VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Lautakunnat

Valtiovarainministeriön julkaisuja – 2020:19

Valtiovarainministeriön julkaisuja 2020:19

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Valtiovarainministeriö, Helsinki 2020

Valtiovarainministeriö

ISBN PDF: 978-952-367-292-5

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2020

Kuvailulehti

Julkaisija	Valtiovarainministeriö		19.3.2020
Tekijät	Tiedonhallintalautakunta		
Julkaisun nimi	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:19		
Diaari/hankenumero	-	**Teema**	Lautakunnat
ISBN PDF	978-952-367-292-5	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-292-5		
Sivumäärä	36	**Kieli**	Suomi
Asiasanat	tiedonhallintalaki, tiedonhallintalautakunta, lautakunnat, tietoturva, julkinen hallinto, luokitukset, asiakirjat, tiedonhallintalautakunta		

Tiivistelmä

Tiedonhallintalain 18§:n mukaan valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 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.

Turvallisuusluokitusmerkinnällä kerrotaan tiedon vastaanottajille, miten tietoja tulee käsitellä. Tietojärjestelmissä merkintä voidaan tehdä esimerkiksi metatietoihin. Asiakirjoissa merkintä voidaan tehdä myös asiakirjan liitteeseen.

Tiedonhallintalautakunta hyväksyi suosituksen 11.2.2020.

Kustantaja	Valtiovarainministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: vnjulkaisumyynti.fi

Presentationsblad

Utgivare	Finansministeriet		19.3.2020
Författare	Informationshanteringsnämden		
Publikationens titel	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (Rekommendation om behandling av säkerhetsklassificerade handlingar)		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:19		
Diarie-/ projektnummer	-	**Tema**	Nämnder
ISBN PDF	978-952-367-292-5	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-292-5		
Sidantal	36	**Språk**	Finska
Nyckelord	informationshanteringslagen, informationshanteringsnämnden, nämnder, datasäkerhet, offentlig förvaltning, klassificeringar, handlingar		

Referat

Enligt 18 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) ska myndigheter vid statliga ämbetsverk och inrättningar, domstolar och nämnder som har inrättats för att behandla besvärsärenden säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationssäkerhetsåtgärder som ska vidtas vid behandlingen av dem. Anteckning om säkerhetsklass ska göras, om en handling eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999) och om obehörigt avslöjande eller obehörig användning av handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.

Anteckningen om säkerhetsklass berättar för mottagaren hur informationen ska behandlas. I informationssystem kan anteckningen göras till exempel i metadata. I en handling kan anteckningen också göras i bilagan till handlingen.

Informationshanteringsnämnden godkände rekommendationen den 11 februari 2020.

Förläggare	Finansministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: vnjulkaisumyynti.fi

Description sheet

Published by	Ministry of Finance		19 Month 2020
Authors	Information Management Board		
Title of publication	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (Recommendations on the implementation of management responsibilities in information management)		
Series and publication number	Publications of the Ministry of Finance 2020:19		
Register number	-	**Subject**	Board
ISBN PDF	978-952-367-292-5	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-292-5		
Pages	36	**Language**	Finnish
Keywords	Information Management Unit, Information Management Act, advisory boards, information management, public administration, responsibilities, definitions		

Abstract

The purpose of this recommendation is to guide the management of the Information Management Unit in organising information management as required by the Information Management Act and other legislation. In particular, the recommendation puts into concrete terms the requirements laid down in the Information Management Act, the implementation of which must be ensured by the management.

The recommendation is not binding; it describes how the management of the Information Management Unit can implement the requirements laid down in the Act. The recommendation does not comment on the internal organisation of information management units, which may be due to special legislation.

The recommendation was approved by the Information Management Board on 11 February 2020.

Publisher	Ministry of Finance
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: vnjulkaisumyynti.fi

Sisältö

1 Johdanto

Tämä tiedonhallintolautakunnan antama suositus opastaa valtioneuvoston asetuksen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, jatkossa TLa) asettamien vaatimusten täyttämisessä.

2 Turvallisuusluokan merkitseminen (TLa 3.2-3.5 §)

Turvallisuusluokat merkitään asiakirjaan seuraavasti: turvallisuusluokan I asiakirjaan tehdään merkintä ”ERITTÄIN SALAINEN”, turvallisuusluokan II asiakirjaan merkintä ”SALAINEN”, turvallisuusluokan III asiakirjaan merkintä ”LUOTTAMUKSELLINEN” ja turvallisuusluokan IV asiakirjaan merkintä ”KÄYTTÖ RAJOITETTU”. Mainitun merkinnän lisäksi voidaan käyttää merkintää ”TL I”, ”TL II”, ”TL III” ja ”TL IV”.

Turvallisuusluokka merkitään 2 momentissa säädetystä poiketen ruotsiksi asiakirjoihin, jotka on laadittu ruotsinkielisinä tai käännetty ruotsiksi. Merkintä voidaan tehdä muulloinkin, jos viranomainen pitää sitä tarpeellisena. Turvallisuusluokan I asiakirjaan tehdään merkintä ”YTTERST HEMLIG”, turvallisuusluokan II asiakirjaan merkintä ”HEMLIG”, turvallisuusluokan III asiakirjaan merkintä ”KONFIDENTIELL” ja turvallisuusluokan IV asiakirjaan merkintä ”BEGRÄNSAD TILLGÅNG”.

Asiakirjan turvallisuusluokan tulee käydä ilmi myös tiedonhallintalain 25 §:ssä tarkoitetun asiarekisterin ja muun viranomaisen yleisesti tiedonhallintaan käyttämän tietovarannon asiakirjaa koskevista tiedoista.

Merkintä voidaan tehdä asiakirjaan liitettävään erilliseen asiakirjaan, jos merkintöjen tekeminen asiakirjaan tai merkinnän muuttaminen ei ole teknisesti mahdollista tai jos turvallisuusluokkaa vastaavat käsittelyvaatimukset ovat tarpeen vain tietyn lyhyehkön ajan.

Tiedonhallintalain 18§:n mukaan valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain (621/1999)

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.

Turvallisuusluokitusmerkinnällä kerrotaan tiedon vastaanottajille, miten tietoja tulee käsitellä. Tietojärjestelmissä merkintä voidaan tehdä esimerkiksi metatietoihin. Asiakirjoissa merkintä voidaan tehdä myös asiakirjan liitteeseen. Eräissä tapauksissa on syytä korostaa, mikä osuus asiakirjasta sisältää turvallisuusluokiteltua tietoa. Tämä tieto voidaan merkitä esimerkiksi kappale- tai lukukohtaisesti käyttäen kappaleen tai luvun edessä turvallisuusluokkien lyhenteitä (E), (S), (L) tai (R).

Tietojen turvallisuusluokitus voidaan kertoa myös suullisesti silloin, kun turvallisuusluokiteltuja tietoja käsitellään esimerkiksi kokouksessa.

