkiksi sellaista tilannetta, jossa palvelun tuottajaan kohdistettu lainsäädäntö edellyttää palvelun tuottajaa luovuttamaan salassa pidettäviä tietoja toisen valtion viranomaisille.

25 Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013)

vastaa Valtion tieto- ja viestintätekniikkakeskus Valtori[26] sekä tapauskohtaisesti muut valtion omistamat tuottajat kuten Suomen erillisverkot Oy.[27]

Salassa pidettävien tietojen käsittelyn turvallisuuden varmistamiseksi suositellaan, että palveluja käyttävät organisaatiot ottavat yhteisiin palveluihin kohdistuvat tietoturvavaatimukset huomioon palvelusopimuksissa sekä tarkistavat ne palvelusopimusten tarkistusten yhteydessä yhteistyössä palveluntuottajan kanssa.

Julkisissa hankinnoissa organisaatiot käyttävät myös paljon yhteishankintayksiköitä ja sidosyksiköitä. Salassa pidettävien tietojen turvallisuuden varmistamiseksi on suositeltavaa, että organisaatiot varmistavat salassa pidettäviä tietoja koskevien vaatimusten sisältymisen yhteishankintayksiköiden ja sidosyksiköiden kanssa laadittaviin hankintasopimuksiin sekä mahdollisuuksien mukaan myös näiden yksiköiden kanssa tehtäviin puitesopimuksiin.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- varmistaa, että hankintaprosessissa on pakollisina vaiheina tietoturvavaatimusten määrittely, tarkastus ja hyväksyminen ennen tarjouspyynnön lähettämistä,
- varmistaa, että kaikki edellä mainitut vaiheet dokumentoidaan kirjallisesti,
- edellyttää palveluntuottajaa täyttämään salassa pidettäviin tietoihin kohdistuvat vähimmäisvaatimukset,
- edellyttää palveluntuottajaa osoittamaan uskottavasti, että käytettävät palvelut täyttävät niihin kohdistuvat vähimmäisvaatimukset,
- varmistaa, että käyttöönotto ja muutostenhallintaprosessit sisältävät tietoturvavaatimusten täyttymisen tarkastamisen ennen uusien versioiden käyttöönottoa sekä
- varmistaa, että salassapitoa koskevat vaatimukset on otettu huomioon sekä sopimuksissa että puitesopimuksissa.

26 Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014)

27 Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015)

3.2.2 Käyttöoikeuksien ajantasaisuus

Tietojärjestelmien käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiseksi suositellaan, että organisaatio määrittelee prosessit, joiden mukaisesti käyttöoikeudet ylläpidetään tehtävämuutosten yhteydessä.

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”.

Käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiseksi, niiden tarkistaminen on suositeltavaa kytkeä sellaisiin prosesseihin, jotka tehdään aina tehtävämuutosten yhteydessä. Näin varmistetaan, että tarvittavat muutokset käyttöoikeuksiin tapahtuvat ajantasaisesti.

Lisäksi on suositeltavaa määritellä käyttöoikeuksien ylläpitoprosessi siten, että varsinaiset päätökset käyttöoikeuksista tekevät ne henkilöt, joilla on vastuu salassa pidettävistä tiedoista sekä edellytykset arvioida käyttäjän tarvetta saada käyttöoikeus kyseisiin tietoihin. Lisätietoja Julkri-kriteeristön teknisen turvallisuuden osa-alueesta (TEK) kohdasta ”Pääsyoikeuksien hallinnointi” (TEK-07).

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- tunnistaa järjestelmät, jotka sisältävät salassa pidettäviä tietoja,
- määritellä prosessit käyttöoikeuksien ajantasaisuuden varmistamiseen työsuhteiden sekä ulkoisten palveluiden alkaessa, päättyessä ja muuttuessa,
- erottaa käyttöoikeuksien hyväksyminen ja niiden käytännön toteuttaminen sekä
- tarkistaa salassa pidettävien tietojen käyttöoikeuksien ajantasaisuudet vähintään kerran vuodessa.

3.2.3 Käyttäjien todentaminen ja seuranta

Organisaatiota suositellaan todentamaan salassa pidettävien tietojen käyttäjät riittävän luotettavilla yksilöllisillä käyttäjätunnisteilla sekä varmistamaan käsittelyn turvallisuus riittävällä seurannalla.

Salassa pidettävien tietojen turvallisuuden varmistamiseksi suositellaan, että organisaatiossa on käytössä riittävän luotettavat menetelmät käyttäjien todentamiseen, joita ovat muun muassa:

- yksilölliset henkilökohtaiset käyttäjätunnisteet,
- vähintään salasanaan perustuva menetelmä sekä
- käyttäjätunnusten lukkiutuminen liian monen virheellisen yrityksen jälkeen.

Vahvempia todentamismenetelmiä, kuten esimerkiksi mobiililaitteeseen tai varmennekorttiin perustuvaa monivaiheista todentamista suositellaan käytettäväksi etenkin niissä tilanteissa, kun käyttö tapahtuu vähemmän turvallisesta käyttöympäristöstä. Lisätietoja Julkri-kriteeristön teknisen turvallisuuden osa-alueesta (TEK) kohdasta ”Pääsyoikeuksien hallinnointi” (TEK-07).

