xxx ministeriön julkaisusarja 2020:xx

Suositus salassa pidettävien asiakirjojen käsittelystä

Lautakunnat

Valtiovarainministeriön julkaisuja - 2022

Sisältö

1 Johdanto

Tämä tiedonhallintalautakunnan suositus opastaa salassa pidettävien asiakirjojen[1], jäljempänä *tietojen*, käsittelyssä sekä käsittelyä koskevien vaatimusten täyttämisessä. Kyseessä on suositus, joten lainsäädännön vaatimukset voidaan täyttää myös muilla kuin suosituksessa kuvatuilla tavoilla. Suositus on tarkoitettu ensisijaisesti tiedonhallintayksiköille ja 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*.

1.1 Lainsäädännölliset perusteet

Suositus pohjautuu julkisen hallinnon tiedonhallintalakiin (906/2019), jäljempänä *tiedonhallintalaki* tai *TihL*, missä säädetään muun muassa salassa pidettävien tietojen siirtämisestä tietoverkoissa sekä tietojen luovuttamisesta teknisen rajapinnan avulla viranomaisten välillä. Suositukseen vaikuttaa myös laki viranomaisten toiminnan julkisuudesta (621/1999), jäljempänä *julkisuuslaki* tai *JulkL*, jossa säädetään muun muassa julkisuusperiaatteesta, viranomaisen asiakirjasta, salassapidon perusteista ja salassa pidettävistä asiakirjoista.

Tiedonhallintalain 18 §:ssä ja sitä täydentävässä valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä

[1] JulkL 22, 24 §

turvallisuusluokitteluasetus tai TLA, säädetään turvallisuusluokittelusta, luokittelumerkinnöistä sekä turvallisuusluokiteltavien asiakirjojen käsittelystä.

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 laissa henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (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 suojaamista. Suositusta laadittaessa on pyritty välttämään päällekkäisyyttä muiden suositusten kanssa. Koosteet tässä suosituksessa olevista lainsäädännöstä tulevista vaatimuksista sekä suosituksista ovat liitteissä 1 ja 2.

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 turvallisuus-luokiteltavien asiakirjojen käsittelystä (2021:5) ja Suositus turvallisuus-luokiteltavien 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.

1.3 Salassa pidettävien asiakirjojen käsittely pilvipalveluissa

Yleinen lähtökohta suunniteltaessa salassa pidettävien asiakirjojen 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 organisaa-

tion on kuitenkin selvitettävä pilvipalvelun turvallisuuteen liittyvät riskit sekä palvelun soveltuvuus suunniteltuun käyttötarkoitukseen ottaen huomioon erityisesti seuraavia näkökohtia:

- pilvipalvelun käyttöön ja hallintaan liittyvät riskit,
- lainsäädäntöjohdannaiset ja määräysvaltaan liittyvät riskit,
- voidaanko tietojen saatavuus varmistaa riittävällä tavalla myös vakavissa häiriötilanteissa sekä mahdollisesti myös poikkeusoloissa sekä
- jos käsiteltäviin tietoihin sisältyy henkilötietoja, onko tietojen säilytys ja hallinnointi toteutettu EU:n tietosuoja-asetuksen hyväksymällä alueella.

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

- Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa (2022:4),
- Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) sekä
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) sekä siihen sisältyvä käyttötapaus ”SaaS-pilvipalvelun arviointi”[2].

1.4 Rajaukset

Tämä suositus koskee tiedonhallintalain soveltamista salassa pidettävän tiedon käsittelyyn. Tässä suosituksessa ei ole huomioitu turvallisuusluokiteltaviin tietoihin liittyviä käsittelyvaatimuksia. Suosituksessa ei myöskään ole huomioitu toimialakohtaista lainsäädäntöä, kuten sosiaali- ja terveydenhuollon lainsäädäntöön sisältyviä vaatimuksia salassa pidettäville tiedoille. Suosituksessa ei ole myöskään huomioitu esimerkiksi henkilötietojen käsittelyä koskevasta sääntelystä taikka kansainvälisiin tietoturvallisuusvelvoitteista johtuvia vaatimuksia. Vaikka

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

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[3] tietoja, jotka on jaettu eri turvallisuusluokkiin. Tietojen luovuttamisen näkökulmasta osa tiedoista, jotka eivät ole salassa pidettäviä, voivat olla harkinnanvaraisesti[4] annettavia.