EU-neuvoston turvallisuussäännöissä edellytetään, että EU:n turvallisuusluokitelluissa asiakirjoissa turvallisuusluokka merkitään selvästi kullekin sivulle ja kukin sivu numeroidaan ja päivätään. Lisäksi EU SECRET - ja sitä korkeamman turvallisuusluokan asiakirjojen jokaiselle sivulle merkitään jäljennöksen numero, jos ne on tarkoitus jakaa useampana kappaleena. Näitä käytäntöjä on suositeltavaa soveltaa myös kansallisissa turvallisuusluokitelluissa asiakirjoissa.

Turvallisuusluokitusmerkintöjen leimamallit on esitelty alla.

KÄYTTÖ RAJOITETTU
TL IV
JulkL (621/1999) 24.1 §:n ____k
L (____/ ____) ____ §

LUOTTAMUKSELLINEN
TL III
JulkL (621/1999) 24.1 §:n ____k
L (____/ ____) ____ §

SALAINEN
TL II
JulkL (621/1999) 24.1 §:n ____k
L (____/ ____) ____ §

ERITTÄIN SALAINEN
TL I
JulkL (621/1999) 24.1 §:n ____k
L (____/ ____) ____ §

Turvallisuusluokat, niiden lyhenteet, sekä EU-vastineet on esitelty alla olevassa taulukossa.

Kansallinen turvallisuusluokka				EU turvallisuusluokka	
Turvallisuusluokka I	TL I	ERITTÄIN SALAINEN	(E)	TRÈS SECRET UE/ EU TOP SECRET	TS-UE/ EU-TS
Turvallisuusluokka II	TL II	SALAINEN	(S)	SECRET UE/ EU SECRET	S-UE/ EU-S
Turvallisuusluokka III	TL III	LUOTTAMUKSELLINEN	(L)	CONFIDENTIEL UE/ EU CONFIDENTIAL	C-UE/ EU-C
Turvallisuusluokka IV	TL IV	KÄYTTÖ RAJOITETTU	(R)	RESTREINT UE/ EU RESTRICTED	R-UE/ EU-R

Taulukko 1. Turvallisuusluokat, niiden lyhenteet, sekä EU-vastineet

Taulukossa 1 on esitetty rinnakkain kansalliset ja EU-turvallisuusluokat. Luokkien käsittelysäännöissä on eroja ja **EU-turvallisuusluokkien käsittelyssä tulee noudattaa EU:n turvallisuusluokiteltujen tietojen suojaamista koskevia turvallisuussääntöjä.**

2.1 Säädökset ja lisätiedot

EU neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU)

Kansallisen turvallisuusviranomaisen julkaisema kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje

3 Hallinnolliset alueet (TLa 9.2 § kohta 1)

Tiedonhallintayksikön on määritettävä seuraavat fyysisesti suojatut turvallisuusalueet turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi 10 §:ssä tarkoitetulla tavalla:

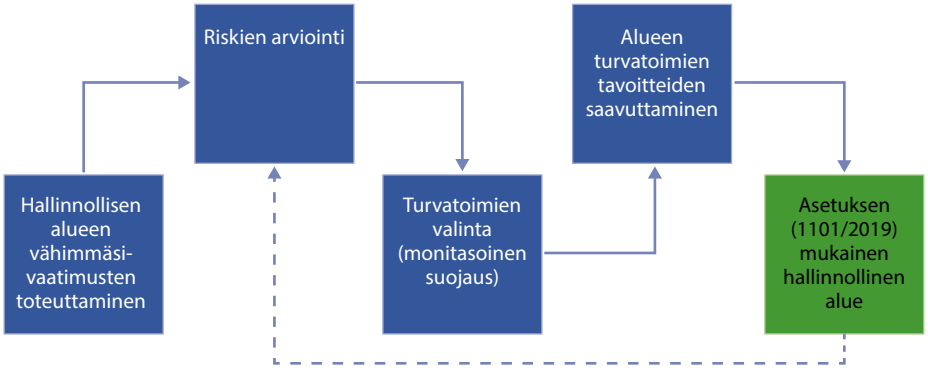
1) hallinnolliset alueet, joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa;

3.1 Hallinnollinen alue

Käytännössä hallinnollisella alueella tarkoitetaan viranomaisen normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta. Niitä voivat olla esimerkiksi palvelintilat, konesalit tai esimerkiksi yritysten tilat. Tilaa hallitseva toimija varmistaa, että tiloihin on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamilla henkilöillä. Hallinnollista aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia.

Tässä suosituksessa esitettyjen hallinnollisen alueen vähimmäisvaatimusten (3.5) lisäksi viranomaisen riskien arvioinnin tulos (luku 3.3) vaikuttaa siihen, mitkä fyysiset turvatoimet tulee valita (luku 3.4) jotta niiden tavoitteet (luku 3.2) saavutetaan. Alueen yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuus on arvioitava uudelleen säännöllisin väliajoin.

Tavoitetilan saavuttamisen prosessi ja säännöllinen arviointi on havainnollistettu seuraavassa kuviossa.



Kuvio 1. Tavoitetilan prosessi ja säännöllinen arviointi

3.2 Fyysisten turvatoimien tavoite ja keinot

Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin:

- varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti
- mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella
- ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet
- estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä.

3.3 Riskien arviointi

Fyysisten turvatoimien valinnan on perustuttava viranomaisen tekemään riskien arviointiin. Siinä on otettava huomioon kaikki asiaan kuuluvat tekijät, erityisesti seuraavat:

- turvallisuusluokiteltujen tietojen turvallisuusluokka
- turvallisuusluokiteltujen tietojen käsittelytapa ja määrä ottaen huomioon, että tietojen suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista
- turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan ympäristö: rakennuksen ympäristö ja sijoittuminen rakennuksessa, tilassa tai sen osassa
- tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille.

3.4 Fyysisten turvatoimien valinta

Viranomaisen on riskien arvioinnin perusteella ja monitasoista suojausperiaatetta soveltaen määriteltävä asianmukainen ja riskiarvioon nähden riittävä turvatoimien yhdistelmä, joka muodostuu hallinnollisista, toiminnallisista ja fyysisistä keinoista, kuten:

- rakenteelliset esteet: fyysinen este, jolla suojattava alue tai tila rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan.
- kulunvalvonta: valvonnalla rajataan pääsyä alueelle tai tilaan. Tavoitteena on havaita luvattomat pääsy-yritykset, estää asiattomien pääsy ja valvoa alueella liikkuvia. Kulunvalvonta voi kohdistua alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonnassa voidaan hyödyntää mekaanisia, sähköisiä tai sähkömekaanisia teknisiä järjestelmiä tai muunlaisia fyysisiä keinoja. Myös vartiointihenkilöstö tai vastaanottovirkailija voi osallistua valvontaan.
- tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä). Järjestelmää voidaan käyttää myös vartiointihenkilöstön asemesta tai tueksi.
- vartiointihenkilöstö: koulutettua, valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää muun muassa kulunvalvonnan tukena sekä alueelle tai tilaan tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemisessa ja toimien estämisessä.
- kameravalvonta: valvontaa voidaan käyttää alueella tai tilassa ilmenevien poikkeamien ennalta estämisessä, hälytysten todentamisessa sekä tapahtuneiden poikkeamien selvittämisessä. Vartiointihenkilöstö voi käyttää kameravalvontaa reaaliaikaisena, aktiivisena kuvan tarkkailuna tai jälkikäteen passiivisena kuvamateriaalin analysointina.
- turvallisuutta ylläpitävät menettelyt: vastuiden ja tehtävien määrittäminen, erilaiset prosessit ja toimintamallit, kuten pääsyoikeuksien ja avainten hallinta, henkilöstön ohjeistus ja perehdyttäminen sekä järjestelmien huolto- ja ylläpitotoimet.
- valaistus: mahdollisia tunkeutujia voidaan estää käyttämällä valaistusta, jonka avulla vartiointihenkilöstö voi valvoa aluetta tehokkaasti, joko suoraan tai kameravalvontajärjestelmää hyödyntämällä.
- muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on estää ja havaita luvaton pääsy tai ehkäistä turvallisuusluokiteltujen tietojen katoaminen tai vahingoittuminen.

