



VALTIOVARAINMINISTERIÖ

Valtionhallinnon toimitilojen tietoturvaohje

LUONNOS 2.11.2012

Lyhyesti VAHTI:sta

Valtiovarainministeriö ohjaa ja yhteen sovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuden linjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTI:n tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohtoa.

VAHTI edistää hallitusohjelman, Yhteiskunnan turvallisuusstrategian (YTS), Julkisen hallinnon ICT-strategian, valtioneuvoston huoltovarmuuspäätöksen, valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä.

Valtioneuvosto teki 26.11.2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätös korostaa VAHTI:n asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elimenä. Periaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTI:ssa koordinoitavaan yhteistyöhön.

VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTI:n toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on kansainvälisestikin verrattuna merkittäväksi katsottava yleinen tietoturvallisuusohjeisto (www.vm.fi/vahti).

Tiivistelmä

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) edellyttää jo perustason tietoturvallisuutta toteutettaessa, että asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja (TTA 5§). Asetus edellyttää lisäksi korotetun ja korkean tason käsittely-ympäristöiltä erillisiä suojaustoimia. Tämän VAHTI-ohjeen näkökulmana on kyseisten vaatimusten toimeenpanon tukeminen valtionhallinnossa.

Alati lisääntyvä kansainvälinen yhteistyö tuo mukanaan vaatimuksen ottaa huomioon kansainvälisten yhteistyökumppaneiden – olivatpa nämä sitten itsenäisiä oikeusvaltioita tai kansainvälisiä organisaatioita – turvallisuusluokitellun tiedon käsittelylle asettamat vaatimukset. Usein nämä vaatimukset näkyvät konkreettisimmillaan tiedon käsittely- ja säilytysympäristöihin kohdistuvina vaateina, väheksymättä sinällään henkilöstölle ja tiedon sähköiselle käsittelylle asetettavia vaatimuksia. Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttää, että Suomi valtiona kunnioittaa kaikessa toiminnassaan niitä turvallisuusvelvoitteita, joihin se kansainvälisen yhteistyön myötä on sitoutunut. Velvoitepohjana toimivat näissä tapauksissa tyypillisesti joko tietoturvallisuutta säättävät valtiosopimukset tai Suomen valtiona muilla tavoin hyväksymät kansainväliset turvallisuussäännökset.

Valtionhallinto on suomalaisen elinkeinoelämän kannalta merkittävä työllistäjä. Valtionhallinnon hankkeisiin, samoin kuin turvallisuusluokiteltua tietoa sisältäviin kansainvälisiin hankkeisiin liittyy usein lainsäädännön sanelema tarve solmia turvallisuussopimuksia valituksi tulleiden elinkeinoelämän toimijoiden kanssa. Ennen turvallisuussopimuksen allekirjoittamista valtionhallinto tarkastaa elinkeinonharjoittajan turvallisuustason. Tätä tarkoitusta varten on laadittu viranomaisten ja elinkeinoelämän yhteistyönä kansallinen turvallisuusauditointikriteeristö (KATAKRI), jonka ylläpidosta vastaa sisäasiainministeriö. Kriteeristö sisältää yksityiskohtaisia toimitilaturvallisuusvelvoitteita, joiden sisältö on mahdollisimman pitkälle otettu huomioon myös tässä ohjeessa vaatimusten kirjon minimoimiseksi.

Ohjetta laadittaessa on huomioitu VAHTI:n vuonna julkaisema 2012 erillinen ICT-varautumisen vaatimuskriteeristö, jonka sisältöä tämä ohje täydentää yksityiskohtaisemmilla vaatimuksilla. Osa valtionhallinnon toimijoista on laatinut hallinnonalallaan sovellettavaksi erillisiä fyysisen turvallisuuden tai toimitilaturvallisuuden vaatimusasiakirjoja. Näiden asiakirjojen vähimmäisvaatimukset on yhteismitallisuussyistä pyritty ottamaan huomioon tätä ohjetta laadittaessa. Salassa pidettävän tiedon siirtyessä valtionhallinnon toimijalta toiselle yhteisillä turvallisuusvaatimuksilla varmistetaan tiedon salassa pysyminen sillä tasolla, jonka asiakirjan laatija on sille asettanut.

Tämän ohjeen sisältämät linjaukset on suositeltavaa ottaa käyttöön myös suunniteltaessa uusia tietoteknisiä laitetoja. Laitetojen turvallisuutta on aiemmin ohjeistettu erillisellä VAHTI-ohjeella (1/2002), jonka voimassaolo päättyy nyt julkaistavan ohjeen myötä.

Ohje on laadittu VAHTI:n alaisessa hankeryhmässä, jonka jäseninä ovat toimineet: Jani Arnell, Karl Gädda, Heikki Hovi, Hellevi Huhanantti, Kari Hurske, Juha Ilkka, Kimmo Janhunen, Olli Jokinen, Reijo Kaariste, Marko Kalliokoski, Kai Knape, Tero Lampén (30.9.2012 asti), Mikko Nissinen, Jari Panhelainen, Pauliina Pekonen, Sakari Perkiömäki, Jaakko Ritola, Kari Santalahti, Aki Tauriainen, Heikki Toivonen, Iina Vuorialho, Erkki Väättäinen ja Juha Åberg.

Sisältö

Lyhyesti VAHTI:sta	2
Tiivistelmä.....	3
1 Yleistä	6
1.1 Ohjeen tausta, tarkoitus ja tavoite	6
2 Normit ja muu viitekehys	7
2.1 Lait	7
2.2 Tietoturvallisuusasetus.....	7
2.3 Ohje tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)	7
2.4 Sisäverkko-ohje (VAHTI 3/2010).....	8
2.5 ICT-varautumisen vaatimukset (VAHTI 2/2012)	8
2.6 Kansallinen turvallisuusauditointikriteeristö (2011)	8
2.7 Euroopan unionin turvallisuusregiimi (2011)	8
2.8 Naton turvallisuussäännöstö (2002)	8
2.9 Muu tausta-aineisto	9
3 Turvallisuusvyöhykkeet.....	9
3.1 Määräytymisperusteet	9
3.1.1 Luokittelu.....	11
3.1.2 Valtionhallinnon toimitilojen turvallisuusvyöhykejako	11
3.1.3 Turvallisuusvyöhykkeiden yleiset vaatimukset	12
3.2 Alueet ja toimitilat	13
3.3 Tietotekniset laitetilat	14
3.4 Yhteiskäyttöiset toimitilat	14
3.5 Merkitseminen	14
3.6 Etätyö.....	14
3.7 Liikkuva työ	15
3.8 Työntekijöiden turvallisuus	15
4 Rakenteelliset turvallisuusvaatimukset.....	15
4.1 Alue.....	15
4.2 Ulkopinnat	15
4.3 Sisäseinät	15
4.4 Ala- ja yläpohjat	16
4.5 Ovirakenteet.....	16
4.5.1 Materiaalivaatimukset.....	16

4.5.2	Karmit ja kiinnitys	16
4.5.3	Lukitusjärjestelyt	16
4.6	Ikkunarakenteet	17
4.6.1	Turvalasit ja kalvot	17
4.6.2	Karmit ja kiinnitys	17
4.6.3	Erillisvaatimukset	17
5	Turvallisuusvalvonta	18
5.1	Vasteaikavaatimukset	18
5.2	Valvontajärjestelmät	18
5.3	Vartiointi	19
6	Toimeenpano ja ohjeistaminen	19
	Liiteluettelo	19
	Liite 1: Turvallisuusvaatimustaulukko	21
	Liite 2: Valtionhallinnon toimitilarakentamisen turvallisuussopimusmallit	34
	Liite 3: Rakentamisdokumentaation käsittelysuositukset	62
	Liite 4: Rakentamishankkeiden turvallisuusaskeleet (esimerkki)	81
	Liite 5: Pohjakuvaesimerkit eri turvallisuusvyöhykkeiden mukaisista työympäristöistä	82
	Liite 6: Tietoteknisten laittilojen turvallisuussuositukset	87
	Liite 7: Määritelmät ja lyhenteet	88
	Liite 8: Lähdeluettelo	92
	Liite 9: Viiteaineiston lähdelainaukset	93
1.	Lait	93
2.	Tietoturvallisuusasetus	93
3.	Ohje tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)	94
4.	Euroopan unionin turvallisuusregiimi (2011)	95
5.	Naton turvallisuussäännöstö (2002)	96
6.	Suomen rakentamismääräyskokoelma	96
	Liite 10: Esimerkkejä valtionhallinnon toimipisteiden turvallisuusvyöhykejaottelusta	98

