VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Lautakunnat

Valtiovarainministeriön julkaisuja – 2020:XX

Valtiovarainministeriön julkaisuja 2020:XX

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Kuvailulehti

Julkaisija	Valtiovarainministeriö		19.3.2020/päivitetty
Tekijät	Tiedonhallintalautakunta		
Julkaisun nimi	Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:XX		
Diaari/hankenumero	-	**Teema**	Lautakunnat
ISBN PDF	978-952-367-292-5/päivitetty	**ISSN PDF**	1797-9714/päivitetty
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-292-5		
Sivumäärä	60	**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. 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.

Tiedonhallintalautakunta hyväksyi suosituksen 11.2.2020, ja tämän toisen, päivitetyn julkaisun X.X.2020.

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

Presentationsblad

Utgivare	Finansministeriet		19.3.2020/päivitetty
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/päivitetty	**ISSN PDF**	1797-9714/päivitetty
URN-adress	http://urn.fi/URN:ISBN:978-952-367-292-5		
Sidantal	60	**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.

Turvallisuusluokitusmerkinnällä kerrotaan tiedon vastaanottajille, miten tietoja tulee käsitellä. 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.

Informationshanteringsnämnden godkände rekommendationen den 11 februari 2020, ja tämän toisen, päivitetyn julkaisun X.X.2020.

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

Description sheet

Published by	Ministry of Finance		19 Month 2020/päivitetty
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/päivitetty	**ISSN (PDF)**	1797-9714/päivitetty
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-292-5		
Pages	60	**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 ja tämän toisen, päivitetyn julkaisun X.X.2020.

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

Sisällys

Kuvat:

Taulukot:

1 Johdanto

Tässä tiedonhallintalautakunnan antamassa suosituksessa opastetaan täyttämään asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetussa valtioneuvoston asetuksessa (1101/2019, jatkossa turvallisuusluokitteluasetus tai TLa) säädettyjä vaatimuksia. Tavoitteena on opastaa menettelytapoja turvallisuusluokittelumerkinnän käyttöön sekä asiakirjojen asianmukaiseen käsittelyyn.

Suositus keskittyy opastamaan, miten viranomainen voi täyttää turvallisuusluokitteluasetuksessa asetetut vaatimukset. Suosituksen soveltamisessa tulee huomioida, että asetuksen vaatimuksia on mahdollisuus toteuttaa usealla tavalla. Viimekädessä viranomaisen riskienhallinnalla on soveltamisessa keskeinen merkitys.

Turvallisuusluokitteluasetusta sovellettaessa tulee huomioida myös muut turvallisuusluokitteluun ja salassapitoon liittyvät keskeiset säädökset. Suomen perustuslaissa (731/1999) 12 §:n ja viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999, jatkossa julkisuuslaki tai JulkL) säädetään muun muassa viranomaisten asiakirjojen julkisuudesta, salassapitoperusteista sekä asiakirjan antamista koskevista velvoitteista.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (EU:n yleinen tietosuoja-asetus) sekä sitä täydentävä tietosuojalaki (1050/2018) sisältävät säännöksiä henkilötietojen käsittelystä ja vaitiolovelvollisuudesta. Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) sisältää säännöksiä muun muassa henkilötietojen käsittelystä rikoksen ennalta estämisestä, paljastamisesta, selvittämisestä tai syyteharkintaan saattamisesta ja yleiseen turvallisuuteen kohdistuvilta uhkilta suojelemisesta tai tällaisten uhkien ehkäisemisestä. Tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista (tietosuoja.fi).

Kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti turvallisuusluokitellun asiakirjan salassapitovelvollisuudesta ja kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004). Kansallinen turvallisuusviranomainen (NSA) on julkaissut erillisen ohjeen turvallisuusluokitellun tiedon käsittelystä. (Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje 2020).

Julkisen hallinnon tiedonhallinnasta annetussa laissa (TihL 906/2019, tiedonhallintalaki) säädetään muun muassa salassa pidettävien asiakirjojen käsittelyvaatimuksista ja

turvallisuusluokitteluvelvollisuudesta. 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.

Turvallisuusluokitteluasetuksessa säädetään turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä. Tässä suosituksessa keskitytään tarkastelemaan turvallisuusluokitteluasetuksen vaatimuksia ja niiden noudattamista tarkemmin.

2 Turvallisuusluokittelun lähtökohdat

Tässä suosituksessa turvallisuusluokiteltavalla asiakirjalla tarkoitetaan tiedonhallintalain 18 §:n 1 momentissa tarkoitettuja asiakirjoja. Turvallisuusluokitteluvelvoite koskee valtion virastoissa ja laitoksissa toimivia virastoja, tuomioistuimia ja valitusasioita käsittelemään perustettuja lautakuntia.[1]

Salassa pidettävän asiakirjan käsittelyä käsitellään tiedonhallintalautakunnan suosituskokoelmassa tiettyjen turvallisuussäännösten soveltamisesta (VM 2020:21).

2.1 Perusteet turvallisuusluokittelulle

Turvallisuusluokiteltu asiakirja on aina salassa pidettävä, mutta salassa pidettävä asiakirja ei aina ole turvallisuusluokiteltu. Turvallisuusluokittelu tehdään, mikäli 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. Tämän lisäksi edellytetään, että 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.[2]

Turvallisuusluokittelu voidaan myös tehdä kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai mikäli asiakirja muutoin liity kansainväliseen yhteistyöhön. Kansainvälisistä

[1] Ks. TihL 18 § 1 mom.
[2] Ks. Turvallisuusluokitteluasetus 3 §:ssä on kuvattu, millaista vahinkoa kulunkin turvallisuusluokan asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa.

tietoturvallisuusvelvoitteista annetussa laissa tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin mainitussa laissa säädetään.

2.2 Turvallisuusluokan arviointi

Asiakirjan turvallisuusluokittelun arviointi perustuu asiakirjan oikeudettoman paljastumisen aiheuttaman vahingon arviointiin. Turvallisuusluokittelun edellyttämää vahinkoa arvioitaessa otetaan huomioon muun muassa:

- mihin laissa mainittuun suojattavaan etuun vahinko kohdistuu;
- mikä on arvioidun vahingon laajuus, suuruus sekä kesto;
- minkälaiset vaikutukset arvioidulla vahingolla voi olla;
- muodostuuko asiakirjojen kasautumisesta riskejä (nk. kasaumavaikutus).

Turvallisuusluokitteluasetuksen 3 §:n 1 momentin kohdissa 1-4 on kuvattu, millaiseen vahinkoon turvallisuusluokka on suhteutettu:

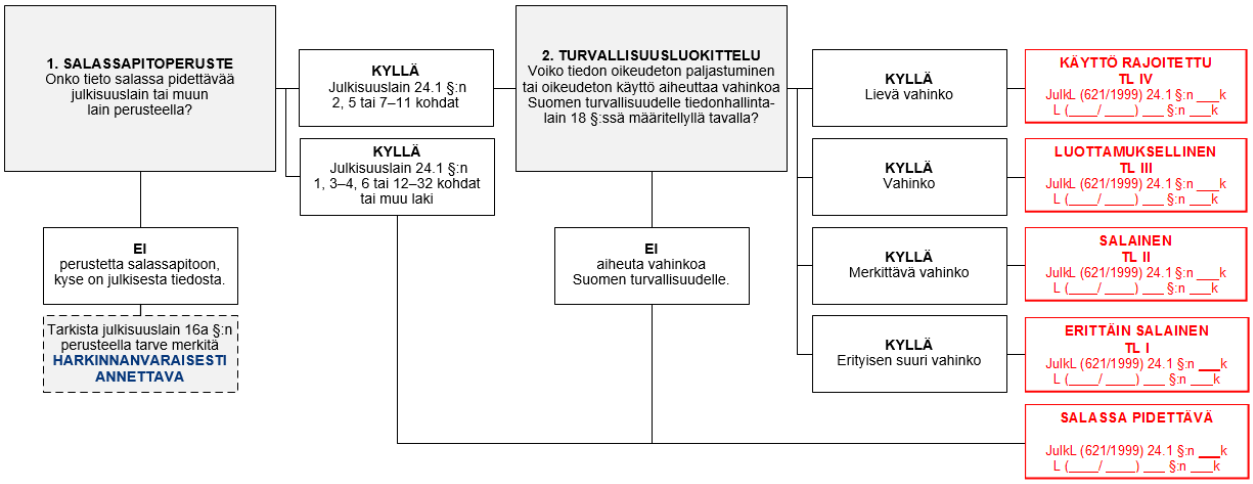
1) turvallisuusluokan I asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle;
2) turvallisuusluokan II asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle;
3) turvallisuusluokan III asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle;
4) turvallisuusluokan IV asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.

Vahinkoedellytyksiä on suositeltavaa arvioida viranomaisessa riskiperusteisesti ennakkoon, jolloin viranomaisessa luokittelu tapahtuu yhdenmukaisella tavalla. Riskiarvioinnissa on otettava huomioon tiedon oikeudettoman paljastumisen tai sen oikeudettoman käytön mahdollisesti aiheuttama vahinko suojattaville eduille. Seuraukset on arvioitava konkreettisesti ottaen huomioon suojattava etu kokonaisuutena.

Yli- ja aliluokittelun välttämiseksi tulee organisaation tuntea omaan toimialaansa liittyvä erityissääntely sekä huolehtia henkilöstön osaamisen vahvistamisesta koskien salassapito- ja

turvallisuusluokittelusääntelyä. Tiedon luokittelee se henkilö, joka antaa asiaan liittyvän toimeksiannon tai luo tiedot ensimmäisen kerran, tai henkilö, joka päättää asiakirjan luokittelusta.

Kuvassa 1 on esitetty arviointiketju salassapidon ja turvallisuusluokan arvioimiseksi. Tiedon luokittelija arvioi tiedon mahdollisen salassapidon sekä sen, mihin säännökseen salassapito perustuu. Jos tieto on salassa pidettävä julkisuuslain 24 §:n 1 momentin 2, 5 tai 7-11 kohdan perusteella ja 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, on kyseessä turvallisuusluokiteltava tieto. Turvallisuusluokiteltavaa tietoa sisältävän asiakirjan osalta on arvioitava potentiaalisen vahingon aste ja tehtävä turvallisuusluokitus vahingon asteen mukaisesti.



Kuva 1: Salassapitoperusteiden arviointiprosessi

Liitteenä (liite 1) olevassa taulukossa on annettu esimerkkejä turvallisuusluokittelun edellyttämän vahingon arvioimiseksi suojattavan edun näkökulmasta. Luokittelu on aina tehtävä tapauskohtaisesti riskiarviointiin perustuen ja otettava huomioon muun muassa tiedon kasautumisvaikutus.

2.3 Turvallisuusluokittelun kansainvälinen vastaavuus

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetut asiakirjat ovat erityissuojattavaa tietoaineistoa, ja ne tulee turvallisuusluokitella siten kuin kansainvälisessä tietoturvallisuusvelvoitteessa määritellään. Laissa tarkoitettu tieto tarkoittaa muiden valtioiden tai kansainvälisten järjestöjen turvallisuusluokiteltua tietoa. Turvallisuusluokitteluasetuksen 4 §:ssä on säädetty Suomen turvallisuusluokituksen vastaavuudesta kansainvälisiä

tietoturvallisuusvelvoitteita toteutettaessa. Säännöstä noudatetaan, ellei kansainvälisestä tietoturvavelvoitteesta muuta johdu. Kansallinen turvallisuusviranomainen (NSA) on julkaissut erillisen ohjeen turvallisuusluokitellun tiedon käsittelystä. (Kansainvälisen turvallisuusluokitellun tiedon käsittelyohje 2020).

Alla olevassa taulukossa on esitetty rinnakkain kansalliset ja EU-turvallisuusluokat sekä niiden lyhenteet. Luokkien käsittelysäännöissä on eroja ja EU-turvallisuusluokkien asiakirjojen käsittelyssä tulee noudattaa EU:n turvallisuusluokiteltujen tietojen suojaamista koskevia turvallisuussääntöjä. [3]

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

[3] Ks. EU-neuvoston turvallisuussäännöt (488/2013)

3 Turvallisuusluokan merkitseminen

3.1 Merkintätavat

Turvallisuusluokkaa kuvaava merkintä kertoo siitä, millaisia tietoturvallisuustoimenpiteitä asiakirjan käsittelyssä tulee noudattaa. Turvallisuusluokitusmerkintää ei saa käyttää, ellei perustetta turvallisuusluokitukselle ole olemassa.