3.5 Hallinnollisen alueen fyysisten turvatoimien vähimmäisvaatimukset

Viranomaisen määrittelemän hallinnollisen alueen tulee täyttää taulukossa esitettävät vähimmäisvaatimukset. Niiden lisäksi viranomaisen tulee suunnitella, vastuuttaa ja toteuttaa riskien arviointiin (luku 3.3) ja monitasoiseen suojausperiaatteeseen (luku 3.4) perustuvat muut riskienhallintatoimenpiteet sekä myös ylläpitää niitä siten, että on mahdollista hyväksyä turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit ja saavuttaa turvatoimien tavoitteet (luku 3.2).

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Alueen raja ja rakenteet (seinät, ovet, ikkunat, lattia- ja kattorakenteet)	Alueella on oltava selkeästi määritelty näkyvä raja. Aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia.	Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita, jotta alueelle kulkua on mahdollista hallinnoida asianmukaisesti. Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi.
Pääsyoikeuksien myöntäminen	Ainoastaan viranomaisen asianmukaisesti valtuuttamilla henkilöillä on itsenäinen pääsy alueelle. Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainten hallinnan menettelyt ja roolit.	Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta. Viranomainen on määritellyt tai hyväksynyt ainakin seuraavat menettelyt ja roolit: - pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. - pääsyoikeuksien ja avainten haltijoista on lista. - pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. - avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu. - avainkortteja, jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.
Vierailijat	Muilla kuin viranomaisen asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina oltava saattaja.	Viranomaisen on täytynyt hyväksyä menettelyohje vierailijoita varten. Viranomaisen hyväksymä vierailijaohje voi käsitellä muun muassa seuraavia asioita: - vieras tunnistetaan ja varustetaan vieraskortilla. - vierailu kirjataan. - vierailijoita ei päästetä tai jätetä tiloihin valvomatta. Vierailun isäntä vastaa ulkopuolisista henkilöistä koko vierailun ajan. - henkilöstö on ohjeistettu vierailijoiden isännöintiä varten - huolehtiminen siitä, ettei vieras pääse oikeudettomasti näkemään, kuulemaan tai muutoin saa haltuunsa turvallisuusluokiteltua tietoa.
Äänieristys	Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta.	Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista.

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Tekniset turvallisuus-järjestelmät	Hankittaessa alueelle turvallisuusluokiteltujen tietojen fyysiseen suojeluun tarkoitettuja laitteita (esimerkiksi soveltuvaksi arvioitu säilytysratkaisu, paperisilppureita, lukkoja, elektronisia kulunvalvontajärjestelmiä, kameravalvontajärjestelmiä, tunkeutumisen ilmaisujärjestelmiä ja hälytysjärjestelmiä) viranomaisen on varmistettava, että laitteet ovat toimintakuntoisia ja soveltuvia niiden käyttötarkoitukseen.	Suosituksena on, että laitteet ovat hyväksyttyjen teknisten standardien ja vähimmäisvaatimusten mukaisia. Laitteet pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä, toiminnan testauksista sekä dokumentaation ajantasaisuudesta laitevalmistajan ohjeiden ja suositusten mukaisesti. Järjestelmäoikeuksien hallinnassa on suositeltavaa noudattaa vähimpien oikeuksien periaatetta.
Tunkeutumisen ilmaisujärjestelmä	Ei vaatimuksia.	Alue tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan korkeaksi.
Salaa katselun estäminen	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu huomioon ottaen, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.
Tila- ja laitetarkastukset (ainoastaan TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella hallinnollisella alueella, jossa käsitellään SALAINEN-turvallisuusluokan tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Myös alue on tarvittaessa tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn jälkeen.	
Tiedon säilyttäminen	Alueella voi säilyttää KÄYTTÖ RAJOITETTU -turvallisuusluokan tietoa. Tiedot tulee säilyttää soveltuvissa lukituissa toimistokalusteissa.	

Taulukko 2. Hallinnollisen alueen fyysisten turvatoimien vähimmäisvaatimukset

4 Turva-alueet (TLa 9.2 § kohta 2)

Tiedonhallintayksikön on määritettävä seuraavat fyysisesti suojatut turvallisuusalueet turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi 10 §:ssä tarkoitetulla tavalla:

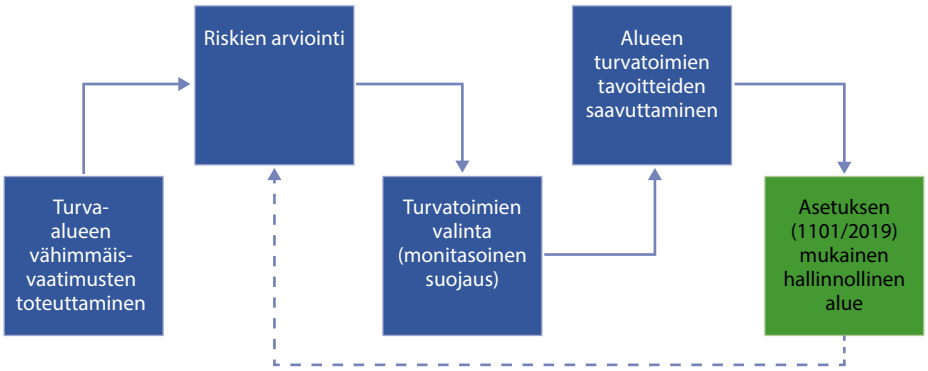
2) turva-alueet, joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle.

4.1 Turva-alue

Turva-alueilla tarkoitetaan viranomaisen työskentelyyn tarkoitettuja, hallinnollisia alueita paremmin suojattuja alueita ja tiloja, joissa käsitellään ja säilytetään turvallisuusluokiteltuja tietoja. Turva-alueita ovat esimerkiksi palvelintilat, konesalit, arkistot tai esimerkiksi yritysten turva-alueiden vaatimukset täyttävät tilat. Turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.

Tässä suosituksessa esitettyjen turva-alueen vähimmäisvaatimusten (luku 4.5) lisäksi viranomaisen riskien arvioinnin tulos (luku 4.3) vaikuttaa siihen, mitkä fyysiset turvatoimet tulee valita (luku 4.4) niiden tavoitteiden (luku 4.2) saavuttamiseksi. Alueen yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuus on arvioitava uudelleen säännöllisin väliajoin.

Tavoitetilan saavuttamisen prosessi ja säännöllinen arviointi on havainnollistettu seuraavassa kuviossa.



