

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

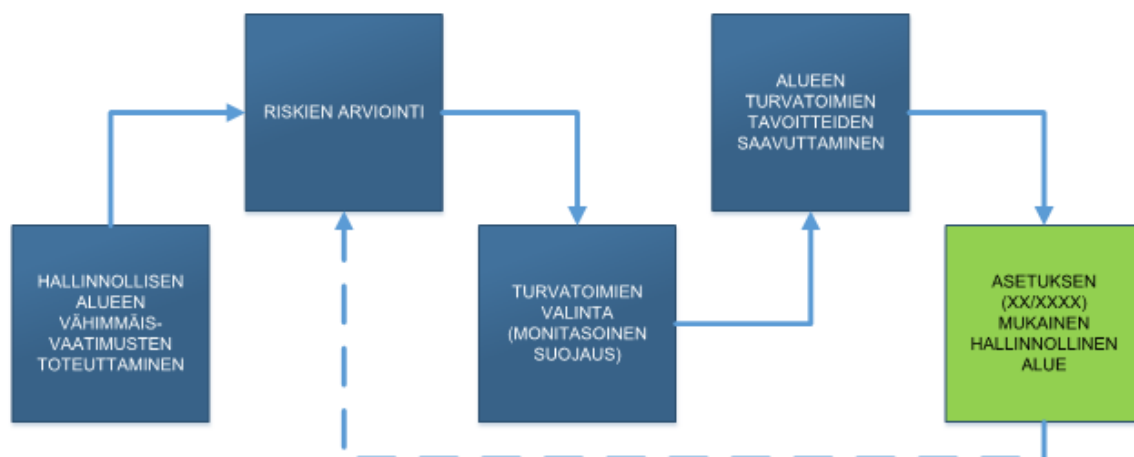
- 1) hallinnolliset alueet, joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamalla henkilöllä on pääsy ilman saattajaa.

HALLINNOLLINEN ALUE

Hallinnollisella alueella tarkoitetaan käytännössä viranomaisen normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta, tai esimerkiksi palvelintiloja tai konesaleja tai yhteisöjen kuten yritysten tiloja, joiden osalta tilaa hallitseva toimija varmistaa, että niihin on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamalla henkilöllä. Hallinnollista aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia.

Tässä kortissa esitettyjen hallinnollisen alueen vähimmäisvaatimusten (kohta 4) lisäksi viranomaisen riskien arvioinnin tulos (kohta 2) vaikuttaa siihen, mitkä fyysiset turvatoimet tulee lisäksi valita (kohta 3), jotta turvatoimien tavoitteet (kohta 1) saavutetaan. Alueen yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuus on arvioitava uudelleen säännöllisin väliajoin.

Tavoitetilan saavuttamisen prosessi ja säännöllinen arviointi on havainnollistettu alla olevassa kuviossa:



1. FYYSISET TURVATOIMIEN TAVOITE

Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin:

- a) varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti;
- b) mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on, ja tarvittaessa henkilöiden turvallisuusselvitysten perusteella;
- c) ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet; ja

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa	
Suosituskortti	
9.2 § kohta 1 Hallinnolliset alueet	versio 0.95/27.11.2019

- d) estämällä salaa tai väkisin tapahtuva tunkeutuminen tai viivyttämällä sitä.

2. RISKIEN ARVIOINTI

Fyysisten turvatoimien valinnan on perustuttava viranomaisen tekemään riskien arviointiin. Riskien arvioinnissa on otettava huomioon kaikki asiaankuuluvat tekijät, erityisesti seuraavat:

- Turvallisuusluokiteltujen tietojen turvallisuusluokka;
- Turvallisuusluokiteltujen tietojen käsittelytapa ja määrä pitäen mielessä, että niiden suuri määrä tai kokoaminen yhteen voi edellyttää tiukempien riskienhallintatoimenpiteiden soveltamista;
- Turvallisuusluokiteltujen tietojen käsittely- ja säilytyspaikan ympäristö; rakennuksen ympäristö, sijoittuminen rakennuksessa, tilassa tai sen osassa; ja
- Tiedustelupalvelujen, rikollisen toiminnan ja oman henkilöstön muodostama arvioitu uhka tiedoille.

