Katakri 2020

Tietoturvallisuuden auditointityökalu viranomaisille

Esipuhe

Ensimmäinen Katakri eli kansallinen turvallisuusauditointikriteeristö valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Katakri valmisteltiin puolustusministeriön johdolla viranomaisten ja elinkeinoelämän yhteistyössä. Tämän jälkeen vastuu Katakrin jatkohallinnoinnista ja päivityksestä siirrettiin sisäministeriölle, jonka koordinoimana Katakrin ensimmäinen päivitysversio valmistui vuonna 2011.

Elokuussa 2012 sisäministeriö asetti neuvoa antavan työryhmän, jonka esityksestä keskeiset ministeriöt (VM, UM, LVM, SM, PLM, VNK) päättivät tammikuussa 2014, että päävastuu Katakrin ylläpidosta ja hallinnoinnista siirtyy ulkoministeriössä toimivalle Kansalliselle turvallisuusviranomaiselle (NSA). Katakrin kolmas, vuonna 2015 julkaistu versio uudisti Katakrin rakenteen ja keskittyi turvallisuusluokitellun tiedon tietoturvallisuuteen. Katakri-nimi oli käytössä jo niin vakiintunut, että se päätettiin säilyttää jatkossakin tämän viranomaisten auditointityökalun nimessä.

Katakrin neljännen version päivitystyö ja hallinnointi on ollut NSA:n yhteistyöryhmän alatyöryhmäksi perustetun ohjausryhmän vastuulla. Ohjausryhmässä ovat olleet edustettuina toimivaltaisten viranomaistahojen lisäksi elinkeinoelämän edustajat. Katakri on osoittautunut toimivaksi työkaluksi, jolla on merkittävää arvoa myös Suomen maineelle tietoturvallisuuteen liittyvissä kysymyksissä sekä suomalaiselle yritysmaailmalle laajemminkin. Katakrin neljännen version päivitystyön taustalla keskeisimpänä tekijänä on ollut vastaaminen 2020 alusta uusiutuneen kansallisen lainsäädännön muutoksiin. Neljännessä versiossa on huomioitu myös digitaalisen tietojenkäsittelyn kehitysaskeleita, sekä täydennetty työkalun tarkoituksenmukaiseen käyttöön liittyviä ohjeistuksia.

Katakrin uudistamistyötä on koordinoinut ohjausryhmä, johon kuuluvat

Mikael Raivio, yksikön päällikön sijainen, lakimies, NSA/ulkoministeriö (pj.)
Tuija Kuusisto, tietohallintoneuvos, valtiovarainministeriö (vpj.)
Rauli Paananen, valtion kyberturvallisuusjohtaja, liikenne- ja viestintäministeriö
Juha Pallaspuro, johtava asiantuntija, valtioneuvoston kanslia
Tapio Pihlajamäki, apulaisturvallisuusjohtaja, puolustusministeriö
Aki Tauriainen, johtaja, Liikenne- ja viestintävirasto Traficom
Kari Santalahti, turvallisuuspäällikkö, sisäministeriö
Elina Immonen, yksikön johtaja, liikenne- ja viestintäministeriö
Toni Lahti, komentajakapteeni, Pääesikunta
Richard Wunsch, komentajakapteeni, Puolustusvoimien tiedustelulaitos
Ilkka Hanski, osastopäällikkö, suojelupoliisi
Tuomas Hyvärinen, hallitussihteeri, puolustusministeriö
Reijo Kaariste, kapteeniluutnantti, Pääesikunta
Mikko Viitasaari, turvallisuusjohtaja, UPM Oyj
Markku Rajamäki, johtava asiantuntija, Elinkeinoelämän keskusliitto (EK)
Ville Jääskeläinen, ylitarkastaja, suojelupoliisi
Tero Leppänen, turvallisuusjohtaja, Insta Group Oy
Ville Salmi, lakimies, NSA/ulkoministeriö (siht.)

Katakrin eri osa-alueita on valmisteltu erillisissä asiantuntijoista koostuvissa alatyöryhmissä, joihin kuuluvat:

Alatyöryhmä T - Turvallisuusjohtaminen

Juha Pallaspuro, valtioneuvoston kanslia (puheenjohtaja)
Anna von Fieandt-Lehtonen, Liikenne- ja viestintävirasto Traficom
Olli-Pekka Soini, Nixu Certification Oy
Toni Lahti, Pääesikunta
Erja Kinnunen, Digi- ja väestötietovirasto

Alatyöryhmä F - Fyysinen turvallisuus

Ville Jääskeläinen, suojelupoliisi (puheenjohtaja)
Janne Allonen, Liikenne- ja viestintävirasto Traficom
Mika Tikkanen, valtioneuvoston kanslia
Kalle Seppänen, UPM Oyj
Jani Rantanen, Pääesikunta

Alatyöryhmä I - Tekninen tietoturvallisuus

Tomi Kelo, Liikenne- ja viestintävirasto Traficom (puheenjohtaja)
Niko Mäkilä, valtioneuvoston kanslia
Antti-Ilari Söderholm, valtioneuvoston kanslia
Ville Kuumola, Insta DefSec Oy
Pinja Koskinen, Liikenne- ja viestintävirasto Traficom
Henri Kettunen, suojelupoliisi
Juha Saarisilta, Ilmavoimat
Mikko Hakuli, verohallinto
Mika Raappana, Valtori
Jarkko Majava, Nixu Oy
Pasi Koljonen, Pääesikunta
Pertti Pyysing, Pääesikunta
Jarmo Pietikäinen, Digi- ja väestötietovirasto
Jan Partanen, Digi- ja väestötietovirasto
Juha Huikari, Puolustusvoimien johtamisjärjestelmäkeskus

Katakri-auditointityökalu on hyväksytty käyttöön NSA:n yhteistyöryhmässä XX.XX.2020. Ajantasainen versio Katakrista on saatavilla sähköisenä.

Johdanto

Katakri on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata *kansallista tai kansainvälistä turvallisuusluokiteltua tietoa*[1]. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri itsessään ei aseta tietoturvallisuudelle[2] ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin.

Keskeisimmät kansalliseen lainsäädäntöön perustuvat vaatimuslähteet ovat laki julkisen hallinnon tiedonhallinnasta (906/2019) sekä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), joita noudatetaan Suomessa niin kansallisen kuin kansainvälisenkin turvallisuusluokitellun tiedon suojaamisessa. Kansainvälisenä lähteenä on käytetty EU:n turvallisuussääntöjä (2013/488/EU), jotka sisältävät EU:n turvallisuusluokitellun tiedon suojaamista koskevat vähimmäisvaatimukset ja perusperiaatteet.

Katakrin rakenne

Katakri on jaettu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen. Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset.

Vaatimukset on kuvattu siten, että ne mahdollistavat erilaisia toteutustapoja. Lisätietokenttiin on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso. Toteutusesimerkit eivät ole sitovia ja ne ovat korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Toteutusesimerkkien lähteinä on hyödynnetty muun muassa tiedonhallintalautakunnan julkaisemia suosituksia, VAHTI-ohjeita sekä EU:n turvallisuussääntöjä täydentäviä suuntaviivoja ja ohjeita.

Vaatimuksissa tai toteutusesimerkeissä ei kuvata kaikkiin ympäristöihin tai erikoistapauksiin riittäviä suojauksia. Esimerkiksi käsiteltäessä sellaisia turvallisuusluokiteltuja tietoja, joiden voidaan olettaa olevan poikkeuksellisen ulkopuolisen kiinnostuksen kohteena, vähimmäissuojauksia on perusteltua täydentää lisäsuojauksilla.

---

[1] Kansainvälisellä turvallisuusluokitellulla tiedolla viitataan Katakrissa EU:n ja soveltuvin osin myös Naton, ESA:n ja OCCAR:in turvallisuusluokiteltuun tietoon. Kahdenvälisten tietoturvallisuussopimusten (GSA, General Security Agreement) piiriin kuuluvat kansainväliset turvallisuusluokitellut tiedot tulee sen sijaan suojata lähtökohtaisesti vastaavilla menettelyillä kuin kansallista vastaavan turvallisuusluokan tietoa suojataan. Kansainvälisen turvallisuusluokitellun tiedon suojaamisessa tulee huomioida kunkin tietoturvallisuussopimuksen mahdolliset erityisehdot. Lisätietoa voimassa olevista tietoturvallisuussopimuksista on saatavilla Ulkoministeriön verkkosivuilta (https://um.fi/voimassa-olevat-tietoturvallisuussopimukset).

[2] Tietoturvallisuudella tarkoitetaan menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (informaation luottamuksellisuus), informaation muuttumattomuus (informaation eheys) sekä informaation käytettävyys. Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joista tavallisimmat ovat henkilöstön luotettavuuden ja toimitilojen turvallisuuden varmistaminen, salassapitosäännökset ja tietojen käytön rajoittaminen vain sovittuun sekä erilaiset tietojen käsittelyyn ja siirtoon liittyvät menettelytapavaatimukset. Tietoturvallisuusvaatimukset kattavat informaation koko elinkaaren, toisin sanoen tietojen hankkimisen, muokkaamisen, käytön, luovutuksen, arkistoinnin ja hävittämisen. (HE 66/2004) Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä (L 906/2019).

Käyttö

Katakria voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Yritysturvallisuusselvityksen käyttötapausta kuvataan yksityiskohtaisemmin liitteessä I. Tietojärjestelmien arvioinnin käyttötapausta kuvataan yksityiskohtaisemmin liitteessä II. Katakria voidaan käyttää apuna myös yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä.

Turvallisuusjärjestelyjen riittävyyden arvioinnin tulee pohjautua järjestelmälliseen riskienarviointiin. Turvallisuusriskien hallinnalla on pyrittävä toteuttamaan turvatoimien yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Katakrin turvallisuusmalli sekä riskienhallinnan rooli eri käyttötapauksissa kuvataan liitteessä III.

Kansalliseen ja EU:n turvallisuusluokiteltuun tietoon kohdistuvat suojaamisvaatimukset ovat valtaosin yhteneviä. Yksittäiset eroavaisuudet ilmenevät lähdeviitteistä. Katakria voidaankin käyttää sekä kansallisen että kansainvälisen turvallisuusluokitellun tiedon suojaamiseen. Turvallisuusluokittelemattoman kansallisen salassa pidettävän tiedon suojaamista voidaan peilata turvallisuusluokan IV vaatimuksiin soveltuvin osin.

Toimivaltaiset viranomaiset Katakrin tuetuissa käyttötapauksissa

Kun arviointi tehdään osana kansallista yritysturvallisuusselvitystä, T- ja F-osa-alueissa toimivaltainen viranomainen on suojelupoliisi tai Pääesikunta ja I-osa-alueessa Liikenne- ja viestintävirasto (726/2014, 9 §). Kansainvälisen turvallisuusluokitellun tiedon suojaamiseen liittyvissä Katakrin käyttötapauksissa puolustusministeriö, Pääesikunta ja suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Liikenne- ja viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa (588/2004, 4 §). Kansainvälisessä yritysturvallisuusselvitysprosessissa (FSC, Facility Security Clearance) T- ja F-osa-alueissa toimivaltaisena viranomaisena toimii suojelupoliisi tai Pääesikunta ja I-osa-alueessa Liikenne- ja viestintävirasto.

Kun arviointi tehdään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annetun lain (1406/2011) mukaisesti, Liikenne- ja viestintävirasto selvittää, täyttääkö tietojärjestelmä tai tietoliikennejärjestely ne tietoturvallisuutta koskevat vaatimukset, jotka on otettu arviointiperusteeksi (1406/2011, 7 §). Tilanteissa, joissa kansallista turvallisuusluokiteltua tietoa käsittelevän tietojenkäsittely-ympäristön arvioinnin suorittaa Liikenne- ja viestintäviraston hyväksymä tietoturvallisuuden arviointilaitos (1406/2011, 3 §), arviointilaitoksen tulee toimia Liikenne- ja viestintäviraston myöntämän arviointilaitoshyväksynnän ehtojen mukaisesti siten, että toimivaltaisen viranomaisen hyväksyntää edellyttävät vaatimuskohdat arvioi ja hyväksyy Liikenne- ja viestintävirasto.

Soveltamisala

Katakrin tuetuissa käyttötapauksissa (L 726/2014, L 588/2004, L 1406/2011) turvallisuusluokitellun tiedon käsittelyn tulee tapahtua kokonaisuudessaan Suomen lainsäädännön piirissä. Poikkeuksena kansainväliseen viranomaisyhteistyöhön liittyvät erityistapaukset, joissa muun muassa toimivalta- ja tarkastusvastuista on kyseisten maiden turvallisuusviranomaisten kesken erikseen sovittu, ja käsiteltävät tiedot on luovutettavissa kyseisen kansainvälisen viranomaisyhteisön jäsenmaille.

Katakri on laadittu työkaluksi normaaliolojen toimintaan, ja siinä ei käsitellä esimerkiksi poikkeusolojen edellyttämiä erillissuunnitelmia. Katakria voidaan tiedon omistavan viranomaisen erillishyväksyntään pohjautuen soveltaa myös normaalioloista poikkeaviin olosuhteisiin, esimerkiksi toimintaan viruspandemian tai sotilaallisen konfliktin olosuhteissa.

Osa-alue T: Turvallisuusjohtaminen

Turvallisuusjohtamisen osa-alueessa käsitellään niitä menetelmiä, joilla turvallisuus ja sen hallinta jalkautetaan osaksi koko organisaation toimintaa. Turvallisuusjohtamisen osa-alue kattaa hallinnollisen tietoturvallisuuden ja henkilöstöturvallisuuden. Turvallisuusjohtamisen vaatimuksilla pyritään siihen, että organisaatiolla on toimiva turvallisuuden hallintajärjestelmä sekä riittävät menettelyt sen varmistamiseksi, että viranomaisen turvallisuusluokiteltuja tietoja käsittelevä henkilöstö toimii asianmukaisesti.

Turvallisuusjohtamiseen liittyviä prosesseja tulee käsitellä kokonaisuuksina. Turvallisuuden hallintamenettelyt tulee suhteuttaa riskienarvioinnin perusteella suojattavaan tietoon ja kohdeorganisaation toimintaan.

Turvallisuusjohtamisen osa-alueen tarkoituksenmukainen käyttö edellyttää arvioinnin kohdentamista siihen osaan organisaatiosta, jolla on vaikutus turvallisuusluokitellun tiedon käsittelyyn. Tarkoituksenmukaisena kohdentamisena voi olla tietojenkäsittely-ympäristöä hallinnoiva organisaation osa, esimerkiksi tytäryhtiö tai vastaava. Erityisesti henkilöstöturvallisuuden vaatimusten arvioinnissa tulee huomioida, että riittävä toteutustapa voi vaihdella kohdekohtaisesti. Esimerkiksi turvallisuusluokan II tietojen käsittely-ympäristön henkilöstön ohjeistuksen sisältö eroaa yleensä merkittävästi koko organisaatiota koskevista yleisistä ohjeistuksista.

Organisaation tulee varmistaa, että turvallisuusluokiteltuja tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta.

Hyvään turvallisuusjohtamiseen kuuluu menettelytapojen ja erityisesti riskien arvioinnin dokumentointi. Turvallisuusjohtamiseen liittyvät suunnitelmat ja ohjeet sekä arvioinnin tulokset ja johtopäätökset tulisi esittää kirjallisena. Dokumentteihin kannattaa täydentää tiedot toimenpiteiden toteutumisesta. Toteutuneet toimenpiteet voivat osoittaa turvallisuusjohtamisen arvioinnin olleen tuloksekasta. Dokumentoinnilla tarkoitetaan kirjalliseen muotoon saatettavissa olevaa tallennetta, kuten Intranet-sivu ja toiminnanohjausjärjestelmän työmääräys (tiketti).

Hallinnollinen tietoturvallisuus

T-01 - Johdon tuki, ohjaus ja vastuu - Turvallisuusperiaatteet	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Organisaation johto vastaa, että a) organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan, b) turvallisuusperiaatteet ovat turvallisuusluokiteltujen tietojen suojaamisen kannalta kattavat ja tarkoituksenmukaiset, c) turvallisuusperiaatteet ohjaavat tietoturvallisuustoimenpiteitä, ja d) organisaatiossa on järjestetty riittävä valvonta turvallisuusluokiteltujen tietojen tiedonhallintaan liittyvien velvoitteiden ja ohjeiden noudattamisesta.	906/2019 4 § 1 ja 2 mom	9 artiklan 1 kohta
	Lisätietoja		
	Yleistä Johdon tuki, ohjaus ja vastuu ilmenevät sillä, että organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan. Tällä osoitetaan, että johto on sitoutunut organisaation turvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina, osana yleisiä toimintaperiaatteita, politiikkaa tai strategiaa. Hyväksytyt turvallisuusperiaatteet ovat turvallisuusluokiteltujen tietojen suojaamisen kannalta kattavat sekä tarkoituksenmukaiset ja ne ohjaavat tietoturvallisuustoimenpiteitä. Tietoturvallisuustoimenpiteiden toteutumista seurataan ja toteutumisesta raportoidaan ylimmälle johdolle säännöllisesti. Organisaation johdon on huolehdittava siitä, että organisaatiossa on järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Tiedonhallinnan ja turvallisuusluokiteltujen tietojen käsittelyn yleisestä valvonnasta vastaavat organisaation johto ja esimiehet. Valvontaa voidaan toteuttaa myös tietojärjestelmissä automaattisesti		

	erilaisten kontrollien avulla. Organisaatiossa tulisi olla kuvattuna, miten valvontavastuu on järjestetty johdolle ja esimiehille sekä miten valvonnan toimivuutta arvioidaan. *Muita lisätietoja* ISO/IEC 27002:2017 5.1.1; ISO/IEC 27001:2017 5.1; ISO/IEC 27001:2017 5.2; ISO/IEC 27001:2017 5.3; ISO/IEC 27001:2017 9.3; PiTuKri TJ-01; Tiedonhallintalautakunnan suositus 2020:18

T-02 - Turvallisuustyön tehtävien ja vastuiden määrittäminen	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Organisaatio on määritellyt tietoturvallisuuden hoitamisen tehtävät ja vastuut.	906/2019 4 § 2 mom	7 artiklan 5 kohta
	Lisätietoja		
	Yleistä Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. Turvallisuuteen liittyvät tehtävät ja vastuut tulee kirjata organisaation ja työntekijöiden työjärjestyksiin ja tehtävänkuvauksiin sekä toimintaohjeisiin. Organisaation johdon tehtävänä on määritellä turvallisuusluokitellun tiedon tiedonhallintaan liittyvät vastuut. Kysymys ei ole tiedonhallintavastuiden delegoinnista, vaan niiden määrittelystä. Vastuut tulisi määritellä erityisesti tietoturvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä tietoturvallisuuden kokonaisvastuussa olevista henkilöistä. *Toteutusesimerkki* 1) Organisaatio on määritellyt turvallisuuden toteuttamisen tehtävät ja vastuut ainakin seuraavilta osin: a) turvallisuusjohtaminen b) fyysinen turvallisuus c) tekninen tietoturvallisuus 2) Vastuumäärittely sisältää turvallisuusluokitellun tiedon käyttöympäristön omistajan sekä turvallisuuteen liittyvät vastuut.		

	3) Turvallisuusdokumentaation kattavuuden ja ajantasaisuuden säännöllinen seuranta on vastuutettu. Turvallisuusdokumentaatio kattaa turvallisuusluokiteltuun tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta, ja se on tarvittavien tahojen saatavilla. *Yritysturvallisuusselvityksissä huomioitavaa* Selvityksen kohteella tulee olla turvallisuusvastaava (Facility Security Officer, FSO). Turvallisuusvastaava on henkilö, jolla on riittävä turvallisuusosaaminen ja jonka yrityksen johto on nimittänyt vastaamaan yrityksen turvallisuusasioista turvallisuusluokiteltujen tietojen suojaamiseen liittyvissä kysymyksistä. Turvallisuusvastaava tekee yhteistyötä toimivaltaisten turvallisuusviranomaisten kanssa. Turvallisuusvastaava huolehtii, että selvityksen kohde toteuttaa edellytetyt tietoturvallisuustoimenpiteet. *Muita lisätietoja* ISO/IEC 27002:2017 6.1.1; ISO/IEC 27001:2017 5.1; ISO/IEC 27001:2017 5.2; ISO/IEC 27001:2017 5.3; PiTuKri TJ-02; Tiedonhallintalautakunnan suositus 2020:18

T-03 - Tietoturvallisuus-riskien hallinta	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Organisaatio on arvioinut olennaiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit ja mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.	906/2019 13§ 1mom, 1101/2019 6§-7§	5 artikla, IV liitteen kohdat 4-7 ja 12
	Lisätietoja		
	Tietoturvallisuusriskien hallinta tarkoittaa järjestelmällistä, koordinoitua ja jatkuvaa toimintaa, jonka avulla tunnistetaan, analysoidaan, arvioidaan, käsitellään ja seurataan tietoturvallisuusriskejä. Tietoturvallisuusriskien hallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista, riskien käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista. Katakrin perustana oleva turvallisuusmalli, sekä riskienhallinnan rooli Katakrin tuetuissa käyttötapauksissa on kuvattu liitteessä III. *Toteutusesimerkki* 1) Tietoturvallisuusriskien hallinta on osa organisaation toimintaa ja muuta riskienhallintaa.		

	2) Tietoturvallisuusriskien hallinnan avulla varmistetaan riittävien tietoturvallisuustoimenpiteiden toteuttaminen turvallisuusluokiteltujen tietojen suojaamiseksi. 3) Tietoturvallisuusriskien arvioinnissa ja - analysoinnissa käytetään yleisesti tunnettua, toiminnon näkökulmasta asianmukaista ja päätöstentekoon ymmärrettävää informaatiota tuottavaa menetelmää. 4) Tietoturvallisuusriskien hallintaan osallistuu riittävästi asiantuntijoita. 5) Tietoturvallisuusriskien hallinnassa on otettu huomioon sidosryhmistä ja toimitusketjuista aiheutuvat riskit. Vrt. turvallisuuskriittisten laitteistojen ja ohjelmistojen (vrt. I-01, I-12 ja I-13) toimitusketjuihin liittyvät riskit. 6) Tietoturvallisuusriskien arvioinnista ja analysoinnista saatuja tuloksia hyödynnetään turvallisuusluokiteltujen tietojen tietoturvallisuustoimenpiteiden suunnittelussa ja toteuttamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa sekä muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. 7) Tietoturvallisuustoimenpiteet on mitoitettu riskiperusteisesti ottaen huomioon muun muassa tiedon turvallisuusluokka, määrä, muoto, luokitteluperuste ja sijoitustilat suhteessa arvioituihin riskeihin. 8) Organisaatio on dokumentoinut keskeisiltä osin sovellettavat valvonta- ja turvatoimet ja niiden perusteena olevan riskienarvioinnin. *Muita lisätietoja* SFS-EN ISO/IEC 27001:2017 luku 6.1 ja luvut 8-10, SFS-EN ISO/IEC 27005:2018 luku 6, SFS ISO 31000:2018, VAHTI 22/2017; PiTuKri TJ-03; Tiedonhallintalautakunnan suositukset 2020:29 ja 2020:61.

T-04 - Turvallisuus-ohjeistus	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Organisaatiossa on ajantasaiset ohjeet turvallisuusluokiteltujen tietojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta sekä tietoturvallisuustoimenpiteistä. Ohjeet kattavat turvallisuusluokiteltaviin tietoihin liittyvät prosessit ja käsittely-ympäristöt tietojen koko elinkaaren ajalta.	906/2019 4 §, 13 §; 1101/2019 6 § ja 8 §	I liitteen 29-31 kohdat, IV liitteen 21-22 kohdat
	Lisätietoja		
	Yleistä: Dokumentoimalla turvallisuuden kannalta keskeiset asiat pyritään varmistumaan siitä, että toiminta ei ole henkilöriippuvaista. Vrt. dokumentaation rooli muutoksenhallinnassa ja poikkeamien havainnointikyvyssä (I-16).		

	Organisaation johdon on huolehdittava siitä, että organisaatiossa on ajantasaiset ohjeet tietojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta sekä tietoturvallisuustoimenpiteistä. Käytännössä johto määrittelee, miten ohjeiden ajantasaisuus varmistetaan ja mille toimijoille ohjeiden ajantasaisuudesta huolehtiminen kuuluu. Ohjeiden ajan tasalla pitäminen on suositeltavaa vastuuttaa niille toimijoille, jotka ovat kokonaisvastuussa tietoturvallisuudesta, tietojärjestelmistä, tietovarannoista, rekisterinpidosta, asiakirjapyyntöihin liittyvästä päätöksenteosta, asianhallinnasta ja arkistotoimesta. *Toteutusesimerkki* 1) Mikäli henkilö käsittelee turvallisuusluokiteltuja tietoja, hänelle on selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt. EU:n ja Naton turvallisuusluokiteltujen tietojen käsittely edellyttää, että henkilö antaa lisäksi tietojen suojaamista koskevan vakuutuksen. 2) Turvallisuusohjeistus toteutetaan henkilöstön työtehtävien tarpeet huomioiden. 3) Turvallisuusohjeiden kattavuutta ja ajantasaisuutta seurataan säännöllisesti ja se on tarvittavien tahojen saatavilla. *Muita lisätietoja:* ISO/IEC 27002:2017 7.2.2; ISO/IEC 27002:2017 5.1.1; ISO/IEC 27002:2017 5.1.2; ISO/IEC 27002:2017 12.1.1; ISO/IEC 27001:2017 7.5; VAHTI 4/2003; VAHTI 2/2008; PiTuKri HT-04; Tiedonhallintalautakunnan suositus 2020:18.

T-05 - Turvallisuustyön resurssit	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Organisaatiolla on käytössään riittävä asiantuntemus turvallisuusperiaatteiden varmistamiseksi.	906/2019 4 § 2 mom	IV liitteen 4 kohta
	Lisätietoja		
	Yleistä Riittävällä asiantuntemuksella pyritään varmistamaan, että turvallisuusperiaatteiden tarkoitus toteutuu ja toimet mitoitetaan suhteessa riskeihin. Resurssien riittävyyttä arvioidaan säännöllisesti. Yleisinä vaatimuksina voidaan pitää, että organisaatiolla tulee olla riittävästi henkilöitä, henkilöillä riittävästi osaamista turvallisuudesta, ajantasaiset ohjeet, turvallisuuskoulutusta, asianmukaiset työvälineet sekä turvallisuustoimenpiteiden toimeenpanon valvonta ja tarkastukset on järjestetty.		

	Toteutusesimerkki 1) Turvallisuustehtäviä hoitavilla on riittävä asiantuntemus sekä näistä on näyttöjä. 2) Turvallisuustyön resurssit, tehtävät, vastuut ja valtuudet on määritelty organisaation toimintaan, kokoon ja riskeihin nähden riittävän kattavasti. 3) Resurssit riittävät tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen. 4) Resurssien riittävyyttä arvioidaan säännöllisesti. *Muita lisätietoja* ISO/IEC 27001:2017 7.1; ISO/IEC 27001:2017 7.2; ISO/IEC 27001:2017 5.1

T-06 - Toimintahäiriöt ja poikkeustilanteet	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Organisaatiolla on määritetty ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta pienennettäisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen. a) Organisaatio on huomioinut turvallisuusluokiteltujen tietojen suojaamisen hätätilanteissa. b) Suojaustoimenpiteet ovat riittävät estämään luvattoman pääsyn tietoihin ja tietojen ilmitulon sekä turvaamaan niiden eheyden ja käytettävyyden. c) Turvallisuusluokitellut tiedot on suojattu teknisiltä ja fyysisiltä vahingoilta.	906/2019 15.1§	5 artiklan kohdat 3-4
	Lisätietoja		
	Yleistä Organisaatiolla tulee olla varmuus siitä, että käsiteltävä tieto tai järjestelmä on suojattu fyysisiltä vahingoilta kuten tulipalot, vesivahingot tai ilkivalta sekä sähköisiä menetelmiä käyttäen aiheutetuilta fyysisiltä vahingoilta kuten laitteiden rikkoutuminen. Tietoa tai järjestelmää tulee suojata asianmukaisin, mutta riskiarvioinnin perusteella tarkoituksenmukaisin toimin. Turvallisuusluokiteltujen tietojen elinkaaren kattavan suojauksen avainhenkilöt tulee tunnistaa. Organisaatiolla tulee olla kyky turvallisuusluokiteltujen tietojen suojaamiseen vaikka avainhenkilöt olisivat estyneitä.		