Kuvio 2. Tavoitetilan saavuttamisen prosessi ja säännöllinen arviointi

4.2 Fyysisten turvatoimien tavoite ja keinot

Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin:

- varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti.
- mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella.
- ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet.
- estämällä salaa tai väkisin tapahtuva tunkeutuminen tai viivyttämällä sitä.

4.3 Riskien arviointi

Fyysisten turvatoimien valinnan on perustuttava viranomaisen tekemään riskien arviointiin. Siinä on otettava huomioon kaikki asiaan kuuluvat tekijät, erityisesti seuraavat:

- turvallisuusluokiteltujen tietojen turvallisuusluokka.
- turvallisuusluokiteltujen tietojen käsittelytapa ja määrä ottaen huomioon, että tietojen suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista.
- turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan ympäristö: rakennuksen ympäristö ja sijoittuminen rakennuksessa, tilassa tai sen osassa.
- tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille.

4.4 Fyysisten turvatoimien valinta

Viranomaisen on riskien arvioinnin perusteella ja monitasoista suojausperiaatetta (ks. kommentti kuvion yhteydessä) soveltaen määriteltävä asianmukainen ja riskiarvioon nähden riittävä turvatoimien yhdistelmä, joka muodostuu hallinnollisista, toiminnallisista ja fyysisistä keinoista, kuten:

- rakenteelliset esteet: fyysinen este, jolla suojattava alue tai tila rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan.
- kulunvalvonta: valvonnalla rajataan pääsyä alueelle tai tilaan. Tavoitteena on havaita luvattomat pääsy-yritykset, estää asiattomien pääsy ja valvoa alueella liikkuvia. Kulunvalvonta voi kohdistua alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonnassa voidaan hyödyntää mekaanisia, sähköisiä tai sähkömekaanisia teknisiä järjestelmiä tai muunlaisia fyysisiä keinoja. Myös vartiointihenkilöstö tai vastaanottovirkailija voi osallistua valvontaan.
- tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä). Järjestelmää voidaan käyttää myös vartiointihenkilöstön asemesta tai tueksi.
- vartiointihenkilöstö: koulutettua, valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää muun muassa kulunvalvonnan tukena sekä alueelle tai tilaan tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemisessa ja toimien estämisessä.
- kameravalvonta: valvontaa voidaan käyttää alueella tai tilassa ilmenevien poikkeamien ennalta estämisessä, hälytysten todentamisessa sekä tapahtuneiden poikkeamien selvittämisessä. Vartiointihenkilöstö voi käyttää kameravalvontaa reaaliaikaisena, aktiivisena kuvan tarkkailuna tai jälkikäteen passiivisena kuvamateriaalin analysointina.
- turvallisuutta ylläpitävät menettelyt: vastuiden ja tehtävien määrittäminen, erilaiset prosessit ja toimintamallit, kuten pääsyoikeuksien ja avainten hallinta, henkilöstön ohjeistus ja perehdyttäminen sekä järjestelmien huolto- ja ylläpitotoimet.
- valaistus: mahdollisia tunkeutujia voidaan estää käyttämällä valaistusta, jonka avulla vartiointihenkilöstö voi valvoa aluetta tehokkaasti, joko suoraan tai kameravalvontajärjestelmää hyödyntämällä.
- muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on estää ja havaita luvaton pääsy tai ehkäistä turvallisuusluokiteltujen tietojen katoaminen tai vahingoittuminen.

4.5 Turva-alueen fyysisten turvatoimien vähimmäisvaatimukset

Viranomaisen määrittelemän tai hyväksymän turva-alueen tulee täyttää taulukossa esitettävät vähimmäisvaatimukset. Niiden lisäksi viranomaisen tulee suunnitella, vastuuttaa ja toteuttaa riskien arviointiin (luku 4.3) ja syvyyssuuntaiseen turvallisuuteen (luku 4.4) perustuvat muut riskienhallintatoimenpiteet sekä myös ylläpitää niitä siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit on mahdollista hyväksyä ja turvatoimien tavoitteet (luku 4.2) saavuttaa.

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Alueen raja ja rakenteet (seinät, ovet, ikkunat, lattia- ja kattorakenteet)	Alueella on oltava selkeästi määritelty näkyvä raja. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso.	Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita, jotta alueelle kulkua on mahdollista hallinnoida luotettavasti. Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan merkittäväksi. Mikäli mahdollista, hallinnollisen alueen hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Tämä on otettava huomioon erityisesti uudisrakentamisessa. Hätäpoistumisjärjestelyt eivät saa heikentää turvatoimia.
Kulunvalvonta	Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti.	Kulunvalvonta voidaan toteuttaa joko elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen.
Pääsyoikeuksien myöntäminen	Itsenäinen pääsyoikeus alueelle voidaan myöntää vain viranomaisen asianmukaisesti valtuuttamalle henkilölle: - jonka luotettavuus on varmistettu. - jolla on erityinen lupa tulla alueelle. Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainten hallinnan menettelyt ja roolit.	Luotettavuus tulisi ensisijaisesti varmistaa henkilöturvallisuusselvitysmenettelyn avulla. Alueelle pääsemisen perusteena tulisi olla tiedonsaantitarve. Tapauskohtaisesti erityinen lupa voi tarkoittaa myös työskentelytarvetta alueella. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta. Viranomainen on määritellyt tai hyväksynyt ainakin seuraavat menettelyt ja roolit: pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. - pääsyoikeuksien ja avainten haltijoista on lista. - pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. - avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu. - avainkortteja sekä jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Vierailijat	Muilla kuin niillä henkilöillä, joille on myönnetty itsenäinen pääsyoikeus tilaan (vierailijoilla), on aina oltava saattaja. Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia: - alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka on ilmoitettava selkeästi. - kaikilla vierailijoilla on oltava erityinen lupa tulla alueelle, heillä on aina oltava saattaja ja heidän luotettavuutensa on oltava varmistettu asianmukaisesti, paitsi jos on varmistettu, ettei vierailijoilla ole pääsyä turvallisuusluokiteltuihin tietoihin.	Viranomaisen on täytynyt hyväksyä menettelyohje vierailijoita varten. Viranomaisen hyväksymä vierailijaohje voi käsitellä muun muassa seuraavia asioita: - vieras tunnistetaan ja varustetaan vieraskortilla. - vierailu kirjataan. - vierailijoita ei päästetä tai jätetä tiloihin valvomatta. Vierailun isäntä vastaa ulkopuolisista henkilöistä koko vierailun ajan. - henkilöstö on ohjeistettu vierailijoiden isännöintiä varten. - huolehtiminen siitä, ettei vieras pääse oikeudettomasti näkemään tai kuulemaan turvallisuusluokiteltua tietoa.
Turvallisuusohjeet	Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista asioista: - turvallisuusluokka turvallisuusluokitelluille tiedoille, joita alueella voidaan käsitellä ja säilyttää. - sovellettavat valvonta- ja suojatoimenpiteet. - henkilöt, joilla on pääsy alueelle ilman saattajaa erityisen luvan ja luotettavuuden varmistamisen perusteella. - tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle. - muut asiaan kuuluvat toimenpiteet ja menettelyt.	
Äänieristys	Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta.	Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista.