Lisäksi suositellaan, että organisaatio varmistaa salassa pidettävien tietojen käsittelyn turvallisuuden riittävällä lokitietoihin perustuvalla seurannalla. 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 käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen”.

Esimerkkejä toimenpiteistä, joilla organisaatio voi parantaa käyttäjien todentamista ja käytön seurantaa:

- määritellä politiikan, jonka mukaisesti kaikilla käyttäjillä on yksilölliset käyttäjätunnukset,
- erotella järjestelmien ylläpitoon liittyvät tunnukset normaaleista henkilökohtaisista tunnuksista,
- määritellä salasanan vähimmäisvaatimukset ja varmistaa niiden täyttyminen ohjelmallisesti,
- ottaa käyttöön menettely, jossa kirjauduttaessa järjestelmiin organisaation ulkopuolelta, vaaditaan käyttäjiltä ylimääräinen vahvistus mobiililaitteeseen asennetun sovelluksen avulla sekä

- määritellä salassa pidettävää tietoa sisältäviin järjestelmiin lokienseuranta, joka koostuu useista toisiaan täydentävistä seurantamenetelmistä kuten sääntöperäisistä hälytyksistä mahdollisten väärinkäytösten yhteydessä sekä niitä täydentävistä lokitietojen manuaalisista tarkastuksista.

3.2.4 Salassa pidettävien tietojen jatkuvuudenhallinta

Organisaatioita suositellaan suunnittelemaan ja toteuttamaan riittävät suojaukset salassa pidettävän tiedon luottamuksellisuuden varmistamiseksi myös häiriötilanteissa.[28]

Osana varautumista ja jatkuvuudenhallintaa organisaatiot suunnittelevat toimenpiteitä toiminnan jatkuvuuden varmistamiseksi sekä häiriötilanteista toipumiseksi. Näitä toimenpiteitä, jotka kohdistuvat tyypillisesti organisaation toiminnan kannalta tärkeisiin tai kriittisiin tietoihin on kuvattu Julkri-kriteeristön osa-alueen varautuminen ja jatkuvuuden hallinta (VAR) kriteereissä.

Esimerkkejä toimenpiteistä, jolla organisaatio voi varmistaa, että tiedot pysyvät salassa häiriötilanteiden aikana:

- varmistaa häiriötilanteita hoitavan henkilöstön, mukaan lukien palveluntarjoajien henkilöiden osaamisen ja tietoisuuden käsiteltäviin tietoihin liittyvistä salassa pidon vaatimuksista,
- toteuttaa riskienarviointia palvelun koko elinkaaren ajan,
- suunnitella jatkuvuudenhallinnan prosesseihin riittävät suojaukset tietojen luottamuksellisuuden varmistamiseksi,
- suunnitella korvaavat hallintakeinot niille normaalitilanteissa käytettäville hallintakeinoille, joita ei ole mahdollista toteuttaa häiriötilanteen aikana sekä
- harjoitella säännöllisesti jatkuvuussuunnitelmien mukaista toimintaa häiriötilanteissa kiinnittäen erityistä huomiota salassapidon toteutumiseen.

28 TihL 13 § 1 mom

3.3 Tekniset suositukset

3.3.1 Käsittely-ympäristön erottaminen

Organisaatioita suositellaan erottamaan salassa pidettävien tietojen käsittely-ympäristö julkisista tietoverkoista sekä muista heikomman turvallisuustason ympäristöistä.

Tietojärjestelmien erottelu on eräs vaikuttavimmista tekijöistä salassa pidettävän tiedon suojaamisessa. Erottelun tavoitteena on rajata salassa pidettävän tiedon käsittely-ympäristö hallittavaksi kokonaisuudeksi ja vain riittävän turvallisiin ympäristöihin. Käytännössä julkishallinnon organisaatioissa koko käsittely-ympäristö, jossa käsitellään sekä julkista että salassa pidettävää tietoa, on yleensä erotettu julkisista tietoverkoista.

Tietojenkäsittely-ympäristön kytkemisessä muihin ympäristöihin suositellaan käytettäväksi vähintään palomuuriratkaisua. Lisätietoja Julkri-kriteeristön teknisen turvallisuuden osa-alueesta (TEK) kohdista ”Verkon rakenteellinen turvallisuus” (TEK-01) ja ”Verkon rakenteellinen turvallisuus – käsittely-ympäristöjen erottaminen” (TEK-01.3).

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- erottaa organisaation tietojenkäsittely-ympäristö muista ympäristöistä palomuurilla.

3.3.2 Tiedon salaus ja vastaanottajan varmistaminen

Organisaatioita suositellaan salaamaan salassa pidettävä tieto yleisissä tietoverkoissa salausratkaisuilla, jotka tukevat moderneja salausvahvuuksia ja joissa ei ole tunnettuja haavoittuvuuksia.

Tiedonhallintalain 14 § 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”.

Salausvaatimus voidaan toteuttaa joko tietoliikenteen tai siirrettävän tiedon erillisellä salauksella. Salausratkaisuja, joissa ei ole tunnettuja haavoittuvuuksia ja jotka tukevat moderneja salausvahvuuksia, voidaan pitää riittävän turvallisina useimmille salassa pidettäville tiedoille. Lisätietoja Julkri-kriteeristö teknisen turvallisuuden osa-alueesta (TEK) kohta ”Tiedon salaaminen” (TEK-16) sekä kybertuvallisuuskeskuksen NCSA-toiminnon hyväksymistä salausratkaisuista ja kiintolevyjen elinkaaren hallinnasta.