	Muita lisätietoja ISO/IEC 27002:2013 17.1.1; ISO/IEC 27002:2017 17.1.2; ISO/IEC 27002:2017 17.2.1; ISO/IEC 27002:2017 12.3.1; ISO/IEC 27002:2017 16.1.2; ISO/IEC 27002:2017 16.1.6; VAHTI 2/2009; VAHTI 2/2016; PiTuKri TJ-05; Tiedonhallintalautakunnan suositus 2020:61, luku 6

T-07 - Turvallisuus-poikkeamien hallinta	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Tapahtuneesta tai epäillystä kansainvälisen turvallisuusluokitellun tiedon vaarantaneesta poikkeamasta on ilmoitettava välittömästi toimivaltaiselle turvallisuusviranomaiselle. 2) Organisaatiolla on menettelytavat tietoturvallisuuspoikkeamien asianmukaiseen käsittelyyn. a) Organisaatiolla on ohjeistus ja menettely, jolla tapahtuneesta tai epäillystä turvallisuusluokitellun tiedon vaarantaneesta poikkeamasta saadaan välittömästi tieto organisaation sisällä. b) Organisaatio on määrittänyt, miten ja kenelle poikkeamista tai niiden epäilyistä tulee ilmoittaa. c) Organisaatio on selvittänyt millaiset tietoturvallisuuspoikkeamat edellyttävät viranomaisyhteydenottoa.	1) - 2) 906/2019 4 § 2 mom ja 13 §; 1101/2019 7 §	1) 5 artiklan 4 kohta, 14 artiklan 3 kohta 2) 5 artiklan 4 kohta, 14 artiklan 3 kohta
	Lisätietoja		
	Yleistä Turvallisuusluokiteltuihin tietoihin liittyvien tietoturvallisuuspoikkeamien hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa, odottamattomissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaaliksi. Tehokas poikkeamienhallinta edellyttää myös riittävää resursointia. Turvallisuusluokiteltujen tietojen katsotaan vaarantuneen, kun ne ovat tietoturvatapahtuman seurauksena paljastuneet tai voineet paljastua sivullisille henkilöille. Useat tiedon omistajat (esimerkiksi EU) sekä myös voimassa olevat		

	viranomaishyväksynnät edellyttävät välitöntä ilmoitusta turvallisuusluokitellun tiedon vaarantaneista poikkeamista tai niiden epäilyistä. *Toteutusesimerkki* Turvallisuuspoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu ja koulutettu, 3) dokumentoitu riittävällä tasolla, 4) harjoiteltu, ja erityisesti 5) viestintäkäytännöt ja vastuut on sovittu, sekä on 6) selvitetty, mitkä kansalliset ja kansainväliset säädökset tai organisaation tekemät sopimukset edellyttävät tietoturvapoikkeamista tai niiden epäilystä tiedottamista, ja mitkä ovat tarvittavat toimenpiteet. *Muita lisätietoja* ISO/IEC 27002:2017, luku 16; ISO/IEC 27002:2017 6.1.3; VAHTI 8/2017; PiTuKri TJ-04

T-08 - Tietojen luokittelu	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Tätä vaatimusta sovelletaan vain viranomaisen tietojenhallintaan: 1) Tiedot on luokiteltu lakisääteisten vaatimusten perusteella: a) Tietosisällöltään salassa pidettävät turvallisuusluokiteltavat aineistot ja asiakirjat (ml. luonnokset) varustetaan turvallisuusluokkaa kuvaavalla merkinnällä. b) Asiakirja merkitään asiakirjan osien (esim. liitteet) ylintä turvallisuusluokkaa vastaavalla merkinnällä. c) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi asiakirjasta.	906/2019 18 §; 1101/2019 3 §, 5 §	III liitteen 2, 6 ja 7 kohdat
	Lisätietoja		
	Yleistä		

	Luokittelun tavoitteena on tunnistaa ja mitoittaa turvatoimet tiedon suojaustarpeen perusteella. Luokituksen voi ilmaista eri tavoin riippuen tietoaineistosta, käsittely-ympäristöstä ja käyttäjistä. Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään selkeämmin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet. Tietojärjestelmän tai muun useita tietoaineistoja sisältävän kohteen luokitus määräytyy ensi sijassa korkeimman turvallisuusluokan aineiston mukaan. Mikäli turvallisuusluokiteltua tietoa on runsaasti, on arvioitava, onko kohteen turvallisuusluokka korkeampi. Viranomaisen lukuun tehtävien tai viranomaisilta saatujen turvallisuusluokiteltujen tietojen luokittelusta vastaa viranomainen. Merkintä voidaan tehdä myös viranomaisen toimeksiannosta. *Muita lisätietoja* Tiedonhallintalautakunnan suositus 2020:19; ISO/IEC 27002:2017 8.2.1; ISO/IEC 27002:2017 8.2.2; PiTuKri TJ-06

Henkilöstöturvallisuus

T-09 - Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä on huomioitu työsuhteen elinkaaren eri vaiheissa. Erityisesti tulee huomioida toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä.	906/2019 4 § 2 mom, 12 §, 16 §; 1101/2019 6 § ja 8 §	I liitteen 29 ja 31 kohdat
	Lisätietoja		
	Yleistä Menettelyjä työsuhteen alussa ja aikana ovat esimerkiksi henkilöturvallisuusselvitykset, käsittely-, käyttö- ja pääsyoikeudet, ymmärrys salassapito- ja vaitiolovelvollisuudesta, turvallisuuskoulutus sekä muutoksissa näiden mahdollinen päivittäminen ja muutosten kouluttaminen. Työsuhteen päättymiseen liittyviä menettelyjä ovat esimerkiksi avainten, tunnusten sekä turvallisuusluokiteltujen aineistojen ja materiaalien luovutus, sekä käsittely-, käyttö- ja pääsyoikeuksien poistaminen. Työsuhteen päättyessä on myös oleellista muistuttaa salassapito- ja vaitiolovelvollisuudesta. Edellä olevat toimenpiteet		

	edellyttävät tyypillisesti menettelyohjeita, jotka on koulutettu ja saatavilla tarvittavilla henkilöstöryhmillä. Menettelyohjeet voidaan jakaa esimerkiksi työsuhteen elinkaaren mukaisiin kokonaisuuksiin. Ohjekokonaisuuksia voivat olla esimerkiksi rekrytointiohjeet, perehdyttämisohjeet, työsuhteen aikaisten muutosten ohjeet, työsuhteen päättymisen ohjeet ja ohjeet yksityiskohtaisempiin toimiin kuten esimerkiksi ohjeet käsittely-, käyttö- ja pääsyoikeuksien muutoksiin. *Muita lisätietoja* ISO/IEC 27002:2017 7.1; ISO/IEC 27002:2017 7.2; ISO/IEC 27002:2017 7.3; PiTuKri HT-01

T-10 - Henkilöstön luotettavuuden arviointi	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Turvallisuusluokiteltuja tietoja käsittelevien henkilöiden luotettavuus selvitetään tarvittaessa hakemalla henkilöistä asianmukaisen laajuinen henkilöturvallisuusselvitys 2) Kansainvälisten tietoturvallisuusvelvoitteiden sitä edellyttäessä, henkilölle voidaan myöntää pääsy kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tai sitä korkeamman turvallisuusluokan kansainvälisiin tietoihin vasta sen jälkeen, kun hänelle on myönnetty asianmukaisen tason henkilöturvallisuusselvitystodistus (PSC).	906/2019 12 §	I liitteen 2c, 2b ja 29 kohdat
	Lisätietoja		
	Yleistä Viranomaisen on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Henkilöturvallisuusselvitystä hakee turvallisuusluokitellun tiedon omistava viranomainen. Selvitystä haetaan suojelupoliisilta, joka päättää sen tekemisestä. Selvitystä haetaan Pääesikunnalta, joka päättää sen tekemisestä, jos selvityksen kohteen (henkilö) on tarkoitus hoitaa puolustusvoimien antamaa tehtävää taikka jos selvitys liittyy puolustusvoimien toimintaan tai hankintoihin. Selvitys laaditaan suppeana, perusmuotoisena tai laajana riippuen käsiteltävästä turvallisuusluokitellusta tiedosta. Kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellista henkilöturvallisuusselvitystodistusta (PSC, Personnel Security Clearance) haetaan Ulkoministeriössä toimivalta Kansalliselta turvallisuusviranomaiselta (NSA, National Security		

	Authority). Esimerkiksi EU:n ja Naton turvallisuusluokiteltujen tietojen käsittely edellyttää turvallisuusluokasta III (CONFIDENTIAL) lähtien PSC:tä. *Muita lisätietoja* laki turvallisuusselvityksistä 726/2014; laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004, VNA asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019

T-11 - Salassapito- ja vaitiolovelvollisuus	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Turvallisuusluokiteltua tietoa käsitteleville henkilöille on selvitetty tietojen suojaamista koskevat tietoturvallisuusperiaatteet ja -toimenpiteet ja henkilö on antanut vakuutuksen tietojen suojaamista koskevasta vastuustaan. Salassapito- tai vaitiolositoumusmenettely on käytössä, kun turvallisuusluokiteltua tietoa käsittelee henkilö, jota virkavastuu ei koske.	1101/2019 6 § ja 8 §	I liitteen 2 ja 29 kohta
	Lisätietoja		
	ISO/IEC 27002:2017 7.1.2**;** ISO/IEC 27002:2017 13.2.4; PiTuKri HT-03		

T-12 - Turvallisuus-koulutus	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Johdon on huolehdittava siitä, että organisaatiossa on tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja organisaation lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä tietojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja organisaation ohjeista (vrt. T-04). 2) Turvallisuusluokiteltuun tietoon kohdistuvat uhat sekä ajantasaiset ohjeet (vrt. T-04) on koulutettu henkilöstölle. 3) Turvallisuusluokiteltavien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneista pidetään kirjaa.	906/2019 4 §, 13 §; 1101/2019 6 § ja 8 §	I liitteen 29-31 kohdat, IV liitteen 21-22 kohdat
	Lisätietoja		
	Yleistä:		

	Organisaation johdon on huolehdittava siitä, että organisaatiossa on tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja organisaation lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä tietojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja organisaation ohjeista. Käytännössä johdon on huolehdittava, että organisaation koulutussuunnitelmissa on otettu huomioon, miten organisaatiossa varmistetaan riittävä osaaminen turvallisuusluokiteltujen tietojen tiedonhallintaan, tietojenkäsittelyyn sekä turvallisuusluokiteltuihin tietoihin liittyvistä säädöksistä, määräyksistä ja ohjeista. Koulutus voi olla säännöllistä tai kehityskeskustelujen perusteella tarveperusteista. *Toteutusesimerkki* 1) Mikäli henkilö käsittelee turvallisuusluokiteltuja tietoja, hänelle on selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt. EU:n ja Naton turvallisuusluokiteltujen tietojen käsittely edellyttää, että henkilö antaa lisäksi tietojen suojaamista koskevan vakuutuksen. 2) Turvallisuuskoulutus toteutetaan henkilöstön työtehtävien tarpeet huomioiden. 3) Turvallisuuskoulutuksen sisältö dokumentoidaan. *Muita lisätietoja:* ISO/IEC 27002:2017 7.2.2; ISO/IEC 27002:2017 5.1.1; ISO/IEC 27002:2017 5.1.2; ISO/IEC 27002:2017 12.1.1; ISO/IEC 27001:2017 7.5; VAHTI 4/2003; VAHTI 2/2008; PiTuKri HT-04; Tiedonhallintalautakunnan suositus 2020:18

T-13 - Tiedonsaantitarve ja käsittely-oikeudet	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1. Organisaation on pidettävä ajantasaista luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan II tai III tietoja. 2. Luettelossa on mainittava henkilön tehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu. 3. Pääsy turvallisuusluokiteltuun tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty. 4. Organisaatiolla on menettely, jolla varmistetaan turvallisuusluokiteltujen tietojen käsittelyoikeuksien poistaminen tiedonsaantitarpeen päätyttyä.	906/2019 12 §, 16 §; 1101/2019 8 §, 11 § 1 mom 3 kohta	I liitteen kohdat 2a ja 3
	Lisätietoja		
	Yleistä: Tiedonsaantitarpeen määrittämistä helpottaa se, että organisaatio on kuvannut periaatteet, joilla organisaation henkilöt saavat pääsyn turvallisuusluokiteltuihin tietoihin. Lisäksi on kuvattava prosessi tai menettelytapaohjeet, joilla työtehtäväperusteisesti		

	pääsy myönnetään ja hallinnoidaan. Käsittelyoikeus-, työtehtävä- ja roolimäärittelyissä tulisi ottaa huomioon, ettei synny vaarallisia työ- tai rooliyhdistelmiä. *Muita lisätietoja:* ISO/IEC 27002:2017 9.1.1; ISO/IEC 27002:2017 9.1.2; ISO/IEC 27002:2017 6.1.2; VAHTI 2/2008; PiTuKri HT-05

Osa-alue F: Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten turvatoimien toteuttamista siten, että estetään luvaton pääsy turvallisuusluokiteltuihin tietoihin. Fyysisen turvallisuuden osa-aluetta (F) on mahdollista käyttää arvioitaessa kansallisen tai kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi toteutettuja fyysisen turvallisuuden toimenpiteitä (Vna 1101/2019, 9 §; KvTituL 588/2004, 10 §).

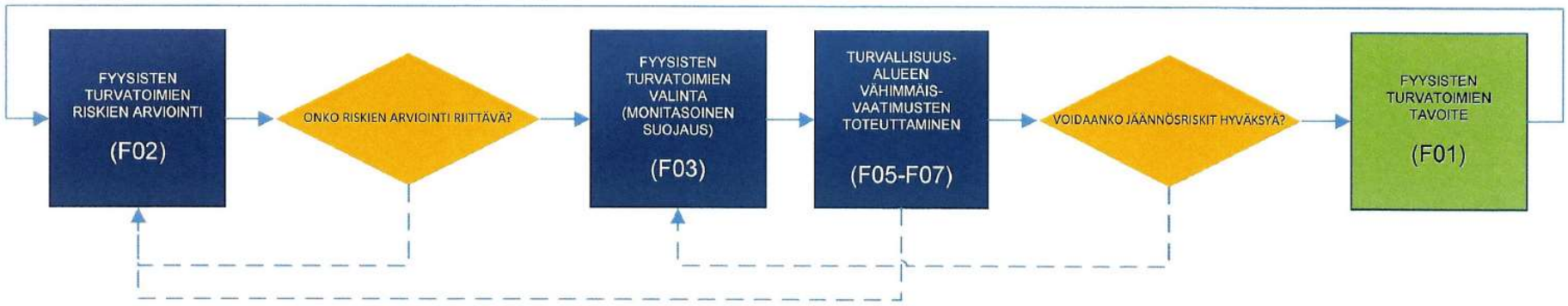
Viranomaisten tietoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia (L 906/2019, 15 §). Uusien toimitilojen osalta fyysisten turvallisuusvaatimusten ja niiden toiminnallisten eritelmien määrittelyn on oltava osa toimitilojen suunnittelua ja rakenteita. Jo olemassa olevien toimitilojen osalta fyysiset turvallisuusvaatimukset on pantava täytäntöön mahdollisimman täydellisesti. (2013/488/EU, II liite kohta 7.)

Turvallisuusluokiteltujen tietojen fyysiseksi suojaamiseksi on määritettävissä kahdentyyppisiä fyysisesti suojattuja turvallisuusalueita: hallinnollisia alueita ja turva-alueita (teknisesti suojatut turva-alueet mukaan luettuina). Fyysisten turvatoimien tavoite tulee täyttyä ennen, kun turvallisuusalueet voidaan hyväksyä. Fyysistä turvallisuutta koskeva riskien arviointi sekä turvallisuusalueiden yksittäisten turvatoimien ja koko monitasoisen suojauksen tehokkuus on arvioitava uudelleen säännöllisin väliajoin ja kunkin auditoinnin yhteydessä (2013/488/EU, II liite, kohta 11). Alueet, joilla säilytetään kansainvälisiä turvallisuusluokiteltuja tietoja, hyväksyy aina Ulkoministeriön NSA-yksikkö ja sen asiantuntijana toimiva Suojelupoliisi tai Pääesikunta (KvTituL 588/2004, 4 §; 2013/488/EU, 8. artikla). F-osa-alueen rakenne on suunniteltu siten, että turvallisuusalueita koskevat vähimmäisvaatimukset on koottu jokaiselle turvallisuusalueelle laadittuun omaan alalukuunsa. Tämän uudistetun rakenteen myötä auditoijan on mahdollista nähdä kaikki arvioitavana olevaa turvallisuusaluetta koskevat vähimmäisvaatimukset ja lisätiedot jäsennellysti yhdessä koossa siirtymättä eri vaatimusten välillä, koska alueiden vähimmäisvaatimukset ovat osin päällekkäisiä.

F-osa-alueen lopussa on auditoinnin suorittamiseen liittyvistä käytännön syistä myös paperimuodossa käsiteltäviä turvallisuusluokiteltuja tietoja koskeva tietoaineistoturvallisuuden osuus. Tietoaineistoturvallisuuden osuudessa käsitellään tiedon elinkaaren hallintaan liittyviä vaatimuksia. Turvallisuusluokitellun tiedon sähköistä käsittelyä koskevat tietoaineistoturvallisuuden vaatimukset on esitetty I-osa-alueessa.

F-osa-alueen tekstissä käytettävällä termillä ”viranomainen” viitataan luovutettavan ja auditoinnin perusteena olevan turvallisuusluokitellun tiedon omistajaan, jonka on turvallisuusluokitteluasetuksen (1101/2019, 6 §) mukaan ennakolta varmistuttava siitä, että auditoinnin kohteelle luovutettavien turvallisuusluokiteltujen tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti. Käytännössä termi ”viranomainen” tarkoittaa Katakria käyttävää auditoijaa. Viranomaisella tarkoitetaan kuitenkin Suojelupoliisia tai Pääesikuntaa, mikäli fyysisten turvatoimien tavoitteiden täyttymisen arviointi kuuluu osaksi niiden lakisääteisiä tehtäviä (KvTituL 588/2004, 4 §; 726/2014, 9 § & 39 §).

Edellä kuvattu fyysisten turvatoimien toteuttamis- ja arviointiprosessi on havainnollistettu alla olevassa kuviossa:



KUVIO: FYYSISTEN TURVATOIMIEN TOTEUTTAMIS- JA ARVIOINTIPROSESSI

Katakri 2020:n F-osa-alue on rakennettu yllä olevan prosessin mukaisesti eteneväksi:

Ensimmäisenä tulee tunnistaa kohdeorganisaatiossa käsiteltävä turvallisuusluokiteltu tieto ja arvioida fyysiseen turvallisuuteen liittyvät riskit (F-02). Auditoijan tulee arvioida kohteen riskien arvioinnin riittävyys ja tarvittaessa edellyttää riskien uudelleenarviointia. Riskien arvioinnin tulokset vaikuttavat tiedonhallintalain (906/2019, 13 §) mukaisesti siihen, mitkä fyysiset turvatoimet tulee valita ja toteuttaa (F-03). Vaatimukset F-05 - F-07 käsittelevät tietojen suojaamiseksi perustettavia turvallisuusalueita ja niiden vähimmäisvaatimuksia. Vähimmäisvaatimukset on johdettu suoraan Valtionvarainministeriön turvallisuusluokiteltavien asiakirjojen käsittelystä antamasta suosituksesta (2020:19), joka perustuu Valtioneuvoston asetukseen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Vähimmäisvaatimusten ja monitasoisen suojauksen toteuttamisen jälkeen auditoija arvioi fyysiset turvatoimet ja sen voidaanko jäännösriskit hyväksyä. Tarvittaessa monitasoista suojausta korjataan, kunnes auditoija hyväksyy jäännösriskit ja fyysisten turvatoimien tavoite (F-01) täyttyy. Riskien arviointi sekä yksittäisten turvatoimien ja koko monitasoisen suojauksen tehokkuus on arvioitava uudelleen säännöllisin väliajoin ja kunkin auditoinnin yhteydessä.

Yleiset vaatimukset

F-01 - Fyysisten turvatoimien tavoite

F-01 – Fyysisten turvatoimien tavoite	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	1) 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 tiedonsaantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella; c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet; ja d) estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä	1) 1101/2019 7 § ja 10 §; VM 2020:19, 12 ja 18	1) II liite, kohta 2
	Lisätietoja		
	Yleistä: Fyysisten turvatoimien tavoite tulee täyttyä ennen kuin turvallisuusalueet voidaan hyväksyä.		

F-02 - Fyysisten turvatoimien riskien arviointi

Fyysisten turvatoimien valinnan on perustuttava riskien arviointiin. Organisaation on sovellettava riskinhallintaprosessia turvallisuusluokiteltujen tietojen suojaamiseksi tiloissaan, jotta varmistetaan, että fyysiset turvatoimet (F-03 - F-07) vastaavat arvioituja riskejä, jäännösriskit voidaan hyväksyä ja valitut turvatoimet täyttävät tavoitteet (F-01). Riskien arvioinnissa tulee huomioida sekä tiedon haltijan että viranomaisen näkemys riskeistä ja valittujen turvatoimien riittävyydestä ja viranomaisen on hyväksyttävä fyysisiin turvatoimiin liittyvä jäännösriski. Organisaation tulee pystyä osoittamaan perustelut valituille turvatoimille. Riskienhallinnan roolia Katakrin tuetuissa käyttötapauksissa on käsitelty myös liitteessä III.

F-02 - Fyysisten turvatoimien riskien arviointi	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	1) Tietojenkäsittelyyn kohdistuvat olennaiset riskit on selvitettävä ja fyysiset turvatoimet (F-03) on mitoitettava riskien arvioinnin	1) 906/2019 13 § 1 mom;	1) II liite, kohta 3

	mukaisesti 2) Riskien arvioinnissa on otettava huomioon kaikki asiaan kuuluvat tekijät, erityisesti seuraavat: a) Turvallisuusluokiteltujen tietojen turvallisuusluokka ja salassapitoperuste; b) Turvallisuusluokiteltujen tietojen käsittely- ja säilytystapa sekä määrä ottaen huomioon, että tietojen suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista; c) Turvallisuusluokiteltujen tietojen käsittely- ja säilytysaika d) Turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan (turvallisuusalue) ympäristö: rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa; e) Hälytystilanteisiin liittyvä vasteaika f) Ulkoistetut toiminnot, kuten huolto-, siivous-, kiinteistö- ja turvallisuuspalvelut g) Tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille Mikäli kyseessä on kansainvälinen turvallisuusluokiteltu tieto, fyysisten turvatoimien valinnan ja riskien arvioinnin on perustuttava Suojelupoliisin tai Pääesikunnan tekemään uhka-arvioon	VM 2020:19, 12 ja 18 2) VM 2020:19, 12 ja 18 3) -	2) II liite, kohta 3 II liite, kohta 3
	Lisätietoja		
	Yleistä: Arvioitaessa fyysisiin turvatoimiin liittyviä riskejä, tulee ottaa huomioon esimerkiksi pääsyoikeuksien hallintaan ja muihin turvallisuusjärjestelyihin liittyviin prosesseihin sisällytettävät tiedonsaantitarpeen, tehtävien eriyttämisen ja vähimpien oikeuksien periaatteet. Fyysisiä turvatoimia koskevan riskien arvioinnin tulee olla säännöllistä ja osa organisaation riskienhallinnan kokonaisuutta. Arvioiduilla riskeillä on nimetyt omistajat. Hyväksyttyjen fyysisten turvatoimien muutoksiin liittyvät riskit tulee arvioida muutosten yhteydessä. Erityisesti korvaavien fyysisten turvatoimien osalta tulee pystyä osoittamaan perustelut valituille turvatoimille.		

F-03 - Fyysisten turvatoimien valinta (monitasoinen suojaus)

Fyysiseen turvallisuuteen liittyvän riskien arvioinnin (F-02) tulokset vaikuttavat siihen, mitkä fyysiset turvatoimet tulee toteuttaa monitasoisen suojauksen periaatetta noudattaen (F-03) vähimmäisvaatimusten (F-05 - F-07) lisäksi, jotta fyysisten turvatoimien tavoite (F-01) täyttyy. Turvatoimien tarpeellisuus tulee arvioida turvallisuusaluekohtaisesti, joten kaikkia fyysisiä turvatoimia ei sovelleta kaikissa tilanteissa ja kaikilla turvallisuusalueilla. Turvatoimien arviointi on kokonaisuus, johon kuuluvat esimerkiksi päätelaitteiden sekä laite- ja ristikytkentätilojen fyysisen turvallisuuden huomioiminen.

Monitasoisella suojauksella tarkoitetaan sitä, että toteutetaan joukko toisiaan täydentäviä turvatoimia. Mikäli mahdollista, turvallisuusalueet ja muut niitä mahdollisesti ympäröivät tilat muodostavat keskenään sisäkkäisiä vyöhykkeitä, joissa turva-alueet ovat sisimpänä. Esimerkki monitasoisesta suojauksesta: Fyysiset turvatoimet on toteutettu siten, että hälytystilanteissa mahdollinen tunkeutuja havaitaan jo kiinteistön tai rakennuksen ulkorajalla, jolloin vartiointihenkilöstö aloittaa siirtymisen turvallisuusalueille estääkseen tunkeutumisen. Turvallisuusalueet ja niitä ympäröivät tilat hidastavat tunkeutumista ja yhdessä vartiointihenkilöstön kanssa estävät tunkeutumisen. Normaalitilanteissa tilojen vyöhykkeistäminen ja tiedonsaantitarpeeseen perustuva pääsyoikeuksien rajaaminen estävät oikeudettoman pääsyn turvallisuusalueille ja tietoon niiltä organisaation omilta työntekijöiltä, joilla ei ole kyseiseen tietoon tiedonsaantitarvetta. Lisäksi turvallisuusjärjestelmät tallentavat erilaisia tietoja mahdollisten laittomien toimien tutkimiseksi.

F-03 - Fyysisten turvatoimien valinta (monitasoinen suojaus)	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Turvallisuusalueilla ja niitä ympäröivissä tiloissa on toteutettava turvallisuusalueen suojausta vaarantavia tekoja ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä, toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä vaarantanutta tekoa edeltäneen turvallisuustason palauttamiseksi viipymättä 2) 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: a) rakenteelliset esteet: fyysinen este, jolla turvallisuusalueet ja sitä ympäröivät tilat rajataan ja luvatonta tunkeutumista vaikeutetaan ja hidastetaan; b) kulunvalvonta: kulunvalvonnalla rajataan pääsyä	1) 1101/2019 7 § 2) VM 2020:19, 13 ja 19 3) VM 2020:19, 23	1) – 2) II liite, kohta 4 3) II liite, kohta 10

	turvallisuusalueille ja sitä ympäröiviin tiloihin. Tavoitteena havaita luvattomat pääsy-yritykset, estää asiattomien henkilöiden 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, vastaanottovirkailija tai oma henkilöstö voi osallistua valvontaan. c) tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä). Järjestelmää voidaan käyttää myös vartiointihenkilöstön tekemän valvonnan asemasta tai tueksi. d) vartiointihenkilöstö: koulutettua, valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää muun muassa kulunvalvonnan tukena sekä turvallisuusalueelle tai sitä ympäröivien tilojen tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemisessa ja toimien estämisessä. e) kameravalvonta: kameravalvontaa voidaan käyttää turvallisuusalueella ilmenevien poikkeamien ennalta ehkäisemisessä, hälytysten todentamisessa sekä tapahtuneiden poikkeamien selvittämisessä. Vartiointihenkilöstö voi käyttää kameravalvontaa reaaliaikaisena, aktiivisena kuvan tarkkailuna tai jälkikäteen passiivisena kuvamateriaalin analysointina. f) 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. g) valaistus: mahdollinen tunkeutuja voidaan havaita valaistuksen avulla ja vartiointihenkilöstö voi valvoa aluetta tehokkaasti, joko suoraan tai h) kameravalvontajärjestelmää hyödyntämällä.		

	i) muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on estää ja havaita luvaton pääsy tai ehkäistä turvallisuusluokiteltujen tietojen katoaminen tai vahingoittuminen. 3) Laitteet on tarkastettava ja huollettava säännöllisin väliajoin.			
	Lisätietoja			
	Yleistä: Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitelty standardeja, joita voidaan käyttää vähimmäisvaatimusten referenssinä. Oikean standardiluokan valinta perustuu aina riskiarvioon, mutta ”yleinen suositus”-sarakkeessa on esitetty useimpiin monitasoisen suojauksen ratkaisuihin riittävä standardin mukainen luokka tai ohje.			
	Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
	Kassakaapit	SFS-EN 1143-1	I – V	II, tarvittaessa huomioitava paloluokitus Riskiarvioinnin edellyttäessä, kassakaappi valvotaan sensoreilla ja kassakaappi ankkuroidaan lattiaan. Kassakaappia ei saa sijoittaa ulkoseinää vasten.
	Elementtiholvit	SFS-EN 1143-1	I – XII	II, Holvia ympäröivässä tilassa tulee olla tunkeutumisenilmaisu tai holvi tulee olla valvottu sensoreilla
	Paperisilppurit	DIN 32757 (vanha)	DIN 1 – DIN 6	DIN 4
		DIN 66399 (uusi)	P1 – P7	P5 – P6
	Lukot heloineen	SFS 7020 (+SFS 5970)	1 – 4	3-4
	Elektroniset kulunvalvontajärjestelmät	SFS-EN 60839-11-1 SFS-EN 60839-11-2	1 – 4	huomioitava esimerkiksi SFS-EN 50131-standardin vaatimukset, mikäli

				kulunvalvontajärjestelmä on osa tunkeutumisen ilmaisujärjestelmää
	Kameravalvontajärjestelmät	SFS-EN 62676	-	Suunnittelu Finanssialan K-menetelmän mukaisesti Kamerat on sijoitettava siten, että turvallisuusluokiteltua tietoa ei siirry kameran välityksellä. Kameravalvontatieto on tallennettava (3 kk) ja liitettävä tunkeutumisen ilmaisujärjestelmään
	Seinät, ovet sekä lattia- ja kattorakenteet	SFS-EN 1627	RC1 – RC6	RC3
	Ikkunat (suojauslasi)	SFS-EN 356	P6B – P8B	P6B
	Tunkeutumisen ilmaisujärjestelmät	SFS-EN 50131	1 – 4	3
	Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto	SFS-EN 50136-1	DP1 - DP4 ja SP5 - SP6	DP3-DP4 (dual path) tai SP5-SP6 (single path)
	Vartioimisliikkeen hälytyskeskus	SFS-EN 50518	-	Liikkeen on oltava standardin mukaisesti pätevä ja lisäksi ylläpidettävä SFS-EN ISO 9001:n mukaista sertifioitua laadunhallintajärjestelmää tai liikkeen tulee olla arvioitu soveltuvin osin tätä standardia vastaavaksi

	Arvioitaessa laitteita ja järjestelmiä on varmistettava, että ne ovat toimintakuntoisia ja soveltuvia niiden käyttötarkoitukseen. Laitteiden ja järjestelmien vastaanottotarkastuksista, käytön aikaisista tarkastuksista ja tehdyistä huolloista tulisi olla nähtävissä dokumentaatio. Järjestelmäoikeuksia arvioitaessa tulisi kiinnittää huomiota vähimpien oikeuksien periaatteen toteutumiseen. Laitteiden ja järjestelmien sijoitustilan tulisi sijaita niiden suojaamalla turvallisuusalueella. Laitteiden ja järjestelmien ja niiden sijoitustilojen asennus-, tarkastus-, huolto- ja siivoustoimet toteutetaan vain alueelle itsenäisen pääsyoikeuden saaneen henkilön toimesta tai valvonnassa.