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Tekniset turvallisuus-järjestelmät	Hankittaessa alueelle turvallisuusluokiteltujen tietojen fyysiseen suojeluun tarkoitettuja laitteita (esimerkiksi soveltuvaksi arvioitu säilytysratkaisu, paperisilppureita, lukkoja, elektronisia kulunvalvontajärjestelmiä, kameravalvontajärjestelmiä, tunkeutumisen ilmaisujärjestelmiä ja hälytysjärjestelmiä) viranomaisen on varmistettava, että laitteet ovat soveltuvia niiden käyttötarkoitukseen. Laitteet on tarkastettava ja huollettava säännöllisin väliajoin.	Suosituksena on, että laitteet ovat hyväksyttyjen teknisten standardien ja vähimmäisvaatimusten mukaisia. Laitteet pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä ja dokumentaation ajantasaisuudesta sekä toiminnan testauksista laitevalmistajan ohjeiden ja suositusten mukaisesti. Järjestelmäoikeuksien hallinnassa on suositeltavaa noudattaa vähimpien oikeuksien periaatetta.
Tunkeutumisen ilmaisujärjestelmä	Alue, jolla ei ole henkilöstöä palveluksessa vuorokauden ympäri, on tarvittaessa tarkastettava normaalin työajan päätteeksi ja satunnaisiin aikoihin työajan ulkopuolella, paitsi jos alueelle on asennettu tunkeutumisen ilmaisujärjestelmä (murtohälytysjärjestelmä).	
Salaa katselun estäminen	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu huomioon ottaen, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden näkösuojasermeillä sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.
Tila- ja laitetarkastukset	Tiloihin, joissa käsitellään turvallisuusluokan I tai II tietoja, saa tuoda ainoastaan viranomaisen hyväksymiä elektronisia laitteita. Myös alue on tällöin tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset on suoritettava myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn jälkeen.	Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista tai hyväksyntää ei voida todentaa (matkapuhelimet ja älykellot yms.), laitteet tulee jättää tilan ulkopuolelle, esimerkiksi tähän tarkoitukseen varattuun säilytyspaikkaan.

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Tiedon säilyttäminen	Alueella voi säilyttää kaikkiin turvallisuusluokkiin kuuluvia tietoja riskien arviointiin ja fyysisten turvatoimien valintaan perusten. LUOTTAMUKSELLINEN - ja sitä korkeamman turvallisuusluokan tietoja tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa. Viranomaisen on määriteltävä säilytysratkaisun avainten ja numeroyhdistelmien hallinnointimenettelyt. Numeroyhdistelmät tulee antaa mahdollisimman harvoille, sellaisille henkilöille, joiden on tarpeen tietää ne. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien säilytysratkaisujen numeroyhdistelmät on vaihdettava -uuden turvallisen säilytyspaikan vastaanoton yhteydessä. -aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos. - aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen. - kun jokin lukoista on huollettu tai korjattu. - vähintään 12 kuukauden välein. Turvallisuusluokitellut tiedot, jotka kuuluvat turvallisuusluokkaan ERITTÄIN SALAINEN, on säilytettävä turva-alueella noudattaen jotakin seuraavista ehdoista: - teknisesti valvottu säilytysratkaisu. - ilman teknistä valvontaa oleva säilytysratkaisu, jonka kunto tarkastetaan säännöllisesti. - ilman teknistä valvontaa oleva säilytysratkaisu, jossa on tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaa koulutettu vasteyksikkö. - erillinen tila, jossa on tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaa koulutettu vasteyksikkö.	

Taulukko 3. Turva-alueen fyysisten turvatoimien vähimmäisvaatimukset

5 Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla (TLa 10 §)

Turvallisuusluokiteltuja asiakirjoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta.

Turvallisuusluokan I asiakirjaa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla.

Turvallisuusluokan II–IV asiakirjaa saa käsitellä turvallisuusalueilla ja niiden ulkopuolella kuitenkin siten, että:

1) turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turva-alueelle;

2) turvallisuusluokan II ja III paperiasiakirjat on säilytettävä turva-alueella;

3) turvallisuusluokan IV asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle;

4) turvallisuusluokan IV paperiasiakirjat on säilytettävä turvallisuusalueella.

Sen estämättä, mitä 3 momentin 1 ja 3 kohdassa säädetään tietojärjestelmän sijoittamisesta turvallisuusalueille, turvallisuusluokan II–IV asiakirjoja saa käsitellä myös 9 §:n 1 kohdassa tarkoitetuilla hallinnollisilla alueilla ja niiden ulkopuolella 11 ja 12 §:n vaatimukset täyttävän päätelaitteen ja tietoliikennejärjestelyn avulla. Turvallisuusluokan II asiakirjan käsittelyyn käytetty päätelaite on kuitenkin säilytettävä turva-alueella. Jos turvallisuusluokan III tai IV sähköisiä asiakirjoja säilytetään päätelaitteessa turva-alueiden ulkopuolella, ne on suojattava turvallisuusluokalle riittävän turvallisella salausratkaisulla. Päätelaitteen tietoturvallisuudesta on huolehdittava.

5.1 Tietojen käsittelyn ja säilytyksen perusperiaatteet

	KÄSITTELY		SÄILYTYS	
Turvallisuusluokka	Hallinnollinen alue	Turva-alue	Hallinnollinen alue	Turva-alue
TL I ERITTÄIN SALAINEN	Ei.	Kyllä, jos pääsy tietoihin on suojattu sivullisilta.	Ei.	Soveltuvaksi arvioidussa säilytysratkaisussa.
TL II SALAINEN	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Kyllä, jos pääsy tietoihin on suojattu sivullisilta.	Ei.	Soveltuvaksi arvioidussa säilytysratkaisussa.
TL III LUOTTAMUKSELLINEN	Kyllä, jos pääsy tietoihin on suojattu sivullisilta.	Kyllä, jos pääsy tietoihin on suojattu sivullisilta.	Ei.	Soveltuvaksi arvioidussa säilytysratkaisussa.
TL IV KÄYTTÖ RAJOITETTU	Kyllä, jos pääsy tietoihin on suojattu sivullisilta.	Kyllä, jos pääsy tietoihin on suojattu sivullisilta.	Soveltuvaksi arvioidussa, lukitussa toimistokalusteessa.	Soveltuvaksi arvioidussa, lukitussa toimistokalusteessa.

Taulukko 4. Tietojen käsittelyn ja säilytyksen perusperiaatteet

Sähköistä käsittelyä tai säilyttämistä turvallisuusalueen ulkopuolella on käsitelty luvussa 5.6.

5.2 Riskien arviointi

Tiedon käsittelyn ja säilytyksen suojaamiseksi valittavien fyysisten turvatoimien on perustuttava viranomaisen tekemään riskien arviointiin. Riskinhallintaprosessissa on otettava huomioon kaikki asiaankuuluvat tekijät, erityisesti seuraavat:

- turvallisuusluokiteltujen tietojen turvallisuusluokka.
- turvallisuusluokiteltujen tietojen käsittelytapa ja määrä. On huomattava, että niiden suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista.
- turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan ympäristö; rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa.
- tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu riski tiedoille.