1 Yleistä

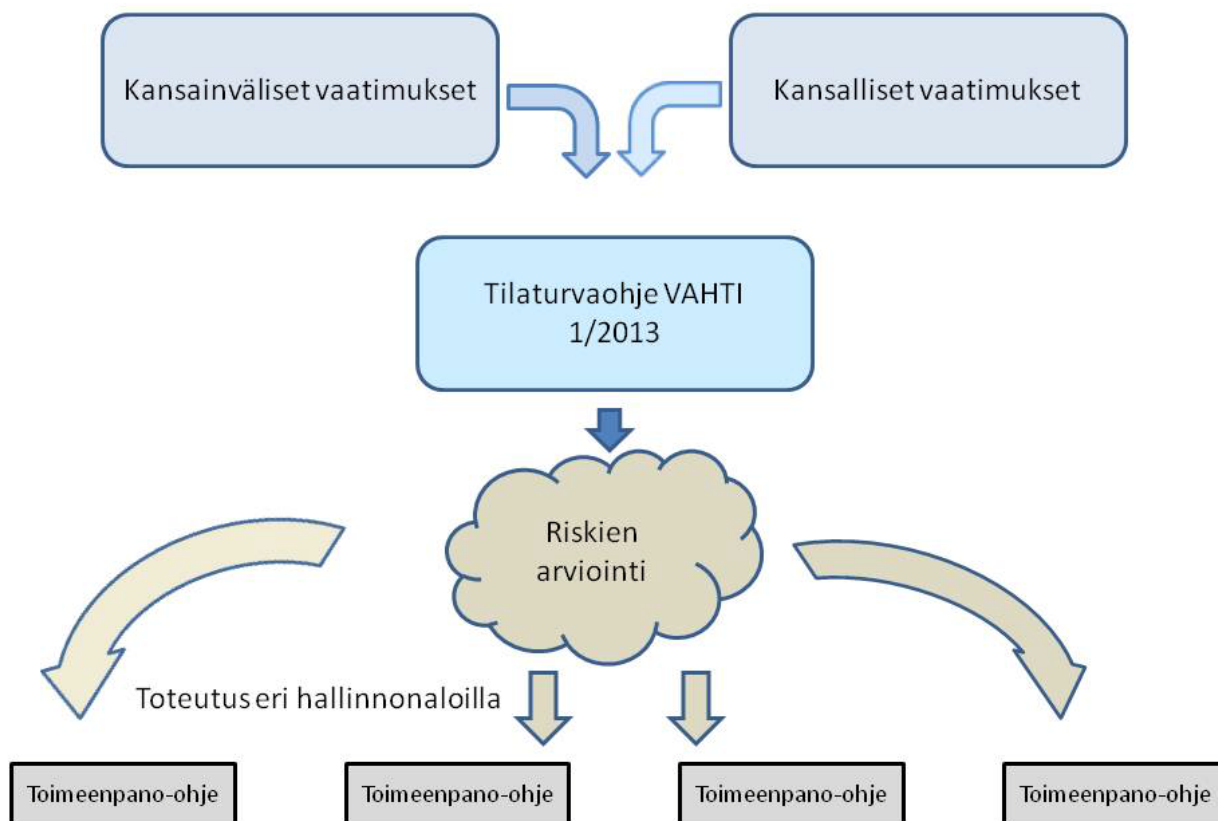
1.1 Ohjeen tausta, tarkoitus ja tavoite

Ohje on laadittu tukemaan valtionhallinnon toimijoita toimitilaturvallisuuteen liittyvissä ratkaisuissa. Ratkaisujen tavoitteina on osaltaan varmistaa salassa pidettävien tietojen salassa pysyminen. Ohjeen tavoitteena on myös luoda yhteisiä hyviä menettelytapoja ja käytäntöjä niin lakisääteisten velvoitteiden kuin muidenkin kansallisten ja kansainvälisten toimitilaturvallisuusvaatimusten toteuttamiseksi. Ohje ei ota kantaa työ- tai palo- ja pelastusturvallisuuden erillisratkaisuihin, joista vastuuviranomaiset ohjeistavat erikseen. Nämä ratkaisut on kuitenkin syytä huomioida myös turvallisuusrakentamisessa osana rakenne- ja rakennussuunnittelun perusteita.

Ohjetta laadittaessa on pyritty huomioimaan ratkaisujen kustannustehokkuus ja tätä kautta toivottavasti saavutettavat säästöt vakioitujen toimintamallien ja rakenneratkaisujen kautta. Toimitilojen turvallisuus on keskeinen elementti useiden tietoturva vaatimusten täyttymisen osalta.

Tässä ohjeessa ja sen liitteissä esitetään fyysisen turvallisuuden yleisvaatimukset kaikkien valtionhallinnon toimitilojen osalta, painottuen salassa pidettävien tietojen suojaustasojen IV, III ja II mukaisten tietojen käsittelyyn ja säilytykseen. Suojaustason I vaatimukset niille toimitiloille, joissa käsitellään kyseistä tietoa muutoin kuin satunnaisesti, esitetään vaatimusten tarvisijoille erikseen vastuuviranomaisten toimesta.

Valtionhallinnon tilaturvaohjeen sovellusperiaate



2 Normit ja muu viitekehys

Tässä luvussa kuvataan lyhyesti ne perusteet ja vaikuttimet, joille tämän ohjeen toimitilaturvallisuutta ohjaava sisältö perustuu. Yksityiskohtaisemmat lainaukset alla mainituista lähteistä on koottu liitteeseen 9.

2.1 Lait

Laki viranomaisten toiminnan julkisuudesta (621/1999) ja valtioneuvoston asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999) määrittelevät yleisellä tasolla, minkä tyyppiset asiakirjat ovat salassa pidettäviä.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttää, että Suomi valtiona kunnioittaa kaikessa toiminnassaan kansainvälisen yhteistyön mukaisia turvallisuusvelvoitteita. Velvoitepohjana toimivat kansainvälisessä kanssakäymisessä tyypillisesti joko tietoturvallisuutta säättävät valtiosopimukset tai Suomen muuten hyväksymät kansainväliset turvallisuussäännösten.

Laki turvallisuuselvityksistä (177/2002) uusiutuu vuoden 2013 kuluessa. Uusi laki on kattavuudeltaan edeltäjänsä laajempi ja sisältää paitsi säädökset henkilöturvallisuuselvitysten toteuttamiseksi, myös säädökset yritysturvallisuuselvitysten hoitamiseksi.

2.2 Tietoturvallisuusasetus

Valtioneuvoston asetuksessa tietoturvallisuudesta valtioneuvostossa (681/2010) antaa asiakirjan käsittelylle määritelmän (3§), normittaa tietoturvallisuuden perusteita (4§) sekä asettaa vaatimuksia tietojenkäsittely- ja säilytystilojen turvallisuudelle (5§). Tietoturvallisuusasetuksen pykälä 14 säättää asiakirjan säilyttämiseen ja käsittelyyn käytettävistä tiloista. Pykälä 15 asettaa vaatimuksia asiakirjan käsittelylle viranomaisen toimitilojen ulkopuolella. Elinkaariteemaa sivuavassa pykälässä 21 säädetään asiakirjan arkistoinnista ja hävittämisestä.

2.3 Ohje tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)

Tietoturva-asetuksen toimeenpanoa edesauttava VAHTI-ohje 2/2010 (*Ohje tietoturvallisuudesta valtioneuvostossa annetun asetuksen täytäntöönpanosta*) linjaa omalta osaltaan toimitilaturvallisuuden perusteita. Ohje kiinnittää lisäksi huomiota valvonta- ja kiinteistöautomaatiojärjestelmien tietoturvallisuuteen, tilojen äänieristykseen sekä sähkömagneettisen hajasäteilyn haittojen eliminoimiseen (luku 4.4).

2.4 Sisäverkko-ohje (VAHTI 3/2010)

Sisäverkko-ohje sivuaa suosituksiltaan toimitilaturvallisuutta, mutta ei mene tältä osin varsinaisesti konkretiaan. Lähtökohta on pääsääntöisesti riskienhallinnallinen ja tässä mielessä ohjeistetaan mm. yhteistyön perusteita ulkopuolisten toimijoiden kanssa (luku 8).

2.5 ICT-varautumisen vaatimukset (VAHTI 2/2012)

Tietoteknisten ympäristöjen varautumista ja jatkuvuuden hallintaa ohjaamaan laadittu VAHTI-ohje 1/2012 kuvaa erityisesti varautumiseen pohjautuvia vaatimusperusteita eri tietoturvaluokitusasteiden toteuttamista silmällä pitäen. Ohje luo strategisia suuntaviivoja myös fyysisen turvallisuuden vaatimuksille.

2.6 Kansallinen turvallisuusauditointikriteeristö (2011)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on laadittu elinkeinonharjoittajien turvallisuustason tarkastamista silmällä pitäen silloin, kun viranomainen joutuu todentamaan vaaditun turvallisuustason turvallisuusauditoinnin avulla. Kriteeristön vaatimuksia voidaan käyttää myös julkishallinnon oman turvallisuustason määrittämisessä ja siihen liittyvissä tarkastuksissa. Turvallisuusauditointi voidaan antaa erillisen hyväksyntämenettelyn jälkeen kaupallisen toimijan tehtäväksi silloin, kun kyseessä ei ole kansainvälisen tietoturvaluokitusvelvoitteen toteutumiseen liittyvä auditointi.

KATAKRI:n yhtenä osiona on yksityiskohtainen fyysisen turvallisuuden vaatimusluettelo perustasolle, korotetulle tasolle ja korkealle tasolle. Vaatimukset pohjautuvat sekä suomalaisten viranomaisten sisäisiin vaatimuksiin, että kansainvälisiin turvallisuussäännöstöihin ja standardeihin.