F-04 - Tiedon käsittely ja säilytys

Turvallisuusluokiteltuja tietoja on kaikissa tilanteissa käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin estetään sivullisilta. Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen tietoon että laittomalta tiedustelulta. Suojaaminen tarkoittaa käytännössä esimerkiksi suoran näkö- tai kuuloyhteyden estämistä turvallisuusluokiteltuun tietoon sekä tiedon tai tietoa sisältävän päätelaitteen riittävän turvallista säilyttämistä. Tietojen käsittelyssä on huomioitava lisäksi toiminta työskentelytaukojen aikana, jolloin paperiasiakirjat ja päätelaitteet on turvallisuusluokan perusteella sijoitettava soveltuvalle turvallisuusalueelle ja/tai säilytysyksikköön tauon ajaksi.

Turvallisuusluokiteltujen tietojen käsittely ja säilytys turvallisuusalueilla (F-05 - F-07) on pääsääntö, mutta on tilanteita – kuten etätyö tai satunnaiset työtehtävät turvallisuusalueiden ulkopuolella – jolloin tietoa joudutaan käsittelemään myös määritettyjen turvallisuusalueiden ulkopuolella.

Katakrissa käytettävällä termillä "päätelaite" tarkoitetaan tietojärjestelmää tai sen osaa, jota henkilö käyttää työtehtäviensä hoitamiseen liittyvään sähköiseen tietojenkäsittelyyn.

F-04 - Tiedon käsittely ja säilytys turvallisuus-alueilla ja niiden ulkopuolella	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Kansallisia turvallisuusluokiteltuja tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. 2) Kansainvälisiä turvallisuusluokiteltuja tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta.	1) 1101/2019 10 §; VM 2020:19, 26-30 2) -	1) - 2) II liite, kohdat 23-28
	Lisätietoja		
	Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon käsittelyn ja säilytyksen reunaehdot on kuvattu alla olevissa taulukoissa.		
	KANSALLISEN TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY JA SÄILYTYS		
		KÄSITTELY	**SÄILYTYS**

	TURVALLISUUSLUOKKA	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue	Turva-alue	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue	Turva-alue
	TL II SALAINEN	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Ei Päätelaitteessa: Ei	Paperiasiakirjat: Ei Päätelaitteessa: Ei	Paperiasiakirjat: Kyllä, soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa
	TL III LUOTTAMUKSELLINEN	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Ei Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: Ei Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: Kyllä, soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa
	TL IV KÄYTTÖ RAJOITETTU	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Ei Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa	Paperiasiakirjat: Kyllä, soveltuvassa lukitussa toimistokalusteessa	Paperiasiakirjat: Kyllä, soveltuvassa lukitussa toimistokalusteessa

		Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	ja lisäehtojen täyttyessä*	Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa	Päätelaitteessa: Kyllä, vaatimukset täyttävässä laitteessa
	Lisäehdot: * Tietoja voi säilyttää vaatimukset täyttävässä päätelaitteessa, mikäli päätelaitetta säilytetään: a) valvotussa tilassa (ks. F-05.5) tai b) soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla.						
	KANSAINVÄLISEN TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY JA SÄILYTYS						
	TURVALLISUUS-LUOKKA	**KÄSITTELY**			**SÄILYTYS**		
		Turvallisuus-alueiden ulkopuolella	**Hallinnollinen alue**	**Turva-alue**	**Turvallisuus-alueiden ulkopuolella**	**Hallinnollinen alue**	**Turva-alue**
	II SECRET	Kyllä, jos tietojen haltija noudattaa lisäehtoja*	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Ei	Ei	Kyllä, kassakaapissa tai holvissa
	III CONFIDENTIAL	Kyllä, jos tietojen haltija noudattaa lisäehtoja*	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Ei	Ei	Kyllä, kassakaapissa tai holvissa
	IV RESTRICTED	Kyllä, jos noudatetaan lisäehtoja**	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Kyllä, jos pääsy tietoihin on suojattu sivullisilta	Kyllä, tilapäisesti, jos tietojen haltija noudattaa lisäehtoja***	Kyllä, soveltuvassa lukitussa toimistokalusteessa	Kyllä, soveltuvassa lukitussa toimistokalusteessa

	LISÄEHDOT: *** Kansainvälisten turvallisuusluokkien II (SECRET) ja III (CONFIDENTIAL) tiedon käsittely turvallisuusalueiden ulkopuolella** On mahdollista, jos tiedon käsittelijä: - kuljettaa tietoja F-08.1 mukaisesti - on sitoutunut noudattamaan Suojelupoliisin tai Pääesikunnan antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy tietoihin on suojattu sivullisilta - pitää tiedot kaikkina aikoina henkilökohtaisessa valvonnassaan; ja - on ilmoittanut asiasta asiaankuuluvalle kirjaamolle, jos kyseessä on paperimuodossa oleva tieto **** Kansainvälisen turvallisuusluokan IV (RESTRICTED) tiedon käsittely turvallisuusalueiden ulkopuolella** On mahdollista, jos tiedon käsittelijä: - kuljettaa tietoja F-08.1 mukaisesti - on sitoutunut noudattamaan Suojelupoliisin tai Pääesikunnan antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy tietoihin on suojattu sivullisilta ***** Kansainvälisen turvallisuusluokan IV (RESTRICTED) tiedon säilytys turvallisuusalueiden ulkopuolella** On mahdollista, jos tiedon käsittelijä: - on sitoutunut noudattamaan Suojelupoliisin tai Pääesikunnan antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä Naton turvallisuusluokiteltuja tietoja koskevat alue- ja käsittelyvaatimukset on varmistettava tapauskohtaisesti toimivaltaiselta viranomaiselta.
	<u>Turvallisuusluokitelluista tiedoista keskusteleminen turvallisuusalueilla ja niiden ulkopuolella</u>: Tiedoista keskusteleminen on mahdollista turvallisuusalueilla ja niiden ulkopuolella, jos estetään, että sivulliset eivät pääse kuulemaan henkilöiden turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta. <u>TEMPEST-riskien arviointi:</u> Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös I-14-kohdassa käsiteltävä TEMPEST-riski, jota voidaan yleensä pienentää muuttamalla tiedon käsittelypaikan sijaintia kiinteistössä. Arvioidaan lisäksi tarve EMP- ja HPM-suojaukselle.

Turvallisuusalueiden vaatimukset

F-05 - Hallinnollinen alue

Hallinnollisella alueella tarkoitetaan normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta. Turvallisuusluokitellun tiedon omistaja varmistaa, että niihin on itsenäinen pääsy ainoastaan ennalta valtuutetuilla henkilöillä.

Hallinnollisen alueen tulee täyttää tässä osiossa esitetyt vähimmäisvaatimukset. Vähimmäisvaatimusten lisäksi tulee suunnitella, vastuuttaa, toteuttaa ja ylläpitää riskien arviointiin (F-02) ja monitasoiseen suojausperiaatteeseen (F-03) perustuvat muut riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä ja turvatoimien tavoitteet (F-01) saavutetaan.

<table>
<tr><td rowspan="4">F-05.1 - alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)</td><td>Vaatimus</td><td>Lähde (906/2019 ja/tai 1101/2019)</td><td>Lähde (2013/488/EU)</td></tr>
<tr><td>Alueella on oltava selkeästi määritelty näkyvä raja. Aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia</td><td>1101/2019 9 § 1 mom 1 kohta; VM 2020:19, 15</td><td>II liite, kohta 14</td></tr>
<tr><td colspan="3">Lisätietoja</td></tr>
<tr><td colspan="3"><u>Yleistä:</u>
Alueen rakenne voi olla normaalia toimistorakennetta. Aluetta rajaavia rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Näitä vahvennuksia tulee arvioida suhteessa alueen ympäröivien tilojen antamaan muuhun suojaan sekä vartiointihenkilöstön vasteaikaan.

Alueen aukot, jotka eivät ole käytössä kulkemiseen, on voitava lukita tai sulkea, jotta alueelle kulkua voidaan hallinnoida asianmukaisesti. Mikäli hallinnollisen alueen rajoilla on käytetty mekaanista lukkoa, lukon avainten kopiointi tulisi olla estetty patenttisuojalla.

Mikäli mahdollista, hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Tämä on otettava huomioon erityisesti uudisrakentamisessa.

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät ratkaisut ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardeja, joita voidaan käyttää referenssinä arvioitaessa aluetta rajaavia rakenteita:</td></tr>
</table>

Kohde	Referenssistandardi	Standardin luokat	Yleinen suositus
Seinät ja ovet sekä lattia- ja	SFS-EN 1627	RC1 – RC6	-

	kattorakenteet			
	Ikkunat (suojauslasi)	SFS-EN 356	P6B – P8B	-

F-05.2 - pääsyoikeuksien myöntäminen	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Ainoastaan viranomaisen asianmukaisesti valtuuttamilla henkilöillä on itsenäinen pääsy alueelle. Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainhallinnan menettelyt ja roolit.	1101/2019 9 §; VM 2020:19, 15	II liite, kohdat 14 ja 30

Lisätietoja

Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen.

Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien ja avainhallinnan menettelyistä.

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.
- avaimen luovutusperuste kirjataan dokumenttiin.
- avaimet voidaan luovuttaa vain kulkuoikeuden omaavalle henkilölle.
- Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa avainten hallintaoikeuteen.

Alueelle pääsyä tulee valvoa, mikäli se on riskien arvioinnin perusteella tarkoituksenmukaista. Kulunvalvonta voi olla tarkoituksenmukaista esimerkiksi, jos alueella käsitellään turvallisuusluokan III tai korkeampaa tietoa. Suositus kulunvalvonnan toteuttamisesta:

- Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita.
    - Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi.
    - Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle.
    - Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin
    - Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu

Hallinnollisen alueen vara-avaimia säilytetään turvallisesti ja suljettuna sinetöityyn, sulkemispäiväyksellä ja kuittauksella

varustettuun säilytyskuoreen. Vaihtoehtoisesti avaimia voidaan säilyttää kulunvalvontaan liitetyssä avainkaapissa. Avaimet luovutetaan työtehtävään liittyen ja kuittausta vastaan. Menettely on kuvattu turvallisuuden hallintaohjeissa. Hallinnolliselle alueelle ei saa päästä alemman luokan tilaan sopivalla yleisavaimella.

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua:

Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
Lukot heloineen	SFS 7020 (+SFS 5970)	1 – 4	3-4
Elektroniset kulunvalvontajärjestelmät	SFS-EN 60839-11-1 SFS-EN 60839-11-2	1 – 4	huomioitava esimerkiksi SFS-EN 50131-standardin vaatimukset, mikäli kulunvalvontajärjestelmä on osa tunkeutumisen ilmaisujärjestelmää

F-05.3 - Vierailijat	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	Muilla kuin viranomaisen asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina oltava saattaja.	1101/2019 9 §; VM 2020:19, 15	II liite, kohta 14
	Lisätietoja		
	Toteutusesimerkki: Viranomaisen on täytynyt hyväksyä menettelyohje vierailijoita varten. Vieraiden isännällä tulee olla itsenäinen pääsyoikeus turvallisuusalueelle, jolle hän vie vieraat sekä oikeus isännöidä vieraita. Viranomaisen hyväksymä vierailijaohje voi käsitellä muun muassa seuraavia asioita: - Vieras tunnistetaan ja varustetaan vieraskortilla. - Vierailu kirjataan. - Vierailijoita ei päästetä tai jätetä turvallisuusalueille 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. - Henkilökunta on ohjeistettu reagoimaan ilman tunnistetta liikkuviin henkilöihin. Alueella tehtävät huoltotoimenpiteet tapahtuvat vain alueelle itsenäisen pääsyoikeuden saaneen henkilön toimesta tai valvonnassa. Turvallisuusluokitellun tiedon käsittely alueella on huolto-, asennus- ja siivoustoimien aikana kielletty, jos on vaara, että edellä mainittuja toimenpiteitä suorittava henkilöstö saa tiedon turvallisuusluokitellusta tiedosta.

F-05.4 - Äänieristys	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	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.	VM 2020:19, 15	-
	Lisätietoja		
	Yleistä: Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta. Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista. Äänieristystä voidaan arvioida esimerkiksi kuuntelemalla keskustelua tilan ulkopuolelta ovien, seinien sekä ilmastointiputkien ja muiden läpivientien kohdalta. Tilan äänieristystä voidaan myös tarvittaessa verrata rakenteille annettavaan ilmaääneneristävyysvaatimukseen (40dB). Ilmaääneneristävyysvaatimus ei kuitenkaan sellaisenaan saa ohjata äänieristyksen arviointia. Äänieristysvaatimus voidaan tarvittaessa saavuttaa esimerkiksi tilan uudelleen sijoittelulla, rakenteiden ja läpivientien eristävyyden parantamisella tai arvioitavan tilan ulkopuolisten tilojen taustamelulla.		

	Vaatimus	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**

<table>
<tr><td rowspan="3">F-05.5 - Tunkeutumisen ilmaisujärjestelmät</td><td>Ei vaatimuksia.</td><td>VM 2020:19, 16</td><td>-</td></tr>
<tr><td colspan="3">Lisätietoja</td></tr>
<tr><td colspan="3">
<u>Yleistä:</u>
Alue ja sinne johtavat ovet voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa lukittavassa toimistokaapissa ja murtoriski arvioidaan todennäköiseksi.

Alue tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen mahdollista tunkeutumisen ilmaisujärjestelmää tai korvaavaa järjestelyä arvioitaessa tulee ottaa huomioon alueen rakenteita koskevan vaatimuksen yhteydessä käsitelty vasteaika-arvio. Mikäli alue on valvottu tunkeutumisen ilmaisujärjestelmällä, alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä.

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua:
<table>
<tr><th>Laitteet ja järjestelmät</th><th>Referenssistandardi</th><th>Standardin luokat</th><th>Yleinen suositus</th></tr>
<tr><td>Tunkeutumisen ilmaisujärjestelmät</td><td>SFS-EN 50131</td><td>1 – 4</td><td>2</td></tr>
<tr><td>Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto</td><td>SFS-EN 50136-1</td><td>DP1 - DP4
ja
SP5 - SP6</td><td>DP3-DP4 (dual path) tai SP5-SP6 (single path)</td></tr>
<tr><td>Vartioimisliikkeen hälytyskeskus</td><td>SFS-EN 50518</td><td>-</td><td>Liikkeen on oltava standardin mukaisesti pätevä ja lisäksi ylläpidettävä SFS-EN ISO 9001:n mukaista sertifioitua laadunhallintajärjestelmää tai liikkeen tulee olla arvioitu soveltuvin osin tätä standardia vastaavaksi</td></tr>
</table>
</td></tr>
</table>

F-05.6 - Salaa katselun estäminen	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu huomioon ottaen, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.	VM 2020:19, 16	II liite, kohta 6
	Lisätietoja		
	Yleistä: Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.		

F-05.7 - Tila- ja laitetarkastukset (ainoastaan TL II / EU-S)	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	1) Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella hallinnollisella alueella, jossa käsitellään turvallisuusluokan II tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. 2) Myös alue on tarvittaessa tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta.	1) VM 2020:19, 16 2) VM 2020:19, 16	1) II liite, kohta 18 2) II liite, kohta 17 c
	Lisätietoja		
	Yleistä: Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista tai hyväksyntää ei voida todentaa (esim. matkapuhelimet, älykellot, jne.), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun Katso kohta F-07 - Teknisesti suojattu turva-alue.		

	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)

F-05.8 - Tiedon käsittely ja säilyttäminen	1) Alueella voi säilyttää turvallisuusluokan IV tietoa. Tiedot tulee säilyttää soveltuvassa lukitussa toimistokalusteessa. Tietoja sisältävä päätelaite tulee säilyttää soveltuvassa lukitussa toimistokalusteessa, mikäli mahdollista. 2) Alueella voi säilyttää kansallista turvallisuusluokan III tietoa kyseisen turvallisuusluokan vaatimukset täyttävässä päätelaitteessa, mikäli päätelaitetta säilytetään: a) valvotussa tilassa tai b) soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla. Mahdollinen tilan valvonta tulee toteuttaa F-05.5-vaatimuksen mukaisesti. Poiketen kansallisen turvallisuusluokitellun tiedon säilyttämissäännöistä, kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tietoa ei voi säilyttää hallinnollisella alueella. 3) Soveltuvien lukittujen toimistokalusteiden avaimet tai pääsykoodit ovat sellaisten henkilöiden hallussa, joilla on tiedonsaantitarve säilytysyksikössä säilytettävään tietoon. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien toimistokalusteiden numeroyhdistelmät on vaihdettava: a) uuden turvallisen säilytyspaikan vastaanoton yhteydessä b) aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos. c) aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen. d) kun jokin lukoista on huollettu tai korjattu. e) vähintään 12 kuukauden välein. 4) Alueella voi käsitellä turvallisuusluokkien IV-II tietoa, jos pääsy tietoihin on suojattu sivullisilta. Päätelaitteessa olevan turvallisuusluokitellun tiedon käsittelyssä tulee lisäksi huolehtia, että päätelaite ja tietoliikennejärjestelyt täyttävät niihin kohdistuvat vaatimukset.	1) 1101/2019 10 § 3 mom 4 kohta; VM 2020:19, 16 2) 1101/2019 10 § 4 mom; VM 2020:19, 28-29 3) - 4) 1101/2019 10 § 4 mom; VM 2020:19, 26-28	1) II liite, kohta 24 2) II liite, kohta 26 3) II liite, kohta 31 4) II liite, kohta 25
	Lisätietoja		
	Yleistä:		

	Tietojen käsittelyssä on huomioitava esimerkiksi toiminta työskentelytaukojen aikana, jolloin paperimuodossa olevat tiedot sekä ja päätelaitteet on turvallisuusluokan perusteella tarvittaessa sijoitettava turva-alueelle ja/tai soveltuvaan säilytysyksikköön tauon ajaksi. Erityisesti päätelaitteen eheyden (koskemattomuuden) vaarantuminen tulee pystyä estämään tai vähintään luotettavasti havaitsemaan tilanteissa, joissa kansallisen turvallisuusluokan III tiedon käsittelyyn käytettyä päätelaitetta joudutaan tilapäisesti säilyttämään hallinnollisella alueella. Mikäli turvallisuusluokitellun tiedon säilytysyksikkönä käytetään lukittua toimistokalustetta, on varmistuttava siitä, että tunkeutumisesta jää murtojälki. Tiedoista keskusteleminen on mahdollista, jos estetään, että sivulliset eivät pääse kuulemaan henkilöiden turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta. TEMPEST-riskien arviointi: - Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös Katakri:n I-14-kohdassa käsiteltävä TEMPEST-riski, jota voidaan yleensä pienentää muuttamalla tiedon käsittelypaikan sijaintia kiinteistössä. Arvioidaan lisäksi tarve EMP ja HPM-suojaukselle.

F-06 - Turva-alue

Turva-alueella tarkoitetaan viranomaisen työskentelyyn tarkoitettuja, hallinnollista aluetta paremmin suojattuja alueita ja tiloja, joissa turvallisuusluokiteltuja tietoja käsitellään ja säilytetään. Turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.

Turva-alueen tulee täyttää tässä osiossa esitetyt vähimmäisvaatimukset. Vähimmäisvaatimusten lisäksi tulee suunnitella, vastuuttaa, toteuttaa ja ylläpitää riskien arviointiin (F-02) ja monitasoiseen suojausperiaatteeseen (F-03) perustuvat muut riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä ja turvatoimien tavoitteet (F-01) saavutetaan.

F-06.1 - Alueen raja ja rakenteet	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**

(seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)	1) Alueella on oltava selkeästi määritelty näkyvä raja. 2) Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso.	1) 1101/2019 9 § 1 mom 2 kohta; VM 2020:19, 21 2) VM 2020:19, 21	1) II liite, kohta 15 2) II liite, kohta 22

Lisätietoja

Yleistä:

Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita tai sulkea kalteroinnilla tai vahvoilla terässäleiköillä, jotta alueelle kulkua on mahdollista hallinnoida luotettavasti. Aukot on valvottava tunkeutumisen ilmaisujärjestelmällä, mikäli alueella ei ole henkilöstöä palveluksessa vuorokauden ympäri tai tiloja ei tarkasteta normaalin työajan päätteeksi ja satunnaisiin aikoihin työajan ulkopuolella.

Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen rajan ja rakenteiden olisi tällöin oltava betonia, terästä, tiiltä tai vahvaa puuta. Puutteelliset rakenteet, kuten normaali toimistorakenne on vahvennettava. Seinäelementtejä ei saa voida irrottaa kokonaisina tilan ulkopuolelta. Näitä vahvennuksia tulee arvioida suhteessa alueen ympäröivien tilojen antamaan muuhun suojaan sekä vartiointihenkilöstön vasteaikaan. Ovien rakenteita tarkastettaessa on kiinnitettävä huomiota karmin rakenteeseen, oven ja karmin välykseen, sekä karmien kiinnitykseen seinärakenteeseen.

Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, tulisi alueen seinien, lattian, katon, ikkunoiden ja ovien täytettävä vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja. Lisäksi myös tiedon erillisen säilytystilan kuoren rakenteen tulee täyttää vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja.

Hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Tämä on otettava huomioon erityisesti uudisrakentamisessa. Mikäli hätäpoistumistien on välttämätöntä kulkea turva-alueen kautta, tulee varmistua, että hätäpoistumistie on varustettu tunkeutumisen ilmaisujärjestelmällä. Turva-aluetta jonka läpi kulkee hätäpoistumistie ei voida hyväksyä, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua.

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät ratkaisut ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardi, jota voidaan käyttää referenssinä arvioitaessa aluetta rajaavia rakenteita:

Kohde	Referenssistandardi	Standardin luokat	Yleinen suositus

	Seinät ja ovet sekä lattia- ja kattorakenteet	SFS-EN 1627	RC1 – RC6	RC 3
	Ikkunat (suojauslasi)	SFS-EN 356	P6B – P8B	P6B

F-06.2 - Kulunvalvonta	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti.	1101/2019 9 § 1 mom 2 kohta; VM 2020:19, 21	II liite, kohta 15
	Lisätietoja		
	Yleistä: Kulunvalvonta voidaan toteuttaa joko elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueen rajalla voidaan käyttää kaksipuoleista kulunvalvontaa. Tarvittaessa käytetään kaksoistunnistusta sisään ja/tai ulos mentäessä. *Toteutusesimerkki:* Suositus kulunvalvonnan toteuttamisesta: • Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita. • Turva-alueen kulkuoikeudet myöntää nimetty vastuuhenkilö organisaatiossa • Kulunvalvonnan hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu: o Myönnetyistä kulkuoikeuksista laaditaan dokumentti ja sitä ylläpitää nimetty vastuuhenkilö. o Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi. o Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle. o Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin. o Organisaatioon kuuluvan henkilöstön ja ulkopuolisten henkilöiden luettelot pidetään erillään. o Kulkuoikeudet katselmoidaan säännöllisin väliajoin esimerkiksi 6kk:n välein organisaatiosta nimetyn vastuuhenkilön toimesta. o Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu, jos se on hyvin hallinnoitu o Peruskäyttäjän työasemalta tapahtuva oven avaus turva-alueelle pitää olla estetty • Turva-alueelle kulkuoikeus on vain alueelle oikeutetulla henkilöllä. Kulku alueelle pitää olla myöhemmin todennettavissa. • Kulku tilaan pitää olla myöhemmin todennettavissa. • Tunnisteiden tulee käyttää nykyaikaista ja salattua lukutekniikkaa tai organisaation tulee järjestää tunnisteidenhallinta		

organisaation turvallisuusohjeiden mukaisesti.

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardi, jota voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua:

Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
Elektroniset kulunvalvontajärjestelmät	SFS-EN 60839-11-1 SFS-EN 60839-11-2	1 – 4	huomioitava esimerkiksi SFS-EN 50131-standardin vaatimukset, mikäli kulunvalvontajärjestelmä on osa tunkeutumisen ilmaisujärjestelmää

F-06.3 - Pääsyoikeuksien myöntäminen	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	1) Itsenäinen pääsyoikeus alueelle voidaan myöntää vain viranomaisen asianmukaisesti valtuuttamalle henkilölle, jonka luotettavuus on varmistettu ja jolla on erityinen lupa tulla alueelle. 2) Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainten hallinnan menettelyt ja roolit 3) Mikäli turva-alueella käsitellään ja säilytetään kansainvälistä turvallisuusluokiteltua tietoa, itsenäinen pääsyoikeus alueelle voidaan myöntää vain viranomaisen asianmukaisesti valtuuttamalle henkilölle, jolla on voimassaoleva kansainvälinen henkilöturvallisuusselvitys (PSC) ja erityinen lupa tulla alueelle tiedonsaantitarpeensa perusteella	1) 1101/2019 9 § 1 mom 2 kohta; VM 2020:19, 21 2) VM 2020:19, 21 3) -	1) - 2) II liite, kohta30 3) II liite, kohta 15
	Lisätietoja		
	Yleistä: 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.

Toteutusesimerkki:
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.
- avaimen luovutusperuste kirjataan dokumenttiin.
- avaimet voidaan luovuttaa vain kulkuoikeuden omaavalle henkilölle.
- Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa avainten hallintaoikeuteen.

Turva-alueen vara-avaimia säilytetään soveltuvassa säilytysyksikössä ja suljettuna sinetöityyn, sulkemispäiväyksellä ja kuittauksella varustettuun säilytyskuoreen. Vaihtoehtoisesti avaimia voidaan säilyttää kulunvalvontaan liitetyssä avainkaapissa. Avaimet luovutetaan työtehtävään liittyen ja kuittausta vastaan. Menettely on kuvattu turvallisuuden hallintaohjeissa. Turva-alueelle ei saa päästä alemman luokan tilaan sopivalla yleisavaimella.

Vartiointi-, kiinteistönhoito- ja huoltohenkilöstölle jaettavat turva-alueen avaimet tulee olla sinetöitynä poikkeuksellisien tilanteiden hoitamista varten. Hälytystilanteessa alueelle voidaan edellyttää saapuvan kaksi henkilöä samanaikaisesti, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardi, jota voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua:

Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
Lukot heloineen	SFS 7020 (+SFS 5970)	1 – 4	3-4

F-06.4 - Vierailijat	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	1) Muilla kuin niillä henkilöillä, joille on myönnetty itsenäinen pääsyoikeus tilaan (vierailijoilla) on aina oltava saattaja. 2) Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia: a) alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka on ilmoitettava selkeästi; b) kaikilla vierailijoilla on oltava erityinen lupa tulla alueelle, heillä on aina oltava saattaja ja heidän luotettavuutensa on oltava varmistettu asianmukaisesti, paitsi jos on varmistettu, ettei vierailijoilla ole pääsyä turvallisuusluokiteltuihin tietoihin.	1) 1101/2019 9 § 1 mom 2 kohta; VM 2020:19, 22 2) VM 2020:19, 22	1) II liite, kohta 15 2) II liite, kohta 16
	Lisätietoja		
	Toteutusesimerkki: Viranomaisen on täytynyt hyväksyä menettelyohje vierailijoita varten. Vieraiden isännällä tulee olla itsenäinen pääsyoikeus turvallisuusalueelle, jolle hän vie vieraat sekä oikeus isännöidä vieraita. Vieraan tuominen alueelle edellyttää ennakkoilmoitusta ja alueen turvallisuudesta vastaavan hyväksyntää. Viranomaisen hyväksymä vierailijaohje voi käsitellä muun muassa seuraavia asioita: - Vieras tunnistetaan ja varustetaan vieraskortilla. - Vierailu kirjataan. - Vierailijoita ei päästetä tai jätetä turvallisuusalueille 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. - Henkilökunta on ohjeistettu reagoimaan ilman tunnistetta liikkuviin henkilöihin. Alueella tehtävät huoltotoimenpiteet tapahtuvat vain alueelle itsenäisen pääsyoikeuden saaneen henkilön toimesta tai valvonnassa.		