5.3 Tietojen säilyttäminen

Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvat tiedot on säilytettävä soveltuvaksi arvioiduissa lukituissa toimistokalusteissa hallinnollisella tai turva-alueella. Niitä voidaan tilapäisesti säilyttää turva- tai hallinnollisen alueen ulkopuolella, jos tietojen haltija on sitoutunut noudattamaan viranomaisen antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä.

Turvallisuusluokkaan LUOTTAMUKSELLINEN, SALAINEN tai ERITTÄIN SALAINEN kuuluvat tiedot on säilytettävä turva-alueella soveltuvaksi arvioidussa säilytysratkaisussa, kuten kassakaapissa tai holvissa. Sähköistä käsittelyä tai säilyttämistä turvallisuusalueen ulkopuolella on käsitelty luvussa 5.6.

5.4 Tietojen käsittelyn vähimmäisvaatimukset

Turvallisuusluokkaan KÄYTTÖ RAJOITETTU, LUOTTAMUKSELLINEN tai SALAINEN kuuluvia tietoja on käsiteltävä hallinnollisella tai turva-alueella.

ERITTÄIN SALAINEN -turvallisuusluokkaan kuuluvia tietoja on käsiteltävä turva-alueella.

Asiakirjojen käsittely (TL IV - TL II) on mahdollista myös turvallisuusalueiden ulkopuolella, mikäli on toteutettu riskiarvioon perustuvia, korvaavia toimenpiteitä sen varmistamiseksi, että pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta.

Tiedon käsittelyn tulee täyttää taulukossa 4 esitetyt vähimmäisvaatimukset. Vähimmäisvaatimusten tulee täyttyä riippumatta siitä, millä turvallisuusalueella tietoa käsitellään. Vähimmäisvaatimusten lisäksi viranomaisen tulee suunnitella ja toteuttaa riskien arviointiin (ks. luku 5.2) perustuvat muut riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä.

5.5 Sähköinen käsittely hallinnollisella alueella

Tiedon käsittelyyn käytettävän tietojärjestelmän tai tietoliikennejärjestelyn tulee olla kyseisen turvallisuusluokan mukaisesti suojattu. Esimerkiksi turvallisuusluokan III mukaisesti suojattu päätelaite voidaan tuoda hallinnolliselle alueelle tai sen ulkopuolelle, josta päätelaite ottaa turvallisuusluokan III mukaisella tietoliikennesalauksella suojatun yhteyden turva-alueella sijaitsevaan, turvallisuusluokan III tietovarantoon tietojen käsittelyn ajaksi.

Päätelaitetta ei tule jättää ilman valvontaa hallinnolliselle alueelle, vaan se tulee palauttaa käsittelyn jälkeen säilytettäväksi turva-alueelle, ellei päätelaitteen luottamuksellisuudesta, eheydestä ja käytettävyydestä pystytä muuten varmistumaan (vrt. luku 5.6). Turvallisuusluokkien III tai II kiinteää tietoverkkoa ei voi ulottaa hallinnolliselle alueelle.

5.6 Turvallisuusluokkien IV tai III tietojen käsittely ja säilyttäminen päätelaitteessa

Tilanteissa, joissa turvallisuusluokan IV tai III tietoa käsitellään ja säilytetään kyseisen turvallisuusluokan mukaisessa päätelaitteessa turvallisuusalueiden ulkopuolella, tai turvallisuusluokan III tietoja hallinnollisella alueella, päätelaitteessa olevien tietojen tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella salausratkaisulla, ja erityisesti päätelaitteen kyseiselle turvallisuusluokalle riittävästä eheydestä tulee varmistua, jotta tiedon luottamuksellisuus ei vaarannu päätelaitteen eheyden menetyksen seurauksena.

Tyypillisin tapa eheydestä varmistumiseen on päätelaitteen suojaaminen turvallisuusalueiden fyysisellä pääsynhallinnalla, mukaan lukien esimerkiksi kaikki tietojärjestelmään liittyvät fyysiset palvelimet, verkkolaitteet, päätelaitteet ja kaapeloinnit. Esimerkiksi turvallisuusluokan IV tietojärjestelmän eheyden suojaamisessa yleisiä turvallisuusluokiteltuun tietoon kohdistuvia riskejä vastaan voi riittää tietojärjestelmän tietovarantojen sijoittaminen hallinnolliselle tai turva-alueelle, sekä riittävällä salauksella varustettujen päätelaitteiden osalta myös rajattu säilytys muussa lukittavassa tilassa, esimerkiksi virkamiehen kotona.

Turvallisuusluokan III tietojärjestelmät tulisi kokonaisuudessaan sijoittaa turva-alueelle. Mikäli turvallisuusluokan III tietojen käsittelyyn käytettävää päätelaitetta joudutaan säilyttämään hallinnollisella alueella tai jopa turvallisuusalueiden ulkopuolella, voidaan fyysisen pääsynhallinnan tuoman eheyssuojauksen puuttumista pyrkiä riskiperustaisesti kompensoimaan esimerkiksi päätelaitteen sijoittamisella luvattoman pääsyn paljastavaan koteloon tai pakkaukseen. Saatavilla on esimerkiksi niin sanottuja turvasalkkuja, jotka pyrkivät havaitsemaan salkun sisältöön kohdistuvat luvattomat pääsy-yritykset siten, että luvattomasta pääsystä tuotetaan ilmoitus päätelaitteen luvalliselle käyttäjälle tai käyttäjän organisaatiolle, tai että pääsystä jää jälki kyseiseen koteloon tai pakkaukseen.

Viranomaisen tulee riskienarvioinnissaan kuitenkin huomioida, että turvallisuusalueiden ulkopuolella toimiessa sekä turvallisuusluokiteltuun tietoon, että sen käsittelyyn käytettäviin päätelaitteisiin kohdistuu erityisesti turvallisuusluokasta III lähtien riskejä, joiden riittävä pienentäminen voi olla useissa käyttötapauksissa erittäin haastavaa, ellei jopa mahdotonta. Käsittelyssä tulee huomioida lisäksi salakatselulta ja -kuuntelulta suojautuminen, sekä riskipohjaisesti myös esimerkiksi hajasäteilyriskejä vastaan suojautuminen.

Mikäli päätelaitteella käsitellään kansallisen turvallisuusluokitellun tiedon lisäksi kansainvälisesti turvallisuusluokiteltua tietoa, on turvallisuusluokan III päätelaitteen säilyttämisessä otettava huomioon myös kansainväliset tietoturvavelvoitteet, joissa turva-alueen ulkopuolinen säilyttäminen voi olla kokonaan kielletty.

PAPERIASIAKIRJOJEN KÄSITTELY	
Turvallisuuden osa-alue	**Vähimmäisvaatimus**
Tiedonsaantitarpeen rajaamisperiaatteen toteutuminen	Tietojen käsittely on mahdollista, jos pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta. Sivullisella tarkoitetaan kaikkia niitä henkilöitä, joilla ei ole määriteltyä tiedonsaantitarvetta käsiteltävään turvallisuusluokiteltuun tietoon.
Salaa katselun vastatoimenpiteet	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan luettuna, on toteutettava asianmukaiset toimenpiteet tällaisen riskin hallitsemiseksi.
Teknisen tiedustelun vastatoimenpiteet (ainoastaan TL I ja TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään käsittelyalueella, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Käsittelyalue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn takia.