Julkisuuslain 22 §:ssä[5] säädetään asiakirjasalaisuudesta. Julkisuuslain 24 §:n 1 momentissa on eritelty viranomaisen salassa pidettävät asiakirjat, joita ovat muun muassa:

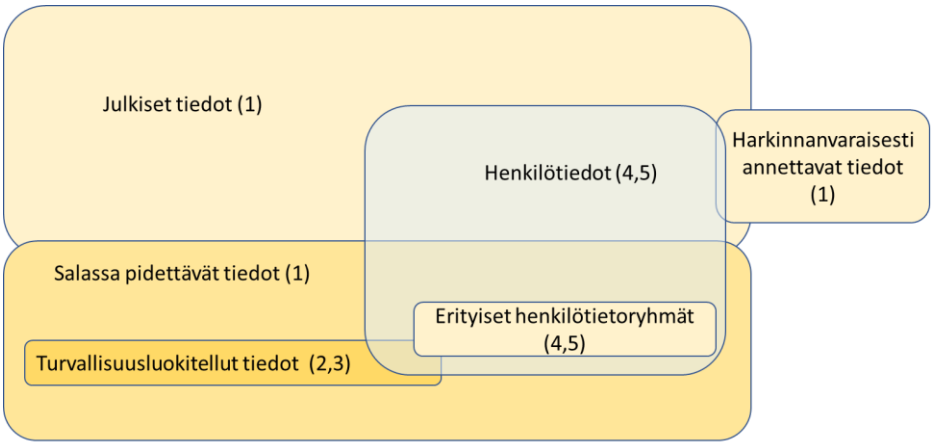
> 17) asiakirjat, jotka sisältävät tietoja valtion, hyvinvointialueen, kunnan tai muun julkisyhteisön tai (julkisuuslain) 4 §:n 2 momentissa tarkoitetun yhteisön, laitoksen tai säätiön liikesalaisuudesta,
>
> 20) asiakirjat, jotka sisältävät tietoja yksityisestä liikesalaisuudesta, samoin kuin sellaiset asiakirjat, jotka sisältävät tietoja muusta vastaavasta yksityisen elinkeinotoimintaa koskevasta seikasta,

[3] TihL 18 § ”Turvallisuusluokiteltavat asiakirjat valtionhallinnossa” sekä Turvallisuusluokitteluasetus 3 § ”Turvallisuusluokittelu ja turvallisuusluokan merkitseminen”.
[4] JulkL 16 a § ”Muuhun kuin salassa pidettävään asiakirjaan tehtävät merkinnät”, 9 § ”Tiedonsaanti julkisesta asiakirjasta”, sekä 17 § ”Tiedonsaantioikeuksien huomioon ottaminen päätöksenteossa”.
[5] JulkL 22 § ”Asiakirjasalaisuus”.

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;

Alla olevassa kuviossa on selvennetty julkisten, salassa pidettävien, turvallisuusluokiteltavien, henkilötietojen ja erityisiin henkilötietoryhmiin liittyvien tietojen suhdetta toisiinsa. Kuvio on suuntaa antava eikä se sisällä toimialakohtaisia säädöksiä. Osittain kuvion ulkopuolelle on sijoitettu harkinnanvaraisesti annettavat tiedot, joista tiedonsaanti on viranomaisen harkinnassa. Harkinnanvaraisia 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. Käytännössä monet erityisiin henkilötietoryhmiin kuuluvat tiedot ovat lain mukaan salassa pidettäviä. Osa henkilötiedoista ja erityisiin henkilötietoryhmiin liittyvistä tiedoista voivat olla myös turvalli-

suusluokiteltavia. Henkilötietojen käsittelyssä on noudatettava tietosuojalainsäädäntöä sekä salassa pidettävän tiedon käsittelyä koskevia vaatimuksia, jos tiedot ovat 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 ylemmän tason tietoturvallisuusvaatimuksia.

Tiedonhallintalaki ei sisällä kovin yksityiskohtaisia vaatimuksia salassa pidettävien tietojen tietoturvallisuustoimenpiteistä. TihL 13 § 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.

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (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[6] 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 suojattu 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.