	Turvallisuusluokitellun tiedon käsittely alueella on huolto-, asennus- ja siivoustoimien aikana kielletty, jos on vaara, että edellä mainittuja toimenpiteitä suorittava henkilöstö saa tiedon turvallisuusluokitellusta tiedosta.

F-06.5 - Turvallisuusohjeet	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista asioista: a) turvallisuusluokka tiedoille, joita alueella voidaan käsitellä ja säilyttää. b) sovellettavat valvonta- ja suojatoimenpiteet. c) henkilöt, joilla on pääsy alueelle ilman saattajaa erityisen luvan ja luotettavuuden varmistamisen perusteella d) tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle e) muut asiaan kuuluvat toimenpiteet ja menettelyt.	1) VM 2020:19, 22	1) II liite, kohta 21
	Lisätietoja		
	Yleistä: Turvallisuusohjeet kattavat turvallisuusluokiteltuun tietoon liittyvät prosessit ja turvallisuusalueet koko tiedon elinkaaren ajalta (ks. F-08). Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti. Turvallisuusohjeiden ajantasaisuus sekä jalkautuminen varmistetaan säännöllisesti, vähintään vuosittain.		

F-06.6 - Äänieristys	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	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.	VM 2020:19, 22	-
	Lisätietoja		
	Yleistä: Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta.		

	Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista. Äänieristystä voidaan arvioida esimerkiksi kuuntelemalla keskustelua tilan ulkopuolelta ovien, seinien sekä ilmastointiputkien ja muiden läpivientien kohdalta. Tilan äänieristystä voidaan myös tarvittaessa verrata rakenteille annettavaan ilmaääneneristävyysvaatimukseen (40dB). Ilmaääneneristävyysvaatimus ei kuitenkaan sellaisenaan saa ohjata äänieristyksen arviointia. Äänieristysvaatimus voidaan tarvittaessa saavuttaa esimerkiksi tilan uudelleen sijoittelulla, rakenteiden ja läpivientien eristävyyden parantamisella tai arvioitavan tilan ulkopuolisten tilojen taustamelulla.

F-06.7 - Tunkeutumisen ilmaisujärjestelmät	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	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).	VM 2020:19, 23	II liite, kohta 19
	Lisätietoja		
	Yleistä: Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet) ja/tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi. Alueen mahdollista tunkeutumisen ilmaisujärjestelmää tai korvaavaa järjestelyä arvioitaessa tulee ottaa huomioon alueen rakenteita koskevan vaatimuksen yhteydessä käsitelty vasteaika-arvio. Mikäli alue on valvottu tunkeutumisen ilmaisujärjestelmällä, alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä. Ilmoituksensiirto tulisi toteuttaa valvottuna tai kahdennettuna yhteytenä. Ilmoituksensiirtolaitteen avulla tulee siirtää vartioimisliikkeelle tai muuhun turvallisuusvalvomoon vähintään seuraavat tiedot: murto, päälle/pois, sabotaasi, vika. Järjestelmää tulee operoida henkilökohtaisen koodin avulla. Alueen tunkeutumisen ilmaisujärjestelmän hallinta tulee olla organisaation omassa hallinnassa. Järjestelmän hallintaan, sen antamiin hälytyksiin ja vastetoimintaan liittyvät menettelyt tulee arvioida. Ilmoituksensiirron (1krt/kk) ja vasteajan (1krt/v) testaus tulee olla säännöllistä ja dokumentoitua. Vartiointihenkilöstön tulee olla kohdekoulutettu alueella toimimiseen. Hälytystilanteessa alueelle voidaan edellyttää saapuvan kaksi henkilöä samanaikaisesti, mikäli turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin		

turvallisuusluokiteltuihin tietoihin tai alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa ratkaisua:

Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
Tunkeutumisen ilmaisujärjestelmät	SFS-EN 50131	1 – 4	3
Tunkeutumisen ilmaisujärjestelmän ilmoituksensiirto	SFS-EN 50136-1	DP1 - DP4 ja SP5 - SP6	DP3-DP4 (dual path) tai SP5-SP6 (single path)
Vartioimisliikkeen hälytyskeskus	SFS-EN 50518	-	Liikkeen on oltava standardin mukaisesti pätevä ja lisäksi ylläpidettävä SFS-EN ISO 9001:n mukaista sertifioitua laadunhallintajärjestelmää tai liikkeen tulee olla arvioitu soveltuvin osin tätä standardia vastaavaksi

F-06.8 - Salaa katselun estäminen	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu huomioon ottaen, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.	VM 2020:19, 23	II liite, kohta 6
	Lisätietoja		
	Yleistä: Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.		

F-06.9 - Tila- ja laitetarkastukset (ainoastaan TL II / EU-S)	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella turva-alueella, jossa käsitellään turvallisuusluokan II tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. 2) Myös alue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta.	1) VM 2020:19, 23 2) VM 2020:19, 23	1) II liite, kohta 18 2) II liite, kohta 17 c
	Lisätietoja		
	Yleistä: Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista tai hyväksyntää ei voida todentaa (matkapuhelimet ja älykellot yms.), laitteet tulee jättää tilan ulkopuolelle Katso kohta F-07 - Teknisesti suojattu turva-alue		

F-06.10 - Tiedon käsittely ja säilyttäminen	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Alueella voi säilyttää kaikkiin turvallisuusluokkiin kuuluvia tietoja riskien arviointiin ja fyysisten turvatoimien valintaan perusten. 2) Turvallisuusluokan III ja sitä korkeamman turvallisuusluokan tietoja tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa. Myös päätelaite tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa, mikäli mahdollista. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen	1) 1101/2019 10 § 2) VM 2020:19, 24 3) VM 2020:19, 21 ja 24 4) VM 2020:19, 24 5) 1101/2019 10 §	1) II liite, kohdat 24, 26 ja 28 2) II liite, kohta 26 3) II liite, kohta 31 4) II liite kohta 28 5) II liite kohdat 23, 25 ja 27

	säilytyksen edellyttämä turvallisuustaso. 3) Säilytysyksikön avaimet tai pääsykoodit ovat sellaisten henkilöiden hallussa, joilla on tiedonsaantitarve säilytysyksikössä säilytettävään tietoon. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien säilytysyksiköiden numeroyhdistelmät on vaihdettava: a) uuden turvallisen säilytyspaikan vastaanoton yhteydessä b) aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos. c) aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen. d) kun jokin lukoista on huollettu tai korjattu. e) vähintään 12 kuukauden välein. 4) Alueella voi käsitellä kaikkiin turvallisuusluokkiin kuuluvia tietoja, jos pääsy turvallisuusluokiteltuihin tietoihin estetään sivullisilta		
	Lisätietoja *Yleistä:* Tietojen käsittelyssä on huomioitava esimerkiksi toiminta työskentelytaukojen aikana, jolloin paperimuotoiset tiedot sekä päätelaitteet on tarvittaessa sijoitettava soveltuvaan säilytysyksikköön tauon ajaksi. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, tulisi alueen seinien, lattian, katon, ikkunoiden ja ovien täytettävä vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja. Lisäksi myös tiedon erillisen säilytystilan kuoren rakenteen tulee täyttää vähintään standardin SFS-EN-1627 luokkaa RC3 vastaava suoja. Mikäli turvallisuusluokitellun tiedon säilytysyksikkönä käytetään lukittua toimistokalustetta, on varmistuttava siitä, että tunkeutumisesta jää murtojälki. Tiedoista keskusteleminen on mahdollista, jos estetään, että sivulliset henkilöt eivät pääse kuulemaan henkilöiden turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta.		

TEMPEST-riskien arviointi:

- Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös Katakri:n I-14-kohdassa käsiteltävä TEMPEST-riski, jota voidaan yleensä pienentää muuttamalla tiedon käsittelypaikan sijaintia kiinteistössä. Arvioidaan lisäksi tarve EMP ja HPM-suojaukselle.

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa säilytysratkaisua:

Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
Kassakaapit	SFS-EN 1143-1	I – V	II, tarvittaessa huomioitava paloluokitus Riskiarvioinnin edellyttäessä, kassakaappi valvotaan sensoreilla ja kassakaappi ankkuroidaan lattiaan. Kassakaappia ei saa sijoittaa ulkoseinää vasten.
Elementtiholvit	SFS-EN 1143-1	I – XII	II, Holvia ympäröivässä tilassa tulee olla tunkeutumisenilmaisu tai holvi tulee olla valvottu sensoreilla

F-07 - Teknisesti suojattu turva-alue

Teknisesti suojattua turva-aluetta ei ole määritelty kansallisesti (1101/2019, 9 §), mutta alue on osa Euroopan neuvoston ja Naton turvallisuussääntöjen määrittelemiä turva-alueita. Alue voidaan perustaa EU:n ja Naton turvallisuusluokiteltujen tietojen suojaamiseksi.

Alueet, joilla käsitellään tai säilytetään kansainvälistä turvallisuusluokiteltua tietoa ja joiden on erityisesti tunnistettu tarvitsevan suojausta salaa kuuntelulta (audio eavesdropping), on määriteltävä teknisesti suojatuiksi turva-alueiksi. Organisaation tulee määritellä teknisesti suojattu turva-alue, mikäli se järjestää turvallisuusluokkien EU SECRET / NATO SECRET tietoihin liittyviä kokouksia tai keskustelee tiedoista säännöllisesti toimitiloissaan.

F-07 - Teknisesti suojattu turva-alue	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Teknisesti suojattuihin turva-alueisiin sovelletaan turva-alueen vähimmäisvaatimusten (F-06) lisäksi seuraavia vaatimuksia: a) alueilla on oltava tunkeutumisen ilmaisujärjestelmä (murtohälytysjärjestelmä), alueet on pidettävä lukittuina silloin, kun niitä ei käytetä, ja niitä on vartioitava silloin, kun ne ovat käytössä. b) kaikkien henkilöiden kulkua ja materiaalien tuontia alueelle on valvottava; c) alueet on tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin Suojelupoliisin tai Pääesikunnan vaatimusten mukaisesti. Tällaiset tarkastukset on suoritettava myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn johdosta; ja d) Alueella saa olla ainoastaan kyseiselle alueelle hyväksyttyjä tietoliikenneyhteyksiä, puhelimia, muita viestintävälineitä tai elektronisia laitteita. 2) Kaikki viestintä-, sähkö- tai elektroniset laitteet on tarkastettava, ennen kuin niitä käytetään alueilla, joilla pidetään EU SECRET / NATO SECRET -turvallisuusluokan tietoihin liittyviä kokouksia tai tehdään tällaisiin tietoihin liittyvää työtä, silloin kun EU:n tai Naton	1) - 2) - 3) -	1) II liite, kohta 17 2) II liite, kohta 18 3) II liite, kohdat 3 ja 13

	turvallisuusluokiteltuihin tietoihin kohdistuva uhka arvioidaan korkeaksi, ja näin varmistettava, ettei niillä voi tahattomasti eikä laittomasti välittää ymmärrettävässä muodossa olevia tietoja turva-alueen rajojen ulkopuolelle. 3) Suojelupoliisi tai Pääesikunta päättää teknisesti suojattuun turva-alueeseen liittyvästä uhka-arvioinnista, riskien hallintatoimenpiteistä ja mahdollisen tilapäisesti perustettavan teknisesti suojatun turva-alueen turvallisuusjärjestelyjen hyväksynnästä tapauskohtaisesti.		
	Lisätietoja		
	Yleistä: Teknisesti suojattu turva-alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten. Alueella tulee olla lista kyseiselle alueelle hyväksytyistä tietoliikenneyhteyksistä, puhelimista, muista viestintävälineistä tai elektronisista laitteista		

Tietoaineistoturvallisuuden vaatimukset

F-08 - Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden osiossa on kuvattu vaatimukset turvallisuusluokiteltujen tietojen paperimuodossa tapahtuvaan käsittelyyn tiedon elinkaaren eri vaiheissa. Mikäli turvallisuusluokiteltujen paperimuodossa olevien tietojen kirjaamiseen, tulostamiseen, kopioimiseen tai tuhoamiseen käytetään tietojärjestelmiä (esimerkiksi monitoimilaite), tulee tietojärjestelmän turvallisuus arvioida I-osa-alueen vaatimusten mukaisesti.

F-08.1 - Tietojen välitys postilla ja kuriirilla	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Turvallisuusluokitellut tiedot tulee kuljettaa viranomaisen ohjeita noudattaen.	1) 906/2019 4 § 2) 1101/2019 13 § 3) 1101/2019 13 §	1) 9 artiklan 4 kohta 2) III liite, kohdat 32 ja 37

	2) Turvallisuusluokitellut tiedot on pakattava niin, että ne on suojattu luvattomalta ilmitulolta. 3) Turvallisuusluokiteltuja tietoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet viranomaisen hyväksymällä salauksella. 4) Turvallisuusluokan IV salaamattomia tietoja voidaan kuljettaa postipalvelujen tai kaupallisten kuriiripalvelujen välityksellä. 5) Turvallisuusluokan II-III salaamaton tieto on kuljettamista varten pakattava asianmukaisesti sekä kuljetettava se jatkuvan valvonnan alaisuudessa vastaanottajalle. Mainitun tiedon saa kuljettaa vastaanottajalle myös muulla viranomaisen hyväksymällä turvallisella tavalla, jolla tiedon luottamuksellisuus ja eheys varmistetaan kyseiselle turvallisuusluokalle riittävällä tavalla. 6) Kansainvälisiä turvallisuusluokiteltuja tietoja koskevat vaatimukset varmistettava tapauskohtaisesti toimivaltaiselta viranomaiselta.	4) 1101/2019 13 § 5) 1101/2019 13 § 6) -	3) 9 artiklan 4 kohta 4) III liite, kohdat 34 ja 40 5) - 6) III liite, luku V
	Lisätietoja		
	Yleistä: Osaa kansainvälisistä tai kansallisista turvallisuusluokitelluista tiedoista ei välitetä koskaan postin välityksellä, hyväksyttävät menettelyt tulee varmistaa viranomaiselta tapauskohtaisesti. Tarvittavia ohjeita antaa kansallinen turvallisuusviranomainen. Mikäli käytetään tiedon turvallisuusluokalle hyväksyttyä salausta (vrt. I-12), voidaan ko. turvallisuusluokan ympäristössä salattu ja tietovälineelle (esim. CD-ROM) siirretty salattu tieto toimittaa sekä Suomen sisällä, että ulkomaille vapaavalintaisella (posti, kaupallinen kuriiri, henkilökuriiri, sotilaskuriiri tai vast.) menettelyllä. *Toteutusesimerkki:* Turvallisuusluokan IV tiedoille vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:		

	1) Tieto pakataan suljettavaan kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuoren tai vastaavan on oltava läpinäkymätön). 2) Tieto toimitetaan kotimaassa tavallisena postina, kirjattuna kirjeenä tai viranomaisen ko. turvallisuusluokalle hyväksymän kuriirimenettelyn mukaisesti. Ulkomaille toimitus postin välityksellä vain viranomaisen erillishyväksyntään pohjautuen. 3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä. 4) Organisaatiossa on tunnistettu vaatimukset ja toteutettu menettelyt erityissuojattavien tietojen (esimerkiksi salausavaimet) välittämiseksi. Turvallisuusluokkien III tiedoille vaatimus voidaan täyttää siten, että kohdan 4 lisäksi toteutetaan seuraavat toimenpiteet: 5) Tieto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä). 6) Tieto toimitetaan ko. turvallisuusluokiteltuun tietoon oikeutetun organisaation henkilön toimesta jatkuvan valvonnan alaisuudessa vastaanottajalle. Vaihtoehtoisesti toimitus viranomaisen ko. turvallisuusluokalle hyväksymän kuriirimenettelyn mukaisesti. 7) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä turvallisuusselvitettyä henkilöstöä. Turvallisuusluokan II tiedoille vaatimus voidaan täyttää siten, että kohtien 4, 6 ja 7 lisäksi toteutetaan seuraavat toimenpiteet: 8) Tieto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää turvallisuusluokasta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän turvallisuusluokiteltua tietoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä). Sisäkuoren on oltava sinetöity. Vastaanottaja on ohjeistettava tarkistamaan sinetöinnin eheys ja ilmoitettava välittömästi, mikäli eheyden vaarantumista epäillään.

F-08.2 - Turvallisuus-luokiteltujen tietojen jäljentäminen	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Jäljennöksiin ja käännöksiin sovelletaan alkuperäistä tietoa koskevia turvatoimia. <u>*Turvallisuusluokka II*</u> Kohdan 1 lisäksi 2) Turvallisuusluokan II tietojen kopiot ja niiden käsittelijät on luetteloitava.	1) 1101/2019 2 § 2 mom 2) 1101/2019 14 § 1 mom 4 kohta 3) 1101/2019 14 § 1 mom 3 kohta 4) -	1) III liite, kohta 27 2) - 3) - 4) III liite, kohta 26

	3) Turvallisuusluokan II tietojen kopiointia varten on hankittava tiedon laatineen viranomaisen lupa. 4) Kansainvälisiä turvallisuusluokiteltuja tietoja saa jäljentää ja kääntää tiedon haltijan pyynnöstä, mikäli tiedon luovuttaja ei ole sitä kieltänyt.		
	Lisätietoja		
	Yleistä: Tulostimet ja kopiokoneet tulkitaan tietojärjestelmiksi ja niiden tulisi siten täyttää ko. turvallisuusluokan vaatimukset sekä teknisen, fyysisen että hallinnollisen tietoturvallisuuden osalta. *Toteutusesimerkki:* Turvallisuusluokkien III-IV tiedoille vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Kopioita käsitellään kuten alkuperäistä tietoa. 2) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus tietoon ja tarve tietosisältöön. 3) Kopion/tulosteen saa ottaa vain ko. turvallisuusluokan vaatimukset täyttävällä laitteella. Turvallisuusluokan II tiedoille vaatimus voidaan täyttää siten, että kohtien 1-3 lisäksi toteutetaan seuraava toimenpide: 4) Kopiointi ja käsittelijät merkitään diaariin/rekisteriin tai luetteloidaan jollakin muulla vastaavalla menettelyllä.		

F-08.3 - Turvallisuus-luokiteltujen tietojen kirjaaminen	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Kansainvälisiä turvallisuusluokiteltavia tietoja käsittelevien organisaatioiden on määriteltävä vastaava kirjaamo. Kirjaamo on määritettävä turva-alueeksi. 2) Kansallisten turvallisuusluokkien II-III ja kansainvälisen turvallisuusluokan III (CONFIDENTIAL) tai sitä korkeamman luokan tiedon vastaanottaminen ja lähettäminen tulee kirjata. 3) Turvallisuusluokan III tietojen ja niitä korkeamman tason tietojen käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi). 4) Kansainvälisten turvallisuusluokan III (CONFIDENTIAL) tieto ja sitä korkeamman tason tieto tulee kirjata sille tarkoitetussa kirjaamossa.	1) - 2) 1101/2019 14 § 1 mom 2 kohta 3) 1101/2019 14 § 1 mom 1 kohta 4) -	1) III liite, kohta 17 2) 9 artiklan 2 kohta 3) 9 artiklan 2 kohta 4) 9 artiklan 2 kohta; III liite, 19 kohta

	Lisätietoja
	Yleistä: Kirjaamisella tarkoitetaan sellaisten menettelyjen soveltamista, joilla rekisteröidään tiedon elinkaari, mukaan lukien sen jakelu ja hävittäminen. Jos kyseessä on tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa järjestelmän omien prosessien avulla. Tiedon elinkaaren rekisteröinnin käytännön toteutukset edellyttävät tyypillisesti muun muassa tapahtumien jäljitettävyydestä varmistumista.

F-08.4 - Ei-sähköisten tietojen tuhoaminen	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
	1) Säilytysajan päättymisen jälkeen turvallisuusluokiteltavat tiedot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla. *Turvallisuusluokka II* Kohdan 1 lisäksi 2) Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle. 3) Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö. 4) Kansainvälisen turvallisuusluokitellun tiedon tuhoamisen osalta sekä kirjaajan että todistajan, jos jälkimmäisen läsnäoloa vaaditaan, on allekirjoitettava tuhoamistodistus, joka tallennetaan kirjaamoon. Kirjaamon on säilytettävä kansainvälisten turvallisuusluokkien III (CONFIDENTIAL) ja II (SECRET) tietojen tuhoamistodistukset vähintään viiden vuoden ajan. 5) Kansainvälisen turvallisuusluokan II (SECRET) tiedon tuhoaminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään tuhottavan tiedon turvallisuusluokkaa vastaava henkilöturvallisuusselvitys (PSC).	1) 906/2019 21 § 2 mom, 1101/2019 15 § 2) 1101/2019 15 § 2 mom 3) 1101/2019 15 § 2 mom 4) - 5) - 6) -	1) III liite, kohta 46 2) - 3) - 4) III liite, kohta 45 5) III liite, kohta 44 6) III liite, kohta 43

	6) Kansainvälisen turvallisuusluokan III (CONFIDENTIAL) ja sitä korkeamman tason tiedot on tuhottava niistä vastaavassa kirjaamossa niiden haltijan tai toimivaltaisen viranomaisen määräyksestä. Kirjaustiedot on päivitettävä vastaavasti.		

Lisätietoja

Yleistä:

Ei-sähköisten tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.

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

Suosituksena on, että monitasoisen suojauksen kokonaisuuteen sisältyvät laitteet ja järjestelmät ovat eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia. Alla olevassa taulukossa on esitetty standardeja, joita voidaan käyttää referenssinä arvioitaessa soveltuvaa tietojen tuhoamistapaa:

Laitteet ja järjestelmät	Referenssistandardi	Standardin luokat	Yleinen suositus
Paperisilppurit	DIN 32757 (vanha)	DIN 1 – DIN 6	DIN 4
	DIN 66399 (uusi)	P1 – P7	P5

Käytettäessä edellä mainittuja silppukokoja, voidaan silppuamisesta syntyvä jäte hävittää normaalin toimistojätteen mukaisesti. Tuhoamiseen voidaan käyttää silppuamisen korvaavana tai sitä tukevana suojauksena myös muita menetelmiä, joilla tietojen kokoaminen estetään luotettavasti (esimerkiksi paperisilpun polttaminen).

Osa-alue I: Tekninen tietoturvallisuus

Katakrin teknisen tietoturvallisuuden osa-alueessa kuvataan vaatimukset, joita soveltamalla pyritään varmistamaan turvallisuusjärjestelyjen riittävyys viranomaisen turvallisuusluokitellun tiedon sähköisissä käyttöympäristöissä. Vaatimukset on jaettu tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden osioihin. Tiettyihin asiakokonaisuuksiin (esimerkiksi hallintayhteydet, langattomat verkot, etäkäyttö ja varmuuskopiointi) on ryhmitelty niihin liittyvät vaatimukset.

Tilanteissa, joissa organisaation tavoitteena on saada tietojärjestelmälle toimivaltaisen viranomaisen myöntämä hyväksyntä, tulee organisaation toteuttamien suojausten olla riittäviä sekä organisaation oman että toimivaltaisen viranomaisen riskienarvioinnin havaintoihin nähden. Riskienarvioinnin rooli korostuu myös muutostenhallinnassa. Esimerkiksi uusien palvelujen tai rajapintojen lisääminen olemassa olevaan tietojenkäsittely-ympäristöön voi tuoda riskejä, joiden pienentämiseksi on perusteltua tehdä muutoksia myös olemassa oleviin tietojenkäsittely-ympäristön osiin sekä turvallisuuden ylläpitämisen toimiin. Tietojärjestelmäarvioinnin käyttötapauksia on kuvattu yksityiskohtaisemmin liitteessä II. Riskienhallinnan rooli Katakrin tuetuissa käyttötapauksissa kuvataan yksityiskohtaisemmin liitteessä III.

Kustannusten hallitsemiseksi suositellaan erityisesti tiedon tarkoituksenmukaista luokittelua, sekä turvallisuusluokitellun tiedon käsittely-ympäristön eriyttämistä ja rajaamista mahdollisimman suppeaksi. Esimerkiksi eriyttämällä turvallisuusluokan III käsittely-ympäristöt turvallisuusluokan IV käsittely-ympäristöistä, turvallisuusluokan III suojausmenetelmiä ei edellytetä toteutettavaksi kuin vain turvallisuusluokan III tiedon käsittely-ympäristössä.

Arvioitaessa viranomaisen turvallisuusluokitellun tiedon käsittely-ympäristöä kokonaisuudessaan, on arvioinnissa huomioitava kaikki teknisen tietoturvallisuuden osa-alueessa kuvatut vaatimukset. Tiettyjen vaatimusten kohdalla (erityisesti I-12, I-14, I-17 ja I-18) hyväksyttävissä oleva toteutustapa riippuu siitä, käsitelläänkö kyseisessä järjestelmässä kansallista vai kansainvälistä turvallisuusluokiteltua tietoa.

Turvallisuusluokitellun tiedon sähköiseen käsittelyyn liittyy riskejä, jotka eroavat muiden tietoaineistojen, esimerkiksi henkilötietojen, käsittelyyn kohdistuvista riskeistä. Turvallisuusluokitellun tiedon sähköisen käsittelyn suunnittelussa ja arvioinnissa on huomioitava myös lainsäädäntöjohdannaiset riskit[3]. Katakrin tuetuissa käyttötapauksissa toimivaltaisen viranomaisen hyväksyntä edellyttää tyypillisesti[4] sitä, että sähköinen käsittely-ympäristö on kokonaisuudessaan Suomen lainsäädännön alaisuudessa.

Arvioitaessa viranomaisen turvallisuusluokitellun tiedon käsittely-ympäristöä, osa ympäristöstä voi olla toteutettuna pilviteknologiaa hyödyntäen. Pilviteknologian käyttö ei kuitenkaan muuta keskeisiä riskejä eikä niiden pienentämiseen käytettävien vähimmäissuojausten tarpeellisuutta tai

[3] Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa palveluntarjoajat toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun asiakkaiden turvallisuusluokiteltuihin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä turvallisuusluokitellun 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.

[4] Poikkeuksena esimerkiksi kansainväliseen viranomaisyhteistyöhön liittyvät järjestelmähankkeet, joissa järjestelmäkokonaisuuksien osien tarkastamisen ja hyväksyntien toimivallasta ja vastuusta on kyseiseen viranomaisyhteistyöhön osallistuvien jäsenmaiden turvallisuusviranomaisten kesken erikseen toisin sovittu.

velvoittavuutta. Pilvipalveluihin liittyvien erityisriskien ja vähimmäissuojausten suhdetta on käsitelty yksityiskohtaisemmin Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen julkaisemassa Pilvipalveluiden turvallisuuden arviointikriteeristössä (PiTuKri).

Tietoliikenneturvallisuus

I-01	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - Verkon rakenteellinen turvallisuus	*Turvallisuusluokka IV* 1) Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä. 2) Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä. 3) Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla (vrt. I-12 ja I-15). *Turvallisuusluokat III-II* Kohtien 1 ja 3 lisäksi: 4) Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymän yhdyskäytäväratkaisun käyttöä.	1) 1101/2019 11 §:n k 1 ja 2 2) 1101/2019 11 §:n k 1 ja 2 3) 1101/2019 12 § ja 11 §:n k 7, ja 906/2019 14 § 4) 1101/2019 11 §:n k 1	1) IV liitteen 32-35 kohdat 2) IV liitteen 32-35 kohdat 3) 9 artiklan 4 kohta, IV liitteen 25 ja 35 kohdat 4) IV liitteen 32-35 kohdat
	Lisätietoja		
	Yleistä Tietojärjestelmien erottelu on eräs vaikuttavimmista tekijöistä turvallisuusluokitellun tiedon suojaamisessa. Erottelun tavoitteena on rajata turvallisuusluokitellun tiedon käsittely-ympäristö hallittavaksi kokonaisuudeksi, ja erityisesti pystyä rajaamaan turvallisuusluokitellun tiedon käsittely vain riittävän turvallisiin ympäristöihin. Tietojenkäsittely-ympäristöjen oletetaan lähtökohtaisesti olevan toisilleen ei-luotettuja myös tilanteissa, joissa yhdistetään eri organisaatioiden hallinnoimia tietojenkäsittely-ympäristöjä toisiinsa. Saman turvallisuusluokan käsittely-ympäristöjä voidaan liittää toisiinsa ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymän salausratkaisun avulla (esimerkiksi organisaation eri toimipisteiden ko. turvallisuusluokan käsittely-ympäristöjen yhteenliittäminen julkisen verkon ylitse). Huom: Turvallisuusluokan ylitys hallintaliikenteen (vrt. I-04) osalta edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymää yhdyskäytäväratkaisua. Käytännössä hallintaliikenne rajataankin lähes poikkeuksetta turvallisuusluokittain. Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut (dark fiber) tulkitaan julkisiksi verkoiksi. Vrt. I-12 ja I-15.		

Toteutusesimerkkejä

Turvallisuusluokan IV tietojenkäsittely-ympäristön yhdistäminen eri turvallisuusluokan ympäristöihin voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla turvallisuuskriittisten alemman turvallisuusluokan ympäristöä käyttävien palvelujen (web-selailu, Internetin kautta reitittyvä sähköposti, ja vastaavat) liikenne kulkemaan erillisten sisältöä suodattavien välityspalvelinten kautta. Turvallisuusluokan IV käsittely-ympäristöjä on mahdollista kytkeä Internetiin ja muihin ei-luotettuihin verkkoihin, edellyttäen että kytkennän tuomia riskejä pystytään muilla suojauksilla pienentämään turvallisuusluokalle IV riittävästi. Internet-kytkentäisyyden tuomien riskien pienentäminen turvallisuusluokalle IV edellyttää erityisesti ohjelmistopäivityksistä huolehtimista (vrt. I-19), vähimpien oikeuksien periaatteen mukaisia käyttöoikeuksia (vrt. I-06), järjestelmäkovennuksia (vrt. I-08) sekä kykyä poikkeamien havainnointiin ja korjaaviin toimiin (vrt. I-11). Tyypillinen käyttötapa turvallisuusluokan IV käsittely-ympäristölle on organisaation "toimistoverkon" tietojenkäsittely-ympäristön osa, joka voi muodostua esimerkiksi päätelaitepalveluista, sovelluspalveluista, tietoliikennepalveluista sekä niiden suojaamiseen liittyvistä järjestelyistä.