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- huolehtia suunnitelmallisesta avaintenhallinnasta,
- käyttää tietojärjestelmien välisissä tiedonsiirroissa palvelinvarmenteita sekä
- tunnistaa henkilöt vahvalla sähköisellä tunnistamismenetelmällä tai muulla riittävän turvallisella tavalla.

3.3.3 Järjestelmäkovennukset

Organisaatioita suositellaan ottamaan käyttöön menettelytapa, jolla salassa pidettäviä tietoja sisältävät järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on niin kutsuttu kovennettu asennus.

Järjestelmissä on usein paljon ominaisuuksia, jotka ovat oletusarvoisesti päällä. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, kasvaa riski järjestelmissä olevien salassa pidettävien tietojen oikeudettomaan käyttöön.

Tästä johtuen suositellaan, että salassa pidettäviä tietoja sisältävät järjestelmät kovennetaan järjestelmällisen menettelyn avulla, jossa vaihdetaan oletussalasanat, poistetaan käytöstä ei välttämättömät palvelut sekä rajoitetaan yhteydet ja ominaisuudet vähimpien oikeuksien periaatteen mukaisesti. Lisätietoja Julkri-kriteeristön teknisen turvallisuuden osa-alueesta (TEK) kohdasta ”Järjestelmäkovennus” (TEK-10).

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- tunnistaa kovennettavat kohteet,
- määritellä kovennusten toteutus(tapa),
- koventaa kohteet määritysten mukaisesti sekä
- varmistaa kovennusten pysyminen päällä säännöllisesti, erityisesti päivitysten jälkeen, koko tietojärjestelmän elinkaaren ajan.

3.3.4 Haittaohjelmasuojaukset

Organisaatioita suositellaan suunnittelemaan ja toteuttamaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, havaitsemiseen ja tilanteen korjaamiseen.

Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä, käyttöoikeuksien rajauksilla, ajantasaisilla turvallisuuspäivityksillä, poikkeamien havainnointikyvyllä, henkilöstön turvatietoisuudesta varmistumalla sekä haittaohjelmien torjuntaohjelmistojen käytöllä. Lisätietoja Julkri-kriteeristön teknisen turvallisuuden osa-alueesta (TEK) kohdasta ”Haittaohjelmilta suojautuminen” (TEK-11).

3.3.5 Ohjelmistohaavoittuvuuksien hallinta

Organisaatioita suositellaan toteuttamaan tietojenkäsittely-ympäristön koko elinkaaren ajalle luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.

Ohjelmistohaavoittuvuuksien hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Organisaatio voi pienentää ohjelmistohaavoittuvuuksiin liittyviä riskejä järjestelmällisellä ohjelmistohaavoittuvuuksien seurannalla ja asentamalla tietoturvapäivitykset viipymättä. Lisätietoja Julkri-kriteeristön kohdasta ”Ohjelmistohaavoittuvuuksien hallinta” (TEK-19).

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- seurata viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita,
- asentaa tarpeellisiksi arvioidut tietoturvapäivitykset ja tarkastaa niiden onnistuminen,
- velvoittaa toimittajat hankinnan vaatimuksissa ja sopimuksissa järjestelmälliseen ohjelmistohaavoittuvuuksien seurantaan ja tietoturvapäivitysten toimittamiseen viipymättä,

- tarkastaa verkon ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat kattavasti haavoittuvuusskannauksella vuosittain ja aina merkittävien muutosten jälkeen sekä
- järjestää löytyneiden haavoittuvuuksien sekä päivitysmenettelyjen puutteiden käsittelyn siten, että tietojenkäsittely-ympäristön suojaamiseen oleellisesti vaikuttavat heikkoudet poistetaan, korjataan tai muuten rajoitetaan siten, että salassa pidettävien tietojen käsittely ei vaarannu.

Sanasto

Termi	Määritelmä	Lähde
asiakirja	kirjallinen esitys, kuvallinen esitys tai sellainen käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuva tiettyä kohdetta tai asiaa koskeva viesti, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla Asiakirjan käsite on laaja, asiakirjoja ovat esimerkiksi paperinen dokumentti, kuva, ääni, video tai viesti.	JulkL 5 § 1 mom
erityisiin henkilötieto-ryhmiin kuuluva henkilötieto	sellainen henkilötieto, josta ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettinen tai biometrinen tieto, terveyttä koskeva tieto tai luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskeva tieto	Tietosuoja-asetus 9 art.
haavoittuvuus	puute, vika tai toimintatapa, joka altistaa turvallisuuteen kohdistuville uhkille Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, ohjelmistoissa, laitteissa, prosesseissa tai ihmisten toiminnassa. Haavoittuvuus voi olla esimerkiksi ohjelmassa oleva virhe, joka mahdollistaa väärinkäytöksiä estävien rajoitusten kiertämisen toiminnassa.	VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään; 9.6.2022 (Digi- ja väestötietovirasto)
haittaohjelma	ohjelma, joka tarkoituksellisesti aiheuttaa koneen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa Haittaohjelmia ovat esimerkiksi virukset, madot ja troijanhevoset sekä näiden yhdistelmät.	Kyberturvallisuuden sanasto (TSK 52, 2018)
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 Hallinnollinen alue tai tila voi olla esimerkiksi toimistotila, useista eri toimistotiloista muodostuva kokonaisuus, palvelintila, konesali tai jonkin yrityksen tai muun yhteisön tila. Turvallisuusluokitusasetuksessa hallinnollinen alue on turvallisuusluokiteltujen asiakirjojen suojaamiseksi määritelty alue, jolla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa.	Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4) TLA 9 § 1 kohta