Edellä olevan perusteella suositellaan, että organisaatiot ottavat käyttöön tietoturvariskien arviointiin soveltuvan riskienarviointimenetelmän[7] 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 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 TL III tason toimenpiteiden soveltamista.

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

[6] esimerkiksi SFS-ISO/IEC 27002 Tietoturvallisuuden hallintakeinojen menettelyohjeet

[7] Esimerkiksi: SFS-ISO/IEC:27001 Luku 6 tai SFS-ISO 31000

Esimerkki kasautumisvaikutuksesta:
- 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.

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 ajalta.

TihL 13 § 1 momentin mukaan ”Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.” Lisäksi TihL 13 § 4 momentin mukaan ”Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.” Tiedonhallintalautakunnan suosituksessa (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 sekä
- varmistaa riittävällä seurannalla, että edellä kuvatut suositukset täyttyvät.

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

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:
- organisaatio määrittelee ja ohjeistaa salassa pidettävien tietojen käsittelyyn sallitut järjestelmät,
- organisaatio määrittelee järjestelmien tietoturvavaatimukset siten, että ne ovat riittävän turvallisia organisaation salassa pidettävien tietojen käsittelyyn,
- organisaatio varmistaa vaatimusten toteutumisen,
- organisaatio tarkastaa valmisohjelmistojen tietoturvamääritykset ja varmistaa niiden täyttymisen hankinnan yhteydessä sekä
- organisaatio suosii ohjelmistoja, joiden turvallisuus on osoitettu riippumattoman 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.

Julkisuuslain 25 § 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.

Salassapito merkitään asiakirjoihin suomeksi ”SALASSA PIDETTÄVÄ”, ruotsiksi ”SEKRETESSGELAGD”. Salassapitomerkinnöistä ei ole annettu tarkempaa yhtenäistä suositusta, mutta seuraava havainnekuva ilmentää dokumenttimuotoisiin asiakirjoihin tehtävää salassapitomerkintää.

Kuvio 2: Havainnekuva salassapitomerkinnästä.

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. Tämä tieto voidaan merkitä esimerkiksi kappale- tai lukukohtaisesti käyttäen kappaleen tai luvun edessä lyhenteitä (J) tai (SALPID). Jos salassapito perustuu säännökseen, jossa on vahinkoedellytyslauseke, merkintä voidaan tehdä kuitenkin niin, että siitä ilmenee vain se säännös, johon salassapito perustuu.

Toisaalta on huomioitava, että itse salassa pidettävä tieto ei saa näkyä metatiedoissa kuten esimerkiksi asiakirjan nimekkeessä[8]. Tieto salassapidosta voidaan merkitä tietojärjestelmiin metatiedoilla ja dokumenttimuotoisiin asiakirjoihin leimamerkinnöillä. Suositeltavia metatietoja ovat salassapitoaika, salassapidon päättyminen tai päättymisajankohta sekä tieto salassapidon perusteesta. Tarkempia tietoja metatiedoista ja rekisteröinnistä löytyy tiedonhallintalautakunnan suosituksista asiankäsittelyn ja palvelujen metatiedoista[9].

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.

[8] Suositus asiankäsittelyn metatiedoista VM 2021:33 s. 20

[9] Suositus asiankäsittelyn metatiedoista VM 2021:33, Suositus viranomaisten asiakirjojen metatiedoista palveluja tuotettaessa VM 2022:42

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.

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 asiakirjoja ei pidetä salassa perusteettomasti ja että salassapitoa koskevat merkinnät ovat ajan tasalla.

Julkisuuslain 25 § 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.

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.[10]

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 § 1 mom 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 § 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 4 kohdan mukaisesti tiedonhallintayksikön 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,

[10] Julkisuuslaki 31 § 1 mom.

- 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[11] ne tilanteet, joissa luovutetaan salassa pidettävää tietoa.

Julkisuuslain 26 § - 32 §:ssä on säädetty yleisistä perusteista salassa pidettävän tiedon antamiselle 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.[12] Ohjeissa tulee ottaa huomioon nämä sekä mahdollinen erityislainsäädäntö.