3. FYYSISTEN TURVATOIMIEN VALINTA

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

- rakenteelliset esteet: fyysinen este, jolla suojattava alue tai tila rajataan ja luvattonta tunkeutumista vaikeutetaan ja hidastetaan;
- kulunvalvonta: kulunvalvonnalla rajataan pääsyä alueelle tai tilaan. tavoitteena havaita luvattomat pääsy-yritykset, estää asiattomien pääsy ja valvoa alueella liikkuvia. kulunvalvontaa voidaan kohdistaa alueeseen, alueen yhteen tai useampaan rakennukseen tai rakennuksen alueisiin tai huoneisiin. Valvonta voidaan toteuttaa mekaanisia, sähköisiä tai sähkömekaanisia teknisiä järjestelmiä hyödyntämällä, vartiointihenkilöstön ja/tai vastaanottovirkailijan toimesta tai muunlaisin fyysisin keinoin;
- tunkeutumisen ilmaisujärjestelmä: rakenteellisen esteen tarjoaman turvallisuustason parantamiseksi voidaan käyttää tunkeutumisen ilmaisujärjestelmää (murtohälytysjärjestelmä) luvattoman tunkeutumisen havaitsemiseksi. valvontaa voidaan käyttää myös tiloissa, huoneissa ja rakennuksissa vartiointihenkilöstön sijasta tai sen tueksi;
- vartiointihenkilöstö: koulutettua, valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä vartiointihenkilöstöä voidaan käyttää turvallisuusvalvontatehtävissä muun muassa kulunvalvonnan tukena sekä alueelle tai tilaan tunkeutumista suunnittelevien henkilöiden aikeiden havaitsemiseksi ja toimien estämiseksi (vaste);
- kameravalvonta: kameravalvontaa voidaan käyttää alueella tai tilassa ilmenevien poikkeamien ennalta estämisessä, hälytysten todentamiseksi sekä tapahtuneiden poikkeamien selvittämisessä. vartiointihenkilöstö voi käyttää kameravalvontaa reaaliaikaisena aktiivisena kuvan tarkkailuna tai jälkikäteen passiivisena kuvamateriaalin analysointina;
- turvallisuutta ylläpitävät menettelyt: vastuiden ja tehtävien määrittäminen, erilaiset prosessit ja toimintamallit kuten pääsyoikeuksien ja avainten hallinta, henkilöiden ohjeistus, perehdyttäminen sekä järjestelmien huolto- ja ylläpitotoimet;
- valaistus: mahdollisia tunkeutujia voidaan estää käyttämällä valaistusta, jonka ansiosta vartiointihenkilöstö voi valvoa aluetta tehokkaasti joko suoraan tai kameravalvontajärjestelmää hyödyntämällä; ja
- muut asianmukaiset fyysiset toimenpiteet, joiden tarkoituksena on luvattoman pääsyn estäminen ja havaitseminen tai turvallisuusluokiteltujen tietojen katoamisen tai vahingoittumisen ehkäiseminen.

4. HALLINNOLLISEN ALUEEN FYYSISET TURVATOIMIEN VÄHIMMÄISVAATIMUKSET

Viranomaisen määrittelemän hallinnollisen alueen tulee täyttää taulukossa esitettävät vähimmäisvaatimukset. Vähimmäisvaatimusten lisäksi viranomaisen tulee suunnitella, vastuuttaa, toteuttaa ja ylläpitää riskien arviointiin (kohta 2) ja monitasoiseen suojausperiaatteeseen (kohta 3) perustuvat muut riskienhallintatoimenpiteet siten, että turvallisuusluokiteltuihin tietoihin kohdistuvat jäännösriskit voidaan hyväksyä ja turvatoimien tavoitteet (kohta 1) saavutetaan.