Turvallisuusluokitteluasetuksen 3 §:n 2-5 momentissa säädetään turvallisuusluokkien merkitsemisestä. Turvallisuusluokkia ja niitä kuvaavia merkintöjä on neljä:

- Turvallisuusluokan I asiakirjaan tehdään merkintä ”ERITTÄIN SALAINEN”,
- Turvallisuusluokan II asiakirjaan merkintä ”SALAINEN”
- Turvallisuusluokan III asiakirjaan merkintä ”LUOTTAMUKSELLINEN” ja
- Turvallisuusluokan IV asiakirjaan merkintä ”KÄYTTÖ RAJOITETTU”.

Merkinnän lisäksi voidaan käyttää merkintää ”TL I”, ”TL II”, ”TL III” ja ”TL IV”.

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

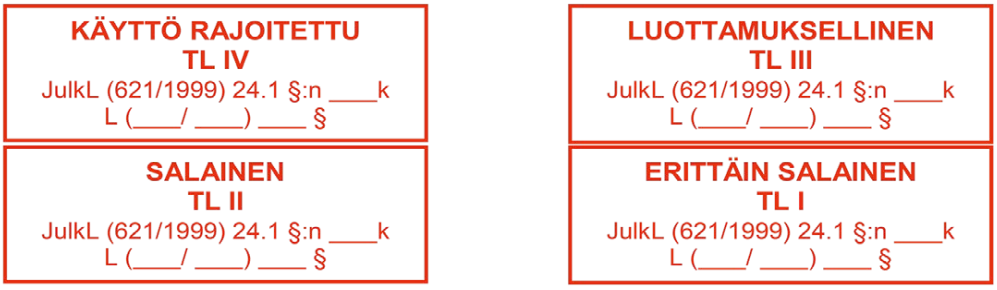
Asiakirjan turvallisuusluokan tulee käydä ilmi myös tiedonhallintalain 25 §:ssä tarkoitetun asiarekisterin ja muun viranomaisen yleisesti tiedonhallintaan käyttämän tietovarannon asiakirjaa koskevista tiedoista. [4] Merkintä voidaan tehdä asiakirjan liitteeseen tai liitettävään erilliseen asiakirjaan, jos merkintöjen tekeminen asiakirjaan tai merkinnän muuttaminen ei ole teknisesti mahdollista tai jos turvallisuusluokkaa vastaavat käsittelyvaatimukset ovat tarpeen vain tietyn lyhyehkön ajan.[5]

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). Jos asiakirjan turvallisuusluokka on kaikissa osuuksissa sama, voidaan nämä kohdat merkitä hakasulkeilla ja asiakirjan alkuun kirjoittaa teksti ”hakasulkeilla merkitty teksti on salassa pidettävää ja turvallisuusluokan X tietoa”.

Tietojen turvallisuusluokitus voidaan kertoa myös suullisesti silloin, kun turvallisuusluokiteltuja tietoja käsitellään esimerkiksi kokouksessa. Kansainvälisesti yleisenä käytäntönä on merkitä turvallisuusluokka, sivunumero ja päiväys selvästi kullekin sivulle. Korkeamman turvallisuusluokan

[4] Ks. turvallisuusluokitteluasetus 3 § 4 mom
[5] Ks. turvallisuusluokitteluasetus 3 § 5 mom

asiakirjojen jokaiselle sivulle merkitään usein myös jäljennöksen numero, jos ne on tarkoitus jakaa useampana kappaleena. Näitä käytäntöjä on suositeltavaa soveltaa myös kansallisissa turvallisuusluokitelluissa asiakirjoissa.



Kuva 2: Turvallisuusluokitusmerkintöjen leimamallit.

3.2 Merkinnän poistaminen ja muuttaminen

Jos asiakirjan turvallisuusluokittelulle ei enää ole perusteita lain mukaan tai turvallisuusluokkaa on tarpeen muuttaa, 3 §:ssä tarkoitetun merkinnän poistamisesta tai muuttamisesta on tehtävä asianmukainen merkintä asiakirjaan, johon alkuperäinen merkintä on tehty sekä asiakirjan 3 §:n 4 momentissa tarkoitettuihin tietoihin. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa. (TLa 5 § 1 mom).

Asiakirjan luokittelua muutettaessa tehdään seuraavat toimenpiteet:

- mikäli asiakirjaa on käsitelty paperimuodossa, yliviivataan turvallisuusluokkaa tai salassapitoa osoittava leima
- leiman alle kirjoitetaan ”salassapito päättynyt”, päivämäärä ja toimivaltaisen virkamiehen allekirjoitus
- tieto asiakirjan julkiseksi tulosta on tehtävä myös asiakirjarekisteriin
- sähköisiin asiakirjoihin merkintä tehdään metatietoja muuttamalla ja esimerkiksi tietopyyntöjen kohteena olevat asiakirjat varustetaan erillisellä saatteella, jossa kerrottaan salassapidon päättymisaika.

Jos asiakirja on saatu toiselta viranomaiselta, turvallisuusluokkaa koskevan merkinnän saa poistaa tai muuttaa ainoastaan asiakirjan laatineen viranomaisen tai sen viranomaisen luvalla, jonka käsiteltäväksi asia kokonaisuudessaan kuuluu, jollei ole selvää, ettei perusteita turvallisuusluokan käytölle enää ole (TLa 5 §). Turvallisuusluokittelua koskevan merkinnän tarve arkistoitujen tai valtionhallinnon viranomaisella säilytettävänä olevien asiakirjojen osalta on arvioitava, jos valtionhallinnon viranomainen ottaa asiakirjan muuhun käsittelyyn (TLa 16 §).

3.3 Aiemmin käytössä olleet luokitukset ja salassapitomerkinnät

Eri viranomaisilla on ollut aiemmin erilaisia merkintä- ja luokittelukäytäntöjä. Vanhat asiakirjat säilyttävät alkuperäisen merkintänsä, kunnes asiakirja on tarpeen ottaa uudelleen käsittelyyn. Tällöin on tapauskohtaisesti uudelleen arvioitava salassapitomerkinnän tarve ajantasaisten säännösten mukaisesti. Käsittelyssä voidaan ohjeellisesti rinnastaa salassapitomerkintöjä alla olevan vertailutaulukon mukaisesti:

Ministeriöiden luokituksia ennen vuotta 2010	**Luokitukset 2010-2019**	**Luokitus 2020 lähtien**
Erittäin salainen	ERITTÄIN SALAINEN, suojaustaso I (ST I)	ERITTÄIN SALAINEN TL I
Salainen	SALAINEN, suojaustaso II (ST II)	SALAINEN TL II
	LUOTTAMUKSELLINEN, suojaustaso III (ST III)	LUOTTAMUKSELLINEN TL III
Luottamuksellinen	KÄYTTÖ RAJOITETTU, Suojaustaso IV (ST IV)	KÄYTTÖ RAJOITETTU TL IV
Salassa pidettävä	SALASSA PIDETTÄVÄ, Suojaustaso III (ST III), Suojaustaso IV (ST IV)	SALASSA PIDETTÄVÄ

Taulukko 2. Aiempien luokitusten vertailu.

4 Asiakirjojen turvallinen käsittely

4.1 Asiakirjan käsittelyn rekisteröinti ja seuraaminen

Tiedonhallintalain 25 §:n mukaan tiedonhallintayksikön on ylläpidettävä viranomaisen käsittelyssä olevista ja olleista asioista asiarekisteriä, johon rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. Viranomaisen on rekisteröitävä viipymättä sille saapunut tai sen laatima asiakirja asiarekisteriin. Asiarekisteriä ylläpidetään asiakirjajulkisuuden toteuttamiseksi tietopyyntöjen yksilöimiseksi, asiakirjojen ja muiden niitä vastaavien tietojen jäsentämiseksi, asiankäsittelyyn liittyvien toimenpiteiden järjestämiseksi, asiankäsittelyaikojen seuraamiseksi sekä prosessien ohjaamiseksi. Sen lisäksi, mitä 26 §:ssä (TiHL) säädetään, asiakirjan rekisteröinnistä on käytävä ilmi asiakirjan saapumisajankohta. Tiedonhallintalautakunnan alaisessa toimintalähtöisen asianhallinnan jaostossa on valmistella suositus, mikä koskee asianhallinnan toteuttamista tiedonhallintayksikössä sekä asiakirjan rekisteröintiä.

Turvallisuusluokitusasetuksen 14 §:ssä määritellään asiakirjojen käsittelyn seuraamiseksi toteutettavista toimenpiteistä, kuten turvallisuustarkoituksia varten tehtävästä rekisteröinnistä. Käsittelyoikeuksia myönnettäessä on otettava huomioon turvallisuusluokitusasetuksen 8 §:ssä olevat määräykset käsittelyoikeuksista ja niiden luetteloinnista.

4.1.1 Asiakirjan rekisteröinti ja seuraaminen TL IV

Turvallisuusluokan IV (TL IV) asiakirja ensisijaisesti laaditaan ja rekisteröidään käytössä olevalla asianhallintajärjestelmällä, jos järjestelmä täyttää TL IV vaatimukset. Asiakirjaan on merkittävä vastaanottajaorganisaatiot tai henkilöt. Turvallisuusluokka IV asiakirja merkitään turvallisuusluokan IV leimalla ja tarvittaessa lisäksi salassa pidettävä leimalla. Salassapidon perusteena oleva lainkohta on merkittävä asiakirjaan ja metatietoihin.

4.1.2 Asiakirjan rekisteröinti ja seuraaminen TL III

Turvallisuusluokan III (TL III) asiakirja ensisijaisesti laaditaan ja rekisteröidään käytössä olevalla asianhallintajärjestelmällä, jos järjestelmä täyttää TL III vaatimukset. Jollei käytössä ole TL III vaatimukset täyttävää asianhallintajärjestelmää, niin rekisteröinti on mahdollista tehdä vaatimukset täyttävään sähköisen erillisrekisteriin tai manuaalisesti. Myös asiakirjan lähettäminen ja vastaanottaminen on rekisteröitävä (TLa 14 §). Sen lisäksi turvallisuusluokka III asiakirjan käsittelyä tulee seurata sähköisessä lokissa, tietojärjestelmässä, asiarekisterissä tai itse asiakirjassa (TLa 14 §). Asiakirjaan on merkittävä vastaanottajaorganisaatiot tai henkilöt.

Turvallisuusluokka III asiakirja merkitään turvallisuusluokan III leimalla ja tarvittaessa lisäksi salassa pidettävä leimalla. Salassapidon perusteena oleva lainkohta on merkittävä asiakirjaan ja metatietoihin.

4.1.3 Asiakirjan rekisteröinti ja seuraaminen TL II

Turvallisuusluokan II (TL II) asiakirja ensisijaisesti laaditaan ja rekisteröidään käytössä olevalla asianhallintajärjestelmällä, jos järjestelmä täyttää TL II vaatimukset. Jollei käytössä ole TL II vaatimukset omaavaa asianhallintajärjestelmää, niin rekisteröinti on mahdollista tehdä vaatimukset täyttävään sähköisen erillisrekisteriin tai manuaalisesti. Myös asiakirjan lähettäminen ja vastaanottaminen on rekisteröitävä (TLa 14 §). Sen lisäksi turvallisuusluokka II asiakirjan käsittelyä tulee seurata sähköisessä lokissa, tietojärjestelmässä, asiarekisterissä tai itse asiakirjassa (TLa 14 §). Asiakirjaan on merkittävä vastaanottajaorganisaatiot tai henkilöt.

Turvallisuusluokan II (TL II) asiakirja merkitään turvallisuusluokan II leimalla ja tarvittaessa lisäksi salassa pidettävä leimalla. Salassapidon perusteena oleva lainkohta on merkittävä asiakirjaan ja

metatietoihin. Rekisteröinnistä on käytävä ilmi, kenelle asiakirja on jaettu. Turvallisuusluokan II käsittelijät on luetteloitava (TLa 14 § 1 mom. 4 kohta). Luettelointiin voidaan käyttää esimerkiksi erillistä kansilehteä, johon merkitään asiakirjan vastaanottaja ja tietoon tutustuneiden nimet. Kun asiakirja palaa kirjaamoon (rekisteröintipisteeseen) niin kansilehteen on kertynyt tieto asiakirjan tietoon tutustuneista. Jos käytössä on turvallisuusluokituksen II vaatimukset täyttävä järjestelmä, mikä mahdollistaa sähköisen käsittelyn seurannan, niin käsittelijöiden seuranta voidaan tehdä lokituksella tai muilla järjestelmän tiedoilla.