2.7 Euroopan unionin turvallisuusregiimi (2011)

Euroopan unionin turvallisuusluokitellun tiedon turvaamiseen tähtäävä turvallisuussäännöstö on laadittu neuvoston pääsihteeristön johdolla ja hyväksytty eduskunnan toimesta noudatettavaksi myös Suomessa niissä tapauksissa, joissa EU:n luokiteltua tietoa käsitellään suomalaisten viranomaisten tai yhteisöjen toimesta. Säännöstö on syytä tuntea myös silloin, kun suomalaista turvallisuusluokiteltua tietoa harkitaan luovutettavaksi EU-käyttöön.

EU:n turvallisuussäännöstö sisältää melko yksityiskohtaiset vaatimukset fyysisen turvallisuuden toimenpiteille. Nämä vaatimukset on lähtökohtaisesti otettu huomioon KATAKRI:ssa ja myös tässä ohjeessa niiltä osin, kuin ne kutakin valtionhallinnon toimijaa koskettavat (taulukko 1).

2.8 Naton turvallisuussäännöstö (2002)

Suomi noudattaa Naton kanssaan tekemässään kumppanuusyhteistyössä Naton asettamia tietoturvaluokitusvaatimuksia (C-M 2002(49)) silloin, kun kyseessä on Naton turvallisuusluokitellun tiedon suojaaminen. Naton turvallisuussäännösten sisältö on syytä ottaa huomioon myös silloin, kun suomalaista turvallisuusluokiteltua tietoa harkitaan luovutettavaksi Nato-käyttöön.

2.9 Muu tausta-aineisto

Valtionhallinnon toimitilaturvallisuusohjetta laadittaessa on käytetty hyväksi edellä mainittujen säädösten ja säännösten lisäksi paitsi Suomen rakentamismääräyskokoelman määräyksiä sekä eräitä salassa pidettäviksi luokiteltuja turvallisuussäännöstöjä. Näitä ovat puolustusvoimien tilaturvallisuusmääräys (2011) sekä sisäasiainhallinnon tilaturvallisuusmääräys (2011). Ohjetta on soveltuvilta osin peilattu myös tietoturvallisuuden hallintaa ohjaavaa standardia ISO/IEC- 27002:2005 vastaan.

3 Turvallisuusvyöhykkeet

Turvallisuusvyöhykkeet ovat rajattuja alueita, joiden ulkokuoren ja sen aukkojen turvallisuuteen kohdistuu erityisiä vaatimuksia.

3.1 Määräytymisperusteet

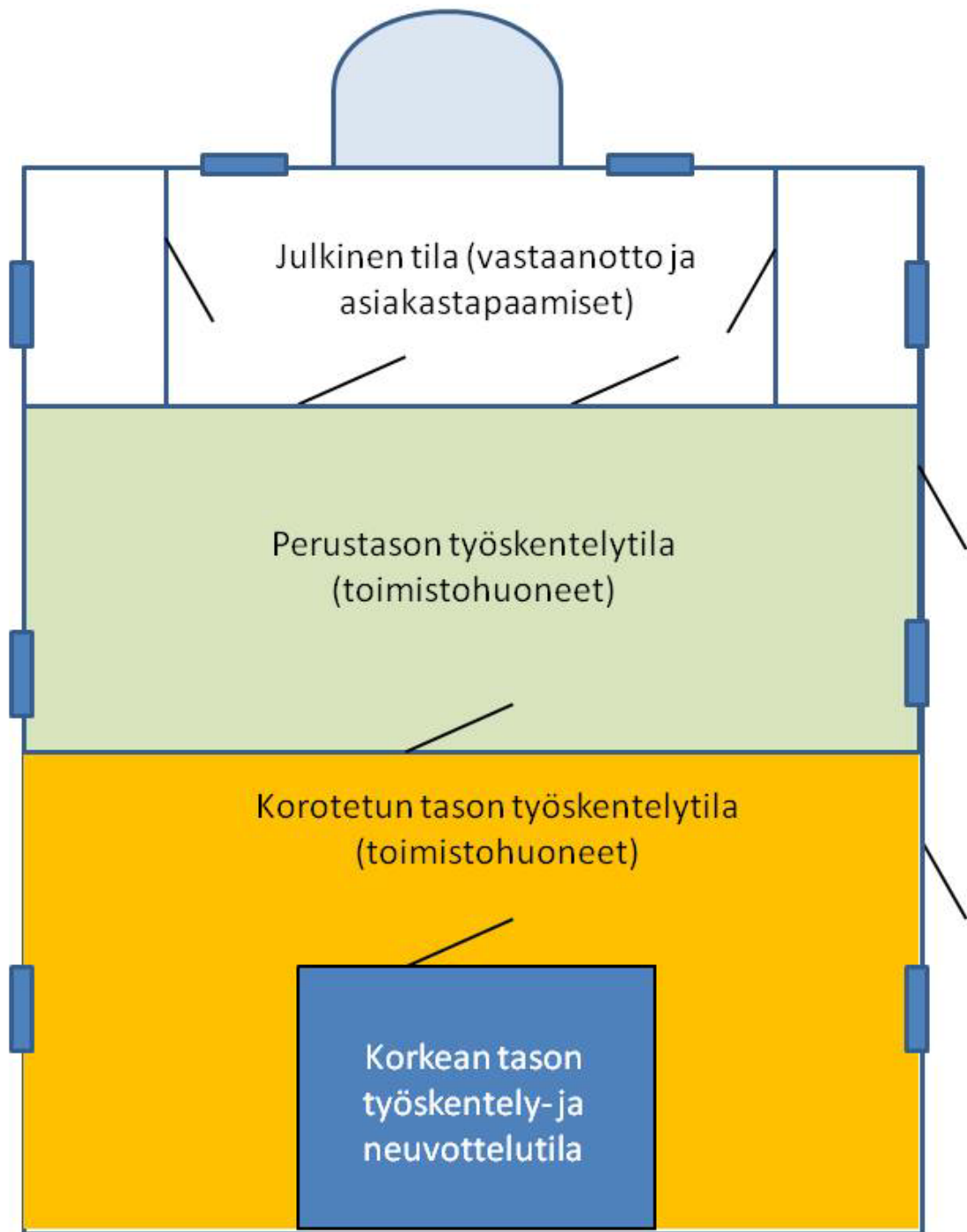
Turvallisuusvyöhykejako perustuu sekä kansalliseen lainsäädäntöön (TTA 14§) että kansainvälisten velvoitteiden toteuttamiseen¹. Vyöhykemäärittelyyn vaikuttavat oleellisesti riskianalyysin pohjalta tehdyt uhka-arviot, salassa pidettävän tiedon suojaustaso ja se, kuinka tietoa käsitellään (sähköisesti/paperiasiakirjoina/suullisesti) sekä jätetäänkö tieto tilaan säilytykseen vai ei.

Organisaation tulee analysoida toimintaympäristöönsä kohdistuvat riskit, jotta normeissa ja muissa säännöstoissa kuvatut turvallisuusvyöhykkeet saadaan nimettyä. Sen tulee myös arvioida, minkä suojaustason asiakirjoja milläkin vyöhykkeellä käsitellään ja/tai säilytetään. On myös arvioitava, miten kukin työskentelypisteen sijoitus täyttää sille asetetut suojaustasovaatimukset.

Organisaatio luokittelee tekemänsä riskienarvioinnin perusteella hallinnassaan olevat alueet ja sillä/niillä sijaitsevat toimitilansa ja laatii luokittelun perusteella vyöhykekartan. Siihen merkitään ne alueet ja toimitilat, joilla on luvallista käsitellä ja/tai säilyttää kunkin suojaustason tai turvallisuusluokan tietoa. Vyöhykekarttaa laadittaessa on syytä huomioida liitteessä 1 esitetyt vaatimukset. Näin vyöhyketilat saadaan määritettyä mahdollisimman kustannustehokkaasti. Liitteen 1 vaatimukset tulee erityisesti huomioida uudiskohteiden suunnittelussa ja rakentamisessa. Liitteessä 4 on esitetty projektikaavio siitä, miten toimitilaturvallisuus uudisrakennushankkeessa tulisi huomioida. Liitteeseen 10 on koottu joitakin esimerkkejä valtionhallinnon toimitilojen turvallisuusvyöhykejaotteluista.

¹ kansainväliset tietoturvaluussopimukset, ks. FINLEX

Esimerkki toimipisteen turvallisuusvyöhykekartasta



3.1.1 Luokittelu

Turvallisuusvyöhykkeiden muodostamisen ja vyöhykkeitä koskevien vaatimusten tulee vastata lainsäätäjän tarkoitusta. Turvallisuusvyöhykejako on johdettava tiedon luokitteluperusteista ottaen huomioon organisaation toiminnan muut tilaturvallisuuteen liittyvät vaatimukset. Julkisuuslain 24 §:ssä on määritelty, mitkä asiakokonaisuudet ovat salassa pidettäviä. Tietoturvallisuusasetuksen 8 §:ssä on säännökset salassa pidettävien asiakirjojen ja tietojen luokituksen perusteista. Suojaustasoluokittelun perusteet on esitetty 9 §:ssä ja turvallisuusluokittelun perusteet 11 §:ssä.