[11] TihL 4 § 2 mom 2 k

[12] Yleisöltä salassa pidettäviä asiakirjoja voidaan esimerkiksi luovuttaa ennalta määritellylle tiedonsaajalle julkisuus- tai salassapito-olettaman sisältävän säännöksen osoittamissa rajoissa (julkisuuslain 17 §:n 2 ja 3 momentti sekä 23 §:n 2 momentti).

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.

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.[13] Alla oleva havainnekuvio ilmentää harkinnanvaraisesti annettaviin dokumenttimuotoisiin asiakirjoihin tehtävää merkintää.

[13] Julkisuuslaki 6 §, 7 §, 9 § 2 mom

Kuvio 3: Havainnekuvio harkinnanvaraisesti annettavasta merkinnästä.

JulkL 16 § 3 mom 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.

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 harkinnan varaisesti 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 ja työntekijöiden 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 tai toteuttamalla muita toimenpiteitä, jotka pienentävät riskiä salassa pidettävien tietojen tulemisesta sivullisen tietoon.[14]

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:

- sijoittaa salassa pidettäviä tietoja sisältävät tietojärjestelmät ja tietovarannot vähintään riittävällä tavalla suojatulle alueelle. Arviointiin voi hyödyntää turvallisuusluokitteluasetuksessa kuvattua hallinnollisen alueen tyyppisiä vaatimuksia,[15]
- 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.

[14] TihL 13 § 1 mom, 15 § 2 mom
[15] 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.[16]

Turvallisuusalueilla ja niitä ympäröivissä tiloissa 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.

Lisätietoja tilaturvallisuuteen liittyvistä asioita löytyy tiedonhallintalautakunnan suosituksesta (2021:65).[17] Kansallisarkisto antaa tarkempaa ohjausta arkistotilojen vaatimuksista.[18]

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.[19]

---

[16] TihL 15 § 2 mom

[17] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, 2021:65, luku 12.

[18] Kansallisarkisto AL/19699/07.01.01.00/2012

[19] TihL 4 § 2 mom, 13 § 4 mom

Käsittelyprosessin aikana tietoa muokataan, välitetään, säilytetään ja käsitellään myös yhteisesti hyvin monin eri tavoin useissa eri tietojärjestelmissä. Mikäli tietoja ei käsitellä riittävän turvallisissa järjestelmissä, vaarantuu koko käsittelyketjun turvallisuus sekä menetetään osa siitä hyödystä, joka on saavutettu salassa pidettävien tietojen käsittelyyn tarkoitettujen järjestelmien suojauksilla.

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.

3.1.4 Etäkäyttö

Organisaatioita suositellaan määrittelemään ja ohjeistamaan salassa pidettävien tietojen käsittelyyn liittyvät menettelyt, kun työskennellään etänä tai muissa ei turvallisissa tiloissa.[20]

Lainsäädäntö ei estä salassa pidettävien tietojen käsittelyä suojattujen alueiden ulkopuolella kuten julkisissa tiloissa tai etätöissä. Käsiteltäessä salassa pidettäviä tietoja tällaisissa ei-turvallisissa tiloissa, käsittelyyn liittyy kuitenkin erilaisia

[20] TihL 4 § 2 mom

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.[21]

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa:
- ohjeistaa saako salassa pidettäviä tietoja käsitellä suojattavien alueiden ulkopuolella ja missä laajuudessa,
- listata tietojärjestelmät, 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 suojattujen alueiden ulkopuolella sekä
- ohjeistaa hyvät käytännöt käsittelyn turvallisuuden parantamiseksi ei turvallisessa ympäristössä.

3.1.5 Ohjeistaminen

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

Tiedonhallintalain 4 § 2 mom 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. Alla olevassa taulukossa on esimerkkejä ohjeistuksen helppokäyttöisyyden varmistamiseksi.

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,

[21] TihL 13 § 1 mom

- 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 keskeiset tietoturvaohjeet yhteen paikkaan, josta organisaation käyttäjien on helppo löytää ne,
- hävittää vanhentuneet ohjeet 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 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 (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[22]. Näiden palveluiden tuottamisesta vastaa Valtion tieto- ja viestintätekniikkakeskus Valtori sekä tapauskohtaisesti muut valtion omistamat tuottajat kuten Suomen erillisverkot Oy tai CSC-Tieteen tietotekniikan keskus Oy.[23]

Salassa pidettävien tietojen käsittelyn turvallisuuden varmistamiseksi suositellaan, että palveluja käyttävät organisaatiot ottavat yhteisiin palveluihin kohdistuvat tietoturvavaatimukset huomioon palvelusopimuksissa sekä tarkastavat ne palvelusopimusten vuosittaisten tarkastusten yhteydessä yhteistyössä palvelun-tuottajan 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,

[22] Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 1226/2013

[23] Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 132/2014

- 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.