4.1.4 Asiakirjojen rekisteröinti ja seuraaminen TL I

Turvallisuusluokan I (TL I) asiakirja laaditaan vaatimukset täyttävällä erillistyöasemalla. Asiakirjan lähettäminen ja vastaanottaminen on rekisteröitävä (TLa 14 §). Turvallisuusluokka I asiakirjan käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai itse asiakirjaan (TLa 14 § 1 mom. 1 kohta). Luettelointiin voidaan käyttää esimerkiksi erillistä kansilehteä, johon merkitään asiakirjan vastaanottaja ja tietoon tutustuneiden nimet.

4.2 Asiakirjan luovuttaminen ja vastaanottaminen

Tietoaineistojen käsittelylle asetettavat vaatimukset koskevat koko tiedon elinkaarta. Tiedon käsittelijä on erityisessä asemassa näiden vaatimusten toteuttamisessa. Hän vastaa kaikissa tietotyön tilanteissa siitä, että henkilökohtainen tiedon käsittely tapahtuu oikein ja työnantajan hänelle osoittamilla/hyväksymillä työvälineillä. Viranomaisen tiedolle on ominaista, että tiedolle on tunnistettava tai määriteltävä toimivaltaa käyttävä viranomainen tai hänen edustajansa. Tällä toimivaltaa käyttävällä viranomaisella on keskeinen vastuu sen toimivaltaan kuuluvasta tiedosta. Viranomaisten velvollisuudesta huolehtia tietojen salassapidosta ja suojaamisesta luovuttaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten säädetään julkisuuslain 26 §:n 3 momentissa. Tieto luovutetaan tiedonsaantiin oikeutetulle. Salassapito- ja vaitiolovelvollisuudesta sekä hyväksikäyttökiellosta säädetään julkisuuslain 22 ja 23 §:ssä.

4.2.1 Asiakirjojen luovuttaminen

Valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle. Vaatimus ei koske asianosaisen tiedonsaantioikeuteen perustuvaa tiedon antamista asiakirjan sisällöstä. (TLa 6 §).

Viranomaisen tulee ylläpitää turvallisia menettelyjä, joiden avulla vain tietoon oikeutetut pääsevät käsittelemään turvallisuusluokiteltavaa tietoa. Viranomaisen tulee todentaa riittävän vahvalla

menettelyllä henkilöt ja/tai palvelua pyytävät tahot tarjotessaan käsittelymahdollisuuden turvallisuusluokiteltuun tietoon.

Tiedon antaminen viranomaisen hallussa olevasta asiakirjasta määräytyy julkisuuslain mukaan. Asiakirjan luokittelumerkintä ei vaikuta viranomaisen velvollisuuteen tapaus- ja asiakirjakohtaisesti arvioida asiakirjan julkisuutta silloin, kun joku pyytää asiakirjasta tiedon julkisuuslain nojalla. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaiset merkinnät eivät jätä salassapidolle harkintamahdollisuutta, toisin kuin julkisuuslain mukaiset merkinnät.

Asiakirjan antamisesta päättää julkisuuslain 14 §:n mukaan se viranomainen, jonka hallussa asiakirja on, jollei laissa toisin säädetä. Jos viranomaiselta pyydetään asiakirjaa, jonka toinen viranomainen on laatinut tai joka kuuluu toisen viranomaisen käsiteltävänä olevaan asiaan, viranomainen voi siirtää tiedonsaantipyynnön sille viranomaiselle, joka on laatinut asiakirjan tai jonka käsiteltävään asiaan se kuuluu (JulkL 15 § 1 mom). Jos viranomaiselta pyydetään asiakirjaa, johon tiedonhallintalain mukaisesti on ollut velvollisuus tehdä asiakirjaa käsiteltäessä noudettavia tietoturvallisuusvaatimuksia koskeva turvallisuusluokkamerkintä ja jonka muu viranomainen on laatinut, viranomaisen on siirrettävä asia asiakirjan laatineen viranomaisen ratkaistavaksi. (JulkL 15 § 3 mom).

Asiakirjan salassapitovelvollisuus on riippuvainen ajankohdasta, josta käsin asiaa tarkastellaan. Salassapito- tai turvallisuusluokittelumerkintä merkintä osoittaa tilanteen silloin, kun tietoaineisto laaditaan. Asiakirjan sisältämän tiedon paljastumisen potentiaaliset seuraukset voivat muuttua ajan kuluessa. Tämän vuoksi tiedonsaantipyyntöä ratkaistaessa on selvitettävä, ovatko perusteet salassapidolle ja mahdolliselle turvallisuusluokitukselle edelleen olemassa.

Turvallisuusluokittelusasetuksen 5 §:n 1 momentin mukaan: jos asiakirjan turvallisuusluokittelulle ei enää ole perusteita lain mukaan tai turvallisuusluokkaa on tarpeen muuttaa, 3 §:ssä tarkoitetun merkinnän poistamisesta tai muuttamisesta on tehtävä asianmukainen merkintä asiakirjaan, johon alkuperäinen merkintä on tehty sekä asiakirjan 3 §:n 4 momentissa tarkoitettuihin tietoihin. Tyypillisesti turvallisuusluokan muutoksesta päättää asiakirjan esittelijä tai ratkaisija. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa.

4.2.2 Vastaanottajan toimenpiteet (muut kuin valtionhallinto)

Turvallisuusluokitteluvelvollisuus on valtion virastoissa ja laitoksissa toimivilla viranomaisilla, tuomioistuimilla ja valitusasioita käsittelemään perustetuilla lautakunnilla (TihL 18 §). Turvallisuusluokiteltuja aineistoja vastaanottavat myös tahot, joita turvallisuusluokittelu ei koske.

Näitä ovat muun muassa kunnat, kuntayhtymät ja pelastuslaitokset sekä yksityiset tahot toimeksiantoa suorittaessaan. Vastaanottajan on käsiteltävä asiakirjaa sovitusti (turvallisuussopimus tai vastaava) sekä luovuttavan viranomaisen ohjeistuksen mukaisesti. Vastaanottajan on varmistettava, ettei turvallisuusluokiteltu asiakirja päädy sivullisille. Vastaanottavan tahon on suositeltavaa täydentää omia käsittelyohjeitaan saamillaan turvallisuusluokiteltavien asiakirjojen ohjeilla sekä järjestää niihin liittyvää koulutusta.

Tiedonhallintalain 25 §:n mukaisesti tiedonhallintayksikön on rekisteröitävä viipymättä sille saapunut tai sen laatima asiakirja asiakirjarekisteriin. Turvallisuusluokiteltu asiakirja on aina myös salassa pidettävä, joten salassapitoa, vaitiolovelvollisuutta ja hyväksikäyttökieltoa koskevat julkisuuslain säännökset (22 ja 23 §) säännökset koskevat automaattisesti turvallisuusluokiteltua aineistoa. Asiakirjan vastaanottaja, esimerkiksi kirjaamo tarkistaa kenellä virkamiehellä on virkatehtäviensä puolesta tarve käsitellä asiakirjaa. Lähettäessään asiakirjaa kyseiselle virkamiehelle on huomioitava asiakirjan kuljetukseen liittyvät menettelytavat kappaleesta 4.4.

4.3 Asiakirjan siirtäminen tietoverkon kautta

Turvallisuusluokiteltuja asiakirjoja saa siirtää viranomaisen turvallisuusalueiden ulkopuolelle tai kyseistä turvallisuusluokkaa alemman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain riittävän luotettavasti 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. (TLa 12 §). Jotta kyseessä olevaa kohtaa salaamattomuudesta tai alemman tason salauksesta voidaan soveltaa, tulee fyysisen pääsynhallinnan estää valtuuttamattomilta pääsy kyseessä olevaan tietoon. Siirtämisessä on huomioitava seuraavia näkökohtia.

1) Siirrettäessä turvallisuusluokiteltua tietoa fyysisesti suojattujen alueiden ulkopuolella, esimerkiksi julkisen verkon kautta, aineisto/liikenne suojataan riittävän turvallisella salauksella.
    - julkiseksi verkoksi tulkitaan esimerkiksi Internet ja operaattorien tarjoamat MPLS-verkot.
    - käytännön toteutustapoina esimerkiksi käyttäjien päätelaitteiden ja viranomaisen tietojärjestelmien väliset VPN-ratkaisut, organisaatioiden verkkojen välinen IPSec-salaus, sekä loppukäyttäjille tarjottavat turvaposti- ja tiedostosalausratkaisut.

2) Siirrettäessä turvallisuusluokiteltua tietoa fyysisesti suojattujen alueiden ja vähintään vastaavalla tasolla suojatun verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella.
3) Salauskäytäntöjen ja salausavainten hallinnan prosessit on suunniteltu ja toteutettu. Käytännöt ja prosessit on kuvattu, ohjeistettu ja koulutettu käyttäjille.
4) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Prosessit edellyttävät vähintään
    - kryptografisesti riittävän vahvoja avaimia,
    - turvallista avaintenjakelua,
    - turvallista avainten säilytystä,
    - säännöllisiä avaintenvaihtoja,
    - vanhojen tai paljastuneiden avainten vaihdon ja
    - valtuuttamattomien avaintenvaihtojen estämisen.
5) Viranomaisen turvallisuusluokitellun tiedon suojaamisessa valinnassa suositellaan nojautumaan ensisijaisesti Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen NCSA-toiminnon arvioimiin ja hyväksymiin salausratkaisuihin.
    - on huomioitava salausratkaisujen konfigurointi ja käyttö turvallisiksi arvioitujen asetusten mukaisesti

4.4 Asiakirjan kuljettaminen

Kuljetukseen liittyvät riskit on arvioitava sekä tarvittavat tietoturvallisuustoimenpiteet on suunniteltava ja toteutettava riskilähtöisesti tunnistettujen riskien perusteella. Turvaluokitteluasetuksen 13 §:n mukaan turvallisuusluokiteltuja asiakirjoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet riittävällä salauksella. Viranomainen voi arvioida kyseiselle turvallisuusluokalle riittävän salausratkaisun. Mikäli tiedon tallennusväline on riittävästi salattu, se voidaan lähettää esimerkiksi postitse vastaanottajalle. Turvallisuusluokiteltujen asiakirjojen kuljettaminen viranomaisen fyysisesti suojattujen turvallisuusalueiden ulkopuolella on toteutettava turvallisesti. Salausratkaisujen turvallisuutta on käsitelty tarkemmin luvussa 7.11.

4.4.1 Salaamattomien turvallisuusluokan IV asiakirjojen kuljettaminen

Turvallisuusluokan IV asiakirjan kuljettamisessa on huomioitava turvallisuusluokitteluasetuksen 13 §:n asettamat vaatimukset sähköisten tietovälineiden riittävästä salauksesta. Salaamattoman asiakirjan kuljettamista koskevat vaatimukset eivät koske turvallisuusluokan IV asiakirjoja, joten

niitä sisältäviä tiedon tallennusvälineitä sekä paperisia asiakirjoja on mahdollista kuljettaa myös salaamattomina ja antaa esimerkiksi postin kuljetettavaksi. Lähetyksestä ei kuitenkaan ulkoisesti saa käydä ilmi, että se sisältää salassa pidettävää tietoa.

4.4.2 Salaamattomien turvallisuusluokan III – I asiakirjojen kuljettaminen

Turvallisuusluokan III-I salaamaton asiakirja (paperinen tai sähköinen eli muistitikku, CD- tai DVD-levy yms.) pakataan kuljettamista varten asianmukaisesti sekä kuljetetaan jatkuvan valvonnan alaisuudessa vastaanottajalle. Asiakirja toimitetaan vastaanottajalle henkilökuriirin tai kuriiripalvelun toimesta tai vastaanottaja hakee asiakirjan. Käytetyn menettelyn sekä siihen liittyvien toimijoiden tulee olla viranomaisen hyväksymiä kyseisen turvallisuusluokan asiakirjojen toimittamiseen viranomaisen riskiperustaisen arvion pohjalta.