Turvallisuusluokitusmerkintää koskevat erityissäännökset (TTA 11§)

Jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomastoiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7—10 kohdassa tarkoitetulla tavalla, salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä. Turvallisuusluokitusmerkintä tehdään:

- 1) suojaustasoon I kuuluvaan asiakirjaan merkinnällä "ERITTÄIN SALAINEN";
- 2) suojaustasoon II kuuluvaan asiakirjaan merkinnällä "SALAINEN";
- 3) suojaustasoon III kuuluvaan asiakirjaan merkinnällä "LUOTTAMUKSELLINEN";
- 4) suojaustasoon IV kuuluvaan asiakirjaan merkinnällä "KÄYTTÖ RAJOITETTU".

3.1.2 Valtionhallinnon toimitilojen turvallisuusvyöhykejako

Valtionhallinnon toimitilat jaetaan turvallisuusvyöhykkeisiin käsiteltävän ja säilytettävän tiedon turvaamiseksi asiakirjojen luokitteluun pohjautuen. Julkisten asiakirjojen käsittely ei edellytä käsittelyympäristöltään erityisiä korotettuja turvallisuustoimia. Sama pätee myös suojaustason IV tietojen tilapäiskäsittelyyn.

Mikäli tilassa käsitellään ja säilytetään rutiininomaisesti **suojaustason IV** tietoja, tulee toimitilojen täyttää liitteessä 1 esitetyt VIHREÄN vyöhykkeen vaatimukset.

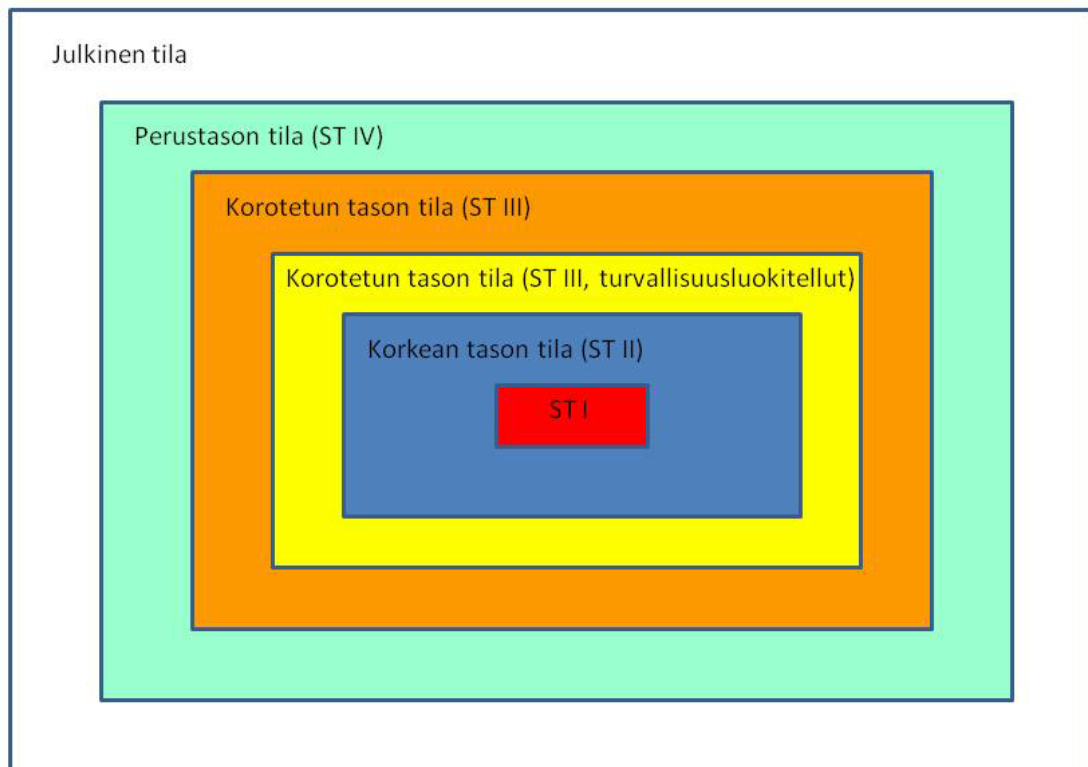
Toimitilassa, jossa muutoin kuin tilapäisesti käsitellään tai säilytetään **suojaustasoon III** luokiteltuja tietoja, joita ei kuitenkaan ole turvallisuusluokiteltu, tulee täyttää liitteessä 1 esitetyt ORANSSIN vyöhykkeen vaatimukset.

Toimitilassa, jossa muutoin kuin tilapäisesti käsitellään tai säilytetään **suojaustasoon III** luokiteltuja tietoja, jotka on **turvallisuusluokiteltu** (TTA 11§) perustuen joko kansalliseen tai kansainväliseen suojaustarpeeseen, tulee täyttää liitteessä 1 esitetyt KELTAISEN vyöhykkeen vaatimukset.

Toimitilassa, jossa muutoin kuin tilapäisesti käsitellään **suojaustasoon II** luokiteltuja tietoja, tulee täyttää liitteessä 1 esitetyt SINISEN vyöhykkeen vaatimukset.

Toimitilan, jossa muutoin kuin tilapäisesti käsitellään **suojaustasoon I** luokiteltuja tietoja, tulee täyttää viranomaisen erillisvaatimukset (ei käsitellä tässä ohjeessa). Tällainen toimitila merkitään vyöhykekarttoihin PUNAISELLA värillä.

Turvallisuusvyöhykkeiden värit suositellaan kirjoitettavan isoilla kirjaimilla erotuksena yleiskielestä.



Turvallisuusvyöhykkeiden väritunnukset

3.1.3 Turvallisuusvyöhykkeiden yleiset vaatimukset

Uudisrakentamista ohjataan ympäristöministeriön asetuksilla ja Suomen rakentamismääräyskokoelman määräyksillä. Rakentamismääräyskokoelmaa, samoin kuin Sähkötieto ry:n julkaisemaa ST-kortistoa (sähkö- ja telelaitteiden kattavat ja yksityiskohtaiset asennusohjeet) on syytä käyttää yleisinä suunnitteluperusteina.

Seuraavissa kohdissa käydään läpi valtionhallinnon toimitilaturvallisuusvaatimuksia yleisellä tasolla. Yksityiskohtaisemmat vaatimukset on esitetty turvallisuusvyöhykkeittäin liitteessä 1.

Rakenteelliset vaatimukset

Rakenteellisten järjestelyjen kansainväliset vaatimukset ovat melko yleispiirteisiä. Kansallisessa KATAKRI:ssa esitetään huomattavasti yksityiskohtaisempia vaatimuksia. Hallinnonalojen sisäiset tilaturvallisuusvaatimukset menevät osin KATAKRI:akin tarkemmalle tasolle.

Valvonta ja kulunvalvonta

Valvonta ja kulunvalvonta liittyvät henkilöstön hallintaan ja toisaalta työntekijöiden tiedonsaantitarpeeseen. Korotetun tai korkean tason käsittelytiloihin ei tule päästä ilman myönnettyä oikeutta ja sähköistä kulunvalvontaa, eivätkä asiattomat saa liikkua korotetun tason käsittelytiloissa

saattamattomina. Perustason tiloissa tulee voida käsitellä suojaustason IV tietoa ilman, että sen sisältö paljastuu ulkopuolisille.

Tilojen lukitus

Tilojen lukituksen yksityiskohdat on määritelty ainoastaan kansallisissa vaatimuksissa. Vaatimus on, että tilojen lukituksen pitää olla järjestetty siten, etteivät oikeudettomat pääse tilaan. Lukitusta käytetään yhtenä kulunvalvonnan elementtinä ja se on keskeisin vyöhykkejaon mahdollistava tekijä.

Henkilöiden tunnistus

Asiattomien pääsy työtiloihin tulee estää. Turvallisuusvyöhykkeelle saapuvan henkilön tunnistamista vaaditaan perustasolta lähtien. Korkeammille turvallisuustasojille siirryttäessä henkilön liikkuminen turvallisuusvyöhykkeellä muuttuu valvonnaltaan lokipohjaiseksi.

Tietojen ja asiakirjojen säilytys

Tietojen ja asiakirjojen säilytysmenetelmiin kohdistuu suoria kansainvälisiä ja kansallisia vaatimuksia². Suojaustason IV tietoa voidaan säilyttää lukituskaapissa tai laatikossa, kun tila on muuten riittävästi valvottu. Suojaustason III tai sitä kriittisempi tieto vaatii säilytyspaikakseen vaatimusten mukaisen kassakaapin tai holvin.

Hajasäteily

Sähkömagneettisen hajasäteilyn uhka on kansainvälisten vaatimusten mukaisesti otettava huomioon jo korotetun tason tiedonkäsittely-ympäristöissä. Kansallinen ohjeistus luo erityisesti korotetun tason suojausvaatimusten toteuttamiselle enemmän tulkintavaraa.

Uhkaa torjutaan riskiarvioon ja mahdollisesti vaimennusmittauksiin perustuen kansainvälisen TEMPEST-standardin mukaisin toimenpitein. Standardi ei ole julkinen. Standardin kansallisesta tulkinnasta ja suojautumisen ohjauksesta vastaa toimivaltaisena viranomaisena Viestintäviraston NCSA-FI -yksikkö. Hajasäteilyn vastatoimet voidaan jakaa karkeasti kahteen menetelmään: laitteiden suojaaminen metallikoteloinnilla tai työskentelytilan suojaaminen rakenteellisilla ratkaisuilla (esim. ns. Faradayn häkki). Tavoitteena on, ettei salassa pidettävää tietoa sisältävää sähkömagneettista säteilyä pääse vuotamaan tilasta ulos vaimennusvaatimukset ylittävällä tasolla.