Taulukko 5. Paperiasiakirjojen käsittely

TIEDON KÄSITTELY SÄHKÖISESTI	
Turvallisuuden osa-alue	**Vähimmäisvaatimus**
Tiedonsaantitarpeen rajaamisperiaatteen toteutuminen	Tietojen käsittely on mahdollista, jos pääsy turvallisuusluokiteltuihin tietoihin on suojattu sivullisilta. Sivullisella tarkoitetaan kaikkia niitä henkilöitä, joilla ei ole määriteltyä tiedonsaantitarvetta käsiteltävään turvallisuusluokiteltuun tietoon.
Salaa katselun vastatoimenpiteet	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan luettuna, on toteutettava asianmukaiset toimenpiteet tällaisen riskin hallitsemiseksi.
Teknisen tiedustelun vastatoimenpiteet (ainoastaan TL I ja TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuinniitä käytetään jollakin alueella, jolla tietoja käsitellään, käsittelyalueella, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Käsittelyalue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn takia.
Tempest-riskit (ainoastaan TL I - III)	Käsiteltäessä sähköisessä muodossa tietoja, jotka kuuluvat turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä korkeampaan, on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi.

Taulukko 6. Tiedon käsittely sähköisesti

TIEDON KÄSITTELY SUULLISESTI	
Turvallisuuden osa-alue	**Vähimmäisvaatimus**
Tiedonsaantitarpeen rajaamisperiaatteen toteutuminen	Tietojen käsittely on mahdollista, jos sivulliset henkilöt eivät pääse kuulemaan henkilöiden turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Sivullisella tarkoitetaan kaikkia niitä henkilöitä, joilla ei ole määriteltyä tiedonsaantitarvetta käsiteltävään turvallisuusluokiteltuun tietoon. Äänieristyksen osalta tulee huomioida, että myös alueen sisällä voi työskennellä henkilöitä, joilla ei ole tiedonsaantitarvetta keskusteltavaan tietoon.
Teknisen tiedustelun vastatoimenpiteet (ainoastaan TL I ja TL II)	Käsittelyalueella on oltava tunkeutumisen ilmaisujärjestelmä ja alue on pidettävä lukittuna silloin, kun sitä ei käytetä. Käsittelyalueelle tulevia henkilöitä ja aineistoja on valvottava. Käsittelyalue on tarvittaessa tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn takia. Käsittelyalueella ei saa olla luvattomia - tietoliikenneyhteyksiä - puhelimia muita viestintävälineitä elektronisia laitteita. Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään käsittelyalueella, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi.

Taulukko 7. Tiedon käsittely suullisesti

6 Tietojärjestelmien erottelu (TLa 11.1§ kohta 1)

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteutettava siten, että:

ne erotetaan niissä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän luotettavasti alemman turvallisuustason tietojärjestelmistä ja tietoliikennejärjestelyistä;

Tietojärjestelmien erottelu on vaikuttavimpia tekijöitä salassa pidettävän tiedon suojaamisessa. Erottelun tavoitteena on rajata salassa pidettävän tiedon käsittely-ympäristö hallittavaksi kokonaisuudeksi ja erityisesti pystyä rajaamaan tiedon käsittely vain riittävän turvallisiin ympäristöihin.

Turvallisuusluokan IV tietojärjestelmien ja tietoliikennejärjestelyjen erottelu eri turvallisuusluokkien ympäristöistä voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla turvallisuuskriittisten, alemman turvallisuusluokan palvelujen (esimerkiksi web-selailu ja internetin kautta reitittyvä sähköposti) liikenne kulkemaan erillisten, sisältöä suodattavien välityspalvelinten kautta. Turvallisuusluokan IV tietojärjestelmiä ja tietoliikennejärjestelyjä on mahdollista kytkeä internetiin ja muihin ei-luotettuihin verkkoihin edellyttäen, että kytkennän aiheuttamia riskejä pystytään pienentämään riittävästi muiden suojausten avulla turvallisuusluokan IV edellyttämälle tasolle. Tämä vaatii erityisesti ohjelmistopäivityksistä huolehtimista, vähimpien oikeuksien periaatteen mukaisia käyttöoikeuksia, järjestelmäkovennuksia sekä kykyä poikkeamien havainnointiin ja korjaaviin toimiin. Tyypillinen käyttötapa turvallisuusluokan IV käsittely-ympäristölle on organisaation ”toimistoverkon” tietojenkäsittely-ympäristön osa, joka voi muodostua esimerkiksi työasemista ja asianhallintajärjestelmistä sekä niiden suojaamiseen liittyvistä järjestelyistä. Vastaava, palomuureilla ja muilla suodatuksilla toteutettu erottelu soveltuu myös turvallisuusluokittelemattoman, salassa pidettävän tiedon suojaamiseen, kuten myös julkisen tiedon eheyden ja käytettävyyden suojaamiseen.

Turvallisuusluokasta III alkaen erottelu eri turvallisuusluokkien ympäristöihin voidaan tehdä riittävän turvallisilla yhdyskäytäväratkaisuilla. Niissä yleisenä suunnitteluperiaatteena on toteuttaa Bell-LaPadula-mallin säännöt ”No Read Up” ja ”No Write Down”. Yhdyskäytäväratkaisujen tulee toisin sanoen luotettavasti estää ylemmän turvallisuusluokan tiedon kulkeutuminen alemman turvallisuusluokan ympäristöön. Suunnitteluperiaatteita käsitellään yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa.

Turvallisia yhdyskäytäväratkaisuja ovat esimerkiksi vain yksisuuntaisen liikennöinnin mahdollistavat datadiodiratkaisut. Turvallisuusluokan II tietojärjestelmien ja tietoliikennejärjestelyjen erottelu voidaan toteuttaa lähtökohtaisesti vain korkean luotettavuuden tarjoavien datadiodiratkaisujen avulla. Turvallisuusluokan I erottelu tulee lähtökohtaisesti toteuttaa täydellisellä fyysisellä eristämisellä ja vain poikkeustapauksissa datadiodiratkaisujen avulla. Turvallisten yhdyskäytäväratkaisujen käytännön toteutuksia käsitellään yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa.

Tietojärjestelmien ja tietoliikennejärjestelyjen liittämisessä alemman turvallisuusluokan järjestelmiin ja järjestelyihin on otettava huomioon myös kansainväliset tietoturvavelvoitteet, joissa liittäminen voi olla kokonaan kielletty. Valtionhallinnon viranomainen voi pyytää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (22.12.2011/1406) mukaan Kyberturvallisuuskeskukselta järjestelmien tai järjestelyjen vaatimustenmukaisuuden arviointia. Arvioinnin pyytäminen erityisesti turvallisuusluokkien I ja II tietojärjestelmien ja tietoliikennejärjestelyjen liittämisestä alemman turvallisuusluokan järjestelmiin ja järjestelyihin on suositeltavaa, jotta niiden turvallisuudesta vastuussa olevalla viranomaisella on riskienhallintapäätöstensä tueksi käytettävissä myös Kyberturvallisuuskeskuksen asiantuntija-arvio liittämisen mahdollisista jäännösriskeistä.