3.2.2 Käyttöoikeuksien ajantasaisuus

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

TihL 16 § 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 tarkastaminen 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
- tarkastaa 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 esimerkiksi 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. [24]

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

[24] TihL 13 § 1 mom

- harjoitella säännöllisesti jatkuvuussuunnitelmien mukaista toimintaa häiriötilanteissa kiinnittäen erityistä huomiota salassapidon toteutumiseen.

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.

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).

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.

TihL 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).

Esimerkkejä toimenpiteistä, joita organisaatio voi toteuttaa viranomaisten välisessä tiedonvaihdossa:
- tietojärjestelmien välisissä tiedonsiirroissa palvelinvarmenteet sekä
- henkilöiden vahva sähköinen tunnistaminen.

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 ja asentaa tarpeellisiksi arvioidut turvapäivitykset,
- tarkastaa asentumisten onnistumisen säännöllisesti, vähintään kuukausittain,
- tarkastaa verkon ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat kattavasti esimerkiksi 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	Asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.	JulkL 5 § 1 mom
Erityisiin henkilötietoryhmiin kuuluva henkilötieto	Sellainen henkilötieto, josta ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettinen tai biometrinen tieto, terveyttä koskeva tieto tai luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskeva tieto.	Tietosuoja-asetus 9 art.
Haavoittuvuus	alttius tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmi-	TEPA-termipankki

	sen toiminnassa. Esimerkiksi ohjelmistossa voi olla haavoittuvuus, joka mahdollistaa järjestelmän väärinkäytön.	
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.	TEPA-termipankki
Hallinnollinen alue	Asetuksessa hallinnollisella alueella tarkoitetaan turvallisuusluokiteltujen asiakirjojen suojaamiseksi määriteltyä aluetta, jolla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa. Tässä suosituksessa hallinnollisella alueella tarkoitetaan viranomaisen normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta, tai esimerkiksi palvelintiloja tai konesaleja tai yhteisöjen kuten yritysten tiloja, joiden osalta tilaa hallitseva toimija varmistaa, että niihin on itsenäinen pääsy ainoastaan	TLA 9 § 1 mom 1 kohta

	viranomaisen ennalta valtuuttamilla henkilöillä.	
Hallintakeino	Hallintakeinolla tarkoitetaan riskiä muuttava toimenpide. Hallintakeinoja ovat kaikki riskiä muuttavat prosessit, politiikat, laitteet, käytännöt tai muut toimenpiteet.	ISO/IEC 27000:2016
Hallintajärjestelmä	Joukko toisiinsa liittyviä tai vaikuttavia organisaation osia, joilla määritellään politiikat ja tavoitteet sekä prosessit, joilla nämä tavoitteet saavutetaan.	ISO/IEC 27000:2016
Henkilötieto	Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai jonkin hänelle tunnusomaisen tekijän perusteella.	Tietosuoja.fi
Julkinen asiakirja, julkisuusperiaate	Viranomaisen asiakirja, jota ei ole säädetty tai määrätty salassa pidettäväksi. Jokaisella on oikeus saada tieto viranomaisen asiakirjasta, joka on julkinen.	JulkL 1 § ja 9 §

Kovennus	Tässä suosituksessa kovettamisella tarkoitetaan prosessia, jossa järjestelmä turvataan vähentämällä sen haavoittuvuuden pinta-alaa. Käytettävissä olevien hyökkäystapojen vähentämiseen kuuluu tyypillisesti oletussalasanojen vaihtaminen, tarpeettomien ohjelmistojen poistaminen, tarpeettomat käyttäjätunnukset tai kirjautumiset sekä tarpeettomien palveluiden poistaminen käytöstä tai poistaminen.	
Lokitiedot	Loki tarkoittaa aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin.	Traficom – Näin keräät ja käytät lokitietoja
Metatieto	Metatieto on tiedon kontekstia, sisältöä ja rakennetta sekä niiden hallintaa ja käsittelyä koko elinkaaren ajan kuvaava tieto. 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.	TEPA-termipankki