Termi	Määritelmä	Lähde
hallintakeino **synonyymi: kontrolli**	toimenpide, jolla pyritään muuttamaan riskiä tai säilyttämään se Termiä hallintakeino käytetään joskus kontrollin synonyyminä, mutta usein hallintakeino viittaa kokonaisratkaisuun (esim. tunnistautuminen tai hyvä hallintotapa), joka voi sisältää useita konkreettisia kontrolleja. Kontrollit voivat olla prosesseja, toimintaperiaatteita, laitteita, käytäntöjä, kertaluonteisia toimenpiteitä tai muun tyyppistä toimintaa.	VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään; 9.6.2022 (Digi- ja väestötietovirasto)
henkilötieto	tieto, jonka perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.	Tietosuoja-asetus 4 art. 1 kohta Rikosasioiden tietosuojalaki 3 § 1 mom 1 kohta
julkinen asiakirja	viranomaisen asiakirja, jota ei ole säädetty tai määrätty salassa pidettäväksi	JulkL 1 § ja 9 §
julkisuus-periaate	periaate, jonka mukaan viranomaisten asiakirjat ovat julkisia, jollei julkisuuslaissa tai muussa laissa erikseen toisin säädetä	JulkL 1 §
kovennus	prosessi, jossa järjestelmä turvataan vähentämällä sen haavoittuvuuden pinta-alaa Käytettävissä olevien hyökkäystapojen vähentämiseen kuuluu tyypillisesti oletussalasanojen vaihtaminen sekä tarpeettomien ohjelmistojen, käyttäjätunnusten kirjautumisten ja palveluiden poistaminen käytöstä.	Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
loki	aikajärjestyksessä kirjattu tallenne tapahtumista ja niiden aiheuttajista Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin eli lokitetaan. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.	Traficom – Näin keräät ja käytät lokitietoja TihL 17 §
metatieto	tieto, joka kuvaa aineiston kontekstia, sisältöä tai rakennetta sekä ohjaa ja dokumentoi sen käsittelyä ja hallintaa Metatietoa voidaan käyttää mm. aineiston hakuun, paikallistamiseen ja tunnistamiseen. Metatiedot ovat olennaisia aineistojen löytämisen, luetteloinnin ja käytön kannalta. Metatiedot sisältävät sekä aineiston kuvailutietoja että teknisiä, järjestelmän metatietoja.	Tietotermit (2018)

Termi	Määritelmä	Lähde
palomuuri	ohjelma tai laite, jonka on tarkoitus estää luvaton tai asiaton pääsy verkosta tai verkon osasta toiseen Palomuuria käytetään usein internetin ja lähiverkon välillä. Palomuuritekniikka perustuu muurin läpi kumpaankin suuntaan kulkevan tietoliikenteen suodattamiseen ennalta määriteltyjen sääntöjen mukaisesti. Palomuuri päästää läpi vain luvallisen liikenteen.	Kyberturvallisuuden sanasto (TSK 52, 2018)
riski	epävarmuuden vaikutus tavoitteisiin Vaikutus on poikkeama odotetusta. Se voi olla myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia ja uhkia. Riski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä. Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin.	Kyberturvallisuuden sanasto (TSK 52, 2018)
salassa pidettävä asiakirja	viranomaisen asiakirja, joka on julkisuuslaissa tai muussa laissa säädetty salassa pidettäväksi tai jonka viranomainen on lain nojalla määrännyt salassa pidettäväksi tai asiakirja, joka sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus	JulkL 22 § ja 24 §
salassa pidettävä tieto	asiakirjan sisältämä tieto, jonka luonteesta johtuen asiakirja on salassa pidettävä	Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
tietoaineisto	asiakirjoista ja muista vastaavista tiedoista muodostuva, tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus	TihL 2 §
tiedonhallinta-yksikkö	viranomainen tai usean viranomaisen muodostama hallinnollinen kokonaisuus, jonka tehtävänä on järjestää tiedonhallintansa tiedonhallintalain vaatimusten mukaisesti Tiedonhallintayksiköitä ovat valtion virastot ja laitokset; tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat; eduskunnan virastot; valtion liikelaitokset; hyvinvointialueet; hyvinvointiyhtymät; kunnat; kuntayhtymät; itsenäiset julkisoikeudelliset laitokset; yliopistolaissa tarkoitetut yliopistot sekä ammattikorkeakoululaissa tarkoitetut ammattikorkeakoulut.	VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään; 9.6.2022 (Digi- ja väestötietovirasto) TihL 2 ja 4 §
tietojärjestelmä	tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuva kokonaisjärjestely Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja ohjelmistojen käsittelyyn käytettävät päätelaitteet.	TihL 2 §