3.2 Alueet ja toimitilat

Alueen rajaaminen parantaa sen valvontaa. Tyypillisin tapa rajata alue on rakentaa sen ympärille aita. Mikäli alueen rajaaminen aidalla on mahdotonta, voidaan aluerajoista ilmoittaa kylteillä, joissa on mahdollista kertoa esim. kameravalvonnasta.

Ympäröivän alueen varustaminen kameravalvonnalla ja muilla ilmaisimilla antaa luvattomia tunkeutumisia silmällä pitäen mahdollisuuden suurempaan vasteaikakertymään. Näin itse toimitiloihin kohdistuu vähemmän turvallisuusvaatimuksia. Näillä korvaavilla menettelyillä voidaan joissakin tapauksissa saavuttaa merkittäviä kustannussäästöjä.

² arkistolaki, ks. liite 9

Toimitilavyöhykkeitä määritettäessä on syytä ottaa huomioon kunkin toiminnan luonne muutenkin kuin riski- ja uhka-arvioihin perustuen. Onko luokiteltua tietoa käsiteltävä kaikissa tiloissa? Voidaanko työprosessien muutoksilla poistaa kokonaan joidenkin turvallisuusvaatimusten toteutustarve? Onko työntekijän päästävä lukemaan suojaustason II raportti suoraan tietojärjestelmästä? Voitaasiinko siitä ottaa hänelle paperikopio, jolloin hänen työtilaansa ei ehkä kohdistuisi vaatimuksia sähkömagneettiselta hajasäteilyltä suojautumiseksi?

3.3 Tietotekniset laitetilat

Tietoteknisiä laitetiloija³ koskevat yleisellä tasolla samat vaatimukset, kuin vastaavan tasoiseksi määritettyä normaalia toimitilaa. Laitetilojen turvallisuusrakentamisessa on syytä painottaa tiedon käytettävyyteen tähtääviä toimia muille toimitiloille asetettavia vaatimuksia enemmän. Erillisvaatimukset on tuotu yksityiskohtaisesti esille liitteessä 6. Liitteessä 1 on esitetty erikseen tärkeimmät teknisten laitetilojen turvallisuusvaatimukset (vaatimukset 39-).

3.4 Yhteiskäyttöiset toimitilat

Mikäli toimitilat ovat osittain tai kokonaan kahden tai useamman valtionhallinnon toimijan käytössä, toteutetaan turvallisuusratkaisut ylintä tiloissa käsiteltävää tai säilytettävää salassa pidettävää tietoa vastaaviksi. Kaikki tiloja miehittävät toimijat nimeävät vastuuhenkilön huolehtimaan siitä, että yhdessä valmistellut turvallisuusjärjestelyt kattavat kunkin työyhteisön toiminnan ja huolehtivat sen henkilöstöosan turvallisuuskoulutuksesta, jolla on pääsy yhteiselle turvallisuusvyöhykkeelle. Turvallisuusrakentamisen toteutus- ja/tai vuokrakustannukset sovitaan ennen hankkeen käynnistämistä.

3.5 Merkitseminen

Turvallisuusvyöhykkeiden merkitsemisessä merkintöjen fyysinen näkyvyys ei ole itseisarvo. Vyöhykkeet voidaan erottaa toisistaan esimerkiksi työntekijöiden tunnistamin värikoodein. Vyöhykkeiden rajat koulutetaan koko henkilöstölle. Henkilökortit voidaan haluttaessa varustaa värikoodein, jotka osoittavat suoraan kulkuoikeuden eri turvallisuusvyöhykkeille.

3.6 Etätyö

Henkilön työskennellessä organisaation toimitilojen ulkopuolella tulee hänen huolehtia siitä, että työskentely-ympäristö täyttää tässä ohjeessa esitetyt vaatimukset ottaen huomioon kulloinkin käsiteltävän aineiston suojaustason. Suojaustasoon IV kuuluvia asiakirjoja voidaan käsitellä tilapäisissä työskentely-ympäristöissä uhkaympäristö asian mukaisesti huomioon ottaen ilman erillisiä fyysisiä turvallisuustoimia. Mikäli vähintään suojaustasoon III kuuluvaa, turvallisuusluokiteltua aineistoa käsitellään tai säilytetään organisaation toimitilojen ulkopuolella, ei kyseisen tilan turvallisuustoimia voida mitoittaa tilapäistyöskentelyn mukaisiksi. Kuljetettaessa luokiteltuja tietoja pääasiallisen toimipisteen ja etätyöpisteen välillä on huolehdittava tietoaineiston turvallisuudesta joko kuriiritoiminnan keinoin tai esimerkiksi salassa pidettävää tietoaineistoa sisältävien muistimedioiden asianmukaisella salauksella.

³ määritelmä: ks. liite 7

3.7 Liikkuva työ

Liikkuvaan työhön liittyy korostunut ja jatkuva uhka-arviointitarve. Käsiteltäessä vähintään suojaustasoon III luokiteltuja tietoja liikkuvassa työympäristössä⁴, tulee hallinnonalan tai organisaation itsensä antaa asiasta erilliset fyysisen turvallisuuden soveltamisohjeet, jotka tähtäävät jäännösriskien minimoimiseen.

3.8 Työntekijöiden turvallisuus

Tässä ohjeessa esitettyjä fyysisen turvallisuuden toimenpiteitä toteutettaessa tulee huolehtia siitä, etteivät tiedon turvaamiseen tähtäävät ratkaisut aiheuta henkilöturvallisuusriskejä.

4 Rakenteelliset turvallisuusvaatimukset

4.1 Alue

Sen lisäksi, mitä alaluvussa 3.2 on tuotu esille, on toimitilaa ympäröivän alueen turvallisuudessa syytä ottaa huomioon seuraavaa:

- uhka-arvioon perustuen liikkumista alueella voidaan rajata aidoilla, porteilla ja ajoesteillä
- uhka-arviossa esille tulleet kriittiset kohteet katetaan tallentavalla kameravalvonnalla
- uhka-arviossa otetaan huomioon pysäköintipaikkojen sijainti toimitilaan nähden; uhkaesimerkkinä ajoneuvosta käsin toteutettava elektroninen tiedustelu, äärimmäisenä uhkana autopommi
- lastaus- ja purkualueet; uhka-arviossa huomioidaan samat kuin edellä olevassa.

4.2 Ulkopinnat

Toimitilarakennuksen ulkopinnan, alapohja mukaan lukien, tulee olla vahvuudeltaan sellainen, ettei siitä pääse paljastumatta tunkeutumaan läpi toimipaikan turvallisuussuunnitelmassa määritettynä vasteaikana. Vahvana rakenteena voidaan pitää teräsbetoniseinää tai metallilevyillä päällystettyä betonivaluharkkoseinää. Seinäelementtejä ei saa voida irrottaa tilan ulkopuolelta. Työmenetelmiä harkittaessa on huomattava, että esimerkiksi oikein raudoitettu valuharkkoseinä antaa paremman suojan, kuin väärin menetelmiä käyttäen metallilevyillä päällystetty tavanomainen valuharkkoseinä.

4.3 Sisäseinät

Sisäseinien rakennevaatimukset riippuvat ratkaisevasti muusta turvallisuustoteutuksesta. Mikäli sisäseinä toimii yleisen tilan ja korotetun/korkean tason tilan jakajana, sen rakenteelle asetetaan suuremmat

⁴ esim. poliisiautossa

vaatimukset kuin valvottujen turvallisuusvyöhykkeiden väliselle sisäseinälle. Seinän rakenteessa on jälleen oleellista riittävän (kumulatiivisen) vasteajan⁵ muodostuminen tai sen osana toimiminen.

Äänieristys on merkittävää erityisesti silloin, kun sisäseinän ulkopuolinen tila ei kuulu työyhteisön valvonnan piiriin tai kun kyseinen tila kuuluu toiseen turvallisuusvyöhykkeeseen. Mikäli huonetilassa keskustellaan enemmän kuin satunnaisesti suojaustasojen II tai I asioista, äänieristykselle asetetaan suuret vaimennusvaatimukset. Myös tällaisen tilan ilmanvaihto- ja kaapelikanavat on varustettava puheääntä tehokkaasti vaimentavilla ääniloukuilla.

4.4 Ala- ja yläpohjat

Ala- ja yläpohjan rakenteisiin pätee sama kuin sisäseinän rakenteisiin; ylä- ja alapuolisen tilan kuuluminen tai kuulumattomuus kohteen oman valvonnan piiriin vaikuttaa rakennevaatimuksiin. Niiden tilojen, joissa käsitellään enemmän kuin satunnaisesti suojaustasojen II tai I tietoja, lattiarakenteessa suositellaan käytettävän esimerkiksi erillistä pintavalua tyyppillisen ontelolaattarakenteen päällä. Ylös nostettu lattia tai alas laskettu katto parantavat äänieristystä, mutta niiden piiloon jäävää tilaa on valvottava teknisesti, mikäli tiloissa käsitellään suojaustasojen II tai I tietoja useammin kuin satunnaisesti. Kerrosten väliset IV- ja/tai kaapelikuilut tulee valvoa tunkeutumisenilmaisulla sekä huomioida äänen välittyminen kuilujen kautta.