Turvallisuusluokasta III lähtien yhdistäminen eri turvallisuusluokkien ympäristöihin voidaan toteuttaa toimivaltaisen viranomaisen hyväksymillä, riittävän turvallisilla yhdyskäytäväratkaisuilla. Turvallisten yhdyskäytäväratkaisujen yleisenä suunnitteluperiaatteena on toteuttaa Bell-LaPadula -mallin säännöt "No Read Up" ja "No Write Down". Yhdyskäytäväratkaisun tulee toisin sanoen luotettavasti estää ylemmän turvallisuusluokan tiedon kulkeutuminen matalamman turvallisuusluokan ympäristöön. Turvallisten, hyväksyttävissä olevien yhdyskäytäväratkaisujen suunnitteluperiaatteita ja yleisiä ratkaisumalleja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa (www.ncsa.fi > "Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista").

Turvallisuusluokan III käsittely-ympäristöt ovat moniportaisesti loogisesti tai fyysisesti ei-luotetuista verkoista/järjestelmistä eristettyjä kokonaisuuksia. Fyysisellä eristämisellä tarkoitetaan OSI-mallin fyysisen kerroksen tasolla tapahtuvaa erottelua. Turvallisuusluokan III käsittely-ympäristöihin ei pääsääntöisesti kytketä mitään muita verkkoja/järjestelmiä. Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri turvallisuusluokan järjestelmiin/verkkoihin, se on yleensä perustelluinta järjestää erillisellä tietokoneella, jota ei kytketä turvallisuusluokan III verkkoon. Toimivaltainen viranomainen voi tapauskohtaisesti hyväksyä myös turvallisuusluokan III käsittely-ympäristön fyysisen kytkemisen erikseen tarkastettuun ja hyväksyttyyn verkkoon/järjestelmään. Tällaiset erikseen hyväksytyt verkot/järjestelmät jakautuvat pääsääntöisesti neljään käyttötilanteeseen:

A. Tiedonsiirtojärjestelmät

Turvallisuusluokan III järjestelmä/verkko voi olla tiedonsiirtojärjestelmä kahden tai useamman fyysisen pisteen välillä. Tällöin jokaisen kytketyn pisteen tulisi olla turvallisuustasoltaan vastaavalla tasolla. Verkkotason rajapinta on useimmiten muotoa [fyysisesti eristetty verkko/työasema] - [palomuurilaitteisto/-ohjelmisto] – [turvallisuusluokalle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto]

	- [Internet] – [palomuurilaitteisto/-ohjelmisto] - [turvallisuusluokalle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [fyysisesti eristetty verkko/työasema]. Vastaavilla järjestelyillä voidaan toteuttaa myös turvallisuusluokan II mukainen ratkaisu. B. Palvelujärjestelmät Turvallisuusluokan III järjestelmä/verkko voi olla esimerkiksi tietokantapalvelu, jota käytetään useasta fyysisestä pisteestä. Verkkotason rajapinta on tällöin vastaava kuin käyttötilanne A:ssa. C. Yhdyskäytäväratkaisut C1. Turvallisuusluokan III tiedon käsittely-ympäristöön voidaan siirtää tietoa alemman turvallisuusluokan ympäristöstä erillisen, vain yksisuuntaisen liikenteen sallivan yhdyskäytäväratkaisun (esim. datadiodi) kautta. Vastaavilla järjestelyillä voidaan toteuttaa myös turvallisuusluokan II mukainen ratkaisu. C2. Turvallisuusluokan III tiedon käsittely-ympäristöstä voidaan siirtää matalamman turvallisuusluokan tietoa matalamman turvallisuusluokan ympäristöön sisältösuodatusratkaisun kautta. Sisältösuodatusratkaisun käyttö edellyttää tiedon tunnistamista ylemmän tason ympäristössä, ja vain matalamman tason tiedon siirtymisen sallimista ylemmän tason ympäristöstä matalamman tason ympäristöön. D. Muut käsittely-ympäristöt Muut turvallisuusluokan III käsittely-ympäristöt ovat yleisimmin organisaation tuotekehitysverkkoja tai muita turvallisuusluokan III tiedon käsittely-ympäristöjä. Tällaisiin järjestelmiin voidaan kytkeä esimerkiksi vain tätä ympäristöä palveleva päivityspalvelin. Päivityspalvelimelta voidaan sallia keskitetty turvapäivitysten ja haittaohjelmatunnisteiden jakelu tietyin rajauksin. Jaeltavat päivitykset ja tunnistekannat voidaan tuoda päivityspalvelimelle ilmaraon yli, tai vaihtoehtoisesti esimerkiksi datadiodin läpi. Turvallisuusluokan II käsittely-ympäristöt ovat lähtökohtaisesti fyysisesti eristettyjä kokonaisuuksia, joihin sallitaan turvallisuusluokan ylittävä liikennöinti vain datadiodien tai vastaavien OSI-mallin fyysisellä kerroksella toimivien yksisuuntaisten yhdyskäytäväratkaisujen kautta. *<u>Kasautumisvaikutus</u>* Suuresta määrästä tietyn turvallisuusluokan tietoa koostuvissa tietojärjestelmissä asiakokonaisuus voi nousta luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan. Määrä ei ole kuitenkaan ainoa tekijä, vaan joskus esimerkiksi kahden eri tietolähteen yhdistäminen voi johtaa tietovarannon luokituksen nousemiseen. Tyypillisesti kasautumisessa on kysymys IV-luokan tiedosta (esimerkiksi suuri määrä turvallisuusluokan IV tietoa voi muodostaa yhdistettynä turvallisuusluokan III tietovarannon).

	Kasautumisvaikutuksen arviointiin ei tunneta yleistä, kaikkiin tilanteisiin sellaisenaan sopivaa laskentatapaa. Kasautumisvaikutuksen arvioinnissa tulee huomioida tiedonhallintalaki (906/2019), jonka mukaan turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain (1999/621) 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. 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 lain 1999/621 mukaan turvallisuusluokiteltavaa esimerkiksi III-luokan mukaiseksi. Kun kohteen keskeisen tietovarannon turvallisuusluokka tulkitaan kasautumisvaikutuksesta johtuen yksittäisten tietoalkioiden tasoa korkeammaksi, tulisi tietovarannon määritellyt suojausmenetelmät toteuttaa korkeamman tason 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. Kun arviointityökaluna käytetään Katakria, tulisi kasautumisvaikutus tulkita siten, että tietovarannon suojauksilta edellytetään korkeamman tason mukaisena tietovarannon fyysisen turvallisuuden lisäksi kohtia I-13 (sovelluskerroksen turvallisuus), I-10 ja I-11 (jäljitettävyys ja havainnointikyky) sekä I-06 (tehtävien eriyttäminen). Onkin huomioitava, että kasautumisvaikutuksen seurauksena yhdellä luokalla noussut tietovarannon turvallisuusluokka ei edellytä hyväksyttävää yhdyskäytäväratkaisua tietovarannon (esim. TL III) ja päätelaitteiden (esim. TL IV) välille. Kasautumisvaikutuksen seurauksena turvallisuusluokan III tietovarantojen hallintaratkaisuissa tulee lisäksi erityisesti huomioida, että hallintaan käytettävät päätelaitteet ovat luotettavasti eroteltuja Internet-kytkentäisistä verkoista. *Muita lisätietoja* Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista; CIS Critical Security Controls (v7.1) / 13; CIS Critical Security Controls (v7.1) / 14; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 13.1.1; ISO/IEC 27002:2017 13.1.3; Tiedonhallintalautakunnan suositus (2020:19, luku 6); PiTuKri TT-01

I-02 **Vähimpien oikeuksien periaate - Tietoliikenne-verkon**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti.	1101/2019 7 § ja 11 §:n k 2 ja 3	IV liitteen 16, 18, 19 ja 33-34 kohdat
	Lisätietoja		

vyöhykkeistäminen ja suodatussäännöstö ko. turvallisuusluokan sisällä	*Yleistä* Tietoliikenneverkon jakaminen ko. turvallisuusluokan sisällä erillisille verkko-alueille (vyöhykkeet ja segmentit) voi tarkoittaa esimerkiksi hankekohtaista työasema- ja palvelinerottelua. Verkkoalueiden välisen liikenteen valvonnan ja rajoittamisen voi toteuttaa turvallisuusluokan IV verkon ulkorajalla esimerkiksi siten, että kaikki sisäänpäin tulevat yhteydenavausyritykset estetään ja ulospäin lähtevät yhteydet rajataan vain välityspalvelimen kautta tulevaan web-selailuun sekä sähköpostiliikenteeseen. Kaikkien turvallisuusluokkien verkoissa riittävä vähimpien oikeuksien periaatteen huomiointi edellyttää tyypillisesti myös sitä, että turvallisuusluokan sisällä eri verkkoalueiden välillä sallitaan vain tarpeelliset yhteydet (lähde-kohde-protokolla) ja että muut yhteysyritykset havaitaan. Suojauksia voidaan täydentää ja tukea myös niin sanotulla Zero Trust -lähestymistavalla, jossa eri toimijoiden toimintamahdollisuuksia voidaan rajoittaa ja valvoa erityisesti toimijoiden ja toiminteiden tunnistamiseen ja todentamiseen pohjautuen. Kytkentöjen ja konfiguraatioiden turvallisesta toiminnasta tulee varmistua säännöllisesti, vrt. I-03. Kaikkia liitettyjä tietotekniikkajärjestelmiä tulisi lähtökohtaisesti käsitellä epäluotettavina ja varautua yleisiin verkkohyökkäyksiin. Yleisiin verkkohyökkäyksiin varautumiseen sisältyy esimerkiksi vain tarpeellisten toiminnallisuuksien pitäminen päällä. Toisin sanoen jokaiselle päällä olevalle toiminnallisuudelle tulisi olla perusteltu toiminnallinen tarve. Toiminnallisuus tulisi rajata suppeimpaan toiminnalliset vaatimukset täyttävään osajoukkoon (esimerkiksi toiminnallisuuksien näkyvyyden rajaus). Lisäksi tulisi ottaa huomioon esimerkiksi osoitteiden väärentämisen (spoofing) estäminen ja verkkojen näkyvyyden rajaaminen. Turvallisuusluokalla IV tulisi myös ottaa huomioon palvelunestohyökkäyksen uhka, mikäli järjestelmä liitetään ei-luotettuun verkkoon. Suodatusten tulisi perustua vähimpien oikeuksien periaatteeseen ja suodatuksen tulisi sallia vain erikseen hyväksytty liikennöinti (default-deny). Suodatuksissa tulisi huomioida myös eri protokollien (esim. IPv4, IPv6, GRE, IPSec-tunnelit, reititysprotokollat, sekä myös ylempien kerrosten protokollat, esim. HTTP, SSH, FTP ja SMTP) toiminnallisuudet. Tarpeettomat protokollat tulisi poistaa käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa niille ei ole todellista käyttöperustetta, ja varmistettava liikennöinnin estyminen (verkko-, työasema- ja palvelintason) palomuurien suodatussäännöillä. Mikäli työasemissa, palvelimissa, verkkolaitteissa tai muissa vastaavissa järjestelmissä käytetään esimerkiksi IPv6-toiminnallisuutta, tulisi ottaa huomioon sen vaikutukset erityisesti liikenteen suodatukseen (palomuurauksen tulisi kattaa myös IPv6-liikenne) sekä reititykseen. Myös eri protokollien yhdistämis- ja yhteiskäyttöratkaisujen (esim. IPv4-IPv6-toteutukset, NAT-64, Teredo) vaikutukset tulisi ottaa huomioon verkon/järjestelmien turvallisuuden kokonaissuunnittelussa. *Toteutusesimerkki* Turvallisuusluokkien IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Tietoliikenneverkko on jaettu ko. turvallisuusluokan sisällä erillisiin verkko-alueisiin (vyöhykkeet, segmentit). 2) Verkko-alueiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan (default-deny).

	3) Tietojenkäsittely-ympäristössä on varauduttu yleisiin verkkohyökkäyksiin. *Muita lisätietoja* BSI IT-Grundschutz-Compendium Edition 2019; CIS Critical Security Controls (v7.1) / 12; CIS Critical Security Controls (v7.1)/ 14; ISO/IEC 27002:2017 13.1.1; ISO/IEC 27002:2017 13.1.2; ISO/IEC 27002:2017 13.1.3; PiTuKri TT-01; PiTuKri TT-02

I-03	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan - Suodatus- ja valvonta-järjestelmien hallinnointi	1) Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan. a) Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen ja poistaminen on vastuutettu ja organisoitu. b) Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia. c) Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.	1) 1101/2019 11 §:n k 2, 906/2019 13 §	1) IV liitteen 8-12 kohdat
	Lisätietoja		
	Yleistä Liikennettä suodattavia ja/tai valvovia järjestelmiä ovat tyypillisesti palomuurit, reitittimet, IDS- ja IPS-järjestelmät sekä vastaavia toiminnallisuuksia sisältävät verkkolaitteet, palvelimet ja sovellukset. Riittävän dokumentaation toteutus edellyttää yleensä esimerkiksi verkkorakenteen kuvaamista verkkoalueineen (vyöhykkeet ja segmentit) sillä tarkkuudella, että dokumentaation pohjalta voidaan tarkastaa verkon vastaavan toimivaltaisen viranomaisen hyväksymää rakennetta. Käytettävyyden ja riittävän dokumentoinnin varmistamisen kannalta tarkoituksenmukainen ratkaisu on usein suodatus- ja valvontajärjestelmien asetusten (konfiguraatioiden, ml. esimerkiksi palomuurisäännöstöt) varmuuskopiointi, ja varmuuskopioiden turvallisuusluokan mukainen säilytys.		

	Asetusten ja halutun toiminnan tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu erityisesti kohteessa tapahtuvien muutosten tiheydestä ja kohteen laajuudesta. Esimerkiksi organisaation turvallisuusluokan IV tietojenkäsittely-ympäristön palomuurisäännöstöt voivat olla laajoja ja muutoksia voi olla tarve tehdä usein. Tällaisissa ympäristöissä riittävä tarkastustiheys voi olla esimerkiksi vuosineljänneksittäin tai puolivuosittain. Toisaalta sellaisissa suppeissa ympäristöissä, missä suodatussäännöstöihin ei ole tarve tehdä muutoksia kuin hyvin harvoin, voi riittää vuosittaiset tarkastukset. Suodatus- tai valvontaohjelmiston toiminnallisuuksiin voi tulla muutoksia tai uusia ominaisuuksia myös säännöllisesti tehtävissä ohjelmistopäivityksissä. Suodatussäännöstön ja muun toiminnallisuuden oikeellisuus onkin perusteltua varmistaa myös säännöllisesti asennettavien ohjelmistopäivitysten yhteydessä. Uusien ominaisuuksien (esimerkiksi hienojakoisemman suodatuksen) hyödyntämismahdollisuudet ja käyttöönotto tulee arvioida osana muutostenhallintaa (vrt. I-16). *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 11; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 13.1.2; ISO/IEC 27002:2017 18.2.1; ISO/IEC 27002:2017 18.2.3;

I-04 **Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - Hallintayhteydet**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole toimivaltaisen viranomaisen ko. turvallisuusluokille hyväksymää yhdyskäytäväratkaisua. 2) Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu toimivaltaisen viranomaisen hyväksymällä salaustuotteella. 3) Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen. 4) Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.	1) 1101/2019 11 §:n k 1 2) 1101/2019 12 § ja 11 §:n k 7, ja 906/2019 14 § 3) 1101/2019 12 § ja 906/2019 14 § 4) 906/2019 16 §, 1101/2019 11 §:n k 3	1) IV liitteen 32-35 kohdat 2) 9 artiklan 4 kohta 10 artiklan 6 kohta, IV liitteen 25 kohta 3) IV liitteen 31 kohta 4) IV liitteen 16 ja 18-19 kohdat
	Lisätietoja		
	Yleistä Laitteilla/liittymillä tarkoitetaan alla kuvatuissa toteutusesimerkeissä järjestelmiä, joihin pitäisi olla hallintaoikeudet vain ylläpitäjillä tai vastaavilla. Tällaisia ovat tyypillisesti esimerkiksi palomuurit, reitittimet, kytkimet, langattomat tukiasemat, palvelimet, työasemat, erilliset konsoliliittymät (esim. iLO, iDrac) ja Blade-runkojen hallintaliittymät.		

	Hallintayhteyksien suojausten arvioinnissa tulisi huomioida erityisesti se, miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan turvallisuusluokitellut tiedot. Useimmat hallintayhteystavat mahdollistavat pääsyn turvallisuusluokiteltuun tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisääntöjä), mikä tekee näistä erityisen houkuttelevan kohteen myös pahantahtoisille toimijoille. Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn turvallisuusluokiteltuun tietoon, tulisi hallintayhteys ja siihen käytettävät päätelaitteet rajata lähtökohtaisesti samalle turvallisuusluokalle, kuin mitä ko. tietojenkäsittely-ympäristökin. Matalamman tason ympäristön hallinta voi tietyissä erityistapauksissa olla mahdollista ylemmän turvallisuusluokan hallintaympäristöstä käsin, edellyttäen, että turvallisuusluokkien rajoilla on toimivaltaisen viranomaisen ko. turvallisuusluokille hyväksymä yhdyskäytäväratkaisu, joka estää ylemmän turvallisuusluokan tietojen kulkeutumisen matalamman turvallisuusluokan ympäristöön. Erityisesti yhteysprotokollien ohjelmistohaavoittuvuuksista johtuen matalamman tason ympäristöjen hallintamahdollisuudet rajautuvat riskiperusteisesti tyypillisesti vain kansallisen turvallisuusluokan IV ympäristöistä tapahtuvaan matalamman tason ympäristöjen hallintaan. Ylemmän turvallisuusluokan ympäristön hallinta ei lähtökohtaisesti ole hallintaliikenteen turvallisuuskriittisestä luonteesta johtuen mahdollista matalamman turvallisuusluokan ympäristöistä. Ylemmän turvallisuusluokan ympäristöstä voidaan toimivaltaisen viranomaisen hyväksymän yhdyskäytäväratkaisun kautta tarjota joissain tapauksessa (read-only) valvontapääsy luokkaa matalamman turvallisuusluokan ympäristöön. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää ko. turvallisuusluokan sisällä esimerkiksi niin sanottua hyppykonekäytäntöä, jossa kaikki hallintatoimet toteutetaan äärimmilleen kovennettujen, järjestelmä- ja roolikohtaisten hyppykoneiden kautta mahdollistaen samalla kattavan jäljitettävyyden (lokituksen, vrt. I-10). Etähallinnan edellytyksiä on kuvattu tarkemmin vaatimuksessa I-18. *Toteutusesimerkki* Turvallisuusluokkien IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Tietojenkäsittely-ympäristöön ei ole yhteenliitäntää hallintayhteyksille muiden turvallisuusluokkien ympäristöistä ilman toimivaltaisen viranomaisen ko. turvallisuusluokille hyväksymää yhdyskäytäväratkaisua (vrt. I-01). 2) Ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään vain toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymän salausratkaisun (ks. I-12) kautta tilanteissa, joissa hallintaliikenne kulkee matalamman turvallisuusluokan ympäristön kautta.

	3) Tilanteissa, joissa hallintaliikenne kulkee ko. turvallisuusluokan sisällä (ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymän salauksen sisällä tai/ja ko. turvallisuusluokan tiedon säilyttämiseen hyväksytyn turvallisuusalueen sisällä muista ympäristöistä fyysisesti eriytetyn verkon sisällä), a) ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään fyysisesti (esim. konsolikaapeli), tai b) ko. turvallisuusluokan hallintayhteyden liikennekanava on muuten luotettavasti fyysisesti suojattu (esim. turva-alueen sisäiset kaapeloinnit), tai c) ko. turvallisuusluokan hallintatyöasema kytketään laitteeseen/liittymään matalamman tason salauksella (esim. SSH, HTTPS, SCP) suojatulla yhteydellä. 4) Laitteisiin/liittymiin sallitaan hallintayhteydenotot vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyistä lähteistä ja määritellyin käyttäjäoikeuksin. *Muita lisätietoja* Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista; CIS Critical Security Controls (v7.1) / 11; CIS Critical Security Controls (v7.1) / 14; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 13.1.1; ISO/IEC 27002:2017 13.1.2; ISO/IEC 27002:2017 13.1.3; PiTuKri IP-03; PiTuKri TT-01

I-05 **Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - Langaton tiedonsiirto**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Langattomassa tiedonsiirrossa tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla (vrt. I-12).	1101/2019 12 § ja 906/2019 14 §	9 artiklan 4 kohta, IV liitteen 33 ja 35 kohdat
	Lisätietoja		
	Yleistä Radiorajapinnan käyttö langattomassa tiedonsiirrossa (esim. WLAN, 3-5G, Bluetooth) tulkitaan poistumiseksi fyysisesti suojatun turvallisuusalueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan julkisen verkon kautta liikennöinniksi, mikä tulisi ottaa huomioon erityisesti liikenteen salauksessa (vrt. I-12) ja fyysisen turvallisuuden toteuttamisessa. Useisiin langattomiin rajapintoihin liittyy myös protokolla- ja ohjelmistototeutusten puutteita, jotka voivat olla ulkopuolisten hyödynnettävissä. Vastaavaa suojausperiaatetta sovelletaan myös langattomiin oheislaitteisiin (esimerkiksi hiiret, näppäimistöt, kuulokkeet ja kuvansiirtojärjestelmät). Poikkeuksena tilanteet, joilla langattoman rajapinnan käyttöön liittyviä riskejä pystytään luotettavasti pienentämään fyysisen turvallisuuden menettelyillä (esimerkiksi langattoman hiiren käyttö turva-alueen sisällä huoneessa, jonka läheisyyteen pääsy on rajattu vain ko. käsiteltävään tietoon valtuutetuilla henkilöillä). Langattomista laitteista on huomioitava myös		

	älypuhelimet ja vastaavat matalamman turvallisuustason laitteistot, joita ei tule kytkeä tietojenkäsittely-ympäristöön esimerkiksi akun lataamista varten (vrt. I-08, I-09, I-16). *Toteutusesimerkki* Turvallisuusluokkien IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: Langattomassa tiedonsiirrossa tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä (I-12). *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 15; BSI IT-Grundschutz-Compendium Edition 2019; PiTuKri SA-01

Tietojärjestelmäturvallisuus

I-06	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Vähimpien oikeuksien periaate - Pääsyoikeuksien hallinnointi	1) Tietojärjestelmien käyttöoikeudet on määritelty. 2) Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeuksista (vrt. T-13) on varmistuttu. 3) Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä. 4) Käyttöoikeudet on pidettävä ajantasaisina.	1) 1101/2019 8 §, 906/2019 16 § 2) 1101/2019 8 § 3) 906/2019 16 §, 1101/2019 8 § ja 11 §:n k 3 4) 906/2019 16 §	1) Artiklan 7 kohta 1, I liitteen kohta 2 2) Artiklan 7 kohta 1 ja 5, I liitteen kohta 2 3) IV liitteen 19 kohta 4) IV liitteen 8 ja 9 kohta

Lisätietoja

Yleistä

Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon. Käyttöoikeuksien taustalla on suositeltavaa olla jokin sopimus tai muu dokumentoitu peruste, joka voidaan todentaa (esim. työsuhde, sopimus toteutettavasta työstä ympäristössä). Kaikkien käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja aktiivisia ja tarpeettomat käyttäjätunnukset poistetaan välittömästi.

Käyttöoikeudet tulee rajata vain toiminnallisen tarpeen edellyttämään osajoukkoon. Tarpeettoman laajat oikeudet mahdollistavat ko. käyttäjälle, prosessille tai edellä mainitut haltuun saavalle hyökkääjälle tarpeettoman laajat toimintamahdolliset. Käyttöoikeuksien rajaamisella vähimpien oikeuksien periaatteen mukaiseksi voidaan pienentää sekä tahallisten että tahattomien tekojen, kuin myös esimerkiksi haittaohjelmista aiheutuvia riskejä. Erityisesti tulee huomioida, että ylläpito-oikeuksia käytetään vain ylläpitotoimiin. Ylläpitotunnuksella varustettua käyttäjätiliä ei tule käyttää esimerkiksi web-selailuun tai sähköpostin käyttöön.

Pääsyoikeuksien ajantasaisuudesta varmistuminen

Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esim. 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.

Tehtävien erottelu

Tehtävien erottelun riittävä toteutus riippuu merkittävästi kyseessä olevan järjestelmän käyttötapauksista. Useimmissa järjestelmissä riittävä tehtävien erottelu on toteutettavissa järjestelmän ylläpitoroolien (ja henkilöiden) ja lokien valvontaan osallistuvien roolien (ja henkilöiden) erottelulla toisistaan. Usein käytettynä valvontamekanismina on myös se, että kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän ("two man rule").

Tarkastusoikeuden ottaminen huomioon teknisessä toteutuksessa

Turvallisuusluokitellun tiedon omistajat varaavat usein itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti monihankeverkoissa ja muissa vastaavissa ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulisi varmistua siitä, että verkon/järjestelmän rakenne mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä.

Eri omistajien tietojen erottelumenetelmät jakautuvat kolmeen pääluokkaan.
a) Loogisen tason erotteluun (esim. palvelinten virtualisointi ja käyttöoikeuksin rajoitetut verkkolevykansiot) perustuvat menetelmät soveltuvat turvallisuusluokan IV tiedoille.
b) Luotettavaan loogiseen erotteluun (esim. hyväksytysti salatut virtuaalikoneet levyjärjestelmän asiakaskohtaisesti dedikoiduilla levyillä, ja tiedon/tietoliikenteen hyväksytty salaus yhteiskäyttöisillä verkkolaitteilla) perustuvat menetelmät soveltuvat turvallisuusluokille IV ja III.
c) Fyysisen tason erotteluun (dedikoidut fyysiset laitteet) perustuvat menetelmät soveltuvat turvallisuusluokille IV, III ja II.

Huom: Tietojen erotteluvaatimusta ei IV-tasolla sovelleta työasemiin tai muihin vastaaviin suppeisiin tietovarantoihin, edellyttäen, että käytössä on luotettavaksi arvioidut menetelmät kasautumisvaikutuksen ehkäisemiseksi. Tarkastusoikeuden varaavien tiedon omistajien tietoja ei edellytetä eroteltavan myöskään tilanteissa, joissa kaikilta tiedon omistajilta on saatu kirjallinen erillishyväksyntä tarkastusoikeuden mahdollistamien riskien hyväksymisestä.

Toteutusesimerkki

Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
2) Järjestelmän käyttäjistä on olemassa lista.
3) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
4) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu.