Termi	Määritelmä	Lähde
tietoturvallisuuden johtamis- ja hallintajärjestelmä	osa yleistä toimintajärjestelmää, joka luodaan ja toteutetaan toimintariskien arviointiin perustuen ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus Sisältää organisaatiorakenteen, politiikat, suunnittelu- ja kehittämistoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit, mittarit ja resurssit.	Valtiohallinnon tietoturvasanasto (VAHTI 8/2002)
tietoturvariski	tietoturvauhan toteutumisen todennäköisyys ja mahdollisesti toteutuvan vahingon merkittävyys Riskin suuruus riippuu mahdollisen vahingon suuruudesta ja vahinkotapahtuman todennäköisyydestä.	Tiivis tietoturvasanasto (TSK 31, 2004)
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
turvallisuusluokiteltu asiakirja	asiakirja, johon valtion viranomaisen toimesta on tehty turvallisuusluokkaa koskeva merkintä Asiakirja on turvallisuusluokiteltava, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.	TihL 18 § JulkL 24 §
turvallisuusalue	käsite, joka sisältää hallinnolliset alueet ja turva-alueet	TLA 9 §
viranomaisen asiakirja	viranomaisen hallussa oleva asiakirja, jonka viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa Viranomaisen laatimana pidetään myös asiakirjaa, joka on laadittu viranomaisen antaman toimeksiannon johdosta, ja viranomaiselle toimitettuna asiakirjana asiakirjaa, joka on annettu viranomaisen toimeksiannosta tai muuten sen lukuun toimivalle toimeksiantotehtävän suorittamista varten.	JulkL 5 § 2 mom[29]

29 JulkL:n 5 §:n 3–5 momentissa säädetään siitä, mitä asiakirjoja ei ole pidettävä viranomaisen asiakirjana sekä siitä, miten lakia sovelletaan esim. viranomaisten sisäistä työskentelyä varten laadittuihin asiakirjoihin.

Liite: Kooste suosituksista ja niiden lakiperustasta

Luku	Suositus ja lakiperuste
2.1 Salassa pidettävät viranomaisen asiakirjat	Organisaation on tunnistettava, milloin se käsittelee salassa pidettäviä tietoja. TihL 4 § 2 mom 2 kohta.
2.2. Vähimmäis-vaatimukset ja niiden riskilähtöinen täydentäminen	Organisaation tulee täyttää salassa pidettävän tiedon käsittelyä koskevat lainsäädäntöön pohjautuvat vähimmäisvaatimukset. TihL 13 §. Suositellaan, että organisaatiot täydentävät vähimmäisvaatimuksia soveltamalla riskilähtöisesti ylemmän tason tietoturvallisuusvaatimuksia. TihL 13 § 1 mom. Suositellaan, että organisaatiot ottavat käyttöön tietoturvariskien arviointiin soveltuvan riskienarviointimenetelmän sekä soveltavat sitä systemaattisesti salassa pidettävien tietojen käsittelyn tietoturvallisuuden toteuttamisen suunnittelussa. TihL 13 § 1 mom. Mahdollinen kasautumisvaikutus pitää huomioida tiedon suojaamisessa ja mahdollisesti luokittelussa. TihL 13 §.
2.3 Tiedon elinkaari ja salassapito	Organisaation tulee tunnistaa salassa pidettävän tiedon käsittelyyn liittyvät prosessit ja tietojärjestelmät sekä varmistaa riskilähtöisesti, että ne ovat riittävän tietoturvallisia koko tiedon elinkaaren ajan. TihL 13 § 1 ja 4 mom. Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. TihL 13 § 4 mom. Suositellaan, että organisaatiot: • tunnistavat kaikki sen vastuulle kuuluvat salassa pidettävät tiedot ja käsittelijät sekä käsittelyssä käytettävät tietojärjestelmät koko tiedon elinkaaren ajalta, • määrittelevät käsittelyssä käytettävien tietojärjestelmien ja palveluiden tietoturvavaatimukset ottaen huomioon salassa pidettävien tietojen käsittelyyn liittyvät riskit, • varmistavat tietojärjestelmien ja palveluiden tietoturvavaatimusten täyttymisen hankinnan yhteydessä sekä säännöllisesti koko järjestelmän elinkaaren ajan soveltamalla systemaattisesti muutoshallinnan menettelyitä, • suunnittelevat ja ohjeistavat salassa pidettävän tiedon käsittelyprosessit siten, että käsittely on riittävän turvallista sekä • varmistavat riittävällä seurannalla, että edellä kuvatut suositukset täyttyvät ja • ylläpitävät tiedonhallintamallia tietoturvallisuuden hallitsemiseksi. TihL 4 § 2 mom, 5 § ja 13 §.