Turvallisuusluokkien III-I salaamattomien asiakirjojen kuljetukseen lähettäminen voidaan toteuttaa organisaation sisällä keskitetyn toiminnon kautta, joka on tyypillisesti viranomaisen kirjaamo. Kyseisellä toiminnolla tulee olla tarvittavat toimintatavat, ohjeistus ja välineet, joiden avulla turvallinen kuljettaminen voidaan toteuttaa. Sisäiseen toimintoon ja käsittelyketjuun tulee kuulua vain hyväksyttyä henkilöstöä.

Turvallisuusluokkien III-I asiakirjojen kuljettamiseksi organisaatiolla on oltava turvakuoria, salakuoria tai turvapusseja. Nämä suljetaan aina tavallisen kirjekuoren sisälle. Pakkaamisessa tulee huomioida muun muassa se, että pakkaus ei ulkoisesti paljasta sen sisältävän turvallisuusluokiteltua tietoa. Pakkauksen uloimmassa kuoressa on vastaanottavan viranomaisen osoite (tyypillisesti kirjaamo) ja myös palautusosoite, jos vastaanottajaa ei tavoiteta. Vasta pakkauksen ulkokuoren sisällä ilmaistaan pakkauksen sisällön sisältävän turvallisuusluokiteltua tietoa. Kuoren tai pakkauksen on oltava läpinäkymätön.

Sisäisessä jakelussa asiakirja voidaan toimittaa sinettipussissa. Lähetyksen ajankohta ja vastaanottaja on kirjattava lähettäjäorganisaatiossa ja lähettäjän on seurattava lähetyksen perillemenoa. Vastaanottaja tarkistaa kuoren sinetöinnin eheyden ja ilmoittaa välittömästi, jos eheyden vaarantumista on syytä epäillä. Asiakirjan vastaanottaminen vahvistetaan lähettäjälle palauttamalla lähetyskuoressa oleva lähetyksen seurantalomake, tai muulla lähetyksen seurantamenetelmällä.

Turvallisuusluokkien III-I -tietoa sisältävä lähetys osoitetaan ensisijaisesti viranomaisen kirjaamolle, tai muulle lähetyksen ja asiakirjojen rekisteröinnistä vastaavalle taholle. Jos kirjaamo ei tavoita nimettyä vastaanottajaa, voidaan kuori jättää vastaanottavaan organisaatioon asianmukaiseen,

kyseisen turvallisuusluokan edellyttämään säilytyspaikkaan odottamaan kuoren avaamiseen oikeutettua henkilöä. Jos tämä ei ole mahdollista, niin kuori tulee palauttaa lähettäjälle.

4.5 Asiakirjan kopioiminen

Turvallisuusluokitelluista asiakirjoista voidaan ottaa sekä sähköisiä että paperimuotoisia kopioita huomioiden kopiointiin liittyvät rajoitukset ja kopioita koskevat käsittelysäännöt sekä muut turvallisuusluokitellun asiakirjan käsittelyä koskevat vaatimukset (esimerkiksi tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset). Turvallisuusluokan II-I asiakirjaa ei saa kopioida ilman sen laatineen viranomaisen antamaa lupaa (TLa 14 §). Annettu lupa tulee dokumentoida kirjallisesti ja sen tulee sisältää maininta kopiointia koskevasta luvasta sekä mahdollisesta asiakirjan jakelun laajentamisesta. Lupa tulee liittää asiakirjan yhteyteen arkistoon, johon kertyy myös tieto asiakirjan tietoon tutustuneista. Kun turvallisuusluokan II-I asiakirjoja kopioidaan, kopiot ja niiden käsittelijät on luetteloitava (TLa 14 §). Jokainen otettu kopio tulee numeroida ja luetteloida.

Turvallisuusluokkien II-I asiakirjojen kopiointi tulee toteuttaa organisaation sisällä keskitetysti tätä koskevan erillisen ohjeistuksen mukaisesti. Paperiasiakirjojen kopiointiin käytettyjen laitteiden tulee olla hyväksyttyjä viranomaisen toimesta kyseisten turvallisuusluokkien asiakirjojen kopioimiseen.

4.6 Tietojen säilyttäminen

4.6.1 Tietojen säilyttäminen turvallisuusluokka IV (TL IV)

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.

4.6.2 Tietojen säilyttäminen turvallisuusluokat III, II ja I (TL III, TL II, TL I)

Turvallisuusluokkaan LUOTTAMUKSELLINEN, SALAINEN tai ERITTÄIN SALAINEN kuuluvat tiedot on säilytettävä turva-alueella soveltuvaksi arvioidussa säilytysratkaisussa, kuten kassakaapissa tai holvissa. Sähköistä käsittelyä turvallisuusalueen ulkopuolella on käsitelty luvussa 7.1.

4.7 Asiakirjan tuhoaminen

Turvallisuusluokitteluasetuksen 15 §:n mukaan tarpeettomaksi käynyt turvallisuusluokiteltu asiakirja on tuhottava tavalla, jolla kyseiselle turvallisuusluokalle riittävän luotettavasti estetään tietojen palauttaminen sekä kokoaminen uudelleen kokonaan tai osittain. Asiakirjan vastaanottajan

on myös huolehdittava asiakirjan asianmukaisesta tuhoamisesta. Jos asiakirjan on laatinut toinen viranomainen, tarpeettomaksi käyneen turvallisuusluokan I ja II asiakirjan tuhoamisesta on ilmoitettava asiakirjan laatineelle viranomaiselle, jollei sitä palauteta asiakirjan laatineelle viranomaiselle (TLa 15 §). Lähettävä ja vastaanottava viranomainen voivat sopia keskenään ilmoitukseen liittyvistä käytännön menettelytavoista, esimerkiksi että turvallisuusluokka II koskevat ilmoitukset tehdään puolivuosittain. Turvallisuusluokan I ja II asiakirjan tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Asiakirjan valmisteluvaiheen versiot voi tuhota ne laatinut henkilö.

Tekniikan kehitysaskeleet vaikuttavat myös turvallisuusluokiteltujen tietojen luotettavaan tuhoamiseen. Esimerkiksi käytettävissä oleva laskentakapasiteetti mahdollistaa silputun, paperisessa muodossa olleen tiedon koneellisen kokoamisen aikaisempaa tehokkaammin. Toisaalta sähköisessä muodossa olleen tiedon tallennemedioiden (kiintolevyt, USB-muistit ja vastaavat) luotettava tuhoaminen on entistä useammin perusteltua toteuttaa esimerkiksi sulattamalla, perinteisen silppuamisen sijaan.

Tiedon suojaamisesta tulee huolehtia tiedon elinkaaren päättymiseen asti. Tämä tulee huomioida erityisesti tilanteissa, joissa käytetään kolmannen osapuolen palvelua tiedon tuhoamiseen, esimerkiksi kiintolevyjen sulattamiseen. Käytännön toteutusmallina on yleensä menettely, jossa tiedosta vastuussa oleva organisaatio valvoo tiedon tuhoamisprosessin aina elinkaaren päättymiseen saakka.

Myös henkilöstön rooli on syytä huomioida tuhoamisprosesseissa. Organisaation tulee järjestää henkilöstölle yksiselitteinen tapa turvallisuusluokiteltujen tietojen tuhoamiseen. Tämä voi käytännössä tarkoittaa esimerkiksi asianmukaisia paperisilppureita ja henkilöstön turvallisuustietoisuuden varmistumista.

4.7.1 Tuhoaminen silppuamalla turvallisuusluokka IV (TL IV)

Turvallisuusluokan IV tietojen silppuaminen voidaan toteuttaa esimerkiksi siten, että

- paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4),
- magneettisten kiintolevyjen silppukoko on enintään 320 mm2 (DIN 66399 / H-5),
- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5) ja
- optisten medioiden silppukoko on enintään 10 mm2 (DIN 66399 / O-5).

4.7.2 Tuhoaminen silppuamalla turvallisuusluokka III (TL III)

Turvallisuusluokan III tietojen silppuaminen voidaan toteuttaa esimerkiksi siten, että

- paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4),
- magneettisten kiintolevyjen silppukoko on enintään 10 mm2 (DIN 66399 / H-6),
- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5) ja
- optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6).

4.7.3 Tuhoaminen silppuamalla turvallisuusluokka II (TL II)

Turvallisuusluokan II aineistojen silppuaminen voidaan toteuttaa esimerkiksi siten, että

- paperiaineistojen silppukoko on enintään 10 mm2 (DIN 66399 / P6),
- magneettisten kiintolevyjen silppukoko on enintään 10 mm2 (DIN 66399 / H-6),
- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 1 mm2 (DIN 66399 / E-6) ja
- optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6).

4.7.4. Tuhoaminen silppuamalla turvallisuusluokka II (TL I)

Turvallisuusluokan I (TL I) tiedon tuhoamisessa voidaan hyödyntää turvallisuusluokan II silppukokoja, mikäli suojausta täydennetään viranomaisen hyväksymillä menettelyillä. Tällaisia menettelyihin sisältyvät tyypillisesti muun muassa silpun jatkokäsittely valvotusti polttamalla tai/ja sulattamalla.

Käytettäessä edellä mainittuja silppukokoja, voidaan silppuamisesta syntyvä jäte hävittää normaalin toimistojätteen mukaisesti. Esimerkiksi DIN 66399/O-6:n mukaista optisista medioista syntynyttä silppua ei siten turvallisuusluokan III tiedoille edellytetä tuhottavan esimerkiksi valvotun sulatusprosessin mukaisesti.

4.7.4 Tuhoaminen eri menetelmiä yhdistäen

Tuhoamiseen voidaan käyttää silppuamisen korvaavana tai sitä tukevana suojauksena myös muita menetelmiä, joilla tietojen kokoaminen estetään luotettavasti (esimerkiksi silputun kiintolevyn sulattaminen). Myös salauksella pystytään pienentämään huomattavasti turvallisuusluokiteltuihin tietoon kohdistuvia riskejä tiedon ja laitteistojen elinkaarten eri vaiheissa. Sähköisten tietojen tuhoamista on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ylikirjoitusohjeessa (Viestintävirasto 2016).

4.7.5 Sähköisen tiedon tuhoaminen

Erityisesti sähköisten aineistojen luotettavan tuhoamisen menettelyiden tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu turvallisuusluokiteltua tietoa. Menettelyiden tulee olla palvelutuottajien kanssa yhteisesti sovittuja ja on varmistettu, että henkilöstö osaa toimia niiden mukaisesti. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän turvallisuusluokitellun tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti käytöstä

poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys (esimerkiksi toimivaltaisen viranomaisen hyväksymä ylikirjoitusmenettely) ei ole mahdollista, turvallisuusluokiteltua tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että turvallisuusluokiteltua tieto ei päädy sivullisille huoltotoimenpiteen yhteydessä.

5 Asiakirjojen ja tietojenkäsittelyn monitasoisen suojaamisen lähtökohdat

5.1 Tiedonhallinnan ja turvallisuuden suunnittelu

Tiedonhallinta perustuu viranomaisen toiminnan tarpeisiin. Tiedonhallintalaki luo puitteet viranomaisten tietoaineistojen yhdenmukaiseen ja laadukkaaseen hallintaan. Tiedonhallinnan suunnittelussa huomioidaan erilaisissa muodoissa olevat tietoaineistot, eri käsittelyvaiheet, tietoaineistoihin sisältyvien tietojen hallinnointi sekä tiedonhallintayksikössä tapahtuvat muutokset. Tiedonhallintalain 5 §:ssä säädetään tiedonhallintamallista ja muutosvaikutusten arvioinnista. Kun tiedonhallintayksikössä tapahtuu tai suunnitellaan olennaisia hallinnollisia uudistuksia ja otetaan käyttöön tietojärjestelmiä, on tiedonhallintayksikön arvioitava näiden muutosten merkitys myös tietoturvallisuusvaatimuksiin ja -toimenpiteisiin. Muuttuneet vaatimukset on huomioitava tiedonhallintamallissa. Tiedonhallintalautakunnan suosituksissa ”Suositus tiedonhallintamallista” (VM 2020:29) annetaan suositus tiedonhallintamallin laatimiselle ja suosituksessa ”Suositus tiedonhallinnan muutostenvaikutusten arvioinnista” (VM 2020: 53) annetaan suositus muutosvaikutusten arvioinnin tekemisestä.