TURVALLISUUDEN OSA-ALUE	VÄHIMMÄISVAATIMUS	LISÄTIETOJA JA SUOSITUKSIA
Alueen raja ja rakenteet (seinät, ovet, ikkunat, lattia- ja kattorakenteet)	Alueella on oltava selkeästi määritelty näkyvä raja. Alueen rakenteille ei ole vaatimuksia.	Alueen aukot, jotka eivät ole käytössä kulkemiseen on voitava lukita, jotta alueelle kulkua voidaan hallinnoida asianmukaisesti. Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään tietoa ja murtoriski arvioidaan todennäköiseksi.
Pääsyoikeuksien myöntäminen	Ainoastaan viranomaisen asianmukaisesti valtuuttamalla henkilöillä on itsenäinen pääsy alueelle. Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainhallinnan menettelyt ja roolit.	Alueelle pääsyn rajaaminen voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta. Viranomaisen on määritellyt/hyväksynyt menettelyt ja roolit ainakin seuraavilta osin: <ul style="list-style-type: none"> - pääsyoikeuksien ja avainhallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. - pääsyoikeuden ja avainten haltijoista on lista. - pääsyoikeudet tarkastetaan säännöllisesti ja pidetään ajan tasalla. - avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet vastuutettu. - avainkorttia sekä jakamattomia avaimia ja

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa	
Suosituskortti	
9.2 § kohta 1 Hallinnolliset alueet	versio 0.95/27.11.2019

		kulcutunnisteita säilytetään asianmukaisesti.
Vierailijat	Muilla kuin viranomaisen asianmukaisesti valtuuttamalla henkilöillä (vierailijoilla) on aina oltava saattaja.	Viranomaisen tulee olla hyväksynyt menettelyohjeen vierailijoita varten. Viranomaisen hyväksymä vierailijaohje voi käsitellä mm. seuraavia asioita: 1) Vieras tunnustetaan ja varustetaan vieraskortilla. 2) Vierailu kirjataan. 3) Vierailijoita ei päästetä/ jätetä tiloihin valvomatta. Vierailusta vastaava vastaa ulkopuolisista henkilöistä koko vierailun ajan. 4) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten. 5) Huolehditaan siitä, ettei vieras pääse oikeudettomasti näkemään tai kuulemaan turvallisuusluokiteltua tietoa.
Äänieristys	Alueen äänieristyksen tulee estää käsiteltävään tietoon oikeudettomien henkilöiden kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli alueella keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla alueella olevilla henkilöillä ei ole tiedonsaantitarvetta.	Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista.
Tekniset turvallisuusjärjestelmät	Hankittaessa alueelle turvallisuusluokiteltujen tietojen fyysiseen suojeluun tarkoitettuja laitteita (esimerkiksi kassakaappeja, paperisilppureita, lukkoja, elektronisia kulunvalvontajärjestelmiä, kameravalvontajärjestelmiä, tunkeutumisen ilmaisujärjestelmiä ja hälytysjärjestelmiä) viranomaisen on varmistettava, että laitteet ovat toimintakuntoisia ja soveltuvia niiden käyttötarkoitukseen nähden.	Suosituksena on, että laitteet ovat hyväksytyjen teknisten standardien ja vähimmäisvaatimusten mukaisia. Laitteet pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä, toiminnan testauksista, dokumentaation ajantasaisuudesta laitevalmistajan ohjeiden ja suositusten mukaisesti. Järjestelmäoikeuksin hallinta on suositeltavaa toteuttaa vähimpien oikeuksien periaatetta noudattaen.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa	
Suosituskortti	
9.2 § kohta 1 Hallinnolliset alueet	versio 0.95/27.11.2019

	Tunkeutumisen ilmaisujärjestelmä	Ei vaatimuksia.	Alue tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään tietoa ja murtoriski arvioidaan korkeaksi.
	Salaa katselun estäminen	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu mukaan luettuna, on toteutettava asianmukaiset toimenpiteet tällaisen riskin torjumiseksi.	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden näkösuojasermeillä, käyttämällä ikkunoiden sälekaihtimia, verhoja tai tietokoneen näytön suoja.
	Tila- ja laitetarkastukset (ainoastaan TL II)	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään hallinnollisella alueella, jolla käsitellään SALAINEN-turvallisuusluokan tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Myös alue on tarvittaessa tarkastettava fyysisesti ja/tai teknisesti säännöllisin väliajoin. Tällaiset tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänkäynnin tai sen epäilyn johdosta.	
	Tiedon säilyttäminen	Alueella voi säilyttää turvallisuusluokan KÄYTTÖ RAJOITETTU-luokan tietoa. Säilyttäminen tulee tapahtua soveltuvissa lukituissa toimistokalusteissa.	