Luku	Suositus ja lakiperuste
2.4. Salassa pidettävien tietojen merkintä	Organisaatioita suositellaan suunnittelemaan ja toteuttamaan salassa pidettävien tietojen merkitseminen siten, että kaikki henkilöt, jotka käsittelevät tai joille luovutetaan salassa pidettäviä tietoja, ovat tietoisia salassapitovaatimuksesta. TihL 4 § 2 mom ja 13 § 1 mom, JulkL 25 §. Salassa pidettävien tietojen luottamuksellisuuden varmistamiseksi suositellaan, että organisaatio selvittää systemaattisesti missä eri tilanteissa ja millä eri tietojärjestelmillä käsitellään salassa pidettäviä tietoja sekä suunnittelee näihin menettelyt, joiden avulla varmistetaan, että salassa pidettäviä tietoja käsittelevät henkilöt saavat kaikissa tilanteissa tiedon salassapidosta. TihL 4 § 2 mom ja 13 § 1 mom, JulkL 22 §.
2.5 Salassapidon voimassaolo ja päättyminen	Organisaatioita suositellaan suunnittelemaan ja ohjeistamaan, että kaikki ne henkilöt, jotka käsittelevät tai luovuttavat salassa pidettäviä tietoja, tarkistavat salassapidon voimassaolon siten, että tietoja ei pidetä salassa perusteettomasti ja että salassapitoa koskevat merkinnät ovat ajan tasalla. TihL 4 § 2 mom 2 kohta, JulkL 25 § 2 mom ja 31 §.
2.6 Salassapito- ja vaitiolovelvollisuus	Organisaation tulee varmistaa riittävällä ohjeistuksella, viestinnällä ja seurannalla, että kaikilla salassa pidettäviä tietoja käsittelevillä henkilöillä on tietoisuus salassa pidettävien asiakirjojen salassapitovelvollisuudesta, vaitiolovelvollisuudesta sekä hyväksikäyttökiellosta. TihL 4 § 2 mom 2 ja 3 kohta, JulkL 22 § 1 mom ja 23 §.
2.7 Salassa pidettävien tietojen luovuttaminen	Organisaatioita suositellaan määrittelemään ja ohjeistamaan selkeästi, missä tilanteissa, millä perusteilla sekä miten salassa pidettävää tietoa voidaan luovuttaa. TihL 4 § 2 mom 2 kohta, JulkL 7 luku.
2.8 Harkinnan-varaisesti annettavat tiedot	Organisaatioita suositellaan tunnistamaan harkinnanvaraisesti annettavat tiedot ja merkitsemään ne tarvittavassa laajuudessa. TihL 4 § 2 mom, 13 § 1 mom ja JulkL 16 a §. Organisaatioita suositellaan suojaamaan harkinnanvaraisesti annettavat tiedot hyödyntäen riskilähtöisesti salassa pidettävien tietojen suojaamisessa käytettyjä hallintakeinoja. TihL 13 § 1 mom.
3.1.1 Tietojen suojaaminen sivullisilta	Organisaation tulee järjestää salassa pidettävien tietojen käsittely siten, että tiedot eivät vahingossa tai tahallisesti tule sivullisten tietoon. TihL 4 § 2 mom 2 ja 5 kohta, 15 § 2 mom, JulkL 22 §. Organisaatioita suositellaan varmistamaan tietojen suojaaminen sivullisilta käyttämällä salassa pidettävien tietojen käsittelyyn riittävän turvallisia tiloja tai toteuttamalla muita toimenpiteitä, jotka pienentävät riskiä salassa pidettävien tietojen tulemisesta sivullisen tietoon. TihL 13 § 1 mom, 15 § 2 mom.

Luku	Suositus ja lakiperuste
3.1.2 Tilaturvallisuus	Organisaatioiden tulee käsitellä ja säilyttää tietoaineistoja toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia. TihL 15 § 2 mom. Tilaturvallisuuden varmistamiseksi suositellaan toteutettavaksi ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä turvallisuustason palauttamiseksi. TihL 13 § 1 mom, 15 § 2 mom. Organisaatioita suositellaan soveltamaan turvallisuusluokitteluasetuksessa määriteltyjä käsitteitä eri tasoista turvallisuusalueista sekä hyödyntämään Julkri-kriteeristöä yksityiskohtaisten fyysisten suojausten (FYY-05, FYY-06, FYY-07) määrittelyssä. TihL 13 § 1 mom, 15 § 2 mom, TLA 9 §.
3.1.3 Sallitut tietojenkäsittely-ympäristöt	Organisaatiota suositellaan määrittelemään ja ohjeistamaan selkeästi missä järjestelmissä, palveluissa, säilytysratkaisuissa sekä päätelaitteissa saa käsitellä ja säilyttää salassa pidettäviä tietoja. TihL 4 § 2 mom 2 kohta.
3.1.4 Etäkäyttö	Organisaatioita suositellaan määrittelemään ja ohjeistamaan salassa pidettävien tietojen käsittelyyn liittyvät menettelyt, kun työskennellään organisaation määrittelemien turvallisuusalueiden ulkopuolella. TihL 4 § 2 mom 2 kohta, 13 § 1 mom, TLA 10 § Organisaatioita suositellaan arvioimaan etäkäyttöön liittyviä riskejä sekä määrittelemään siltä pohjalta missä ja millä tavalla salassa pidettäviä tietoja saa käsitellä. TihL 13 § 1 mom.
3.1.6 Ohjeistaminen	Organisaatioita suositellaan ohjeistamaan salassa pidettävien tietojen käsittelyyn liittyvät asiat mahdollisimman helppokäyttöisellä tavalla. TihL 4 § 2 mom 2 kohta.
3.2.1 Hankintojen ja järjestelmien turvallisuus	Organisaatioiden tulee sisällyttää salassa pidettävien tietojen käsittelyyn liittyvien tietojärjestelmien ja palveluihin hankinta- ja ylläpitoprosesseihin tietoturvavaatimusten määrittelyt ja niiden täyttymisen varmistaminen. TihL 13 § 4 mom. Osana palveluun kohdistettavien tietoturvavaatimusten määrittelyä suositellaan, että arvioidaan myös palveluntuottajan toimintaan kohdistuvien tietoturvavaatimusten tarpeellisuus ja laajuus. TihL 13 § 4 mom. Organisaatioita suositellaan arvioimaan hankinnan yhteydessä lainsäädäntöjohdannaiset riskit ja huomioimaan ne palvelun tuottajaan ja tietojen fyysiseen sijaintiin liittyvissä vaatimuksissa. TihL 13 § 1 mom. Ylläpitoprosessit suositellaan suunnittelemaan siten, että niiden yhteydessä varmistetaan riittävän säännöllisesti tietoturvavaatimusten ajantasaisuus, asetettujen tietoturvavaatimusten täyttyminen versiopäivitysten yhteydessä sekä yleisesti tunnistettuihin haavoittuvuuksiin liittyvät korjaukset. TihL 13 § 1 mom.