Tiedonhallinnan järjestämisessä olennaista on suunnitella keskeiset toimet ja tietoturvallisuustoimenpiteet. Suunnittelun tulisi perustua riskienhallintaan ja viranomaisen toiminnalle asetettuihin vaatimuksiin. Tietoturvallisuus perustuu erilaisten toimenpiteiden yhdistelmään. Turvallisuusluokitteluasetuksessa (TLa 7 §) säädetään monitasoisesta suojauksesta. Monitasoisella suojauksella varmistetaan, että yhden suojauksen pettäessä, muut turvatoimenpiteet ennaltaehkäisevät, estävät ja rajaavat vahinkoja. Tämän lisäksi suunnitellaan toimia suojausta vaarantavien tekojen ja tapahtumien havaitsemiseksi sekä jäljittämiseksi.

Turvatoimien tehtävänä on myös palauttaa toiminta vaarantumista edeltäneeseen turvatasoon mahdollisimman nopeasti.[6]

5.2 Riskien arviointi

Turvallisuusluokiteltujen tietojen suojaaminen perustuu riskienhallintaan. Turvatoimet suunnitellaan riskien arvioinnin perusteella. Erilaiset arvioinnit ja auditoinnit tukevat riskienhallintaa. Turvatoimia suunniteltaessa huomioidaan erityisesti:

- viranomaisen toiminta/toimiala
- turvallisuusluokiteltujen tietojen turvallisuusluokka, merkitys ja käyttötarkoitus
- henkilöstöturvallisuus, esimerkiksi riski virkamiesten maalittamisesta
- tietojen määrä ja kokoaminen yhteen[7]
- turvallisuusluokiteltujen tietojen käsittelytapa
- turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan ympäristö (rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa)
- tietoihin kohdistuvat uhkatekijät kuten tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu riski tiedoille sekä
- tietoturvallisuustoimenpiteistä aiheutuvat kustannukset

5.3 Tiedon kasautumisen huomioiminen

Kasautumisvaikutuksessa on kyse ilmiöstä, jossa suuri määrä tietoa voi muodostaa yksittäisiä tietoja merkittävämmän asiakokonaisuuden. Tällöin luokittelu ja suojaamistarpeet voivat erota yksittäisten tietoalkioiden luokittelusta ja suojaamistarpeista. Esimerkiksi suuresta määrästä tietyn turvallisuusluokan tietoa koostuvissa tietojärjestelmissä asiakokonaisuus voi nousta luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan. Esimerkiksi suuri määrä turvallisuusluokan IV tietoa voi yhdistettynä muodostaa turvallisuusluokan III tietovarannon. Määrä ei ole ainoa tekijä, vaan joskus esimerkiksi kahden eri tietolähteen yhdistäminen voi johtaa tietovarannon merkityksen kasvamiseen.

Kasautumisvaikutuksen arviointiin ei tunneta yleistä, kaikkiin tilanteisiin sellaisenaan sopivaa laskentatapaa. Kasautumisvaikutuksen arvioinnissa tulee huomioida tiedonhallintalain vaatimukset turvallisuusluokittelun tekemisestä. Suurikaan määrä turvallisuusluokittelematonta salassa pidettävää tietoa ei aina johda kasautumisvaikutukseen ja turvallisuusluokittelun perusteiden täyttymiseen, vaan usein vain turvallisuusluokittelemattomaan salassa pidettävään

[6] Ks. turvallisuusluokitteluasetus 7 §.
[7] Ks. luku 5.3 Tiedon kasautumisen huomioiminen.

tietokasaumaan. Vastaavasti suurikaan määrä turvallisuusluokiteltua tietoa ei aina johda kasautumisvaikutukseen. Kasautumisvaikutuksen tapauskohtainen arviointi edellyttää aina kyseessä olevan tietovarannon nykyisen ja arvioidun tulevan asiasisällön selvittelyä, ja arviota siitä, onko kasauma turvallisuusluokiteltava korkeammalle.

Kasautumista turvallisuusluokitellun IV tai jopa III-luokkaan voi joissain tilanteissa tapahtua myös turvallisuusluokittelemattomista salassa pidettävistä tietoalkioista. Esimerkiksi huoltovarmuudelle keskeisistä yrityksistä tai Suomen kriittistä infrastruktuuria ylläpitävistä yrityksistä kerätyt tiedot saattaisivat olla yksittäisinä tietoalkioina liikesalaisuuksiksi tulkittavia ja siten turvallisuusluokittelemattomaksi salassa pidettäväksi tiedoksi luokiteltavia. Jokin tietoalkioiden joukko voisi kuitenkin muodostaa yhdistettynä tietokasauman, jonka joutuminen ulkopuolisten käsiin voisi aiheuttaa vahinkoa esimerkiksi maanpuolustukselle, huoltovarmuudelle tai/ja poikkeusoloihin varautumiselle. Tällaisen tietokasauman asiasisältö saattaisi olla myös valtion turvallisuuden (yleisen edun) näkökulmasta suojattavaa, ja turvallisuusluokittelun perusteet täyttävää.

Kun tietojärjestelmän tai muun keskeisen tietovarannon turvallisuusluokka tulkitaan kasautumisvaikutuksen takia yksittäisten tietoalkioiden tasoa korkeammaksi, tulisi tietovarannon määritellyt suojausmenetelmät toteuttaa korkeamman turvallisuusluokan vaatimusten mukaisesti. Määritellyillä suojausmenetelmillä tarkoitetaan menetelmiä, joilla rajataan pääsy vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, ja joilla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä havaitaan.

6 Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla

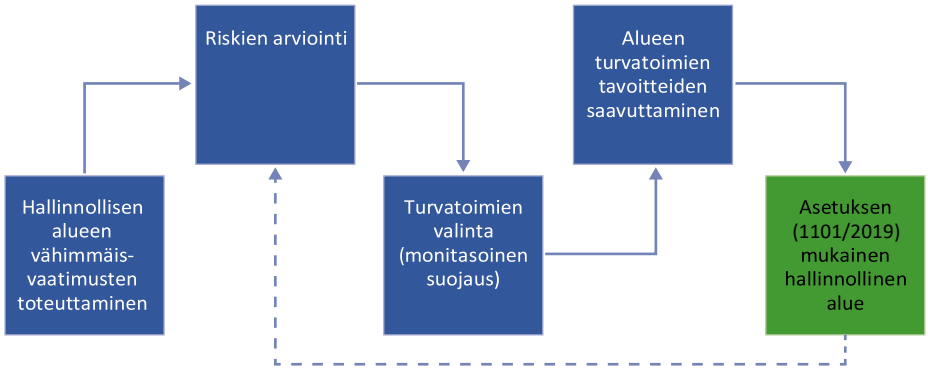
Turvallisuusluokitusasetuksen 9 §:n mukaisesti tiedonhallintayksikön on määritettävä fyysisesti suojatut turvallisuusalueet turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi. Turvallisuusalueita ovat fyysisesti suojatut hallinnolliset alueet ja turva-alueet.

6.1 Suojaaminen hallinnollisilla alueilla

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 lisäksi viranomaisen riskien arvioinnin tulos vaikuttaa siihen, mitkä fyysiset turvatoimet tulee valita. Riskien arviointia on käsitelty kappaleessa 5.2. Alueen yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuus on arvioitava uudelleen säännöllisin väliajoin. Tavoitetilan saavuttamisen prosessi ja säännöllinen arviointi on havainnollistettu seuraavassa kuviossa.



Kuva 3. Tavoitetilan prosessi ja säännöllinen arviointi

6.1.1 Fyysisten turvatoimien tavoite ja keinot

Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin:

a) varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti;
b) mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on, ja tarvittaessa henkilöiden turvallisuusselvitysten perusteella;
c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet ja
d) estämällä salaa tai väkisin tapahtuva tunkeutuminen tai viivyttämällä sitä.

6.1.3 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.

6.1.4 Hallinnollisen alueen fyysisten turvatoimien vähimmäisvaatimukset

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

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 turvallisuusjärjestelmät	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 (kts. kpl 7.6).
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	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai

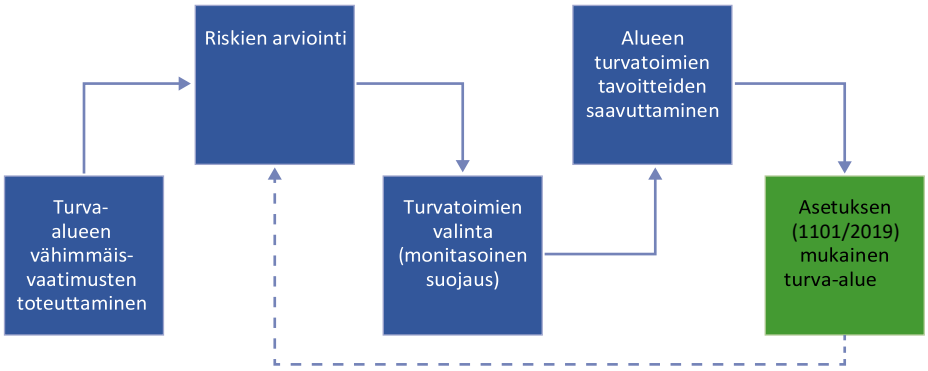
	toimenpiteet.	tietokoneen näytön suojia.
Tila- ja laitetarkastukset (ainoastaan TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella hallinnollisella alueella, jossa käsitellään SALAINEN (TL II) turvallisuusluokan tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Myös alue on tarvittaessa tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn jälkeen.	Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti (esim. matkapuhelimet, älykellot, jne.), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun.
Tiedon säilyttäminen	Alueella voi säilyttää KÄYTTÖ RAJOITETTU (TL IV) -turvallisuusluokan tietoa. Tiedot tulee säilyttää soveltuvissa lukituissa toimistokalusteissa. Jos turvallisuusluokan III tai IV sähköisiä asiakirjoja säilytetään päätelaitteessa turva-alueiden ulkopuolella, ne on suojattava turvallisuusluokalle riittävän turvallisella salausratkaisulla. Päätelaitteen tietoturvallisuudesta on huolehdittava	

Taulukko 3. Hallinnollisen alueen fyysisten turvatoimien vähimmäisvaatimukset

6.2 Turva-alueet

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 ja esimerkiksi yritysten turva-alueiden vaatimukset täyttävät tilat, jos niissä turvallisuusluokitteluasetuksen 10 §:ssä säädetyllä tavalla käsitellään tai säilytetään turvallisuusluokiteltuja asiakirjoja. Turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten, mikäli turva-alueen vähimmäisvaatimukset saadaan kyseiseen tilaan toteutettua.

Tässä suosituksessa esitettyjen turva-alueen vähimmäisvaatimusten lisäksi viranomaisen riskien arvioinnin tulos vaikuttaa siihen, mitkä fyysiset turvatoimet tulee valita. Riskien arviointia on käsitelty kappaleessa 5.2. Alueen yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuus on arvioitava uudelleen säännöllisin väliajoin. Tavoitetilan saavuttamisen prosessi ja säännöllinen arviointi on havainnollistettu seuraavassa kuviossa.



Kuva 4. Tavoitetilan prosessi ja säännöllinen arviointi

6.2.1 Fyysisten turvatoimien tavoite ja keinot

Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin:

a) varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti;
b) mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on, ja tarvittaessa henkilöiden turvallisuusselvitysten perusteella;
c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet; ja
d) estämällä salaa tai väkisin tapahtuva tunkeutuminen tai viivyttämällä sitä.

6.2.2 Fyysisten turvatoimien valinta

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

- rakenteelliset esteet: fyysinen este, jolla suojattava alue tai tila rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan;

- kulunvalvonta: kulunvalvonnalla rajataan pääsyä alueelle tai tilaan. Tavoitteena havaita luvattomat pääsy-yritykset, estää asiattomien pääsy ja valvoa alueella liikkuvia. kulunvalvontaa voidaan kohdistaa alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonta voidaan toteuttaa mekaanisia, sähköisiä tai sähkömekaanisia teknisiä järjestelmiä hyödyntämällä, vartiointihenkilöstön ja/tai vastaanottovirkailijan toimesta tai muunlaisin fyysisin keinoin;

- tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä) luvattoman tunkeutumisen havaitsemiseksi. valvontaa voidaan käyttää myös tiloissa, huoneissa ja rakennuksissa vartiointihenkilöstön sijasta tai sen tueksi;

- vartiointihenkilöstö: koulutettua, valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää turvallisuusvalvontatehtävissä muun muassa kulunvalvonnan tukena sekä alueelle tai tilaan tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemiseksi ja toimien estämiseksi (vaste);

- kameravalvonta: kameravalvontaa voidaan käyttää alueella tai tilassa ilmenevien poikkeamien ennalta estämisessä, hälytysten todentamiseksi 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, henkilöiden ohjeistus, perehdyttäminen sekä järjestelmien huolto- ja ylläpitotoimet;

- valaistus: mahdollisia tunkeutujia voidaan estää käyttämällä valaistusta, jonka ansiosta vartiointihenkilöstö voi valvoa aluetta tehokkaasti joko suoraan tai kameravalvontajärjestelmää hyödyntämällä; ja

- muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on luvattoman pääsyn estäminen ja havaitseminen tai turvallisuusluokiteltujen tietojen katoamisen tai vahingoittumisen ehkäiseminen.