4.5 Ovirakenteet

Ovet ovat yleisimpiä murtautumisreittejä, mistä johtuen niille on laadittu turvallisuusnormeja. Suomen viranomaisten tekemien tunkeutumistestien perusteella kansainväliset normit täyttävät ovet eivät välttämättä kykene takaamaan riittäviä vasteaikoja kaikissa tilanteissa. Ovirakenteet tulee mitoittaa siten, että ne antavat samanlaisen vasteajan kuin muu ympäröivä rakennekehä.

4.5.1 Materiaalivaatimukset

Tilat, joissa rutiininomaisesti käsitellään suojaustason III turvallisuusluokiteltuja tietoja, tulee varustaa standardit täyttävillä (liite 1) metallisilla ovi- ja karmirakenteilla. Tilat, joissa käsitellään enemmän kuin satunnaisesti suojaustasojen II ja I tietoja, on varustettava viranomaisten erityisvaatimukset täyttävillä ovirakenteilla.

Ovirakenteita valittaessa on syytä huomioida myös äänenvaimennukseen kohdistuvat vaatimukset.

4.5.2 Karmit ja kiinnitys

Turvaovet on varustettu teräskarmeilla. Karmien kiinnityksessä on kiinnitettävä erityistä huomiota seinärakenteen kestävyYTEEN (mielellään teräsbetonia) sekä karmin rakenteeseen ja kiinnityspulttien suojaamiseen.

4.5.3 Lukitusjärjestelyt

Vyöhykkeen ulkorajalla olevat ovet on varustettava Finanssialan keskusliiton vaatimukset täyttävällä turvalukituksella. Käytettäessä riippulukkoja esimerkiksi hallioivissa, on vaatimuksena sankaa suojaava rakenne.

⁵ määritelmä: ks. liite 7

Lukkojen sarjoitus tulee suunnitella kohteen käyttötarkoituksen mukaisesti. Avainten ja kulcutunnisteiden tulee olla yksilöllisesti merkittyjä ja niiden jako tulee dokumentoida. Avainten ja kulkuoikeuksien hallintajärjestely tulee olla dokumentoitu ja järjestelyä tulee valvoa. Vastuuhenkilöstöllä tulee olla hallussaan luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortit. Turvallisuusvyöhykkeen jakamattomat avaimet tulee säilyttää asianmukaisessa kassakaapissa tai holvissa.

Varmuuslukitusta suunniteltaessa tulee huomioida myös poistumistieitit. Pelastuslaitoksen pääsy kohteelle on sovittava pelastusviranomaisen kanssa.

Korotetun ja korkean tason turvallisuusvyöhykkeille johtavat ovet on varustettava sähköisellä kulunvalvonnalla.

Korotetun ja korkean tason tiloihin (ST III/ST II) johtavat, turvallisuusvyöhykkeiden väliset luukut tai hätäpoistumistiet on varustettava avattavin kalterein ja valvottava rikosilmoittimilla.

4.6 Ikkunarakenteet

Ikkunat ovat ovien lisäksi tyypillisimpiä murtautumisreittejä, mistä johtuen niille on laadittu turvallisuusnormeja. Suomalaisten viranomaisten tekemien tunkeutumistestien perusteella norminmukaisuus ei aina riitä takaamaan tavoiteltuja vasteaikoja. Ikkunarakenteiden tulee olla erityisesti kiinnitykseltään niin kestäviä, että ne antavat turvallisuuden kokonaisjärjestelyt huomioon ottaen riittävän pitkän vasteajan tunkeutumisyritystä vastaan.

4.6.1 Turvalasit ja kalvot

Tavallinen huonekorkeus on noin kolme metriä, mistä syystä seuraavan kerroksen ikkunan alareuna on yli neljän metrin korkeudessa. Tunkeutuminen tällaisen ikkunan kautta edellyttää työskentelyä tikkailla tai muun apuvälineen varassa. Alle neljän metrin korkeudessa olevat tilat, joissa säilytetään vähintään suojaustason III mukaisesti turvallisuusluokiteltua tietoa, tulee ikkuna-aukkojen osalta varustaa kaltereilla tai vaaditut normit täyttävällä turvalasilla (liite 1). Tilojen, joissa säilytetään suojaustason III turvallisuusluokittelematonta tietoa tai suojaustason IV tietoa, ikkunat on varustettava joko turvalasilla tai turvallisuusluokan 2 turvakalvolla.

4.6.2 Karmit ja kiinnitys

Ikkunoiden kiinnitys karmiin ja karmin kiinnitys ympäröivään seinä rakenteeseen on ratkaisevaa ikkuna-aukkojen kautta tapahtuvan tunkeutumisen estämiseksi. Ikkunan lukituksen ja salpojen tulee olla vahvat. Ikkuna-aukon, joka johtaa tilaan, jossa käsitellään enemmän kuin satunnaisesti vähintään suojaustason III mukaisesti turvallisuusluokiteltua tietoa, karmirakenteen tulee olla sellainen, ettei turvalasia pystytä irrottamaan karmista, eikä karmia pystytä kevyillä käsityökaluilla varustettuna irrottamaan seinä rakenteesta. Yleensä tämä vaatimus saavutetaan käytettäessä teräsbetoniseinään vahvasti kiinnitettävää teräskarmia.

4.6.3 Erillisvaatimukset

Ikkunapinnat tulee peittää silloin, kun tilassa käsitellään turvallisuusluokiteltua tietoa ja on mahdollista, että asiattomat tahot voivat nähdä tilaan sisälle. Näyttöpäätteet on asetettava sellaiseen työskentelyasentoon, ettei informaatio näy ulos.

Tilaan, jossa käsitellään vähintään suojaustason II salassa pidettävää tietoa, johtavat ikkuna-aukot tulee rakentaa edellisessä kohdassa mainituin menetelmin siitä huolimatta, että tilaan johtava ikkuna-aukko sijaitsee yli neljän metrin korkeudessa. Ikkunapinnoissa suositellaan lisäksi käytettävän ilmaisinta (lasirikko/inertia).

5 Turvallisuusvalvonta

Turvallisuusvalvonta on elimellinen osa fyysisen turvallisuuden toteutusta. Mikäli toimitiloissa käsitellään vähintään suojaustasolle III luokiteltuja tietoja, tila on valvottava tunkeutumisen ilmaisujärjestelmällä. Teknisiä järjestelyjä voidaan täydentää henkilövalvonnalla ja vartioinnilla.

Erityisesti korkean tason tiloihin voidaan kohdistaa riskiarvioon pohjautuen erillisiä teknisiä turvallisuustarkastuksia, joiden avulla mm. tilaan mahdollisesti kätkeytynyt tallentimet tai salakuuntelulähettimet pyritään paikantamaan.

5.1 Vasteaikavaatimukset

Turvallisuusvyöhykkeitä sisältävän toimitilan vartiointi ja valvonta on järjestettävä siten, että poliisi- tai vartijahenkilöstö saa indikaation tunkeutumisesta siinä määrin ajoissa, ettei tunkeutuja ehdi saada haltuunsa salassa pidettävää tietoa. Vaadittava kokonaisvasteaika saadaan laskettua liitteen 1 taulukosta johdetulla pisteytyksellä.

5.2 Valvontajärjestelmät

Alueita ja tiloja voidaan valvoa erilaisilla teknisillä järjestelyillä. Näitä ovat

- alueen ja tilojen kameravalvontajärjestelmät,
- alueen ja tilojen kulunvalvontajärjestelmät sekä
- tunkeutumisen ilmaisujärjestelmät.

Kameravalvonnalla voidaan täydentää aluevalvontaa siten, että ensimmäinen indikaatio tunkeutumisesta saadaan mahdollisimman aikaisessa vaiheessa vartijareagoinnin vasteajan lyhentämiseksi. Korkean tason tiloissa voidaan vyöhykkeen turvallisuusvalvontaa täydentää tallentavalla kameravalvonnalla, joka on liitetty joko tunkeutumisen ilmaisujärjestelmään tai kuvan analyysiin perustuvaan ilmaisujärjestelmään. Kamerateat on asetettava siten, ettei niiden välityksellä siirry salassa pidettävää tietoa. On myös huomattava, että kameravalvontajärjestelmä on tietojärjestelmä ja sitä koskevat tietojärjestelmille asetetut turvallisuusvaatimukset. Kameravalvonnasta on tiedotettava tilassa työskenteleville, jottei syyllistyttäisi salakatseluun (RikosL 24 luku). Tapauskohtaisesti kameravalvonta saattaa edellyttää rekisteriselostemenettelyä (henkilötietolaki 2 luku). Ennen kameravalvonnan käyttöönottoa on syytä huomioida myös, mitä laki yksityisyyden suojasta työelämässä (759/2004) säättää kameravalvonnan osalta (5 luku).

Korotetun ja korkean tason tilat on varustettava kulunvalvonnalla siten, että vain oikeutetut henkilöt pääsevät vyöhykkeen sisälle ja heidän kulkunsa vyöhykkeelle ja sieltä ulos voidaan myöhemmin todentaa

(järjestelmäloki). Korkean tason vyöhykkeelle mentäessä tulee sisäänmenovaiheessa käyttää kaksoistunnistusta (esimerkiksi pääsykoodi ja sähköinen tunniste).