Luku	Suositus ja lakiperuste
	Salassa pidettävien tietojen käsittelyn turvallisuuden varmistamiseksi suositellaan, että palveluja käyttävät organisaatiot ottavat yhteisiin palveluihin kohdistuvat tietoturvavaatimukset huomioon palvelusopimuksissa sekä tarkistavat ne palvelusopimusten tarkistusten yhteydessä yhteistyössä palveluntuottajan kanssa. TihL 13 § 1 ja 4 mom. Salassa pidettävien tietojen turvallisuuden varmistamiseksi on suositeltavaa, että organisaatiot varmistavat salassa pidettäviä tietoja koskevien vaatimusten sisältymisen yhteishankintayksiköiden ja sidosyksiköiden kanssa laadittaviin hankintasopimuksiin sekä mahdollisuuksien mukaan myös näiden yksiköiden kanssa tehtäviin puitesopimuksiin. TihL 13 § 4 mom.
3.2.2 Käyttöoikeuksien ajantasaisuus	Tietojärjestelmien käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiseksi suositellaan, että organisaation määrittelee prosessit, joiden mukaisesti käyttöoikeudet ylläpidetään tehtävämuutosten yhteydessä. TihL 16 §. Käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiseksi, niiden tarkastaminen on suositeltavaa kytkeä sellaisiin prosesseihin, jotka tehdään aina tehtävämuutosten yhteydessä. Näin varmistetaan, että tarvittavat muutokset käyttöoikeuksiin tapahtuvat ajantasaisesti. TihL 16 §. Käyttöoikeuksien ylläpitoprosessi suositellaan määrittelemään siten, että varsinaiset päätökset käyttöoikeuksista tekevät ne henkilöt, joilla on vastuu salassa pidettävistä tiedoista sekä edellytykset arvioida käyttäjän tarvetta saada käyttöoikeus kyseisiin tietoihin. TihL 16 §.
3.2.3 Käyttäjien todentaminen ja seuranta	Organisaatioita suositellaan todentamaan salassa pidettävien tietojen käyttäjät riittävän luotettavilla yksilöllisillä käyttäjätunnisteilla sekä varmistamaan käsittelyn turvallisuus riittävällä seurannalla. TihL 4 § 2 mom 5 kohta, 13 § 4 mom, TihL16 §, Salassa pidettävien tietojen turvallisuuden varmistamiseksi suositellaan, että organisaatiossa on käytössä riittävän luotettavat menetelmät käyttäjien todentamiseen, joita ovat muun muassa: yksilölliset henkilökohtaiset käyttäjätunnisteet, vähintään salasanaan perustuva menetelmä sekä käyttäjätunnusten lukkiutuminen liian monen virheellisen yrityksen jälkeen. TihL 13 § 1 mom. Vahvempia todentamismenetelmiä, kuten esimerkiksi mobiililaitteeseen tai varmennekorttiin perustuvaa monivaiheista todentamista suositellaan käytettäväksi etenkin niissä tilanteissa, kun käyttö tapahtuu vähemmän turvallisesta käyttöympäristöstä. TihL 13 § 1 mom, 14 §. Lisäksi suositellaan, että organisaatio varmistaa salassa pidettävien tietojen käsittelyn turvallisuuden riittävällä lokitietoihin perustuvalla seurannalla. TihL 17 §.
3.2.4 Salassa pidettävien tietojen jatkuvuudenhallinta	Organisaatioita suositellaan suunnittelemaan ja toteuttamaan riittävät suojaukset salassa pidettävän tiedon luottamuksellisuuden varmistamiseksi myös häiriötilanteissa. TihL 13 § 1 mom.