	5) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. 6) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen). 7) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti. 8) Tietojärjestelmissä turvallisuusluokitellut tiedot on eritelty vähimpien oikeuksien periaatteen mukaisesti käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä. 9) Tietojärjestelmissä ko. turvallisuusluokan tiedot pidetään erillään julkisista ja muiden turvallisuusluokkien tiedoista, tai eri tason tietoja käsitellään korkeimman turvallisuusluokan mukaisesti. 10) Tietojärjestelmissä tarkastusoikeuden varaavien tiedon omistajien tiedot säilytetään toisistaan ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymällä menetelmällä eroteltuna. Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1-10 lisäksi toteutetaan seuraavat toimenpiteet: 11) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi. 12) Palvelimissa, työasemissa ja muissa tallennusvälineissä turvallisuusluokitellut tiedot säilytetään toimivaltaisen viranomaisen ko. ympäristöön hyväksymällä menetelmällä salattuna (ks. I-12), mikäli salausta käytetään tarkastusoikeuden varaavien eri tiedon omistajien tietojen erotteluun, tai/ja mikäli tallennusvälineitä viedään niiden elinkaaren aikana kyseisen turvallisuusluokan säilyttämiseen hyväksytyn turvallisuusalueen ulkopuolelle. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 4; CIS Critical Security Controls (v7.1) / 14; CIS Critical Security Controls (v7.1) / 16; BSI IT-Grundschutz-Compendium Edition 2019; Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje; NIST - National Checklist Program Repository; ISO/IEC 27002:2017 6.1.2; ISO/IEC 27002:2017 9.1.1; ISO/IEC 27002:2017 9.1.2; ISO/IEC 27002:2017 9.2.1; ISO/IEC 27002:2017 9.2.2; ISO/IEC 27002:2017 9.2.3; ISO/IEC 27002:2017 9.2.4; ISO/IEC 27002:2017 9.2.5; ISO/IEC 27002:2017 9.2.6; PiTuKri IP-01

I-07 **Monitasoinen suojaaminen - Tietojenkäsittely-**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.	1101/2019 11 §:n k 5	IV liitteen 16 ja 19 kohdat
	Lisätietoja		

ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuus-alueen sisällä	*Toteutusesimerkki* Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: Henkilöiden tunnistaminen: 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 tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille. 6) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. Laitteiden tunnistaminen: 7) Turvallisuusluokitellun tiedon käsittelyyn käytetään vain organisaation tarjoamia ja hallinnoimia, kyseiselle turvallisuusluokalle hyväksyttyjä päätelaitteita. Kaikkien muiden laitteiden kytkeminen turvallisuusluokitellun tiedon käsittely-ympäristöön on yksiselitteisesti kielletty. Henkilöstö on ohjeistettu ja velvoitettu toimimaan ohjeistuksen mukaisesti. Tietojärjestelmien tunnistaminen: 8) Tietoa keskenään vaihtavat tietojärjestelmät tunnistetaan käyttötapaukseen soveltuvalla tekniikalla, kuten salasanoilla, avaimilla (esim. API-avain), tunnistevälineillä (tokeneilla, esim. oAuth) tai vastaavilla menetelmillä. Tunnistautuminen tehdään salattuja yhteyksiä pitkin. Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1-5 ja 7 lisäksi toteutetaan seuraavat toimenpiteet: 9) Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta. 10) 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 toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymän turva-alueen sisällä). *Huomioitavaa*

	Turvallisuusluokan IV käsittely-ympäristöissä, joissa uhka palvelunestohyökkäyksen aiheuttamiseen (tunnusten lukitseminen esim. Internet-kytkentäisissä tunnistuspalveluissa) arvioidaan merkittäväksi, tunnuksen lukittuminen voidaan korvata jollain riskiä pienentävällä menettelyllä (esim. vastaamisen hidastamiseen, suodattamiseen tai väliaikaiseen lukitsemiseen perustuvat menettelyt). Turvallisuusluokan IV käsittely-ympäristöissä ei yleensä edellytetä päätelaitteen teknistä tunnistamista, mikäli käyttäjät tunnistetaan. Turvallisuusluokkien III ja II käsittely-ympäristöjen menetelmät vahvasta käyttäjätunnistuksesta ja päätelaitteen tunnistamisesta voidaan joissain tapauksissa toteuttaa siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisesti suojatulta alueelta (yleensä turva-alue, lukittu laitekaappi, tai vastaava), jonka pääsynvalvonnassa käytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla. Tilanteissa, joissa käyttäjätunnistus nojaa fyysisen turvallisuuden menettelyihin, tulee myös fyysisen turvallisuuden menettelyjen täyttää jäljitettävyydelle (vrt. I-10) asetetut vaatimukset erityisesti lokitietojen ja vastaavien tallenteiden säilytysaikojen suhteen. Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force -hyökkäyksiä vastaan. *Muita lisätietoja* BSI IT-Grundschutz-Compendium Edition 2019; CIS Critical Security Controls (v7.1) / 1; CIS Critical Security Controls (v7.1) / 4; CIS Critical Security Controls (v7.1) / 11; CIS Critical Security Controls (v7.1) / 16; ISO/IEC 27002:2017 9.1.2; ISO/IEC 27002:2017 9.4.1; ISO/IEC 27002:2017 9.4.2; ISO/IEC 27002:2017 9.4.3; NIST Special Publication 800-63B; PiTuKri IP-02

I-08 **Vähimmäis-toimintojen ja vähimpien oikeuksien periaate - Järjestelmä-kovennus**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut. 2) Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. 3) Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.	1) 1101/2019 11 §:n k 3 ja 6, 906/2019 13 § 2) 1101/2019 11 §:n k 3 ja 6, 906/2019 13 § 3) 1101/2019 11 §:n k 3 ja 6, 906/2019 13 §	1) IV liitteen 16, 18 ja 19 kohdat 2) IV liitteen 8, 16, 18 ja 19 kohdat 3) IV liitteen 16, 18 ja 19 kohdat

	4) Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan.	4) 1101/2019 11 §:n k 3 ja 6, 906/2019 13 §	4) IV liitteen 8, 16, 18 ja 19 kohdat
	Lisätietoja		
	Yleistä Turvallisen ohjelmistokoodin tekeminen on osoittautunut haastavaksi. 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. Ominaisuudet ovat toisaalta usein myös tarpeettoman turvattomilla asetuksilla. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Jos välttämättömien palvelujen tarpeettoman turvattomia asetuksia ei muuteta, ovat nämä myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, valmiiksi asennettuja tarpeettomia ohjelmistoja ja tarpeettomia käyttäjätilejä. 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, jotta rajoitetaan onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja. Järjestelmän mahdollisesti turvattomat oletusasetukset ja esimerkiksi tarpeettomat oletuskäyttäjätilit tulee muuttaa tai poistaa. Järjestelmillä tarkoitetaan verkon aktiivilaitteita, palvelimia, työasemia, mobiililaitteita, tulostimia, oheislaitteita ja muita tietojärjestelmäksi käsitettäviä laitteita. Palvelinten, työasemien ja vastaavien riittävän kovennuksen voi toteuttaa esimerkiksi DISA STIG:iä, CIS:iä tai vastaavaa tasoa mukaillen. Mikäli turvallisuusluokitellun tiedon käsittelyyn käytetään verkkotulostimia, puhelinjärjestelmiä tai vastaavia, edellä mainittuja periaatteita tulisi soveltaa myös näihin järjestelmiin. Koventamiseen ja kovennetun asennuksen ylläpitämiseen voidaan usein hyödyntää myös konfiguraationhallintatyökaluja. *Toteutusesimerkki* Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:		

1) Kovennettavat kohteet on tunnistettu.
2) Kovennusten toteutus on määritelty.
3) Kohteet on kovennettu määritysten mukaisesti.
4) Kovennusten pysyminen päällä varmistetaan säännöllisesti, erityisesti päivitysten jälkeen koko tietojärjestelmän elinkaaren ajan.

Erityisesti huomioitavaa:

a) Kovennukset kohdistetaan kaikkiin tietojenkäsittely-ympäristön laitteisiin, joita ovat muun muassa verkon aktiivilaitteet, palvelimet, työasemat, mobiililaitteet, tulostimet, oheislaitteet ja muut tietojärjestelmäksi käsitettävät laitteet.
b) Hyökkäyspinta-alan rajaamiseksi laitteissa on päällä vain tarvittavat palvelut, rajapinnat, yhteydet ja väylät, ja nämä toimivat vähimpien oikeuksien periaatteella.
c) Laitteen laiteohjelmisto (firmware, BIOS ja vastaavat), käyttöjärjestelmä, sovellukset sekä muut vastaavat komponentit kovennetaan vähintään valmistajan kovennussuosituksen mukaisesti ja/tai käyttäen yleisesti tunnettua kovennusohjetta. Tämän lisäksi kovennukset räätälöidään järjestelmäkohtaisesti käyttötarkoituksen ja riskien perusteella. Jollei kovennusohjetta käytetylle komponentille ole olemassa, sovelletaan vastaavalle tuotteelle tarkoitettua ohjetta.

Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että kohtien 1-4 lisäksi kovennuksiin käytetään useita kovennusohjeita ja kovennusohjeiden toteutuksen tiukkuutta kiristetään.

<u>Oleellista kovennuksista</u>

1) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin. Salasanoja säilytetään siten, että salasanat ovat suojattuna sekä saatavilla.
2) Ylimääräiset palvelut, sovellukset, yhteydet (myös BIOS-tasolla) ja laitteet on poistettu.
3) Käyttäjät, rajapinnat ja laitteet tunnistetaan (vrt. I-07).
4) Päällä olevat välttämättömät palvelut ovat saavutettavissa vain tarpeellisten verkkojen, laitteiden ja käyttäjätunnusten osalta.
5) Ohjelmistot (esim. laiteohjelmistot, sovellukset) pidetään ajantasaisina (vrt. I-19).
6) Kohteen yhteydet, mukaan lukien hallintayhteydet, ovat rajattuja, kovennettuja, käyttäjätunnistettuja sekä aikarajoitettuja.
7) Käytössä olevat sovellukset, rajapinnat ja vastaavat on kovennettu, rajoitettu ja ominaisuudet on asetettu vähimpien oikeuksien periaatteen mukaiseksi.
8) Ohjelmistot, kuten käyttöjärjestelmät, sovellukset ja laiteohjelmistot, asetetaan keräämään tarvittavaa lokitietoa väärinkäytösten havaitsemiseksi (vrt. I-10).
9) Tietojärjestelmän käynnistäminen tuntemattomalta laitteelta on estetty.

	Korvaavia menetelmiä Mikäli esimerkiksi verkkolaitteen hallinta ei ole teknisesti mahdollista käyttäjän yksilöivällä käyttäjätunnuksella, käyttäjän yksilöivä tunnistaminen voidaan järjestää käyttösäännöillä esimerkiksi siten, että salasanaan pääsy edellyttää kahden henkilön osallistumista. Mikäli ympäristön koko on suurehko, todennuksen järjestämiseen suositellaan kahdennettujen AAA-palvelimien (erityisesti TACACS+, RADIUS tai Kerberos) hyödyntämistä. Erityisesti korkeimpien turvallisuusluokkien ympäristöissä tarpeettomien komponenttien käytönesto on usein perusteltua toteuttaa fyysisesti kyseiset komponentit (esimerkiksi langattomat verkkokortit, kamerat, mikrofonit) laitteesta irrottaen. Tilanteissa, joissa kyseistä komponenttia ei voida fyysisesti irrottaa, korvaavana suojauksena voi joissain tapauksissa hyödyntää esimerkiksi kameroiden teippaamista sekä laitteiston ohjelmallista käytöstäpoistoa sekä käyttäjäasetus-, käyttöjärjestelmä- ja laiteohjelmistotasoilla. Joissain käyttöjärjestelmissä suojausta voidaan täydentää myös poistamalla kyseisen laitteen käyttöön liittyvät ohjelmisto-osiot (kernel module). *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 2; CIS Critical Security Controls (v7.1) / 5; CIS Critical Security Controls (v7.1) / 7; CIS Critical Security Controls (v7.1) / 9; BSI IT-Grundschutz-Compendium Edition 2019; The United States Government Configuration Baseline (USGCB); NATO Best Practice Configuration Guidance; DISA Security Technical Implementation Guides (STIGs); NIST Special Publications (800 Series); NIST - National Checklist Program Repository; Microsoft DSC Environment Analyzer; Microsoft Baseline Management; CIS benchmarks; PiTuKri JT-02

I-09	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Monitasoinen suojaaminen - Haittaohjelma-suojaus	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.	1101/2019 11 §:n k 2	IV liitteen 8, 9, 16, 18, 19, 21 ja 22 kohdat
	Lisätietoja		
	Yleistä Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä (vrt. I-08), käyttöoikeuksien rajauksilla (vrt. I-06), järjestelmien pitämisellä turvallisuuspäivitysten tasolla (vrt. I-19), poikkeamien havainnointikyvyllä (vrt. I-11), henkilöstön turvatietoisuudesta varmistumalla (vrt. T-12) ja myös haittaohjelmantorjuntaohjelmistojen käytöllä. Riskejä voidaan pienentää myös riskialttiiden ympäristöjen eriyttämisellä tuotantoympäristöistä sekä muun muassa siirreltävien medioiden (esimerkiksi USB-muistien)		

	käytön rajauksilla. Torjuntaohjelmistot voidaan jättää asentamatta ympäristöissä, joihin haittaohjelmien pääsy on muuten estetty (esim. järjestelmät, joissa ei ole mitään tiedon tuonti-/vientiliittymiä, tai joissa tarkasti rajatuissa liittymissä toteutetaan siirrettävän tiedon luotettava validointi/sanitointi). *Toteutusesimerkki* Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Järjestelmien käyttöoikeudet on rajattu vähimpien oikeuksien periaatteen mukaisesti (vrt. I-06). 2) Järjestelmät pidetään turvallisuuspäivitysten tasolla (vrt. I-19). 3) Järjestelmät on kovennettuja siten, että vain välttämättömät toiminnallisuudet ja ohjelmistokomponentit käytössä (vrt. I-08). 4) Henkilöstön turvatietoisuudesta on varmistuttu (vrt. T-12). Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta. 5) On tunnistettu järjestelmät, joissa haittaohjelmantorjuntaohjelmistoilla pystytään saamaan lisäsuojausta. 6) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille. Tällaisia ovat tyypillisesti muun muassa julkisen verkon yhdyskäytävät (esim. sähköposti- ja WWW-liikennöinti), sekä ulkoisiin rajapintoihin (muut verkot, USB-mediat ja vastaavat) yhteydessä olevat päätelaitteet. 7) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 8) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä. 9) Haittaohjelmatunnisteet (ja vast.) päivittyvät säännöllisesti. 10) Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan. Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1-10 lisäksi toteutetaan seuraavat toimenpiteet: 11) Kaikki tiedon sisääntuonnin ja ulosviennin käyttötapaukset on tunnistettu. Turvalliset toimintatavat on määritetty, ohjeistettu ja valvonnan piirissä. Turvallisten toimintatapojen piiriin sisältyy tarvearviointi järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. a) Tilanteissa, joissa liityntöjen käytölle ei ole kriittistä tarkastelua kestävää perustetta, liitynnät poistetaan käytöstä. b) Tilanteissa, joissa liityntöjen käytölle on kriittistä tarkastelua kestävät perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä. *Julkisista verkoista eristetyt ympäristöt* Järjestelmissä, joita ei kytketä julkiseen verkkoon, haittaohjelmatunnisteiden päivitys voidaan järjestää esimerkiksi käyttämällä hallittua suojattua päivitystenhakupalvelinta, jonka tunnistekanta pidetään ajan tasalla esimerkiksi erillisestä Internetiin kytketystä

	järjestelmästä tunnisteet käsin siirtämällä (esim. kerran vuorokaudessa), tai tuomalla tunnisteet hyväksytyn yhdyskäytäväratkaisun (ks. I-01) kautta. Huom: Päivitysten eheydestä varmistumiseen tulisi olla menettelytapa (lähde, tarkistussummat, allekirjoitukset, jne.). USB-porttien ja vastaavien liityntöjen käytön tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi, että järjestelmään voi kytkeä vain erikseen määritettyjä luotettavaksi todennettuja muistitikkuja (ja vastaavia), joita ei kytketä mihinkään muuhun järjestelmään. Tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi järjestely, jossa vain organisaation tietohallinnon (tai vast.) jakamia muistivälineitä voidaan kytkeä organisaation järjestelmiin, ja että kaikkien muiden muistivälineiden kytkeminen on kielletty ja/tai teknisesti estetty. Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, tapauskohtaisiin ehtoihin sisältyy usein myös määrittelyt siitä, millä menetelmillä pienennetään tämän aiheuttamaa riskiä. Menetelmänä voi esimerkiksi olla ei-luotetusta lähteestä tulevan muistivälineen kytkeminen eristettyyn tarkastusjärjestelmään, jonne siirrettävä tieto siirretään, ja josta siirrettävä tieto viedään edelleen luotettuun järjestelmään erillistä muistivälinettä käyttäen. Tällaisissa järjestelyissä huomioidaan yleensä turvallisuusluokalla III vähintään muistialueen tarkastaminen, ja turvallisuusluokasta II lähtien myös muistivälineen kontrolleritason räätälöinnin uhat. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 8; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 12.2.1; PiTuKri JT-04

I-10	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtumien jäljitettävyys	1) Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen. 2) 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. 3) Turvallisuusluokan I–III tiedon käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai tietoon (esimerkiksi dokumentin osaksi).	1) 906/2019 17 §, 15 §, 1101/2019 7 § 2) 906/2019 17 § 3) 1101/2019 14 §	1) IV liitteen 16 kohta, III liitteen 18 ja 21 kohdat 2) 3)
	Lisätietoja		

	Yleistä 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 ylläpitohenkilöstöstä. 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 (esim. 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 myös Tiedonhallintalautakunnan suosituksessa (2020:21, luku 7). Toteutus edellyttää usein myös sen huomioon ottamista, että lokien säilytystilaa ja -aikaa kasvatetaan riittäviksi. Suositus: lokeille varataan tilaa ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. Huom: 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. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 6; BSI IT-Grundschutz-Compendium Edition 2019; The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2017 12.4.1; ISO/IEC 27002:2017 12.4.2; ISO/IEC 27002:2017 12.4.3; ISO/IEC 27002:2017 12.4.4; ISO/IEC 27002:2017 18.1.3; VAHTI 3/2009; Tiedonhallintalautakunnan suositus (2020:21, luku 7); PiTuKri JT-01

I-11 **Monitasoinen suojaaminen - Poikkeamien**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja	906/2019 13.1 ja 17 §, 1101/2019 7 §	IV liitteen 16 kohta

havainnointikyky ja toipuminen	tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne viipymättä.		
	Lisätietoja		
	Yleistä 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 (vrt. I-16) 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 III-luokasta lähtien ulkorajan yhdyskäytäväratkaisun sekä verkon/kohteen sisäpuolen liikennöinnin. Hyökkäyksen/väärinkäyttöyrityksen havaitseminen edellyttää useimmissa ympäristöissä käytännössä automatisoitujen havainnointi- ja hälytystyökalujen käyttöä. Lokitietojen manuaalinen tarkastelu on yleensä riittävä vain ympäristöissä, joissa lokimassat ovat hyvin pieniä ja lokien tarkasteluun on osoittaa riittävät henkilöresurssit. 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. Vrt. T-07 (Turvallisuuspoikkeamien hallinta) ja T-12 (Turvallisuuskoulutus).		

	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 (vrt. I-10) 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. 4) On olemassa menettely havaituista poikkeamista toipumiseen. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 6; CIS Critical Security Controls (v7.1) / 19; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 12.4.1; ISO/IEC 27002:2017 13.1.1; ISO/IEC 27002:2017 16.1.4; ISO/IEC 27002:2017 16.1.5; VAHTI 3/2009; PiTuKri JT-01; PiTuKri TJ-05

I-12	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Tietoturvallisuus-tuotteiden arviointi ja hyväksyntä - Salausratkaisut	Toimivaltainen viranomainen on hyväksynyt käytetyt salausratkaisut (ja -tuotteet) ko. turvallisuusluokalle ko. käyttöympäristössä turvallisuusluokiteltujen tietojen luvattoman paljastumisen ja muuntelun estämiseksi.	1101/2019 11 §:n k 7	10 artiklan 6 kohta, IV liitteen 25 kohta
	Lisätietoja		
	Yleistä Erityisesti liikennöitäessä julkisen tai matalamman turvallisuusluokan verkon kautta, salausratkaisut ovat usein ainoita suojauksia turvallisuusluokitellun tiedon luottamuksellisuuden, ja tyypillisesti myös eheyden suojaamisessa. Koska salausratkaisujen mahdollisia puutteita on usein äärimmäisen haastavaa korvata muilla suojauksilla, salausratkaisun valintaan ja turvalliseen käyttötapaan tulee kiinnittää erityistä huomiota. Erilaisiin tietoihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eriävien tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa.		

Erityisesti turvallisuusluokitellun tiedon suojaamisessa korostuu tarve käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salausratkaisun oikeellisesta toiminnasta varmistumisen lisäksi huomioidaan muun muassa salausratkaisun käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun fyysisesti suojatun alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salausratkaisujen arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja kryptografiselle eheydelle.

Usean kansainvälisen turvallisuusviranomaisen salausratkaisuhyväksynnät edellyttävät ratkaisulta erityisesti näyttöä sen oikeellisesta toiminnasta, ja lisäksi tiettyjen erityisvaatimusten (esim. lähdekoodin luovutus ja tarkastus, peukalointi- ja hajasäteilysuojaukset) täyttämistä. Puhtaasti ohjelmistopohjaiset salausratkaisut ovat tyypillisesti hyväksyttävissä IV- ja joissain tilanteissa erityisehdoilla myös III-luokille. II-luokalle ja useimmin myös III-luokalle edellytetään tyypillisesti enemmän alustan luotettavuudelta. Salausratkaisujen hyväksyntäprosessia on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ohjeessa salaustuotearvioinneista ja -hyväksynnistä. Salausratkaisun vähimmäisvaatimuksia on käsitelty myös Kyberturvallisuuskeskuksen ylläpitämässä salausvahvuuskuvauksessa, sekä turvallisen tuotekehityksen ohjeessa.

Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään.

Erityisesti salausratkaisujen osalta tulee riskienarvioinnissa huomioida myös toimitusketjujen turvallisuus. Vaikka salausratkaisu olisi riittävän turvallinen esimerkiksi salausratkaisun valmistajalta lähtiessään, toimitusketjun suojaamispuutteet voivat mahdollistaa salausratkaisun peukaloinnin, ja siten johtaa turvattoman salausratkaisun käyttöönottoon tietojenkäsittely-ympäristön osana.

Toteutusesimerkki
Turvallisuusluokan IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Organisaatiossa on tunnistettu käyttötapaukset, joissa turvallisuusluokitellun tiedon suojaamiseen on tarve käyttää salausratkaisuja. Tunnistetut käyttötapaukset kattavat kaikki tilanteet, joissa turvallisuusluokitellun tiedon suojaaminen nojaa täysin tai osittain salausratkaisuun. Erityisesti on huomioitu liikennöinti julkisen tai matalamman turvallisuusluokan verkon kautta (vrt. I-01), tiedon välitys toiseen organisaatioon (vrt. I-15 ja F-08.1), ja turvallisuusalueiden ulkopuolelle vietävät päätelaitteet (vrt. I-18).
2) On hankittu ko. turvallisuusluokalle a) toimivaltaisen viranomaisen hyväksymät salausratkaisut ja käytetään niitä hyväksynnän yhteydessä määritellyn käyttöpolitiikan ja -asetusten mukaisesti, tai b) toimivaltaisen viranomaisen myöntämät tapauskohtaiset hyväksynnät ja käyttöpolitiikat-/asetukset sellaisille salausratkaisuille, joilla ei ollut entuudestaan voimassaolevaa hyväksyntää.

	3) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen. 4) Salausratkaisun toimitusketjun turvallisuudesta on varmistuttu riittävällä tasolla. Erityisesti salausratkaisun toimitusketju luotettavalta valmistajalta kohteen tietojenkäsittely-ympäristöön on varmistettu. *Muita lisätietoja* Euroopan unionin neuvoston hyväksyttyjen salaustuotteiden lista; Naton hyväksyttyjen salaustuotteiden lista; Kyberturvallisuuskeskuksen hyväksyttyjen salausratkaisujen lista; Kyberturvallisuuskeskuksen ohje salaustuotteiden arvioinneista ja hyväksynnistä; Kansalliset kryptografiset vahvuusvaatimukset; Turvallisen tuotekehityksen ohje; Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje; CIS Critical Security Controls (v7.1) / 18; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 10.1.1; ISO/IEC 27002:2017 10.1.2; ISO/IEC 27002:2017 18.1.5; Tiedonhallintalautakunnan suositus (2020:19, luku 7); PiTuKri SA-01

I-13	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Monitasoinen suojaaminen koko elinkaaren ajan - Ohjelmistojen suojaaminen verkko-hyökkäyksiltä	1) Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu. 2) Tietoturvallisuutta vaarantavia verkkohyökkäyksiä vastaan suojaudutaan ja suojauksista sekä niiden toiminnasta huolehditaan tietojenkäsittely-ympäristön elinkaaren ajan.	1) 906/2019 13 § 2) 1101/2019 11 §:n k 2	1) IV liitteen 8, 9, 10, 16, 19 ja 33 kohdat 2) IV liitteen 10, 11 ja 19 kohdat
	Lisätietoja		
	Yleistä Ohjelmistot ja niiden käyttötarkoitukset eri tietojenkäsittely-ympäristöissä eroavat toisistaan merkittävästi. Vastaavasti myös tarpeet ohjelmistojen turvalliseen toteutukseen ja käyttöönottoon eroavat merkittävästi eri tietojenkäsittely-ympäristöissä ja käyttötarkoituksissa. Esimerkiksi kaikista verkoista fyysisesti eriytetyssä työasemassa käytettävän toimisto-ohjelmiston turvallisuudelle asetettavat tarpeet eroavat tarpeista, jotka kohdistuvat useiden käyttäjien saavutettavissa olevaan asianhallintajärjestelmään.		

	Ohjelmistoihin liittyviä riskejä ja turvallisuustarpeita voidaan arvioida esimerkiksi ohjelmiston käyttötarkoituksen ja sen turvallisuutta mahdollisesti toteuttavan roolin, hyökkäyspinta-alan, sekä käsiteltävien tietojen luonteen ja turvallisuusluokan avulla. Mikäli ohjelmiston käyttötarkoituksena ja roolina on toimia esimerkiksi pääsyä rajaavana mekanismina turvallisuusluokiteltujen tietojen käsittelyssä, ohjelmiston luotettavasta toiminnasta tulisi pystyä varmistumaan. Ohjelmistoon kohdistuva hyökkäyspinta-ala voi vaikuttaa oleellisesti ohjelmistoon kohdistuviin turvallisuustarpeisiin. Tyypillisesti esimerkiksi turvallisuusluokan IV palvelut voivat olla saavutettavissa laajemmin ja heterogeenisemmän joukon toimesta, kuin esimerkiksi turvallisuusluokkien III-II palvelut. Ohjelmistoille asetettavat turvallisuusvaatimukset voivatkin olla turvallisuusluokan IV järjestelmissä joiltain osin tiukempia kuin esimerkiksi sellaisissa tiukasti eristetyissä ja suppeissa korkeamman turvallisuusluokan järjestelmissä, joissa jokaisella käyttäjällä on tiedonsaantitarve (need-to-know) kaikkeen järjestelmässä käsiteltävään tietoon. Käsiteltävien tietojen turvallisuusluokka ja oletettu kiinnostavuus ulkopuolisille toimijoille voi vaikuttaa ohjelmistoon kohdistuvaan riskiin ja suojaustarpeisiin. Esimerkiksi poliittisesti suuren ulkopuolisen kiinnostuksen kohteena olevat tiedot, tai korkealle turvallisuusluokitellut tiedot, voivat vaikuttaa merkittävästi ohjelmistoon kohdistuviin riskeihin ja turvallisuustarpeisiin myös kaikkein edistyneimpiin hyökkäyksiin varautumisessa. Otettaessa käyttöön valmisohjelmistoa sekä tilattaessa räätälöityä tai itse tuotettua ohjelmistoa on tilaajan jo suunnitteluvaiheessa kiinnitettävä huomiota ohjelmiston ja sen käyttämien oheiskomponenttien tietoturvalliseen kehitykseen. Huomiota on kiinnitettävä myös muihin koko ohjelmiston elinkaaren kattaviin tekijöihin. Tekijöitä ovat esimerkiksi käyttöönotonaikaiset vaatimukset, sopimustekniikka, päivityskäytännöt ja muutostenhallinta. Turvallisuusluokitellun tiedon suojaukseen oleellisesti vaikuttavat ohjelmistot on toteutettava turvallisen ohjelmistokehityksen käytäntöihin nojautuen, kattaen sekä ohjelmistokoodin laadun että ohjelmistokehityksen prosessit. Ohjelmiston vaatimusmäärittelyssä tulee jo hankintavaiheessa huomioida lainsäädännöstä johdetut vaatimukset. Erityisesti salauksiin (I-12), hallintaliittymiin (I-04), käyttäjähallintaan ja -tunnistukseen (I-06, I-07), kovennuksiin (I-08) ja jäljitettävyyteen (lokitukseen, I-10) liittyvät kokonaisuudet tulee huomioida myös ohjelmistojen toteutuksissa. Ohjelmistojen toteutukset eivät saa vaarantaa tiedonsaantitarpeen (need-to-know) toteutumista, tai tarjota ulkopuolisille toimijoille pääsyä suojattavaan tietojenkäsittely-ympäristöön tai sen osakokonaisuuksiin. Elinkaaren vaiheissa tulee varmistua erityisesti ohjelmistokorjausten tekemisen vastuutuksista, sekä mahdollistettava ohjelmiston turvallisuuden ylläpito myös uusia hyökkäystekniikoita vasten. Myös valmisohjelmistojen riittävästä laadusta voidaan pyrkiä varmistumaan vastaavia periaatteita noudattaen. Joskus voi tulla tarve käyttää palveluita, joiden ohjelmakoodin ja sen kehityskäytäntöjen näkyvyys on heikkoa tai jopa olematonta. Tällaisten ohjelmistojen luotettavuudesta voidaan pyrkiä saamaan näyttöä esimerkiksi tutkimalla päivitystiheyksiä, dokumentaatiota ja mahdollista muuta näkyvyyttä, kuten olemassa olevia testiraportteja. Tällaisissa tilanteissa voi turvallisen konfiguroinnin lisäksi hyödyntää myös korvaavia suojauksia. Turvallisessa konfiguroinnissa ja korvaavina suojauksina voi tietyin rajoituksin hyödyntää

	esimerkiksi tehostettua havainnointikykyä, kovennuksia, koodin suorituksenaikaista rajoittamista (esim. AppLocker, SELinux, AppArmor), sovelluspalomuureja (WAF), sekä koko ohjelmiston loogista eriyttämistä esimerkiksi virtualisointia hyödyntäen. Ohjelmistojen turvallisuudesta varmistumiseen tulee hyödyntää aihepiirin tarkentavia ohjeita ja standardeja. Näitä ovat esimerkiksi VAHTI Sovelluskehityksen tietoturvaohje (VAHTI 1/2013), OWASP Application Security Verification Standard (ASVS) ja Kyberturvallisuuskeskuksen ohje "Turvallinen tuotekehitys: kohti hyväksyntää". *Toteutusesimerkki* 1) Ohjelmistojen (sovellukset, palvelut, järjestelmät) käyttötarkoitukset ja ohjelmistojen turvallisuutta mahdollisesti toteuttavat roolit on tunnistettu. 2) Ohjelmistojen (sovellukset, palvelut, järjestelmät) turvallisuustarpeet on arvioitu, huomioiden erityisesti ohjelmiston käyttötarkoituksen ja sen turvallisuutta mahdollisesti toteuttavan roolin, hyökkäyspinta-alan, sekä käsiteltävien tietojen luonteen ja turvallisuusluokan. 3) Ohjelmistojen (sovellukset, palvelut, järjestelmät) riippuvuudet ja rajapinnat on tunnistettu. Riippuvuuksiin ja rajapintoihin on kohdistettu ohjelmistoa vastaavat vaatimukset, huomioiden esimerkiksi käytetyt kirjastot, rajapinnat (API:t) ja laitteistosidonnaisuudet. Vaatimuksissa on huomioitu sekä palvelin- että asiakaspuolen osuudet. 4) Kriittiset ohjelmistot (sovellukset, palvelut, järjestelmät) toteutetaan tai toteutus tarkastetaan mahdollisuuksien mukaan luotettavaa standardia vasten tai/ja turvallisen ohjelmoinnin ohjetta hyödyntäen. 5) On varmistettu, että ohjelmistojen (sovellukset, palvelut, järjestelmät) ohjelmakoodin laadun ylläpito, kehitys ja muutoshallinta vastaavat tarpeita koko elinkaaren ajan. 6) On varmistettu, että ohjelmistot (sovellukset, palvelut, järjestelmät) täyttävät lainsäädännöstä johdetut vaatimukset. Erityisesti huomioitava salauksiin (I-12), hallintaliittymiin (I-04), käyttäjähallintaan ja -tunnistukseen (I-06, I-07), kovennuksiin (I-08) ja jäljitettävyyteen (lokitukseen, I-10) liittyvät kokonaisuudet. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 2; CIS Critical Security Controls (v7.1) / 18; BSI IT-Grundschutz-Compendium Edition 2019; CPNI - Development and Implementation of Secure Web Applications; OWASP Application Security Verification Standard Project (ASVS); CWE TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; ISO/IEC 27002:2017 14.1.1; ISO/IEC 27002:2017 14.1.2; ISO/IEC 27002:2017 14.1.3; ISO/IEC 27002:2017 14.2.8; ISO/IEC 27002:2017 14.2.9; VAHTI 1/2013; Turvallinen tuotekehitys: kohti hyväksyntää; PiTuKri MH-02