Tunkeutumisen ilmaisujärjestelmä vaaditaan jo perustason turvallisuusvyöhykkeelle, mikäli siellä käsitellään suojaustason IV tietoja, eikä tietoja säilytetä vaatimukset täyttävässä kassakaapissa tai holvissa. Perustasolla vaatimuksena on luokan⁶ 2 tunkeutumisen ilmaisujärjestelmä (voi olla langaton). Ylemmillä tasoilla edellytetään luokan 3 järjestelmää, jolla valvotaan ovet, aukot, ikkunat, työtilat ja kuori.

Tunkeutumisen ilmaisujärjestelmän toimivuus tulee testata vähintään kaksi kertaa vuodessa toimipaikan turvallisuusdokumentaatioissa kuvatulla tavalla.

5.3 Vartiointi

Vartiointin järjestelyt täydentävät alueen ja tilojen valvontaa. Vartiointihenkilöstö ei käytä turvallisuusluokiteltujen tilojen avaimia muuten kuin poikkeustilanteissa. Avaimia säilytetään tilan haltijan toimesta sinetöidyssä kuoressa. Avainten käyttöperiaatteet on kuvattu selkeästi yksikön turvallisuusohjeistossa.

6 Toimeenpano ja ohjeistaminen

Tämä ohje otetaan käyttöön 1.x.2013 käytettäväksi tietoturvallisuusasetuksen velvoitteiden toimeenpanemiseksi valtionhallinnossa (perustaso 1.10.2013, korotettu ja korkea taso 1.10.2015).

Liiteluettelo

Liite 1: Turvallisuusvaatimustaulukko

Liite 2: Valtion turvallisuussopimusmallit

- rakentamispalvelut (liite 2.1)
- suunnittelu ja konsultointi (liite 2.2)
- kiinteistöpalvelut (liite 2.3)

Liite 3: Rakentamisdokumentaation käsittelysuositukset

- tiedon luokittelumatriisi (liite 3.1)
- tiedon luokitteluohje rakentamishankkeissa (liite 3.2)
- turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa (liite 3.3)

Liite 4: Rakentamishankkeen turvallisuusaskeleet (esimerkki)

⁶ FK:n varmuusluokittelu

Liite 5: Pohjakuvaesimerkit eri turvallisuusvyöhykkeiden mukaisista työympäristöistä

Liite 6: Tietoteknisten laittilojen turvallisuussuositukset

Liite 7: Määritelmät

Liite 8: Lähteet

Liite 9: Viiteaineiston lähdelainaukset

Liite 10: Esimerkkejä valtionhallinnon toimipisteiden turvallisuusvyöhykejaottelusta

Liite 1: Turvallisuusvaatimustaulukko

Tässä liitteessä on esitetty valtionhallinnon toimitilaturvallisuusvaatimukset eri tietoturvasoille.

Taulukossa ilmaistut vaatimukset pohjautuvat kansallisista kriteeristöistä (ks. lähdeluettelo) johdettuihin tulkintoihin. Niiden viranomaisten, jotka käsittelevät EU:n tai Naton turvallisuusluokiteltua tietoa tulee huomioida näiden organisaatioiden erillisvaatimukset, jotka on esitetty omassa sarakkeessaan silloin, kun ne poikkeavat esitetyistä kansallisista vaatimuksista.

Taulukon jatkeeksi on koottu joitakin yksittäisiä **toteutussuosituksia**, joihin viitataan vaatimussarekkeen asteriksilla*. Koska valtionhallinnon työpisteiden toimintaympäristö vaihtelee suuresti, ennen toteutuksia vaatimuksenmukaisuus on syytä varmistaa oman viraston tai hallinnonalan turvallisuusasiantuntijalta.

Vasteaikalaskenta

Osa viranomaisten vaatimuksista on haluttu pitää turvallisuusluokiteltuna tietona. Nämä tiedot toimitetaan tarvitsijalle viranomaisharkintaan perustuen ja niihin viitataan taulukossa termillä ”viranomaisten erillisvaatimukset”. Nämä erillisvaatimukset sisältävät tutkittua tietoa eri turvarakenteiden antamista vasteajoista ja toimivat perustana vasteaikamalliin perustuvalla tasoarvioinnille. Vasteaikamallia käytetään kyseisten viranomaisten ilmoittamaan laskentakaavaan perustuen. Vasteaikamallin sijasta tässä liitteessä keskitytään vaatimuskohtaiseen pisteytysmalliin.

Pisteytys

Vaadittavat vähimmäispisteet lasketaan ottaen huomioon toimintaympäristön yleinen riskitaso, joka voi olla joko matala, keskimääräinen tai korkea. Tyypillisesti tiheä kaupunkirakenne ja kontrollin ulkopuolelle jäävät seinänaapurit (tai vastaavat) aiheuttavat korkean riskitason.

Poikkeamat Korkean riskitason toimintaympäristössä ei sallita lainkaan vakavia poikkeamia. Vakavien poikkeamien korjaamatta jättäminen edellyttää työpisteen johtajan kirjallista ja perusteltua erillispäätöstä. Pisteiden antoperusteet ovat:

1 miinus piste = vakava poikkeama vaatimuksesta

0 pistettä = poikkeama vaatimuksesta

1 pluspiste = lievä poikkeama vaatimuksesta

2 pluspistettä = vaatimukset täyttävä.

Osa-alueiden (ALUE+RAKENTEET+VALVONTAJÄRJESTELYT) yhteenlasketun pistekeskiarvon on oltava matalan riskitason kohteessa **suurempi kuin 1**. Keskimääräisen riskitason kohteen osa-alueiden keskiarvon on oltava **vähintään 1,50**. Korkean riskitason kohteiden osa-alueiden pistekeskiarvon on oltava **vähintään 1,75**.

Mikäli tavoitetason mukaisessa vaatimussarakkeessa lukee ”ei vaatimusta”, ei kohdasta voi saada pisteitä, ellei sarakkeessa lisäksi todeta, että toteutuksella voidaan korvata jonkin toisen vaatimuksen puutteita.

Tapauksissa, joissa vaatimus perustuu riskiarvioon, pisteytys toteutuu ainoastaan silloin, kun riski arvioidaan huomioon otettavaksi. Mikäli yksittäistä riskiä ei katsota tarpeelliseksi huomioida, vaatimuksen toteuttamisesta tai toteuttamatta jättämisestä ei saa plus-, eikä miinus pisteitä.

VAATIMUS	PERUSTASO Turvallisuus- vyöhyke VIHREÄ	KOROTETTU TASO ST III Turvallisuus- vyöhyke ORANSSI	KOROTETTU TASO TL III Turvallisuus- vyöhyke KELTAINEN	KORKEA TASO Turvallisuus- vyöhyke SININEN	EU/NATO erityisvaa- timukset	PIST.
KOHDE:						
Kohteelle määritetty riskitaso (matala/keskimääräinen/korkea):						
A: ALUE						
1. Pysäköintipaikat	Ei vaatimusta	Ei vaatimusta	Ei vaatimusta	Huomioitava elektronisen tiedustelun uhka. Pysäköinti on sallittu alueen haltijan luvalla merkityille paikoille.		
2. Lastaus/ purkausalueet	Ei vaatimusta	Ei vaatimusta	Ei vaatimusta	Huomioitava elektronisen tiedustelun uhka.		
3. Aidat*	Ei vaatimusta, mutta aita voidaan käyttää korvaavana elementtinä.	Ei vaatimusta, mutta aita voidaan käyttää korvaavana elementtinä.	Kyllä	Kyllä		
4. Portit	Ei vaatimusta	Aitarakennetta vastaava porttirakenne.	Aitarakennetta vastaava porttirakenne. Mahdollisuus lukita mekaanisesti, sähköinen kulunohjaus mahdollista.	Aitarakennetta vastaava porttirakenne. Mahdollisuus lukita mekaanisesti, sähköinen kulunohjaus mahdollista.		
5. Ajoesteet*	Ei vaatimusta	Riskiarvion mukaisesti	Riskiarvion mukaisesti	Riskiarvion mukaisesti		
6. Aluevalvonta (kohderakennusta välittömästi ympäröivä alue).	Ei vaatimusta, toteutuksella voidaan korvata rakenteellisen turvallisuuden puutteita	Ei vaatimusta, toteutuksella voidaan korvata rakenteellisen turvallisuuden puutteita	Ei vaatimusta, toteutuksella voidaan korvata rakenteellisen turvallisuuden puutteita	Valvonta riskiarvion mukaisesti, mikäli korkean tason vyöhyke rakennuksen ulkopintana.		
B: RAKENTEET						
7. Seinärakenne	Normaalit seinärakenteet	<u>Ulkoseinät</u> : Luja tiili- tai muu vastaavan lujuuden omaava rakenne. <u>Väliseinät</u> (silloin kun turvallisuus-	<u>Ulkoseinät</u> : Luja betoni tai muu vastaavan lujuuden omaava rakenne. <u>Väliseinät</u> (silloin kun turvallisuus-	Vyöhykettä rajaavien seinien tulee olla teräsbetonia, vahvistettua tiilirakennetta, tai vahvistettua seinärakennetta.		