6.2.3 Turva-alueen fyysisten turvatoimien vähimmäisvaatimukset

Viranomaisen määrittelemän tai hyväksymän turva-alueen tulee täyttää taulukossa esitettävät vähimmäisvaatimukset. Niiden lisäksi viranomaisen tulee suunnitella, vastuuttaa ja toteuttaa riskienarviointiin ja monitasoiseen turvallisuuteen perustuvat muut riskienhallintatoimenpiteet sekä myös ylläpitää niitä siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit on mahdollista hyväksyä ja saavuttaa turvatoimien tavoitteet.

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. Mikäli turva-alueelle pääsy tarkoittaa välitöntä pääsyä siellä käsiteltäviin turvallisuusluokiteltaviin asiakirjoihin tai niihin sisältyviin tietoihin, niin alueelle ilman saattajaa pääsevillä henkilöillä tulee olla myös 8 §:n 1 momentissa tarkoitettu tiedonsaantitarve näihin tietoihin. Jos tiedonsaantitarvetta ei ole, niin tulee toteuttaa tietoturvallisuustoimenpiteitä sen varmistamiseksi, ettei turvallisuusluokiteltaviin tietoihin ole pääsyä.	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 (kts. kpl 7.6).
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 luotettavasti (esim. matkapuhelimet, älykellot, jne.), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun.
Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Tiedon säilyttäminen	Alueella voi säilyttää kaikkiin turvallisuusluokkiin kuuluvia tietoja riskien arviointiin ja fyysisten turvatoimien valintaan perusten. LUOTTAMUKSELLINEN (TL III) - ja sitä korkeamman (TL II, TL I) 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 (TL I), 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 4. Turva-alueen fyysisten turvatoimien vähimmäisvaatimukset

7 Tietojärjestelmien ja tietoliikennejärjestelyjen suojaamisen vähimmäisvaatimukset

Tiedonhallintalain 13 §:n mukaisesti viranomaisen on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Turvallisuusluokiteltuihin tietoihin voidaan usein olettaa kohdistuvan eri tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin.

Turvallisuusluokiteltujen tietojen suojaamisessa tulee huomioida myös lainsäädäntöjohdannaiset riskit [8] . Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa palveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia. Turvallisuusluokiteltujen tietojen käsittely tulisi rajata sellaisiin tietojenkäsittely-ympäristöihin ja tietojärjestelmiin, joiden riskeihin nähden riittävästä tietoturvallisuudesta viranomainen voi varmistua.

Tietojen suojaamisessa ja riskiarvioinnissa on merkitystä myös sillä, koskeeko tietoja kansainvälinen tietoturvallisuussopimus. Toisen maan viranomaisten toimivallan piiriin luovutettavien kansallisten

[8] Ks. turvallisuusluokitteluasetus 3.5 §

turvallisuusluokiteltavien tietojen tulee olla luovutettavissa kyseisen valtion, valtioiden tai kansainvälisen yhteisön jäsenille. Turvallisuusluokiteltuihin kansainvälisiin hankkeisiin liittyviä yksityiskohtia on käsitelty tarkemmin kansallisen turvallisuusviranomaisen (NSA) julkaisemissa ohjeissa Turvallisuusviranomaisten käsikirja yrityksille (2015) ja Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje (2020).

Osa viranomaisen turvallisuusluokitellun tiedon käsittely-ympäristöstä voi olla toteutettu pilviteknologiaa hyödyntäen. Pilvipalveluihin liittyvien erityisriskien ja vähimmäissuojausten suhdetta on käsitelty yksityiskohtaisemmin Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen julkaisemassa Pilvipalveluiden turvallisuuden arviointikriteeristössä (PiTuKri).

7.1 Päätelaitteet ja käsittelyvälineet

Tilanteissa, joissa turvallisuusluokan IV tai III tietoa käsitellään ja säilytetään kyseisen turvallisuusluokan mukaisessa päätelaitteessa turvallisuusalueiden ulkopuolella, tai turvallisuusluokan III tietoja päätelaitteessa 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 tietojärjestelmän eheydestä varmistumiseen on sen 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 ja esimerkiksi turvallisuusluokkien III tai II kiinteää tietoverkkoa ei voi ulottaa hallinnolliselle 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.

7.1.1 Turvallisuusluokka IV (TL IV) käsittelyvälineet

Turvallisuusluokan IV sähköinen käsittely (myös etäyhteyden kautta) on mahdollista tietyillä työnantajan tähän tarkoitukseen osoittamilla, hyväksymillä ja ohjeistamilla työvälineillä ja järjestelmillä. Asiakirjan saa tulostaa verkkoon liitetyllä yhteiskäyttöisellä monitoimilaitteella, edellyttäen, että kyseinen verkko ja monitoimilaite täyttävät turvallisuusluokan IV vaatimukset. Kopiointi on sallittua työtehtäviin liittyvän tarpeen perusteella. Tietoa voi käsitellä virkapaikan ulkopuolella, mikäli näkyvyys tai muu pääsy tietoon on estetty sivullisilta.

7.1.2 Turvallisuusluokka III (TL III) käsittelyvälineet

Turvallisuusluokan III sähköinen käsittely (myös etäyhteyden kautta) on mahdollista tietyillä työnantajan käyttöön osoittamilla, hyväksymillä ja ohjeistamilla työvälineillä ja järjestelmillä. Virkamies ei saa kopioida jakelun laajentamiseksi saamaansa turvallisuusluokan III asiakirjaa, koska asiakirjojen luovutus ja vastaanotto on rekisteröitävä asiakirjakohtaisesti erikseen.

7.1.3 Turvallisuusluokka II (TL II) käsittelyvälineet

Turvallisuusluokan II sähköinen käsittely on mahdollista tietyillä työnantajan käyttöön osoittamilla, hyväksymillä ja ohjeistamilla työvälineillä ja järjestelmillä. Mikäli tietoa käsitellään suullisesti, tulee käsittelyn tapahtua erikseen nimetyissä tiloissa (turva-alueella). Mikäli asiakirjaan tutustuu tai sen sisältämään tietoon perehdytetään muita kuin sen vastaanottaja, on tästä tehtävä merkintä asiakirjan kansilehdelle, jota ei saa poistaa. Vastuu asiakirjaan perehtyneiden nimien lisäämisestä on asiakirjan kuitanneella vastaanottajalla. Laaditun asiakirjan tulostaminen on mahdollista vain erikseen työnantajan käyttöön osoittamilla tai hyväksymillä työvälineillä ja järjestelmillä. Virkamies ei saa kopioida saamaansa turvallisuusluokan II asiakirjaa.

7.1.4 Turvallisuusluokka I (TL I) käsittelyvälineet

Turvallisuusluokan I aineistoa käsitellään pääosin kuten turvallisuusluokan II aineistoa, ottaen huomioon seuraavat tiukemmat vaatimukset: turvallisuusluokan I tietoja saa käsitellä vain turva-alueilla, asiakirja laaditaan vaatimukset täyttävällä työasemalla, asiakirjan saa tulostaa ja kopioida, kyseisen turvallisuusluokan vaatimukset täyttävällä ja viranomaisen hyväksymällä tulostimella. Vertaa eri turvallisuusluokkien tietojärjestelmien erottelu luvusta 7.2.

7.2 Tietojärjestelmien erottelu

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on turvallisuusluokitteluasetuksen 11 §:n 1 momentin 1 kohdan mukaan 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 turvallisuusluokan ympäristöistä voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla turvallisuuskriittisten alemman turvallisuusluokan palvelujen (web-selailu, sähköposti ja vastaavat) 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 (ks. luku 7.6) 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 (palomuuraus, käyttöoikeushallinto, jne.). Vastaava erottelu soveltuu myös turvallisuusluokittelemattoman salassa pidettävän tiedon suojaamiseen, kuten myös julkisen tiedon eheyden ja käytettävyyden suojaamiseen.

Turvallisuusluokasta III lähtien erottelu eri turvallisuusluokkien ympäristöihin voidaan toteuttaa 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. Tällaisia ovat esimerkiksi vain yhdensuuntaisen liikennöinnin mahdollistavat datadiodiratkaisut. Turvallisuusluokan II tietojärjestelmien ja tietoliikennejärjestelyjen erottelu voidaan toteuttaa lähtökohtaisesti vain korkean luotettavuuden tarjoavilla datadiodiratkaisuilla. Turvallisuusluokan I tietojärjestelmien ja tietoliikennejärjestelyjen erottelussa tulee lisäksi huomioida, että erottelu tulee toteuttaa lähtökohtaisesti täydellisellä fyysisellä eristämisellä, ja vain poikkeustapauksissa datadiodiratkaisuilla. Suunnitteluperiaatteita käsitellään yksityiskohtaisemmin Liikenne – ja viestintäviraston Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa.

Tietojärjestelmien ja tietoliikennejärjestelyjen liittämisessä on otettava huomioon myös kansainväliset tietoturvavelvoitteet, joissa liittäminen voi olla kokonaan kielletty. Valtionhallinnon viranomainen voi myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011) mukaan pyytää Liikenne- ja viestintävirastolta tietojärjestelmän tai tietoliikennejärjestelyjen vaatimustenmukaisuuden arviointia. Arvioinnin pyytäminen erityisesti turvallisuusluokkien I ja II tietojärjestelmien ja tietoliikennejärjestelyjen liittämisestä matalamman turvallisuusluokan tietojärjestelmiin tai tietoliikennejärjestelyihin on suositeltavaa, jotta tietojärjestelmän tai tietoliikennejärjestelyn turvallisuudesta vastuussa olevalla viranomaisella on riskienhallintapäätöstensä tueksi käytettävissään myös Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asiantuntija-arvio liittämiseen mahdollisesti liittyvistä jäännösriskeistä. Katso tarkemmin Liikenne- ja viestintäviraston ohje tietojärjestelmien arviointi - ja hyväksymisprosesseista 2019.

7.3 Ohjelmistohaavoittuvuuksien hallinta

Tietojärjestelmän turvallisuus pohjautuu oleellisesti sen käyttämien ohjelmistojen (esimerkiksi käyttöjärjestelmä- ja sovellusohjelmistot) luotettavuuteen. Virheettömien ohjelmistojen tekeminen on osoittautunut haastavaksi. Käytännössä lähes kaikista ohjelmistoista löytyy ohjelmistovirheitä, toisin sanoen haavoittuvuuksia. Haavoittuvuuksia pystytään hyödyntämään tietojärjestelmässä käsiteltävän tiedon suojaamisen ohittamiseen. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Ohjelmistoihin liittyviä riskejä voidaan pienentää huomattavasti asentamalla ohjelmistoihin turvallisuuskorjaukset, toisin sanoen -päivitykset. Keskeistä on järjestää:

a) toimiva, säännöllinen prosessi turvallisuuspäivitysten asentamiseksi ja

b) varmistaa prosessin käytännön toimivuus.

Päivitysprosesseissa huomionarvioista on niiden riittävän nopea päivitysten jalkauttaminen sekä kattavuus. Prosessien tulee kattaa kaikki turvallisuuteen oleellisesti vaikuttavat ohjelmistot, joita tyypillisesti ovat esimerkiksi palvelinten ja päätelaitteiden käyttöjärjestelmät, varusohjelmistot sekä kolmannen osapuolen sovellukset, sekä verkkolaitteiden ohjelmistot. Päivitysprosessien toimivuuden varmistamiseen voidaan käyttää esimerkiksi säännöllisiä konfiguraatiotarkasteluja ja teknisiä haavoittuvuusskannauksia.