Palomuuri	Palomuuri on 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.	TEPA-termipankki
Riski	Riskillä tarkoitetaan haitan tai vaurion todennäköisyyttä ja sen seurauksia. Tietoturvariskeillä tarkoitetaan sellaista tahatonta tai tahallista tekijää, joka vaarantaa tiedon luottamuksellisuutta, eheyttä tai käytettävyyttä. Tietoturvariskin erottaa tietoturvauhasta sillä, että riskin todennäköisyyttä ja vaikutuksia on arvioitu.	
Salassa pidettävä	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 §
Tieto	Tiedolla tarkoitetaan tässä suosituksessa samaa kuin asiakirjalla.	
Tietoaineisto	Asiakirjoista ja muista vastaavista tiedoista muodostuva, tiettyyn viranomaisen	TihL 2 §

	tehtävään tai palveluun liittyvä tietokokonaisuus.	
Tiedonhallintayksikkö	Viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti.	TihL 2 ja 4 §
Tietojärjestelmä	Tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestely. Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja ohjelmistojen käsittelyyn käytettävät päätelaitteet.	TihL 2 §
Turvallisuusluokiteltu asiakirja	on asiakirja, mihin 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 §

Viranomaisen asiakirja	Viranomaisen asiakirjalla tarkoitetaan viranomaisen hallussa olevaa asiakirjaa, 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[25]

[25] 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 1: Kooste dokumenttiin sisältyvistä lainsäädännöstä johdetuista vaatimuksista

Luku	Suositus
2.1 Salassa pidettävät viranomaisen asiakirjat	Organisaation on tunnistettava, milloin se käsittelee salassa pidettäviä tietoja. TihL 4 § 2 mom 2 kohta
2.2. Vähimmäisvaatimukset ja niiden riskilähtöinen täydentäminen	Organisaation tulee täyttää salassa pidettävän tiedon käsittelyä koskevat lainsäädäntöön pohjautuvat vähimmäisvaatimukset. TihL 13 § 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 ajalta. TihL 13 § 1 ja 4 mom Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. TihL 13 § 4 mom
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
3.1.1 Tietojen suojaaminen sivullisilta	Organisaation ja työntekijöiden 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.
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
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. TihL 13 § 4 mom

Liite 2: Kooste dokumenttiin sisältyvistä suosituksista

Luku	Suositus
2.2. Vähimmäisvaatimukset ja niiden riskilähtöinen täydentäminen	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
2.3 Tiedon elinkaari ja salassapito	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 - varmistaa riittävällä seurannalla, että edellä kuvatut suositukset täyttyvät.
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. JulkL 25 §
2.4. Salassa pidettävien tietojen merkintä	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.
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 asiakirjoja ei pidetä salassa perusteettomasti ja että salassapitoa koskevat merkinnät ovat ajan tasalla. TihL 4 § 2 mom 2 kohta, JulkL 31 §