Luku	Suositus ja lakiperuste
3.3.1 Käsittely-ympäristön erottaminen	Organisaatioita suositellaan erottamaan salassa pidettävien tietojen käsittely-ympäristö julkisista tietoverkoista sekä muista heikomman turvallisuustason ympäristöistä. TihL 13 § 1 mom. Tietojenkäsittely-ympäristön kytkemisessä muihin ympäristöihin suositellaan käytettäväksi vähintään palomuuriratkaisua. TihL 13 § 1 mom.
3.3.2 Tiedon salaus- ja vastaanottajan varmistaminen	Organisaatioita suositellaan salaamaan salassa pidettävää tieto yleisissä tietoverkoissa salausratkaisuilla, jotka tukevat moderneja salausvahvuuksia ja joissa ei ole tunnettuja haavoittuvuuksia. TihL 14 § 1 mom.
3.3.3 Järjestelmä-kovennukset	Organisaatioita suositellaan ottamaan käyttöön menettelytapa, jolla salassa pidettäviä tietoja sisältävät järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on niin kutsuttu kovennettu asennus. TihL 13 § 1 mom Organisaatioita suositellaan koventamaan salassa pidettäviä tietoja sisältävät järjestelmät järjestelmällisen menettelyn avulla, jossa vaihdetaan oletussalasanat, poistetaan käytöstä ei välttämättömät palvelut sekä rajoitetaan yhteydet ja ominaisuudet vähimpien oikeuksien periaatteen mukaisesti. TihL 13 § 1 mom.
3.3.4 Haittaohjelma-suojaukset	Organisaatioita suositellaan suunnittelemaan ja toteuttamaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, havaitsemiseen ja tilanteen korjaamiseen. TihL 13 § 1 mom.
3.3.5 Ohjelmisto-haavoittuvuuksien hallinta	Organisaatioita suositellaan toteuttamaan tietojenkäsittely-ympäristön koko elinkaaren ajalle luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi. TihL 13 § 1 mom.

Lähteet

Säädökset

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

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

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

Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015). https://www.finlex.fi/fi/laki/ajantasa/2015/20150010.

Laki sähköisen viestinnän palveluista (914/2014). Laki sähköisen viestinnän palveluista 917/2014 - Ajantasainen lainsäädäntö - FINLEX®.

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013). Laki valtion yhteisten tieto- ja… 1226/2013 - Ajantasainen lainsäädäntö - FINLEX®.

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

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

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

Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014). Valtioneuvoston asetus valtion yhteisten tieto- ja… 132/2014 - Ajantasainen lainsäädäntö - FINLEX®.

Tiedonhallintalautakunnan suositukset

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2021:33). Suositus asiankäsittelyn metatiedoista. http://urn.fi/URN:ISBN:978-952-367-704-3

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

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

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

Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2020:29). Suositus tiedonhallintamallista. http://urn.fi/URN:ISBN:978-952-367-328-1

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

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

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

Tiedonhallintalautakunnan suositus – Valtiovarainministeriö (2022:42). Suositus viranomaisten asiakirjojen metatiedoista palveluja tuotettaessa. http://urn.fi/URN:ISBN:978-952-367-271-0

Ohjeet ja muut materiaalit

Digi- ja väestötietovirasto 2022. VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään 9.6.2022. https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf/6d71d86f-c7bc-6683-9b36-c55d16d4c1f0/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf?t=1668431647827. Viitattu 29.9.2022.

Tietotermit 2018. http://urn.fi/URN:NBN:fi:au:tt:t41. Viitattu 2.11.2022.

Kansallisarkisto 2013. Määräys ja ohjeet arkistotiloista. AL/19699/07.01.01.00/2012. https://arkisto.fi/uploads/normit/valtionhallinto/maarayksetjaohjeet/maarays_ja_ohjeet_arkistotiloista01032013.pdf. Viitattu 16.5.2022.

Sanastokeskus 2018. Kyberturvallisuuden sanasto (TSK 52) . Kyberturvallisuuden sanasto (TSK 52) | Sanastokeskus. Viitattu 29.9.2022.

Sanastokeskus 2004. Tiivis tietoturvasanasto (TSK 31) . Tiivis tietoturvasanasto (TSK 31) | Sanastokeskus Viitattu 29.9.2022.

Suomen standardisoimisliitto SFS ry 2018. SFS-ISO 27005:2018. Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta. SFS - Tietoturvariskit hallintaan standardin ohjeilla. Viitattu 17.10.2022.

Suomen standardisoimisliitto SFS ry 2022. ISO/IEC 27001:2022 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 Tietoturvallisuuden standardisarja | SFS. Viitattu 17.10.2022.

Suomen standardisoimisliitto SFS ry 2022. ISO/IEC 27002:2022 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. ISO/IEC 27000 Tietoturvallisuuden standardisarja | SFS. Viitattu 17.10.2022.

Suomen standardisoimisliitto SFS ry 2018. SFS-ISO 31000:2018. Riskienhallinta. Ohjeet. ISO 31000 Riskienhallinta | SFS. Viitattu 17.10.2022.

Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/etusivu. Viitattu 16.5.2022.

Valtiovarainministeriö. Valtiohallinnon tietoturvallisuuden johtoryhmä 2008. Valtiohallinnon tietoturvallisuussanasto. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto | Suomidigi. Viitattu 19.10.2022.

Viestintävirasto. Kyberturvallisuuskeskus 2016. Kiintolevyjen elinkaaren hallinta. Ylikirjoitus ja uusiokäyttö. Ohje-ylikirjoitus.pdf (kyberturvallisuuskeskus.fi). Viitattu 16.5.2022.

Traficom. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus. 2022. NCSA-toiminnon hyväksymät salausratkaisut. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut | Kyberturvallisuuskeskus. Viitattu 10.8.2022.

Traficom. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus 2020. Näin keräät ja käytät lokitietoja. Näin keräät ja käytät lokitietoja | Kyberturvallisuuskeskus. Viitattu 17.10.2022.

Traficom. Liikenne- ja viestintävirasto. Kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf (kyberturvallisuuskeskus.fi). Viitattu 17.10.2022.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-241-3 (pdf)

Tammikuu 2023