7.4 Turvallisuuden huomioivat muutoshallintamenettelyt

Hyvinkin turvalliseksi suunnittelun tietojärjestelmän turvallisuus rapautuu ajan myötä, mikäli järjestelmään tehdään hallitsemattomia muutoksia. Uskottava järjestelmän turvallisuuden ylläpito edellyttää menettelyä, jossa järjestelmiin vaikuttavien muutosten turvallisuusvaikutukset arvioidaan, mahdollisuuksien mukaan testataan, ja tarpeelliset lisäsuojaukset tarvittaessa toteutetaan ennen muutosten käyttöönottoa. Muutoshallinta mahdollistaa myös järjestelmän tehokkaamman hallinnoinnin sekä tukee muita ylläpitoprosesseja.

7.5 Varmuuskopiointimenettelyt

Varmuuskopiointi on keskeinen suojaus erityisesti tiedon käytettävyyden varmistamisessa. Varmuuskopiointi on toisaalta usein menettely, jossa tiedon muut suojaustarpeet (eheys, luottamuksellisuus) tulee huomioida alkuperäistä tietoa vastaavilla menettelyillä. Varmistus- ja palautusprosessit tulee suunnitella, toteuttaa, testata ja kuvata osana jatkuvuussuunnitelmaa siten, että pystytään vastaamaan organisaatioon ja kyseiseen tietojärjestelmään liittyviin toiminnallisiin tarpeisiin sekä muihin velvoitteisiin. Erityisesti on huomioitava:

- varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO).
- palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO).
- varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti.
- varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä).

- varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto. Suuri määrä tietoa voi edellyttää tiukempia suojauksia (kasautumisvaikutus).
- pääsy varmuuskopioihin on rajattu vähimpien oikeuksien periaatteen (ks. luku 7.6) mukaisesti vain hyväksytyille henkilöille/rooleille.
- varmistus- ja palautusprosessit ovat jäljitettävissä (lokitus) ja valvottuja siten, että luvattomat toimet pyritään havaitsemaan.
- tilanteissa, joissa varmuuskopioita säilytetään toisessa fyysisessä sijainnissa, myös tämän sijainnin tulee olla fyysisen ja loogisen pääsynhallinnan osalta vähintään vastaavalla tasolla.
- tilanteissa, joissa salassa pidettävää tietoa sisältäviä varmuuskopioita siirretään fyysisesti suojatun alueen ulkopuolelle (esimerkiksi konesalien välillä) verkon välityksellä, tiedon/tietoliikenteen tulee olla riittävällä tavalla salattua.
- tilanteissa, joissa salassa pidettävää tietoa sisältäviä varmuuskopioita siirretään fyysisesti suojatun alueen ulkopuolelle siirtomedialla (esimerkiksi varmistusnauhat tai -levyt), siirtomedia siirretään jatkuvan valvonnan alaisuudessa. Siirtomedialle tai sen sisältämälle tiedolle suositellaan salausta.
- varmistusmediat tuhotaan luotettavasti

7.6 Vähimpien oikeuksien periaate

Turvallisuusluokitteluasetuksen 11 §:n 1 momentin 3 kohdan mukaan turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteutettava siten, että tietojärjestelmien käyttäjille annetaan vain ne tiedot, oikeudet ja valtuudet, jotka ovat tehtävien suorittamiseksi välttämättömät.

Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esimerkiksi 6 kuukauden välein. Lisäksi muutoksissa, kuten ylennyksissä, alennuksissa, työnkierron yhteydessä ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä ajantasaisina. Tämä voi edelleen tarkoittaa sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen.

Käyttöoikeuksien hallinnoinnin tulee toteuttaa vähimpien oikeuksien periaatetta:

1. käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).

2. käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon tulee olla ennalta määritelty prosessi.
3. tietojenkäsittely-ympäristön käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä.
4. järjestelmän käyttäjistä tulee ylläpitää listaa. Jokaisesta myönnetystä käyttöoikeudesta tulee jäädä merkintä (paperi tai sähköinen).
5. käyttöoikeuden myöntämisen yhteydessä tulee tarkistaa, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
6. käyttöoikeuksien käsittelyn ja myöntämisen tulee olla ohjeistettu.
7. tarpeettomat käyttäjätilit ja oikeudet tulee poistaa, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan).
8. tulee olla olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.
9. käyttö- ja pääsyoikeudet tulee katselmoida säännöllisesti, vähintään puolivuosittain.

7.7 Käyttäjien ja laitteistojen tunnistaminen

7.7.1 Fyysisesti suojatun hallinnollisen alueen tai turva-alueen sisällä

Turvallisuusluokitteluasetuksen 11 §:n 1 momentin 5 kohdan mukaan turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteuttava siten, että niitä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.

Turvallisuusluokan IV osalta vaatimus käyttäjien ja laitteistojen tunnistamiseen voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet
2) kaikki käyttäjät tunnistetaan ja todennetaan
3) tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti
4) tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen
5) järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille
6) todennus tehdään vähintään salasanaa käyttäen hyväksyttyjen salasanakäytänteiden mukaisesti

Turvallisuusluokkien III-II osalta vaatimus voidaan täyttää siten, että kohtien 1-5 lisäksi toteutetaan seuraavat toimenpiteet:

7) edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta.
8) päätelaitteet tunnistetaan teknisesti (laitetunnistus, 802.1X, tai vastaava menettely) ennen pääsyn sallimista verkkoon tai palveluun, ellei verkkoon kytkeytymistä ole fyysisen turvallisuuden menetelmin rajattu suppeaksi (esim. palvelimen sijoittaminen lukittuun laitekaappiin teknisesti suojatun viranomaisen ko. suojaustasolle hyväksymän turva-alueen sisällä).

7.7.2 Korvaavia menettelyjä

Turvallisuusluokkien III ja II menetelmät vahvasta käyttäjätunnistuksesta ja päätelaitteen tunnistamisesta voidaan joissain tapauksissa toteuttaa siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisesti suojatulta alueelta (yleensä teknisesti suojattu turva-alue, lukittu laitekaappi, tai vastaava), jonka pääsynvalvonnassa käytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.

7.7.3 Lisätietoa

Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että,

a) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle),

b) sisäänkirjauduttaessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa,

c) todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) ovat aina salatussa muodossa, jos ne lähetetään verkon yli,

d) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan ja

e) todennusmenetelmä on suojattu brute force -hyökkäyksiä vastaan.

7.8 Välttämättömät toiminnallisuudet

Turvallisuusluokitteluasetuksen 11 §:n 1 momentin 6 kohdan mukaan turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteuttava siten, että niissä otetaan käyttöön vain käyttövaatimusten kannalta välttämättömät toiminnallisuudet.

Turvallisen ohjelmistokoodin tekeminen on haastavaa. Mitä enemmän ympäristössä on ohjelmistokoodia, sitä enemmän on mahdollisuuksia ohjelmistovirheille, toisin sanoen. haavoittuvuuksille. Mitä enemmän ohjelmistokoodin turvallisuuteen nojaavia palveluja on tarjolla, sitä todennäköisempää on, että palveluissa on myös haavoittuvuuksia. Riskejä voidaan pienentää haavoittuvuuspinta-alaa pienentämällä, toisin sanoen. tarjoamalla vain välttämättömiä palveluja alttiiksi hyökkäyksille.

Järjestelmät ovat yleensä tulvillaan ominaisuuksia. Ominaisuudet ovat yleensä oletusarvoisesti päällä ja helppo ottaa käyttöön, ja ne ovat toisaalta usein tarpeettoman turvattomilla asetuksilla. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, tarpeettomia käyttäjätilejä tai valmiiksi asennettuja tarpeettomia ohjelmistoja.

Koventamisella tarkoitetaan yleisesti järjestelmän asetusten muuttamista siten, että järjestelmän haavoittuvuuspinta-alaa saadaan pienennettyä. Riskien pienentämiseksi järjestelmissä on yleisesti otettava käyttöön vain käyttövaatimusten kannalta olennaiset toiminnot, laitteet ja palvelut, ja esimerkiksi palvelujen näkyvyys tulee rajata mahdollisimman pieneksi. Vastaavasti esimerkiksi automaattisille prosesseille on annettava vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä. Näin voidaan rajoittaa onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja. Järjestelmän mahdollisesti turvattomat oletusasetukset ja esimerkiksi tarpeettomat oletuskäyttäjätilit tulee muuttaa tai poistaa. Lisätietoja koventamisesta Katakrissa.

7.9 Jäljitettävyys

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.

Jäljitettävyydellä tarkoitetaan järjestelmäympäristön tapahtumien kirjaamista siten, että poikkeamatilanteessa voidaan selvittää mitä toimia ympäristössä on tehty, kenen toimesta ja mitä vaikutuksia toimilla on ollut. Keskeisiä tallenteita ovat tyypillisesti kirjautumistietojen lisäksi keskeisten verkkolaitteiden ja palvelinten lokitiedot. Myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein.

Kattavuusvaatimuksen voi useimmin toteuttaa siten, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien lokitus on päällä. Verkkolaitteiden lokeista tulisi myös pystyä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. Tapahtumalokeja olisi syytä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista ja poikkeuksista.

Eräs suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot keskitetylle ja vahvasti suojatulle lokipalvelimelle, jonka tiedot varmuuskopioidaan päivittäin erilliseen, vähintään vastaavan turvallisuusluokan ympäristöön. Lokitietojen kerääminen ja tallennus tulee pyrkiä toteuttamaan siten, että lokitietojen poistaminen tai muuttaminen voidaan havaita myös tilanteissa, joissa esimerkiksi lokilähteen ja lokikeräimen välinen verkkoyhteys ei ole käytettävissä. Vastaavasti esimerkiksi verkosta pysyvästi irtikytkettyjen työasemien lokienkeräys sekä kerättyjen lokitietojen varmistukset edellyttävät säännöllistä prosessia. Sekä ylläpitäjien oikeusturvan, kuin myös tietomurtoepäilyjen tutkinnan tukemiseksi, suositellaan tehtävien erottelua toteutettavaksi siten, että lokitietojen ylläpito on eriytetty muusta ylläpitohenkilöstöön liittyvästä lokituksesta. Jäljitettävyyden toteuttamisessa tulee huomioida myös tilanteet, joissa järjestelmään kirjautuneella on mahdollisuus suorittaa toimintoja toista tiliä käyttäen (user impersonation). Lokitietojen tallennus- ja seurantaohjelmiston toimivuutta tulee myös seurata, ja mahdolliset häiriöt tulee pystyä havaitsemaan lyhyelle aikaviiveellä (esimerkiksi yhden vuorokauden sisällä lokilähteen lopetettua lokien toimittamisen).

Lokitietojen säilytysajoissa tulee huomioida kyseessä olevan käyttötapauksen tarpeet. Esimerkiksi joidenkin tietojen käsittely- ja luovutuslokeille voi olla perusteltua edellyttää eroavia säilytysaikoja, kuin poikkeamatilanteiden selvittämiseksi kerättäville lokitiedoille. Esimerkiksi viranomaistoiminnassa rikosoikeudelliset vanhentumisajat voivat johtaa tyypillisesti vähintään viiden vuoden säilytysaikatarpeisiin. Usein käytettynä käytäntönä on, että 6 kuukauden lokitiedot ovat saatavilla reaaliaikaisesti, ja pidemmän aikavälin lokitiedot ovat tarvittaessa saatavissa muutamien työpäivien viiveellä. Lokitietojen erilaisia käyttötapauksia on käsitelty tarkemmin Tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäädösten soveltamisesta (2020:21, luku 7).

Toteutus edellyttää usein myös sen huomioon ottamista, että lokien säilytystilaa ja -aikaa kasvatetaan riittäviksi. Suositeltavaa on, että lokeille varataan tilaa ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden

kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. On huomioitava, että tilalle on syytä varata reilusti ”puskuria”, sillä poikkeavat tilanteet ja myös tietyt hyökkäystyypit kasvattavat lokimäärää merkittävästi.

Toteutusesimerkki

Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) toimintaan on jalkautettu kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka/-ohje, joka on muodostettu ottaen huomioon toiminnan vaatimukset,

2) tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen,

3) keskeiset tallenteet säilytetään vähintään 6 kuukautta, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. Käsittelylokit ja tallenteet, joita koskee esimerkiksi viranomaistoiminnan rikosoikeudelliset vanhentumisajat, säilytään vähintään 5 vuotta,

4) lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta).

Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1-4 lisäksi toteutetaan seuraavat toimenpiteet:

5) keskeiset tallenteet säilytetään vähintään 5 vuotta, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. Tallenteita, joilla on esimerkiksi poikkeamatilanteiden selvittelyn tai viranomaistoiminnan rikosoikeudelliselta kannalta hyvin vähäistä merkitystä, voidaan säilyttää lyhyemmän ajan, esimerkiksi 2-5 vuotta,

6) lokitiedot varmuuskopioidaan säännöllisesti,

7) samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun ajanlähteen kanssa,

8) on olemassa menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen,

9) syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkinnät.

7.10 Havainnointi

Tekninen poikkeamien havainnointikyky pohjautuu yleensä kolmeen lähteeseen:

1) verkkoliikenteessä näkyviin tapahtumiin,

2) kerättyihin tallenteisiin (lokeihin) ja

3) kohteilla (hosts) näkyviin tapahtuviin.

Riittävä tekninen havainnointikyky pystytään yleensä toteuttamaan edellä mainittuja havainnointilähteitä yhdistelemällä. Mitä tarkemmin kyseinen tietojenkäsittely-ympäristö ja sen normaali toiminta tunnetaan, sitä paremmin pystytään myös havainnoimaan normaalista toiminnasta eroavia tapahtumia. Normaalista toiminnasta eroavien tapahtumien havainnointi tukee myös sellaisten hyökkäysten havainnointia, joista ei ole saatavilla hyökkäysten tunnistetietoja (IoC, Indicator of Compromise). Tietojenkäsittely-ympäristön normaali toiminta tulisi tuntea koko elinkaaren ajalta, aina alkuhetkistä käytöstä poistoon asti. Myös muutostenhallinta tukee poikkeamien havainnointikykyä, muun muassa laitteisto- ja ohjelmistokonfiguraatiomuutosten säännöllisen tarkastelun avulla.

Tarkkailuun ja havaitun hyökkäyksen vaikutusten rajoittamiseen on useita soveltuvia toteutusmahdollisuuksia keskeisten verkkosolmujen tasolla tapahtuvasta tarkastelusta aina työasema-/palvelinkohtaisiin sensoreihin sekä näiden yhdistelmiin. Riippumatta käytetyistä verkkolaitteista ja toimittajista, verkkotason havainnointikyvyn käytännön toteutus edellyttää tyypillisesti verkkoliikenteen normaalin tilan tuntemista. Turvallisuusluokan IV käsittely-ympäristöissä verkkoliikennetason havainnointikyvyn tulisi kattaa erityisesti verkon/kohteen ulkorajan, ja turvallisuusluokka III-luokasta lähtien ulkorajan yhdyskäytäväratkaisun sekä verkon/kohteen sisäpuolen liikennöinnin.

Hyökkäyksen/väärinkäyttöyrityksen havaitseminen edellyttää useimmissa ympäristöissä käytännössä automatisoitujen havainnointi- ja hälytystyökalujen käyttöä. Joissain tilanteissa lokitietojen manuaalinen käsittely on myös mahdollista ja jopa välttämätöntä, mikäli automaattisin keinoin ei esimerkiksi ole havaittu poikkeamaa ja poikkeamatilanne vaatii tarkempaa selvitystä. Tulee myös muistaa, että lokeihin saa kerätä vain tietoturvaan liittyvien toimenpiteiden kannalta välttämättömiä tietoja, eikä toimenpiteitä toteutettaessa saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa. Yleisesti tulee huomioida, että havainnointikyky edellyttää kunkin tietojenkäsittely-ympäristön ominaispiirteiden tuntemista, ja muun muassa

kriittisten kohteiden ja seurattavien tapahtumien määrittelyä ja räätälöintiä kyseessä olevan tietojenkäsittely-ympäristön mukaisesti, sekä havainnointikyvyn jatkuvaa ylläpitoa.

Tietojenkäsittely-ympäristön palauttaminen takaisin suojattuun tilaan kohtuullisessa ajassa edellyttää yleensä suunniteltuja, kuvattuja, koulutettuja sekä harjoiteltuja prosesseja sekä teknisiä menetelmiä. Poikkeamien havainnointikyvyn kehittämisessä ja ylläpitämisessä tulee huomioida myös koko henkilöstön rooli. Esimerkiksi loppukäyttäjien ilmoittamat havainnot voivat tuottaa arvokasta tietoa hyökkäysten tai niiden yritysten havainnointiin.

Toteutusesimerkki

Turvallisuusluokan IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa. On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan,

2) on olemassa menettely, jolla kerätyistä tallenteista ja tilannetiedosta (esimerkiksi muutokset lokikertymissä) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan),

3) on olemassa menettely, jolla tietojenkäsittely-ympäristön kohteista (hosts, esimerkiksi työasemat ja palvelimet) voidaan havainnoida poikkeamia sekä

4) on olemassa menettely havaituista poikkeamista toipumiseen.

7.11 Salausratkaisut

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on turvallisuusluokitteluasetuksen 11 §:n 1 momentin 7 kohdan mukaan toteutettava siten, että käytetyt salausratkaisut ovat tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän turvallisia.

Salassa pidettävien tietojen siirtämisestä yleisessä tietoverkossa säädetään tiedonhallintalain 14 §:ssä. Turvallisuusluokiteltuja asiakirjoja saa turvallisuusluokitteluasetuksen 12 §:n mukaan siirtää

muussa kuin yleisessä tietoverkossa viranomaisen turvallisuusalueiden ulkopuolelle tai kyseistä turvallisuusluokkaa alemman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain salatussa muodossa. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. 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 salauksen 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 riittävyydestä ja salaustuotteen määritysten mukaisesta oikeasta 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). Salaustuotteiden arvioinnissa huomioitaviin tekijöihin kuuluvat myös 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 usein olettaa kohdistuvan

eri tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa.

Salausratkaisujen valinnassa suositellaan nojautumaan ensisijaisesti Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen NCSA-toiminnon arvioimiin ja hyväksymiin salausratkaisuihin (Traficom 2020). Salausratkaisujen hyväksyntään liittyy oleellisesti hyväksyntäprosessissa määritelty käyttöpolitiikka. Käyttöpolitiikkaan sisältyy sellaiset käyttötapaukset ja salausratkaisun asetukset, joiden mukaan toimimalla kyseisen salausratkaisun on arvioitu tuottavan riittävän suojan 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 Liikenne- ja viestintäviraston 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). Lisätietoja Kryptografisista vahvuusvaatimuksista Kyberturvallisuuskeskuksen ohjeessa (Viestintävirasto 2018).

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

8 Käsittely viranomaisten toimitilojen ja tietojärjestelmien ulkopuolelta

Jos turvallisuusluokan IV tai III sähköisiä asiakirjoja säilytetään päätelaitteessa turva-alueiden ulkopuolella, ne on suojattava turvallisuusluokalle riittävän turvallisella salausratkaisulla. Päätelaitteen tietoturvallisuudesta on huolehdittava. Käyttäjät tulee todentaa aina vahvasti, vähintään kahteen tekijään perustuen. Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (2016/533) § 8a säädetään tunnistusmenetelmässä käytettävistä todentamistekijöistä. Tunnistusmenetelmässä on käytettävä vähintään kahta seuraavista todentamistekijöistä. Näitä ovat:

1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;
2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan
3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.

Kun viitataan kahden tekijän käyttöön, niin tunnistustapahtumassa ei riitä kaksi tai kolme salasanaa, koska ne perustuvat ensimmäiseen kohtaan (mitä henkilö tietää). Esimerkiksi pankkitunnisteissa tunnistaminen perustuu siihen, mitä henkilö tietää (käyttäjätunnus ja mahdollinen salasana sekä siihen, mitä hänellä on hallussaan (tunnuslukutaulukko, tunnuslukulaite tai mobiililaite). Valtiolla Valtti-työaseman ja Kauko-VPN:n käyttöesimerkkinä kahden tekijän käytöstä on, mitä henkilö tietää (käyttäjätunnus + salasana) ja siihen liitettynä mitä hänellä on hallussaan (tekstiviesti mobiililaitteeseen).

Fyysisesti suojattujen alueiden ulkopuolella liikennöitäessä yhteyden tulee olla riittävän vahvasti salattu. Tietoturvallisuudesta etätyössä on valmisteilla Valtiovarainministeriön erillinen ohje.

Säädökset

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

Euroopan parlamentin ja neuvoston asetus (EU) luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (679/2016)

Laki digitaalisten palvelujen tarjoamisesta (306/2019)

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

Laki julkisen hallinnon tiedonhallinnasta (906/2019)

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (533/2016)

Laki viranomaisen toiminnan julkisuudesta (621/1999)

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)

Laki Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)

Suomen Perustuslaki (731/1999)

Tietosuojalaki (1050/2018)

Ohjeet ja muut materiaalit

Kansallinen turvallisuusviranomanomainen (NSA) 2020. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje.

Liikenne- ja viestintävirasto 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficom 13/2020.

Liikenne- ja viestintävirasto. 2018. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista.

Liikenne- ja viestintävirasto. 2019. Ohje Liikenne- ja viestintäviraston suorittamista tietojärjestelmien arviointi- ja hyväksyntäprosesseista

NIST National Checklist Program Repository. https://nvd.nist.gov/ncp/repository#

Puolustusministeriö 2015. Tietoturvallisuuden auditointityökalu viranomaisille 2015 (Katakri)

Tietosuojavaltuutetun toimisto. www.tietosuoja.fi

Traficom. Liikenne- ja viestintävirasto 2020. Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät.

Traficom. Liikenne- ja viestintävirasto 2020. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut

Ulkoministeriö 2015. Turvallisuusviranomaisten käsikirja yrityksille.

Valtionvarainministeriö 2020. Suositus tiedonhallintamallista. (2020:29)

Valtiovarainministeriö 2020. Suositus tiedonhallinnan muutosvaikutusten arvioinnista (2020:53)

Valtiovarainministeriö 2020. Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta

Viestintävirasto, Kyberturvallisuuskeskus 2016. Kiintolevyjen elinkaaren hallinta. Ylikirjoitus ja uusiokäyttö. Ohje. 26.10.2016

Viestintävirasto, Kyberturvallisuuskeskus. 2018. Vahvuustaulukot. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset suojaustasot

Liite 1

Alla olevassa taulukossa on annettu esimerkkejä turvallisuusluokittelun edellyttämän vahingon arvioimiseksi suojattavan edun näkökulmasta. Luokittelu on aina tehtävä tapauskohtaisesti riskiarviointiin perustuen. Tiedonhallintayksikössä olisi hyvä laatia toimialakohtainen luokitteluohje, esimerkiksi alla olevan taulukon mukaisesti.

	TL IV	**TLIII**	**TL II**	**TL I**
Kuvaus	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa suojattavalle edulle.	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa suojattavalle edulle.	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa suojattavalle edulle.	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa suojattavalle edulle Toiminta keskeytyy, estyy pysyvästi.
Tarkempi kuvaus	Tiedon paljastumisesta voi aiheutua seuraus tai tapahtuma, jonka vuoksi ei tarvitse keskeyttää toimintaa, saatetaan joutua muuttamaan toiminnallisia suunnitelmia.	Tiedon paljastumisesta voi aiheutua seuraus taikka tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään.	Tiedon paljastumisesta voi aiheutua seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään ja se estyy pitkähköksi ajaksi.	Vahinko on laajamittaista ja kohdistuu esimerkiksi yhteiskunnan toimintakyvyn kannalta keskeisiin kohteisiin/toimintoihin, kuten kriittiseen infrastruktuurin tai elintärkeään toimintaan.
Suojattava etu: Esimerkiksi poikkeusoloihin varautuminen	Mahdollisesti vaarantaa viranomaisen toiminnan. Esimerkiksi olennaisten tietojärjestelmien dokumentit kuten turvajärjestelyt, haavoittuvuudet ja auditointiraportit jatkuvuus- ja toipumissuunnitelmat.	Todennäköisesti vaarantaa viranomaisen toiminnan. Esimerkiksi elintärkeiden toimintojen turvallisuusjärjestelyt, jatkuvuus- ja toipumissuunnitelmat	Mahdollisesti estää viranomaisen toiminnan. Laajan ihmisjoukon turvallisuutta ei voida taata. Esimerkiksi elintärkeiden toimintojen ja niitä tukevien tietojärjestelmien keskeiset dokumentit turvajärjestelyistä, haavoittuvuuksista ja auditoinneista.	Todennäköisesti estää viranomaisen toiminnan ja turvallisuusjärjestelyjen tarkoituksen toteutumisen.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