I-14	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)

Monitasoinen suojaaminen - Hajasäteily (TEMPEST) ja elektroninen tiedustelu	1) Turvatoimia toteutetaan turvallisuusluokiteltuihin tietoihin liittyvässä tietojenkäsittely-ympäristössä toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymillä menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPEST-turvatoimet). 2) Käsiteltäessä turvallisuusluokan III tai II tietoja sähköisesti, on pidettävä huolta, että elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. 3) Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja turvallisuusluokkaan.	1) 1101/2019: 11 § 2) 1101/2019: 11 § 3) 1101/2019: 11 §	1) 10 artiklan 5 kohta 2) 1 artiklan 2 kohta (tarkistettava) 3) 10 artiklan 5 kohta
	Lisätietoja		
	Yleistä Turvallisuusluokan IV käsittely-ympäristöille ei ole erityisiä vaatimuksia. Turvallisuusluokkien III-II käsittely-ympäristöissä raja-arvot ylittävän hajasäteilyn osalta suojautuminen toteutetaan ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymillä menettelyillä. Kansainvälisen turvallisuusluokitellun tiedon tapauksessa toimivaltaisena viranomaisena toimii kansallinen TEMPEST-viranomainen (NTA, National TEMPEST Authority, Suomessa Liikenne- ja viestintäviraston NCSA-toiminto). Turvallisuusluokan III tietojen osalta on laajemmat mahdollisuudet hyväksyä korvaavia menettelyjä riittävän suojauksen saavuttamiseksi. Kohteen hajasäteilyn vastatoimien riittävyys voidaan todentaa vyöhykemittauksella (facility zoning measurement) tai suojatun tilan mittauksella (shielded enclosure measurement). *Muita lisätietoja* Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 11.2.3		

Käyttöturvallisuus

I-15 **Turvallisuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä - Tiedon sähköinen välitys**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	1) Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella, tieto/tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä. 2) Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.	1) 1101/2019 12 § ja 11 §:n k 7, ja 906/2019 14 § 2) 1101/2019 12 § ja 11 §:n k 7, ja 906/2019 14 §	1) 9 artiklan 4 kohta 2) IV liitteen 31 kohta
	Lisätietoja		
	Yleistä Turvallisuusluokitellun tiedon sähköiseen välitykseen liittyy useita riskejä. Riskien pienentäminen hyväksyttävälle tasolle edellyttää sekä henkilöstöön että tekniseen toteutukseen liittyvien tekijöiden huomiointia. Tilanteissa, joissa turvallisuusluokiteltua tietoa on tarve välittää esimerkiksi kahden organisaation välillä julkisen verkon kautta, turvallinen välitys edellyttää turvallisia salausratkaisuja ja avainhallintakäytäntöjä, sekä niiden käyttöön harjaantunutta henkilöstöä. Tilanteissa, joissa salausratkaisun käyttö edellyttää henkilöstön toimia (esimerkiksi turvallisuusluokan IV dokumentin välitys toiseen organisaatioon sähköpostin salattuna liitteenä), tulee kiinnittää erityistä huomiota salausratkaisun turvallisen käytön jalkautukseen henkilöstölle. Teknisesti turvallinen salausratkaisu ei tuota turvallisuusluokitellulle tiedolle riittävää suojausta esimerkiksi tilanteissa, joissa avainhallintakäytännöt ovat puutteellisia, tai joissa henkilöstö ei käytä salausratkaisua siihen liittyvien turvallisen käytön periaatteiden mukaisesti. Turvallisia salausratkaisuja ja avainhallintakäytäntöjä on käsitelty tarkemmin kohdassa I-12. Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut (dark fiber) tulkitaan julkisiksi verkoiksi. Tämä kattaa puhelimen, telekopion (faksi), sähköpostin, pikaviestimet ja muut vastaavat tietoverkon kautta toimivat tiedonsiirtomenetelmät. Turvallisuusluokiteltua tietoa sisältävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) suojaamisperiaatteet kuvataan vaatimuksessa I-18. Radiorajapinnan käyttö langattomissa verkkoyhteyksissä (esim. WLAN, 3-5G, Bluetooth) tulkitaan poistumiseksi fyysisesti suojatun turvallisuusalueen ulkopuolelle. Langattomien verkkojen radiorajapintaa tulisi toisin sanoen käsitellä kuin julkista verkkoa. (Vrt. I-05.)		

	Toteutusesimerkki Turvallisuusluokkien IV-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Siirrettäessä turvallisuusluokiteltua tietoa ko. turvallisuusluokalle hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella verkon kautta tulee ottaa huomioon erityisesti salauksen rooli keskeisenä suojauksena (vrt. I-01, I-12 ja I-18). a) Henkilöstöllä on käytössä työvälineet ja menetelmät turvallisuusluokitellun tiedon suojaamiseksi toimivaltaisen viranomaisen hyväksymällä salausratkaisulla. b) Henkilöstön osaamisesta toimivaltaisen viranomaisen hyväksymän salausratkaisun turvalliseen käyttöön on varmistuttu (esimerkiksi ohjeistus, koulutus ja valvonta). 2) Tilanteissa, joissa turvallisuusluokiteltua tietoa siirretään fyysisesti suojattujen turvallisuusalueiden sisäpuolella, a) ko. turvallisuusluokan liikennekanava on fyysisesti suojattu (esimerkiksi kaapelointi, joka kulkee kokonaisuudessaan suppean, esimerkiksi vain yhden huoneen kattavan ko. turvallisuusluokan tiedon säilytykseen hyväksytyn fyysisesti suojatun turvallisuusalueen sisällä), tai b) tieto suojataan toimivaltaisen viranomaisen erillishyväksyntään perustuen matalamman tason salauksella (esim. HTTPS ko. turvallisuusluokan verkon sisäisessä liikenteessä). *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 13; CIS Critical Security Controls (v7.1) / 14; BSI IT-Grundschutz-Compendium Edition 2019; Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje; ISO/IEC 27002:2017 10.1.1; ISO/IEC 27002:2017 13.2.1; ISO/IEC 27002:2017 13.2.3; PiTuKri JT-05; PiTuKri SA-02; PiTuKri SA-03

I-16	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Turvallisuusluokitellun tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Muutoshallintamenettelyt	1) Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen. 2) Turvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. 3) Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia.	906/2019 13 § ja 15 §	1) IV liitteen 8 kohta 2) IV liitteen 11 ja 16 kohdat 3) IV liitteen 12 kohta

	Lisätietoja *Yleistä* Tietojenkäsittely-ympäristön tietoturvallisuuden ja muutosten luotettava hallinta edellyttää, että ympäristön tekninen rakenne ja esimerkiksi kaikki siihen kuuluvat laitteistot ja ohjelmistot ovat tiedossa. Ajantasaista kirjanpitoa vasten tarvittavat muutokset kyetään koko elinkaaren ajan kohdistamaan täsmällisesti, muutosten vaikutukset ovat helpommin ennustettavissa ja ympäristön turvallisuuden tarkastelu on mahdollista suorittaa. Kirjanpidon toteuttamisessa voi hyödyntää esimerkiksi verkkokuvia, laite- ja ohjelmistokomponenttiluetteloita sekä konfiguraatiotietokantoja. Tietojenkäsittely-ympäristön tietoturvallisuudesta tulee pystyä varmistumaan koko elinkaaren ajan. Tämä edellyttää muutostarpeiden jatkuvaa seurantaa sekä säännöllisiä muutoksia. Muutostarpeita voi seurata esimerkiksi tietojenkäsittely-ympäristön järjestelmien elinkaaren päättymisestä tai nykyisten suojausten kyvyttömyydestä vastata uusiin hyökkäysmenetelmiin. Esimerkiksi ohjelmistojen päivitykset voivat aiheuttaa odottamattomia seurauksia, kuten turvallisuusasetusten ja käyttöoikeuksien muuttumista tai uusien turvattomien palvelujen mukaantuloa tietojenkäsittely-ympäristöön. Haitallisia seurauksia voidaan pyrkiä ennaltaehkäisemään esimerkiksi kattavalla testauksella ja muutoslokien (tyypillisesti esim. changelog, readme) tarkastelulla. Haitallisia seurauksia voidaan pyrkiä havainnoimaan esimerkiksi (testiympäristöön asennettujen) päivitysten jälkeisten konfiguraatioiden tarkastelulla, sekä muun muassa automatisoiduilla skannauksilla ja konfiguraatiovertailuilla. Laitteiston suojauksessa luvattomien laitteiden kytkemistä vastaan voidaan hyödyntää esimerkiksi a) laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan, b) peukalointia vastaan suojattujen laitteiden käyttämistä, tai c) jotain vastaavaa menettelyä (esim. käytettävien laitteiden sinetöintiä). Käytettäessä sinetöintiin perustuvaa menetelmää, tulisi sinettien eheyden tarkastamiseen olla säännöllinen prosessi. Luvattomien muutosten tai laitteistojen tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu kyseessä olevassa kohteessa toteutetuista menetelmistä, joilla rajoitetaan ja valvotaan kohteeseen (tietojärjestelmä, fyysinen tila) pääsyä. Useimmissa ympäristöissä voi riittää tarkastukset esimerkiksi puolivuosittain tai vuosittain. *Toteutusesimerkki* Turvallisuusluokkien IV-III käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Tietojenkäsittely-ympäristön kokoonpanosta on olemassa ajantasainen kirjanpito. Kirjanpidolla tarkoitetaan laitteisto- ja ohjelmistokirjanpitoa, sekä tietoa turvallisuuteen vaikuttavista konfiguraatioista ja menettelyistä.

	2) Tietojenkäsittelyyn ja tietojenkäsittely-ympäristöön liittyviin muutoksiin on käytössä muutostenhallintamenettely. Muutokset ovat jäljitettävissä. 3) On olemassa menetelmät, joilla varmistetaan tietojenkäsittely-ympäristön turvallisuustason säilyminen tehtyjen muutosten yhteydessä. 4) Kirjanpito on sellaisella tasolla, että siitä pystytään selvittämään tietojenkäsittely-ympäristössä käytetyt laitteet ja ohjelmistot versiotietoineen (laite-, käyttöjärjestelmä- ja sovellusohjelmistot) ja se tukee myös haavoittuvuuksien hallintaa (vrt. I-19). 5) Tietojenkäsittely-ympäristöjä tarkkaillaan luvattomien muutosten tai laitteistojen havaitsemiseksi. Tietojenkäsittely-ympäristön kirjanpito pidetään ajan tasalla koko elinkaaren ajan. 6) Tietojenkäsittely-ympäristön turvallisuuden toteuttamiseen liittyvän aineiston (dokumentaatiot, sähköiset kirjanpidot ja vast.) luokittelu- ja suojaamistarpeet on määritetty. Turvallisuusluokan II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1-6 lisäksi toteutetaan seuraavat toimenpiteet: 7) Laitteistot suojataan luvattomien laitteiden (näppäilynauhoittimet, langattomat lähettimet ml. mobiililaitteet ja vastaavat) liittämistä vastaan. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 1; CIS Critical Security Controls (v7.1) / 2; BSI IT-Grundschutz-Compendium Edition 2019; Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje; ISO/IEC 27002:2017 8.1.1; ISO/IEC 27002:2017 12.1.1; ISO/IEC 27002:2017 12.1.2; ISO/IEC 27002:2017 12.5.1; ISO/IEC 27002:2017 14.2.2; ISO/IEC 27002:2017 14.2.8; ISO/IEC 27002:2017 14.2.9; ISO/IEC 27002:2017 18.2.3; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri MH-01

I-17 **Turvallisuusluokiteltujen tietojen käsittely fyysisesti suojattujen alueiden sisällä - Fyysinen turvallisuus**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Turvallisuusluokka IV 1) Turvallisuusluokiteltuja tietoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta (vrt. F-04 ja I-18). 2) Tietojen käsittely on mahdollista toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla (vrt. F-04) ja toimivaltaisen viranomaisen hyväksymillä menettelyillä turvallisuusalueiden ulkopuolella (vrt. I-18).	1) 1101/2019 10 § 2) 1101/2019 10 § 3) 1101/2019 10 § 4) 1101/2019 10 § 5) 1101/2019 10 § 6) 1101/2019 10 §	1) 8 artiklan 3 kohta 2) II liitteen 23 kohta, 8 artiklan 3 kohta 3) II liitteen 24 kohta, 8 artiklan 3 kohta, 9 artiklan 4 kohta 4) II liitteen 24 kohta

	3) Tietojen säilytys on mahdollista toimivaltaisen viranomaisen hyväksymillä turvallisuusalueilla (vrt. F-04) ja toimivaltaisen viranomaisen hyväksymillä menettelyillä turvallisuusalueiden ulkopuolella (vrt. I-18). 4) Turvallisuusluokan IV tietoja sisältävät tietovarannot ja näiden tietojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle (vrt. F-04). <u>*Turvallisuusluokka III-II*</u> Kohtien 1 ja 2 lisäksi: 5) Tietojen säilytys on mahdollista toimivaltaisen viranomaisen hyväksymillä turva-alueilla (vrt. F-04). Vrt. vain kansallisia tietoja koskeva poikkeus kohdassa 6 sekä etäkäyttö kohdassa I-18. 6) Vain kansallisten turvallisuusluokan III sähköisten tietojen säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueen ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla (vrt. I-12), ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä (vrt. F-04). Vrt. etäkäyttö kohdassa I-18.		5) II liitteen 22 ja 26 kohdat, 8 artiklan 4 kohta 6) -
	Lisätietoja		
	<u>*Yleistä*</u> Tilanteissa, joissa turvallisuusluokan III tai II tietoa käsitellään tilapäisesti luokkaa matalamman tason tilassa, tulisi esimerkiksi hajasäteilysuojaus (vrt. I-14) toteuttaa ko. tiedon turvallisuusluokan mukaisesti. Toteutuksessa huomioitava myös esimerkiksi toiminta työskentelytaukojen aikana (tieto vietävä esimerkiksi turva-alueen kassakaappiin tauon ajaksi), näkyvyyden rajaus tilaan (esim. mahdollisten ikkunoiden peittäminen) ja käsittelytilaan pääsyn rajaaminen vain hyväksyttyihin henkilöihin. Hallinnolliselle alueelle, turva-alueille sekä esimerkiksi kassakaapeille asetettavat vaatimukset on kuvattu yksityiskohtaisemmin Katakrin F-osa-alueessa (ks. F-02, F-03 ja F-04). Naton turvallisuusluokiteltujen tietojen käsittelyssä huomioitava, että suojausperiaatteet eroavat osin kansallisiin ja EU:n turvallisuusluokiteltuihin tietoihin sovellettavista. <u>*Sähköinen käsittely hallinnollisella alueella*</u>		

	Tiedon käsittelyyn käytettävän tietojärjestelmän tai tietoliikennejärjestelyn tulee olla kyseisen turvallisuusluokan mukaisesti suojattu. Esimerkiksi turvallisuusluokan III mukaisesti suojattu päätelaite voidaan tuoda hallinnolliselle alueelle tai sen ulkopuolelle, josta päätelaite ottaa turvallisuusluokan III mukaisella liikennesalauksella suojatun yhteyden turva-alueella sijaitsevaan turvallisuusluokan III tietovarantoon tietojen käsittelyn ajaksi. Päätelaitetta ei voi jättää ilman valvontaa hallinnolliselle alueelle, vaan se tulee palauttaa käsittelyn jälkeen säilytettäväksi turva-alueelle, ellei päätelaitteen luottamuksellisuudesta, eheydestä ja käytettävyydestä pystytä muuten varmistumaan (vrt. F-04). Turvallisuusluokkien III tai II kiinteää tietoverkkoa ei voi ulottaa hallinnolliselle alueelle. *Kansallisten turvallisuusluokkien IV tai III tietojen käsittely ja säilyttäminen päätelaitteessa* Tilanteissa, joissa kansallista turvallisuusluokan IV tai III tietoa käsitellään ja säilytetään kyseisen turvallisuusluokan mukaisessa päätelaitteessa turvallisuusalueiden ulkopuolella, tai turvallisuusluokan III tietoja hallinnollisella alueella, päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla (vrt. I-12), ja erityisesti päätelaitteen kyseiselle turvallisuusluokalle riittävästä eheydestä tulee huolehtia toimivaltaisen viranomaisen hyväksymällä menetelmällä (vrt. F-04). Päätelaitteen eheys tulee pystyä varmistamaan riittävällä tasolla, jotta tiedon luottamuksellisuus ei vaarannu päätelaitteen eheyden menetyksen seurauksena. Tyypillisin tapa tietojärjestelmän eheydestä varmistumiseen on sen suojaaminen turvallisuusalueiden fyysisen pääsynhallinnan menettelyin, mukaan lukien esimerkiksi kaikki tietojärjestelmään liittyvät fyysiset palvelimet, verkkolaitteet, päätelaitteet sekä esimerkiksi kaapeloinnit. Esimerkiksi turvallisuusluokan IV tietojärjestelmän eheyden suojaamisessa yleisiä turvallisuusluokiteltuun tietoon kohdistuvia riskejä vastaan voi riittää tietojärjestelmän tietovarantojen sijoittaminen hallinnolliselle tai turva-alueelle, sekä riittävällä salauksella varustettujen päätelaitteiden osalta myös rajattu säilytys muussa lukittavassa tilassa, esimerkiksi virkamiehen kotona. Turvallisuusluokan III tietojärjestelmät tulisi kokonaisuudessaan sijoittaa turva-alueelle. Mikäli turvallisuusluokan III tietojen käsittelyyn käytettävää päätelaitetta joudutaan säilyttämään hallinnollisella alueella (vrt. F-04) 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/ja että pääsystä jää jälki kyseiseen koteloon tai pakkaukseen. Riskienarvioinnissa tulee 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. Turvallisuusluokan III päätelaitteen säilyttämisessä on otettava huomioon myös kansainväliset tietoturvavelvoitteet, joissa turva-alueen ulkopuolinen säilyttäminen voi olla kokonaan kielletty. *Muita lisätietoja* BSI IT-Grundschutz-Compendium Edition 2019; CPNI - Security Advice - Physical Security; ISO/IEC 27002:2017 11.1.1; ISO/IEC 27002:2017 11.1.3; ISO/IEC 27002:2017 11.1.5; ISO/IEC 27002:2017 11.2.1; Tiedonhallintalautakunnan suositus (2020:19, luku 5); PiTuKri FT-02

I-18	Vaatimus	Lähde (906/2019 ja/tai 1101/2019)	Lähde (2013/488/EU)
Turvallisuusluokiteltujen tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - Etäkäyttö ja etähallinta	*Turvallisuusluokka IV* 1) Käyttäjät ja päätelaitteet tunnistetaan riittävän luotettavasti. Tietojen välitys ja käsittely turvallisuusalueiden (vrt. F-04) välillä on mahdollista vain toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymien korvaavien menettelyjen mukaisesti. 2) Turvallisuusluokiteltuja tietoja on turvallisuusalueiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan. 3) Elleivät turvallisuusalueiden ulkopuolelle viedyt turvallisuusluokiteltua tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä, tietovälineitä ei jätetä valvomatta. 4) Järjestelmien etäkäyttö ja -hallinta edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokan tietojen suojaamiseen hyväksymää liikenteen salausta. 5) Päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja päätelaitteen ko. turvallisuusluokalle riittävästä eheydestä tulee huolehtia.	1) 1101/2019 11 §:n k 5 2) 906/2019 4 § 3) 1101/2019 10 § ja 13 § 4) 1101/2019 12 § ja 11 §:n k 7, ja 906/2019 14 § 5) 1101/2019 10 §, 11 § ja 12 § 6) 1101/2019 13 § 7) 1101/2019 10 § (TL II) 8) 1101/2019 10 § (TL III)	1) 8 artiklan 3 kohta, 9 artiklan 4 kohta 2) IV liitteen 22 kohta 3) 9 artiklan 4 kohta, III liitteen 28, 30 ja 33 kohdat 4) 10 artiklan 6 kohta 5) 1 artiklan kohta 2 6) 9 artiklan 4 kohta, III liitteen 28, 30 ja 33 kohdat 7) II liitteen 25-26 kohdat, 8 artiklan 4 kohta 8) -

	Turvallisuusluokka III-II Kohtien 1-5 lisäksi: 6) Turvallisuusluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla. 7) Järjestelmien etäkäyttö ja -hallinta rajataan toimivaltaisen viranomaisen hyväksymälle turvallisuusalueelle (vrt. F-04). 8) Vain kansallisten turvallisuusluokan III sähköisten tietojen etäkäyttö (käsittely) ja säilytys on mahdollista kyseisen turvallisuusluokan mukaisessa päätelaitteessa turva-alueiden ulkopuolella edellyttäen, että a) tiedot on suojattu ko. turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja että b) päätelaitteen tietoturvallisuudesta, erityisesti ko. turvallisuusluokalle riittävästä luottamuksellisuudesta ja eheydestä on huolehdittu toimivaltaisen viranomaisen hyväksymällä menetelmällä.		
	Lisätietoja		
	Yleistä Etäkäytöllä ja -hallinnalla tarkoitetaan perinteisessä merkityksessään organisaation toimitilojen ulkopuolelta tapahtuvaa tietojärjestelmien käyttöä/hallintaa tätä tarkoitusta varten hankitulla päätelaitteella. Normaalisti päätelaitteena toimii organisaation henkilön käyttöön antama kannettava tietokone. Turvallisuusluokitellun tiedon osalta etäkäyttö ja -hallinta soveltuu perinteisessä merkityksessään vain turvallisuusluokan IV tiedoille. Turvallisuusluokasta III lähtien tiedon käsittely edellyttää toimivaltaisen viranomaisen hyväksymää fyysisesti suojattua turvallisuusaluetta, ellei toimivaltainen viranomainen ole hyväksynyt korvaavia menettelyjä, joilla saavutetaan vastaavat fyysisen turvallisuuden olosuhteet (esimerkiksi tietyissä viranomaisoperaatioissa). Poikkeuksena vain kansallisten turvallisuusluokan III sähköisten tietojen etäkäyttö ja säilytys ko. turvallisuusluokan mukaisessa päätelaitteessa (vrt. I-17:n Lisätietoja-kentän kohta "Kansallisten turvallisuusluokkien IV tai III tietojen käsittely ja säilyttäminen päätelaitteessa"). Sekä kansallisten että kansainvälisten turvallisuusluokan III käsittely-ympäristöjen etähallinta tulee rajata toimivaltaisen viranomaisen hyväksymille turvallisuusalueille. Vaatimuksessa 1 tarkoitettuihin toimivaltaisen viranomaisen hyväksymiin korvaaviin menettelyihin sisältyvät turvallisuusluokan IV käsittely-ympäristöissä seuraavat: a. Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta.		

	b. Vain käyttöympäristöön hyväksyttyjä laitteita ja etäyhteyksiä käytetään. Turvallisuusluokkien III ja II käsittely-ympäristöissä korvaavana menettelynä edellytetään lisäksi käytön teknistä sitomista hyväksyttyyn etäkäyttölaitteistoon (esim. laitetunnistus). Henkilöstön koulutuksessa ja ohjeistuksessa on huomioitava erityisesti turvallisuusluokiteltujen tietojen suojaaminen sivullisilta. Sivullisilta suojaamiseen sisältyy muun muassa mahdollisten käsittelypaikkojen valinta ja erilaisiin paikkoihin liittyvät rajoitteet käsittelylle (salakatselun ja salakuuntelun estäminen), päätelaitteiden ja muiden työvälineiden suojaaminen varkauksilta ja peukaloinneilta (säilytys vain lukitussa tilassa ja aina muistialueiden salaus aktivoituna, sekä esimerkiksi suojapakkausten ja -koteloiden käyttö, vrt. I-17:n Lisätietoja-kenttä), sekä muut kyseisten päätelaitteiden ja muiden työvälineiden turvallisen käytön menettelyt. Hallintayhteyksien suojaus on eräs kriittisimmistä tietojärjestelmien turvallisuuteen vaikuttavista tekijöistä (vrt. I-04). Erityisesti turvallisuusluokan IV järjestelmiä voi kuitenkin olla perusteltua pystyä hallinnoimaan myös fyysisesti suojattujen turvallisuusalueiden ulkopuolelta. Tilanteissa, joissa etähallinta nähdään perustelluksi, suositellaan se suojattavan etäkäyttöä kattavammilla turvatoimilla. Esimerkiksi turvallisuusluokan IV järjestelmän etähallintayhteydet voidaan rajata yksittäisiin fyysisiin ja loogisiin pisteisiin. *Muita lisätietoja* CPNI - Personnel Security in Remote Working; CPNI - Configuring and managing Remote Access for Industrial Control Systems; BSI IT-Grundschutz-Compendium Edition 2019; CPNI - Security Advice - Physical Security; ISO/IEC 27002:2017 6.2.1; ISO/IEC 27002:2017 6.2.2; ISO/IEC 27002:2017 7.2.2; ISO/IEC 27002:2017 8.3.1; ISO/IEC 27002:2017 8.3.3; ISO/IEC 27002:2017 11.1.1; ISO/IEC 27002:2017 11.1.3; ISO/IEC 27002:2017 11.1.5; ISO/IEC 27002:2017 11.2.1; ISO/IEC 27002:2017 11.2.3; ISO/IEC 27002:2017 11.2.5; ISO/IEC 27002:2017 11.2.6; ISO/IEC 27002:2017 12.1.1; PiTuKri IP-03; PiTuKri JT-05; PiTuKri SA-02

I-19 **Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Ohjelmisto-**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.	906/2019 13 §	IV liitteen 8, 11 ja 16 kohdat
	Lisätietoja		
	Yleistä		

haavoittu-vuuksien hallinta	Ohjelmistovirheiden, toisin sanoen haavoittuvuuksien, hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. On huomioitava, että haavoittuvaa lähdekoodia on niin käyttöjärjestelmäohjelmistoissa, palvelinsovelluksissa, loppukäyttäjäsovelluksissa, kuin esimerkiksi laiteohjelmistotason (firmware) sovelluksissa ja ajureissa, BIOS:issa ja erillisissä hallintaliittymissä (esim. iLo, iDrac). Ohjelmistovirheiden lisäksi haavoittuvuuksia aiheutuu konfiguraatiovirheistä ja vanhoista käytänteistä, esimerkiksi vanhentuneiden salausalgoritmien käytöstä. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Riskejä voidaan pienentää korjausten asennuksilla. Haavoittuvuuden hallintaa toteuttaessa tulee huolehtia haavoittuvuusskannerin, CMDB:n ja muiden järjestelmien ajantasaisuudesta ja tietoturvallisuudesta. Haavoittuvuuksien hallinnan tulisi tähdätä tarkan tilannekuvan muodostamiseen siten, että toimintaan liittyy ohjelmisto- ja järjestelmäympäristön jatkuva seuranta ja kehittäminen. Osana tilannekuvan ylläpitoa havaittujen puutteiden ja haavoittuvuuksien aiheuttama riski tulisi arvioida suhteessa käyttöympäristöön ja asettaa korjaavat toimenpiteet perustuen tämän arvion kriittisyyteen. Korjaavia toimenpiteitä ovat mm. ohjelmistotoimittajien haavoittuvuuskorjaukset, päivitykset ja konfiguraatiomuutokset, jotka tähtäävät riskin poistamiseen tai rajaamiseen. Lisäksi on syytä seurata käytettävien ohjelmistoversioiden tukea niiden toimittajalta. Vanhentuneisiin ohjelmistoversioihin ei julkaista aktiivisesti päivityksiä, jolloin myös tietoturvahaavoittuvuuksien korjaaminen voi olla mahdotonta. Tehokas prosessimainen haavoittuvuuksien hallinta edellyttää organisoitua ja vastuutettua toimintamallia, sekä yleensä myös organisaation sisäisten ja ulkoisten sidosryhmien yhteistyötä. Ohjelmistohaavoittuvuuksien hallintaa voidaan toteuttaa esimerkiksi siten, että 1) Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen. Poiminnan mahdollistamiseksi on olemassa ajantasainen järjestelmäkirjanpito ohjelmistojen ja näiden versioiden osalta (ks. järjestelmäkirjanpito kohdasta I-16). Ladattujen ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus) ennen niiden jakamista tuotantoympäristöön. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eristetyssä testiympäristössä tai pienellä käyttäjäjoukolla. 2) Päivitysten asentumisen onnistumista tarkastellaan säännöllisesti, vähintään kuukausittain. Tarkasteluun voidaan hyödyntää esimerkiksi keskittyjä päivityksenjako- ja -hallintapalveluita tai vastaavia menettelyjä. 3) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti (haavoittuvuusskannaus, CMDB jne.) säännöllisesti ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. 4) Laitteisto- ja ohjelmistokirjanpidon (vrt. I-16) sekä skannausohjelmiston ajantasaisuudesta ja tietoturvallisuudesta on huolehdittu. Erityisesti skannausohjelmistot voivat edellyttää laajoja pääsyoikeuksia eri tietojenkäsittely-ympäristön osiin tuottaakseen luotettavia havaintoja, mikä tulee huomioida skannausohjelmiston suojaamisessa (pääsynhallinta, jäljitettävyys).