Luku	Suositus
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 Harkinnanvaraisesti annettavat tiedot	Organisaatioita suositellaan tunnistamaan harkinnanvaraisesti annettavat tiedot ja merkitsemään ne tarvittavassa laajuudessa. JulkL 16 a §
2.8 Harkinnanvaraisesti annettavat tiedot	Organisaatioita suositellaan suojaamaan harkinnanvaraisesti annettavat tiedot hyödyntäen riskilähtöisesti salassa pidettävien tietojen suojaamisessa käytettyjä hallintakeinoja. TihL 13 § 1 mom
3.1.1 Tietojen suojaaminen sivullisilta	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
3.1.2 Tilaturvallisuus	Turvallisuusalueilla ja niitä ympäröivissä tiloissa suositellaan toteutettavaksi ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä tekoa edeltäneen turvallisuustason palauttamiseksi. TihL 15 § 2 mom
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. TihL 4 § 2 mom 2 kohta, 13 § 4 mom
3.1.4 Etäkäyttö	Organisaatioita suositellaan määrittelemään ja ohjeistamaan salassa pidettävien tietojen käsittelyyn liittyvät menettelyt, kun työskennellään etänä tai muissa ei turvallisissa tiloissa. TihL 4 § 2 mom 2 kohta, 13 § 1 mom
3.1.4 Etäkäyttö	Organisaatioita suositellaan arvioimaan etäkäyttöön liittyviä riskejä sekä määrittelemään siltä pohjalta missä ja millä tavalla salassa pidettäviä tietoja saa käsitellä etänä. TihL 13 § 1 mom
3.1.5 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	Osana palveluun kohdistettavien tietoturvavaatimusten määrittelyä suositellaan, että arvioidaan myös palveluntuottajan toimintaan kohdistuvien tietoturvavaatimusten tarpeellisuus ja laajuus. TihL 13 § 4 mom
3.2.1 Hankintojen ja järjestelmien turvallisuus	Organisaatioita suositellaan arvioimaan hankinnan yhteydessä lainsäädäntöjohdannaiset riskit ja huomioimaan ne palvelun tuottajaan ja tietojen fyysiseen sijaintiin liittyvissä vaatimuksissa. TihL 13 § 1 mom
3.2.1 Hankintojen ja järjestelmien turvallisuus	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
3.2.1 Hankintojen ja järjestelmien turvallisuus	Salassa pidettävien tietojen käsittelyn turvallisuuden varmistamiseksi suositellaan, että palveluja käyttävät organisaatiot ottavat yhteisiin palveluihin kohdistuvat tietoturvavaatimukset huomioon palvelusopimuksissa sekä tarkastavat ne palvelusopimusten vuosittaisten tarkastusten yhteydessä yhteistyössä palveluntuottajan kanssa. TihL 13 § 1 ja 4 mom
3.2.1 Hankintojen ja järjestelmien turvallisuus	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 §
3.2.2 Käyttöoikeuksien ajantasaisuus	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 §
3.2.2 Käyttöoikeuksien ajantasaisuus	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 §,
3.2.3 Käyttäjien todentaminen ja seuranta	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.
3.2.3 Käyttäjien todentaminen ja seuranta	Vahvempia todentamismenetelmiä, kuten esimerkiksi mobiililaitteeseen tai varmennekorttiin perustuvaa monivaiheista todentamista suositellaan käytettäväksi etenkin niissä tilanteissa, kun käyttö tapahtuu vähemmän turvallisesta käyttöympäristöstä.
3.2.3 Käyttäjien todentaminen ja seuranta	Lisäksi suositellaan, että organisaatio varmistaa salassa pidettävien tietojen käsittelyn turvallisuuden riittävällä lokitietoihin perustuvalla seurannalla.
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
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
3.3.1 Käsittely-ympäristön erottaminen	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 Järjestelmäkovennukset	Organisaatioita suositellaan ottamaan käyttöön menettelytapa, jolla salassa pidettäviä tietoja sisältävät järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on niin kutsuttu kovennettu asennus. TihL 13 § 4 mom
3.3.3 Järjestelmäkovennukset	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. TihL 13 § 4 mom
3.3.4 Haittaohjelmasuojaukset	Organisaatioita suositellaan suunnittelemaan ja toteuttamaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, havaitsemiseen ja tilanteen korjaamiseen.
3.3.5 Ohjelmistohaavoittuvuuksien hallinta	Organisaatioita suositellaan toteuttamaan tietojenkäsittely-ympäristön koko elinkaaren ajalle luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.

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. Viitattu 16.5.2022.

Laki julkisen hallinnon tiedonhallinnasta. https://www.finlex.fi/fi/laki/ajantasa/2019/20190906. Viitattu 16.5.2022.

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

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). https://www.finlex.fi/fi/laki/alkup/2019/20191101

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). Suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä, Julkri. http://urn.fi/URN:ISBN:978-952-367-275-8

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

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

Tiedonhallintalautakunnan suositus – Valtiovarainministeriö (2022:4). 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

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.

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

Traficom Liikenne- ja viestintävirasto 2022. NCSA-toiminnon hyväksymät salausratkaisut. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut. Viitattu 10.8.2022.

Traficom Liikenne- ja viestintävirasto 2020. Näin keräät ja käytät lokitietoja https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja. Viitattu 16.5.2022.

Turvallisuuskomitea 2017. Kokonaisturvallisuuden sanasto. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf. Viitattu 16.5.2022.

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