6.1 Säädökset ja lisätiedot

Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (Kyberturvallisuuskeskus)

Ohje Liikenne- ja viestintävirasto Traficomin suorittamista tietojärjestelmien arviointi- ja hyväksyntäprosesseista (Kyberturvallisuuskeskus)

Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille (Puolustusministeriö): 5. Osa-alue I Tekninen tietoturvallisuus, Vaatimus I 01

7 Salausratkaisut (TLa 11.1 § kohta 7)

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteutettava siten, että:

7) käytetyt salausratkaisut ovat tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän turvallisia.

Tämän suosituksen on tarkoitus tukea myös seuraavien vaatimusten toteuttamista:

a) Tiedonhallintalain 14 § Tietojen siirtäminen tietoverkossa

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

Käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa (306/2019).

b) Turvallisuusluokitusasetuksen 12 § Asiakirjan siirtäminen tietoverkon kautta

Salassa pidettävien tietojen siirtämisestä yleisessä tietoverkossa säädetään tiedonhallintalain 14 §:ssä. Turvallisuusluokiteltuja asiakirjoja saa siirtää muussa kuin yleisessä tietoverkossa viranomaisen turvallisuusalueiden ulkopuolelle tai kyseistä turvallisuusluokkaa alemman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain salatussa muodossa. Jos turvallisuusluokiteltujen asiakirjojen siirtäminen tapahtuu turvallisuusalueella muussa kuin yleisessä tietoverkossa ja tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin, voidaan käyttää salaamatonta siirtoa tai alemman turvallisuustason salausta.

Erityisesti liikennöitäessä julkisen tai matalamman turvallisuusluokan verkon kautta salausratkaisut ovat usein ainoita suojauksia salassa pidettävän tiedon luottamuksellisuuden, ja tyypillisesti myös eheyden suojaamisessa. Koska salausratkaisujen mahdollisia puutteita on usein äärimmäisen haastavaa korvata muilla suojauksilla, salausratkaisun valintaan ja turvalliseen käyttötapaan suositellaan kiinnitettävän erityistä huomiota.

Siirrettäessä salassa pidettävää tietoa fyysisesti suojattujen alueiden ulkopuolella, tai julkisen verkon kautta, aineisto tai liikenne tulee suojata riittävän turvallisella salauksella. Julkiseksi verkoksi tulkitaan esimerkiksi Internet ja operaattorien tarjoamat MPLS-verkot. Käytännön toteutustapoja ovat esimerkiksi käyttäjien päätelaitteiden ja viranomaisen tietojärjestelmien väliset VPN-ratkaisut, organisaatioiden verkkojen välinen (LAN-2-LAN) salaus, sekä loppukäyttäjille tarjottavat turvaposti- ja tiedostosalausratkaisut. Siirrettäessä salassa pidettävää tietoa fyysisesti suojattujen alueiden ja vähintään vastaavalla tasolla suojatun verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella.

Viranomaisen tulee käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salaustuotteen oikeellisesta toiminnasta varmistumisen lisäksi tulee huomioida muun muassa salaustuotteen käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa tilanteesta, jossa salausta käytetään liikennöintiin hallitun, fyysisesti suojatun alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salaustuotteiden arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi kyseisen käyttötapauksen vaatimukset tiedon salassapitoajalle ja eheydelle.

Erilaisiin tietoaineistoihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eri tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa.

Salausratkaisujen valinnassa suositellaan nojautumaan ensisijaisesti kansallisen tietoturvallisuusviranomaisen (Kyberturvallisuuskeskuksen NCSA-toiminto) arvioimiin ja hyväksymiin salausratkaisuihin. Salausratkaisujen hyväksyntään liittyy oleellisesti käyttöpolitiikka ja -asetukset, joiden mukaan toimimalla kyseisen salausratkaisun on arvioitu tuottavan riittävä suoja kyseisen turvallisuusluokan tiedolle.

Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään. Salausratkaisun salausavainten hallinnointiprosessien tuleekin olla suunniteltuja, toteutettuja ja kuvattuja tai ohjeistettuja. Salaisten avainten tulee olla vain valtuutettujen käyttäjien ja prosessien käytössä. Prosessien tulee edellyttää vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, ja f) valtuuttamattomien avaintenvaihtojen estämisen.

Erityisesti salausratkaisujen osalta viranomaisen tulee huomioida myös toimitusketjujen turvallisuus riskienarvioinnissaan. Vaikka salausratkaisu olisi riittävän turvallinen esimerkiksi salausratkaisun valmistajalta lähtiessään, toimitusketjun suojaamispuutteet voivat mahdollistaa salausratkaisun peukaloinnin, ja siten johtaa turvattoman salausratkaisun käyttöönottoon viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn osana.

Vastaanottajan riittävän luotettava varmistaminen riippuu merkittävästi käytetystä salausratkaisusta. Esimerkiksi Kyberturvallisuuskeskuksen turvallisuusluokitellun tiedon suojaamiseen hyväksymien salausratkaisujen käyttöpolitiikoissa otetaan kantaa myös käyttäjien tunnistamiseen silloin, kun kyseistä salausratkaisua käytetään esimerkiksi toisessa organisaatiossa olevalle henkilölle viestintään (esimerkiksi niin sanotut turvapostiratkaisut). Toisaalta useissa salausratkaisuissa vastapuolen tunnistaminen nojaa avaimistonhallinnan luotettavuuteen (esimerkiksi jaettuun salaisuuteen perustuva organisaation toimipisteiden tai kahden eri organisaation verkkojen välinen (LAN-2-LAN) salaus, tai jaettuun salaisuuteen perustuva tiedostosalaus).

Erityisesti turvallisuusluokitellun tiedon välittämisessä tulee myös huomioida, että ilman luotettavaa näyttöä tietojenkäsittely-ympäristöjen (esimerkiksi useamman viranomaisen yhdistävät verkot) suojausten nykytilasta, riittävää salausta tai riittävän luotettavaa vastaanottajan tunnistamista ei välttämättä tarjota kyseisten ympäristöjen sisäänrakennettuna palveluna, vaan se tulee toteuttaa erillisen salausratkaisun tukemana.

Erityisesti turvallisuusluokittelemattoman salassa pidettävän tiedon välittämisessä tulee myös huomioida, että käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa (306/2019).

7.1 Säädökset ja lisätiedot

Vahvuustaulukot: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

Ohje salaustuotteiden arvioinneista ja hyväksynnöistä: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-salaustuotearvioinnit-ja-hyvaksynnat.pdf

Hyväksyttyjä salausratkaisuja: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

Lisätietoa turvallisen salausratkaisun kehittämisen tueksi:

- Turvallinen tuotekehitys - kohti hyväksyntää: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/ Turvallinen_tuotekehitys_Suomi_J003_2018.pdf

Lisätietoa salausratkaisujen käsittelystä arviointikriteeristössä:
Katakri 2015 (erityisesti kohdat I 12, I 01, I 15): http://defmin.fi/katakri

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-292-5 (pdf)

Maaliskuu 2020