	5) Löytyneiden haavoittuvuuksien sekä päivitysmenettelyjen puutteiden käsittely on järjestetty siten, että tietojenkäsittely-ympäristön suojaamiseen oleellisesti vaikuttavat heikkoudet poistetaan, korjataan tai muuten rajoitetaan siten, että turvallisuusluokiteltujen tietojen käsittely ei tarpeettomasti vaarannu. Haavoittuvuuksien vakavuuden arviointiin voi hyödyntää esimerkiksi CVE-luokittelua ja sen suhteuttamista kyseiseen käsittely-ympäristöön toteutettuihin haavoittuvuuksien hyödyntämistä estäviin, rajaaviin ja havaitseviin suojauksiin. *Toteutusesimerkki* Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että haavoittuvuuksien hallintaan on olemassa prosessi, joka sisältää vähintään alla mainitut toimenpiteet: 1) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan aktiivisesti ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti. 2) Päivitysten asentumisen onnistumista tarkastellaan säännöllisesti, vähintään kuukausittain. 3) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus, CMDB jne.) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. 4) Laitteisto- ja ohjelmistokirjanpidon (ml. CMDB) sekä skannausohjelmiston ajantasaisuudesta ja tietoturvallisuudesta on huolehdittu. 5) Löytyneiden haavoittuvuuksien sekä päivitysmenettelyjen puutteiden käsittely on järjestetty siten, että tietojenkäsittely-ympäristön suojaamiseen oleellisesti vaikuttavat heikkoudet poistetaan, korjataan tai muuten rajoitetaan siten, että turvallisuusluokiteltujen tietojen käsittely ei tarpeettomasti vaarannu. Turvallisuusluokkien III ja II käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että kohtien 1-2 ja 4-5 lisäksi toteutetaan seuraava toimenpide: 6) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti vähintään (haavoittuvuusskannaus, CMDB jne.) puolivuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. "Merkittäviin muutoksiin" voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien käyttöönotot ja/tai vanhojen service pack -tason päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne. *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 3; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 12.6.1; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-04

I-20 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Varmuuskopiointi	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Turvallisuusluokiteltua tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto on suojattu.	906/2019 13 ja 15 §, 1101/2019 7 §, 11 § ja 14 §	III liitteen 18 ja 27 kohdat, IV liitteen 8 ja 16 kohdat
	Lisätietoja		
	Yleistä Varmuuskopiointi suositellaan aina mitoitettavan toimintavaatimuksiin. Toimintavaatimuksiin nähden riittävässä varmuuskopioinnissa tulisi huomioida ainakin seuraavat: 1) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO). 2) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO). 3) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti. 4) Palautusprosessin dokumentointi on riittävällä tasolla. 5) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä, jne.). Huom: Varmuuskopiot tulisi suojata fyysisen ja loogisen pääsynhallinnan menetelmin vähintään tiedon (mahdollisesti kasautumisvaikutuksen nostaman) turvallisuusluokan mukaisesti. 6) Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, tarkastusoikeuden (vrt. I-06) mahdollistavat erottelumenettelyt on toteutettava varmistusjärjestelmän liittymien ja tallennemedioiden osalta (esim. omistaja-/hankekohtaiset eri avaimilla salatut nauhat, joita säilytetään asiakaskohtaisissa kassakaapeissa/kassakaappilokeroissa). *Toteutusesimerkki* Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet: 1) Varmuuskopiot käsitellään ja säilytetään niiden elinkaaren ajan vähintään ko. turvallisuusluokan järjestelmissä. 2) Käsiteltäessä samalla varmistusjärjestelmällä tarkastusoikeuden varaavien eri omistajien tietoja, tarkastusoikeuden (vrt. I-06) mahdollistavat erottelumenettelyt on toteutettava ko. turvallisuusluokan mukaisesti varmistusjärjestelmän liittymien ja tallennemedioiden osalta. 3) Mikäli varmuuskopioita siirretään ko. turvallisuusluokan fyysisesti suojatun turvallisuusalueen ulkopuolelle, on menettelyt toteutettava kohtien I-15:ssa (sähköinen välitys) ja/tai F-08.1 (posti/kuriiri) sekä I-18 (kuljetus fyysisesti suojatun turvallisuusalueen ulkopuolelle). 4) Varmistusmediat hävitetään ko. turvallisuusluokan mukaisesti (I-21).		

	5) Järjestelmän ja tiedon palauttamista testataan säännöllisesti esimerkiksi automatisoidusti, jotta tieto voidaan palauttaa oikeaan tilaansa eheyden varmistamiseksi. Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan toteuttaa siten, että kohtien 1-5 lisäksi toteutetaan seuraava toimenpide: 6) Varmuuskopioista on rekisterit ja varmuuskopioiden käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai tietoon (esimerkiksi dokumentin osaksi). (Vrt. I-18) *Muita lisätietoja* CIS Critical Security Controls (v7.1) / 10; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 12.3.1; Tiedonhallintalautakunnan suositus (2020:21, luku 5); PiTuKri KT-03

I-21 **Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen**	**Vaatimus**	**Lähde (906/2019 ja/tai 1101/2019)**	**Lähde (2013/488/EU)**
	Turvallisuusluokka IV 1) Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Ei-sähköisten tietojen osalta ks. F-08.4. *Turvallisuusluokka III* Kohdan 1 lisäksi 2) Sekä kirjaajan että todistajan, jos jälkimmäisen läsnäoloa vaaditaan, on allekirjoitettava tuhoamistodistus, joka tallennetaan kirjaamoon/rekisteröintipisteeseen. Kirjaamon/rekisteröintipisteen on säilytettävä tuhoamistodistukset vähintään viiden vuoden ajan. (vrt. F-08.3). *Turvallisuusluokka II* Kohtien 1-2 lisäksi	1) 1101/2019 15 § 2) 906/2019 13 § 3) 1101/2019 6 ja 8 §, 906/2019 12 § 4) 1101/2019 15 § 5) 1101/2019 15 §	1) II liitteen 8 kohta 8, III liitteen 46 kohta IV liitteen 8 kohta 2) III liitteen 45 kohta ja IV liitteen 8 ja 37-38 kohdat 3) III liitteen 44 kohta ja IV liitteen 8 ja 37-38 kohdat 4) 5)

	3) Tiedon tuhoaminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään tuhottavan tiedon turvallisuusluokkaa vastaava turvallisuusselvitys. 4) Jos tiedon on laatinut toinen viranomainen, tarpeettomaksi käyneen tiedon tuhoamisesta on ilmoitettava tiedon laatineelle viranomaiselle, jollei sitä palauteta tiedon laatineelle viranomaiselle. 5) Tiedon tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Valmisteluvaiheen versiot voi tuhota ne laatinut henkilö.		
	Lisätietoja		
	Yleistä 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 perustelua 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 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 yksikäsitteinen tapa turvallisuusluokiteltujen tietojen tuhoamiseen. Tämä voi käytännössä tarkoittaa esimerkiksi asianmukaisia paperisilppureita ja henkilöstön turvallisuustietoisuudesta varmistumista (vrt. T-12). *Tuhoaminen silppuamalla* Turvallisuusluokan IV tietojen silppuaminen voidaan toteuttaa esimerkiksi siten, että - 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). Turvallisuusluokan III tietojen silppuaminen voidaan toteuttaa esimerkiksi siten, että		

	- 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), - optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6). Turvallisuusluokan II tietojen silppuaminen voidaan toteuttaa esimerkiksi siten, että - 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), - optisten medioiden silppukoko on enintään 5 mm2 (DIN 66399 / O-6). 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. *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 turvallisuusluokiteltuan tietoon kohdistuvia riskejä tiedon ja laitteistojen elinkaarten eri vaiheissa. Sähköisten tietojen tuhoamista on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ylikirjoitusohjeessa (www.ncsa.fi > Asiakirjat > Ylikirjoitusohje). *Sähköisessä muodossa olevien tietojen tuhoamisessa huomioon otettavaa* Sähköisessä muodossa olevien tietojen luotettavan tuhoamisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu turvallisuusluokiteltua tietoa. 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 tietoa ei viedä huoltotoimenpiteen yhteydessä. Tuhoamisen dokumentoinnista löytyy lisätietoja kohdasta F-08.3 (kirjaaminen). *Muita lisätietoja*

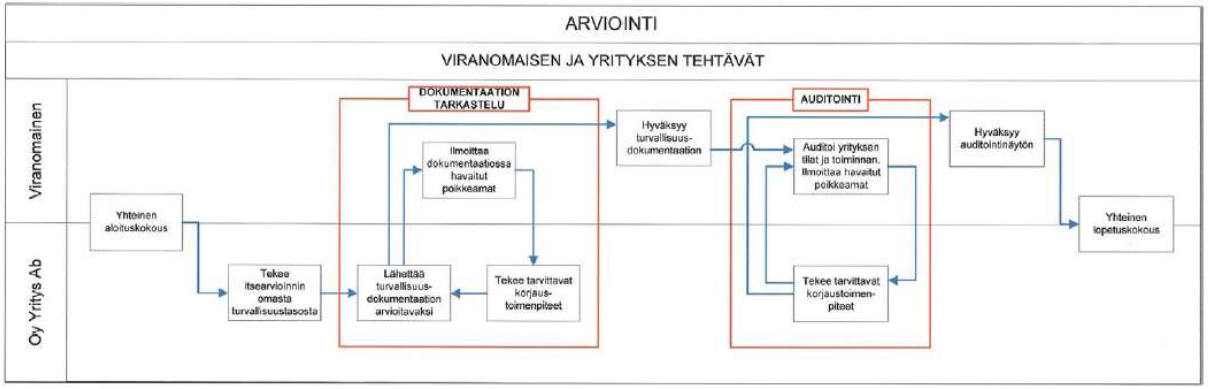
	Kyberturvallisuuskeskuksen ylikirjoitusohje; Secure destruction of sensitive items - CPNI standard - 2014; BSI IT-Grundschutz-Compendium Edition 2019; ISO/IEC 27002:2017 8.3.2; ISO/IEC 27002:2017 11.2.4; ISO/IEC 27002:2017 11.2.7; Tiedonhallintalautakunnan suositus (2020:21, luku 4); PiTuKri SI-02

LIITE I: Yritysturvallisuusselvitys

Katakrin käyttö osana yritysturvallisuusselvitystä

Yritysturvallisuusselvityksistä säädetään turvallisuusselvityslaissa (726/2014). Yritysturvallisuusselvityksessä toimivaltainen viranomainen voi selvittää laissa mainittujen tietolähteiden, yritysten vastuuhenkilöiden henkilöturvallisuusselvitysten sekä yritykseen ja sen toimitiloihin kohdistuvan tarkastusten avulla, miten yritys kykenee huolehtimaan tietoturvallisuutta koskevista turvallisuusvelvoitteistaan. Tarkasteltavia turvallisuusjärjestelyjä ovat muun muassa turvallisuusluokiteltujen tietojen suojaaminen oikeudettomalta paljastumiselta, asiattoman pääsyn estäminen tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään, sekä henkilöstön ohjeistaminen ja kouluttaminen. Katakria voidaan käyttää työkaluna, kun arvioidaan yrityksen toimitiloihin ja tietojärjestelmiin kohdistuvan tarkastuksen avulla yrityksen kykyä huolehtia tietoturvallisuusjärjestelyistä.

Yritysturvallisuusselvitykseen liittyvä arviointiprosessi on esitetty kuvassa 1. Prosessikaaviossa kuvataan viranomaisen ja yrityksen tehtävät arvioinnin eri vaiheissa. Arviointiin sisältyy yrityksen tietojärjestelmien auditointiprosessi silloin, kun se tehdään osana yritysturvallisuusselvitystä.



Kuva 1. Arviointiprosessi.

Yritysturvallisuusselvitys voidaan laatia osittaisena. Jos yritysturvallisuusselvityspyynnössä edellytetään kykyä suojata viranomaisen turvallisuusluokiteltuja tietoja yrityksen toimitiloissa (”FSC with safeguards”), arvioinnissa käytetään turvallisuusjohtamisen (T) ja fyysisen turvallisuuden (F) osa-alueita. Jos yritysturvallisuusselvityspyynnössä edellytetään kykyä viranomaisen turvallisuusluokitellun tiedon sähköiseen käsittelyyn ("FSC with safeguards including CIS") arvioinnissa käytetään lisäksi teknisen tietoturvallisuuden (I) osa-aluetta. Sähköisen käsittelyn arviointi osana yritysturvallisuusselvitystä on kuvattu tarkemmin liitteessä II.

LIITE II: Tietojärjestelmien arviointi

Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista[5] mukaisesti viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa Liikenne- ja viestintävirastoa tai sen hyväksymää tietoturvallisuuden arviointilaitosta[6]. Katakria voidaan käyttää työkaluna selvitettäessä, miten viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tietoturvallisuudesta on huolehdittu suhteessa kansallisiin tai kansainvälisiin suojausvaatimuksiin. Myös viranomaisten tietojärjestelmien turvallisuuden arvioinnissa Katakrin käytön tulee perustua järjestelmälliseen riskienarviointiin, sen pohjalta soveltuviksi valittaviin suojausvaatimuksiin ja niiden täyttymisen arviointiin toteutusesimerkkejä hyödyntäen. Tässä liitteessä kuvataan Katakrin eri käyttötapauksia tietojärjestelmätarkastuksissa. Kuvauksessa keskitytään yritysturvallisuusselvityksen ja viranomaisten tietojärjestelmien arvioinnin käyttötapauksiin, joissa toimivaltaisena viranomaisena on Liikenne- ja viestintävirasto. Kuvaus on jaoteltu käyttötapausten, arviointi- ja hyväksyntäprosessien sekä hyväksynnän ja todistuksen esittelyyn. Kuvauksessa ei käsitellä muita käyttötapauksia, esimerkiksi käyttöä osana organisaation sisäistä turvallisuustyötä.

Käyttötapaukset

Liikenne- ja viestintäviraston NCSA-toiminnon suorittamissa tietojärjestelmätarkastuksissa Katakrin käyttötapaukset on jaettavissa viiteen kokonaisuuteen:

1. Viranomaisen määräämisvallassa olevat tai hankittavaksi suunnittelemat järjestelmät, joista viranomainen on tehnyt Liikenne- ja viestintävirastolle arviointipyynnön (L 1406/2011, L 10/2015[7]).
    - Järjestelmää arvioidaan tällöin viranomaisen tekemän pyynnön mukaisesti joko kansallisen, kansainvälisen tai sekä kansallisen että kansainvälisen turvallisuusluokitellun tiedon näkökulmasta.
2. Valtiovarainministeriön pyynnöstä tehtävät selvitykset valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta (L 1406/2011, L 10/2015).
    - Järjestelmää arvioidaan tällöin Valtiovarainministeriön tekemän pyynnön mukaisesti joko kansallisen, kansainvälisen tai sekä kansallisen että kansainvälisen turvallisuusluokitellun tiedon näkökulmasta.
3. Valtionhallinnon toimijoiden järjestelmät siltä osin, kun ne liittyvät kansainvälisten tietoturvavelvoitteiden täyttämiseen (L 588/2004[8]).
    - Järjestelmää arvioidaan tällöin kansainvälisen turvallisuusluokitellun tiedon näkökulmasta.
4. Kansalliseen tai kansainväliseen yritysturvallisuusselvitysprosessiin hakeutuneiden yritysten järjestelmät siltä osin, kun ne vaativat kansallisen tietoturvallisuusviranomaisen (NCSA) hyväksyntää (L 588/2004) tai/ja selvitystä vaatimustenmukaisuudesta (L 726/2014[9]).
    - Järjestelmää arvioidaan tällöin kansallisen tai/ja kansainvälisen turvallisuusluokitellun tiedon näkökulmasta.

---

[5] Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), https://www.finlex.fi/fi/laki/alkup/2011/20111406.
[6] Laki tietoturvallisuuden arviointilaitoksista (L 1405/2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111405.
[7] Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015), http://www.finlex.fi/fi/laki/alkup/2015/20150010.
[8] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588.
[9] Turvallisuusselvityslaki (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

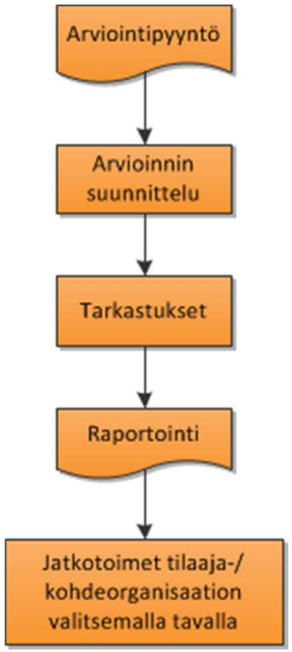
5. Viranomaisten tietojärjestelmät, joista viranomainen hakee Liikenne- ja viestintäviraston hyväksyntää osoittavaa todistusta vaatimustenmukaisuudesta (L 1406/2011).
    - Järjestelmää arvioidaan tällöin kansallisen turvallisuusluokitellun tiedon näkökulmasta.

Tietojärjestelmätarkastusten käyttötapauksia on mahdollista myös yhdistellä arvioinnin tilaajan toiveiden mukaisesti.

Arviointiprosessi

Tietojärjestelmien turvallisuuden arviointiprosessi (L 1406/2011) alkaa, kun arvioinnin kohde toimittaa Liikenne- ja viestintävirastolle arviointipyynnön. Arviointiprosessin keskeisiä muita vaiheita ovat arvioinnin suunnittelu, tarkastukset sekä raportointi. Arviointiprosessia on havainnollistettu yksinkertaistetussa muodossaan kuvassa 4. Arviointiprosessia voidaan hyödyntää esimerkiksi kohdeorganisaation sisäisen turvallisuustyön tukena, jättäen muun muassa jäännösriskien käsittelyn täysin kohdeorganisaation vastuulle. Arviointiprosessia kuvataan yksityiskohtaisemmin ohjeessa "NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma"[10].

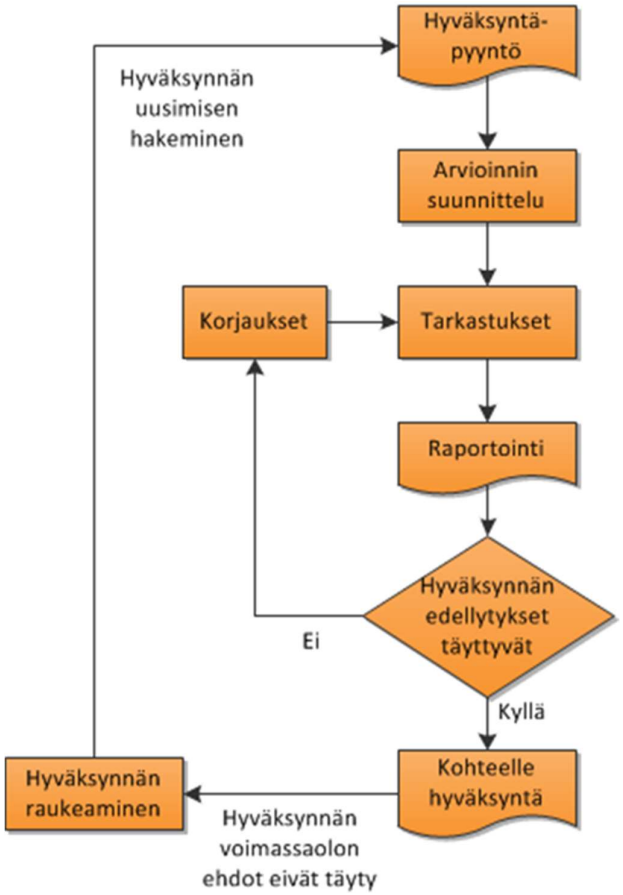
[10] Kyberturvallisuuskeskus. 2019. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.



Kuva 2. Arviointiprosessi yksinkertaistettuna.

Hyväksyntäprosessi

Liikenne- ja viestintäviraston hyväksyntään tähtäävä hyväksyntäprosessi (L 588/2004 tai 1406/2011) alkaa, kun arvioinnin kohde toimittaa Liikenne- ja viestintävirastolle hyväksyntäpyynnön. Hyväksyntäprosessi mukailee arviointiprosessia sillä keskeisellä erolla, että tarkastuksissa mahdollisesti havaittujen poikkeamien tulee olla todennetusti korjattuja ennen, kuin hyväksyntä voidaan myöntää. Hyväksyntäprosessia on havainnollistettu yksinkertaistetussa muodossaan kuvassa 5. Hyväksyntäprosessia voidaan hyödyntää esimerkiksi silloin, kun arvioinnin kohde haluaa osoittaa tietojärjestelmänsä suojausten riittävyyden Liikenne- ja viestintäviraston hyväksynnällä. Hyväksyntäprosessissa riskienarviointi toteutetaan hyödyntäen sekä kohdeorganisaation, että Liikenne- ja viestintäviraston arvioita. Hyväksyntäprosessia kuvataan yksityiskohtaisemmin ohjeessa “NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma”.



Kuva 3. Hyväksyntäprosessi yksinkertaistettuna.

Viranomaishyväksyntä

Liikenne- ja viestintävirasto voi myöntää vaatimukset täyttävälle kansallista tai kansainvälistä turvallisuusluokiteltua tietoa käsittelevälle järjestelmälle hyväksynnän (accreditation). Hyväksynnän myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason säilyttämiseen. Hyväksyntä edellyttää tyypillisesti[11] myös sitä, että järjestelmä on kokonaisuudessaan Suomen lainsäädännön alaisuudessa.

Hyväksynnän voimassaolo raukeaa, mikäli tarkastetussa kohteessa tapahtuu merkittävä sen turvallisuuteen vaikuttava muutos. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten esimerkiksi ohjelmistojen turvapäivitysten asennukset, eivät aiheuta voimassaolevan hyväksynnän raukeamista. Tapauskohtaiset ehdot hyväksynnän raukeamiselle määritellään hyväksynnän myöntämisen yhteydessä. Merkittävät muutokset tulee hyväksyttää etukäteen Liikenne- ja viestintävirastolla.

Liikenne- ja viestintävirastolla on mahdollisuus myöntää järjestelmälle hyväksyntä pohjautuen hyväksytyn arviointilaitoksen suorittamaan arviointiin (L 1405/2011). Myöntämisen keskeisinä ehtoina ovat tehtyjen tarkastusten rajausten yhteneväisyydet haettavan hyväksynnän rajauksiin sekä toimitettujen arviointiraporttien sisältämien tietojen riittävyys. Arviointilaitosten käyttömahdollisuudet rajautuvat kansallisen turvallisuusluokan IV ja tietyin rajauksin myös turvallisuusluokan III tietoa käsitteleviin tietojärjestelmiin ja tietojenkäsittely-ympäristöihin. Hyväksyntää varten Liikenne- ja viestintävirasto suorittaa tarvittaessa tarkentavia arviointeja tai pyytää tilaajaorganisaatiolta lisäselvitystä sen selvittämiseksi ja varmistamiseksi, että kohde täyttää soveltuvat tietoturvallisuusvaatimukset.

[11] Poikkeuksena esimerkiksi kansainväliseen viranomaisyhteistyöhön liittyvät järjestelmähankkeet, joissa järjestelmäkokonaisuuksien osien tarkastamisen ja hyväksyntien toimivallasta ja vastuusta on kyseiseen viranomaisyhteistyöhön osallistuvien jäsenmaiden turvallisuusviranomaisten kesken erikseen toisin sovittu.

LIITE III: Turvallisuuden arviointi Katakrin turvallisuusmallissa

Turvallisuusjärjestelyjen riittävyyden arvioinnin tulee pohjautua järjestelmälliseen riskienarviointiin. Turvallisuusriskien hallinnalla on pyrittävä toteuttamaan turvatoimien yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Tässä liitteessä kuvataan Katakrin perustana oleva turvallisuusmalli, sekä riskienhallinnan rooli Katakrin tuetuissa käyttötapauksissa.

Katakrin turvallisuusmalli

Katakrin turvallisuusmallina on yhdistelmämalli, joka koostuu vähimmäissuojauksista sekä niiden riskiperusteisesta sovittamisesta ja hallinnoinnista kussakin tarkasteltavassa käyttöympäristössä. Vähimmäissuojausten tavoitteena on pienentää yleisiä turvallisuusluokiteltuun tietoon kohdistuvia riskejä hyväksyttävälle tasolle ja vastata sekä lainsäädännön että tiedon omistajien ja/tai originaattorien koko tiedon elinkaarelle asettamiin vähimmäisvaatimuksiin. Riskiperusteinen sovittaminen tukee puolestaan paitsi yleisten turvallisuusluokiteltuun tietoon kohdistuvien riskien myös käyttöympäristökohtaisten riskien pienentämistä. Riskiperusteisen hallinnoinnin tavoitteena on täydentää vähimmäissuojauksia käyttöympäristökohtaisten riskien osalta ja ylläpitää turvallisuutta riskiympäristön muuttuessa.

Riskienhallinnan rooli tuetuissa käyttötapauksissa

Kaikkiin turvallisuusluokitellun tiedon käsittely-ympäristöihin kohdistuu jäännösriskejä. Eri tiedon omistajilla on toisistaan eroava riskinottohalukkuus. Toisaalta eri organisaatioiden riskienhallintaa ohjaavat toisistaan eroavat tekijät. Katakrin tavoitteena ei ole eri organisaatioiden riskienhallinnan täydellinen yhdenmukaistaminen, vaan tuottaa kyseiseen käyttötapaukseen soveltuvaksi arvioitu jäännösriskitaso turvallisuusluokiteltujen tietojen käsittelylle.

Katakrin hyväksyntään tähtäävissä (L 726/2014, L 588/2004) tuetuissa käyttötapauksissa on käytössä kaksivaiheinen riskienhallintamalli. Kaksivaiheisessa riskienhallinnassa kohteen tulee saavuttaa hyväksyttävä jäännösriskitaso sekä kohdeorganisaation että riippumattoman ulkopuolisen arvioijan riskiarvioihin nähden. Kohteen riskienarvioinnissa pystytään usein huomioimaan kohdekohtaiset erityisriskit. Riippumattoman ulkopuolisen arvioijan riskienarvioinnissa korostuu sen varmistaminen, että yleiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit on pienennetty hyväksyttävälle tasolle. Katakrin arviointikäytön (L 1406/2011) tuetussa käyttötapauksessa on käytössä riskienhallintamalli, jossa kohteen suojauksia peilataan riippumattoman ulkopuolisen arvioijan riskiarvioihin nähden. Sekä hyväksyntään tähtäävissä, että arviointikäytön tuetuissa käyttötapauksissa ulkopuolisen arvioijan arvio pohjautuu toimivaltaisella turvallisuusviranomaisella käytettävissään olevaan uhkatietoon. Riskienarvioinnin rooli korostuu erityisesti korvaavien suojausten riittävyyden arvioinnissa.

Katakria voidaan käyttää myös tuetuista käyttötapauksista (L 726/2014, L 588/2004, L 1406/2011) eroaviin käyttötapauksiin, joissa myös soveltuva riskienhallintamalli voi olla eroava. Esimerkiksi käytettäessä Katakria organisaation sisäisessä turvallisuustyössä, organisaation omistamien tietojen suojaamisen tukena, on usein perusteltua hyödyntää organisaation sisäisiä riskienhallinnan käytäntöjä.