		vyöhyke rajoittuu väliseinään): Normaali toimistokäytössä hyväksytty harkko- tai levyseinärakenne	vyöhyke rajoittuu väliseinään): Normaali toimistokäytössä hyväksytty harkko- tai levyseinärakenne vahvistettuna viranomaisten erillisvaatimusten mukaisesti. Seinärakenteita ei saa voida irrottaa tilan ulkopuolelta.	Jos vyöhykkeelle johtavan 3. vyöhykkeen ulkoraja on rakennettu 2. vyöhykkeen määräysten mukaisesti, voidaan väliseinä 2. vyöhykkeen rajalle rakentaa kevytrakenteiseksi.		
8. Äänieristys	Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja.	Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja.	Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. Ääniloukut ilmastointi- ja kaapelikanaviin, mikäli äänen kantautuminen pitää huomioida riskiarvion perustuen.	Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. Ääniloukut ilmastointi- ja kaapelikanaviin, mikäli äänen kantautuminen pitää huomioida riskiarvion perustuen.		
9. Salakuuntelun estäminen	1) Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan suojattavista asioista. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa suojattavista	1) Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa suojattavista asioista.	1) Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa suojattavista asioista.	1) Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa suojattavista asioista.		

	asioista.					
10. Hajasäteilyn estäminen	Ei vaatimuksia.	Ei vaatimuksia.	Arvioidaan tarve huonetilan tai laitteiden suojaamiseksi TEMPEST-vastatoimin.	Tilassa ei käytetä mitään sellaisia elektronisia laitteita, joiden käyttö on kielletty. Lukittavat lokerot matkapuhelimille vyöhykkeen ulkopuolelle. Arvioidaan tarve huonetilan tai laitteiden suojaamiseksi TEMPEST-vastatoimin, samoin kuin tarve EMP-/HPM-suojaukselle.	NATO: Vasta-toimet riski-analyysiin pohjautuen. EU: vasta-toimet riski-analyysiin pohjautuen tasolta EU CONFIDENTIAL alkaen.	
11. Lattia- ja kattorakenteet*	Normaali katto-, välipohja- ja lattiarakenne.	Normaali katto-, välipohja- ja lattiarakenne.	Katto-, välipohja- ja lattiarakenne vahvistetaan viranomaisten erillis-vaatimusten mukaisesti (riskiarvio).	Katto-, välipohja- ja lattiarakenne vahvistetaan viranomaisten erillis-vaatimusten mukaisesti (riskiarvio).		
12. Ikkunat*	Normaali rakenne. Riskianalyysin tulosten perusteella voidaan alle 4 metrin korkeudessa sijaitsevien ikkunoiden lasi kalvottaa vähintään SFS-EN 356 P1A murtosuoja-kalvolla*.	Normaali rakenne, mikäli tilassa tunkeutumisen ilmaisjärjestelmä. Riskianalyysin tulosten perusteella voidaan alle 4 metrin korkeudessa sijaitsevien ikkunoiden lasi kalvottaa vähintään SFS-EN 356 P1A murtosuoja-kalvolla.	Alle 4 m korkeudessa maatasosta, tai alemman kerroksen kattotasanteelta, olevissa ikkunoissa tulee olla standardin SFS-EN 356 P6B mukainen suoja-lasitus. Suoja-lasitus tulee asentaa murtautumisyrityksen kestävään karmiin. Alle 4 metrin korkeudessa olevien ikkunoiden tulee olla sellaisia, ettei niitä pysty avaamaan. Yli 4 m	Pyrittävä ikkunattomiin ratkaisuihin. Mikäli kuitenkin joudutaan käyttämään ikkunoita, ikkunoissa tulee olla standardin SFS-EN 356 P6B mukainen suoja-lasitus, joka ei saa välittää ääniväriähtelyjä uloimpaa lasiin. Lisäksi on huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne sekä lasin kiinnitys karmirakenteeseen siten, ettei	NATO: 5m	

			korkeudessa olevat ikkunat voidaan vahvistaa tarpeen mukaan.	sitä voi irrottaa karmista (esim. vetämällä tai työntämällä). Alle 4 metrin korkeudessa olevien ikkunoiden tulee olla sellaisia, ettei niitä pysty avaamaan. Tarve luodinkestävään suojalasitukseen tulee arvioida tapauskohtaisesti. Luodinkestävässä suojalasituksessa tulee noudattaa standardia SFS-EN 1063.		
13. Kattoikkunat	Kuten muutkin ikkunat.	Kuten muutkin ikkunat.	Kuten muutkin ikkunat.	Ei kattoikkunoita.		
14. Salakatselun estäminen	Huomioitava turvallisuusohjeistuksessa.	Huomioitava turvallisuusohjeistuksessa.	Ikkunoissa tulee olla sälekaihtimet.	Ikkunoissa tulee olla sälekaihtimet.		
15. Ovet	Normaali ovirakenne.	Normaali ovirakenne.	Vyöhykkeen rajalla oltava turvaovi (standardi SFS EN 1627-luokka 3) tai viranomaisten erillisvaatimusten mukaisesti vahvistettu P60-palo-ovi. Oven tulee täyttää myös tilan käyttötarkoituksen mukaiset äänieristysvaatimukset.	Vyöhykkeen rajalla käytettävä turvaovea (standardi SFS EN 1627-luokka 3), jonka tulee täyttää tilan käyttötarkoituksen mukaiset äänieristysvaatimukset. Lisäksi tulee harkita, vaaditaanko vyöhykkeen rajalla vapaan läpikulun estävää kulkuannostelijaa ja aluevalvontaohjelmistoa. Jos läpikulun estävää kulkuannostelijaa ei käytetä		

				vyöhykkeen rajalla, on kulunhallinta hoidettava muulla luotettavalla tavalla, esim. käyttämällä kulunvalvontalukijoita oven molemmin puolin ja ohjelmistona aluevalvontaohjelmaa.		
16. Halliovet tai ajo- ovet, jotka johtavat turvallisuusvyöhykkeen sisään.*	Ei vaatimuksia. Äänieristys huomioitava riskitason mukaisesti.	Hyväksytyt rullakalterit*. Äänieristys huomioitava riskitason mukaisesti.	Palo-oven EI60- tyyppinen vahvennettu läpiajon estävä rakenne.	Palo-oven EI60- tyyppinen vahvennettu läpiajon estävä rakenne.		
17. Muut aukot	Oltava lukittavissa.	Aukot oltava lukittavissa ja valvottavissa.	Tilan kuoren aukot on valvottava tukeutumisen ilmaisinjärjes- telmällä. Aukot on suljettava kalteroinnilla tai vahvoilla terässäleiköillä*.	Tilan kuoren aukot on valvottava tukeutumisen ilmaisinjärjes- telmällä. Aukot on suljettava kalteroinnilla tai vahvoilla terässäleiköillä*.		
18. Hätäpoistumistiet Huom! Lukitus ei saa estää hätäpoistumista.	Ei erillisvaatimuksia	Ei erillisvaatimuksia	Alempien turvallisuus- vyöhykkeiden hätäpoistumistiet eivät saa kulkea vyöhykkeen kautta.	Alempien turvallisuus- vyöhykkeiden hätäpoistumistiet eivät saa kulkea vyöhykkeen kautta.		
19. Asiakirjan säilytysvaatimukset*	Säilytetään lukitussa paikassa, edellyttäen että tila on valvottu tunkeutumisen ilmaisujärjestelmällä työajan ulkopuolella. Ilman em. järjestelyä säilytys kassakaapissa tai holvissa.	Säilytetään lukitussa paikassa, edellyttäen että tila on valvottu tunkeutumisen ilmaisujärjestelmällä työajan ulkopuolella. Ilman em. järjestelyä säilytys kassakaapissa tai holvissa.	Säilytetään holvissa tai kassakaapissa*. Murtosuoja: - holvi EURO V (EN 1143-1) - kassakaappi EURO II (EN 1143-1) ja Paloturva: - 60 P tai 60 DIS (VDMA 24491) - yhdistelmä- kaappi 60P + 60	Säilytetään holvissa tai kassakaapissa. Murtosuoja: - holvi EURO II (EN 1143-1) - kassakaappi EURO II (EN 1143-1) ja Paloturva: - 60 P tai 60 DIS (VDMA 24491) - yhdistelmä- kaappi 60P + 60		

			Diskette (NT FIRE 017)	Diskette (NT FIRE 017)		
20. Lukitus* vyöhykkeen rajalla	Käyttölukko* heloineen ja vastalevyineen.	Käyttölukko* heloineen ja vastalevyineen.	Käyttölukko* heloineen ja vastalevyineen. Lisäksi hakateljellä varustettu varmuuslukko* vastalevyineen tai muu saman murto- ja tiirikointilujuu- den antava rakenne ja riittävät valvonta- järjestelyt.	Käyttölukko* heloineen ja vastalevyineen. Lisäksi hakateljellä varustettu varmuuslukko* vastalevyineen tai muu saman murto- ja tiirikointilujuu- den antava rakenne ja riittävät valvonta- järjestelyt.		
21. Lukitus vyöhykkeen sisällä	Käyttölukko	Käyttölukko	Käyttölukko	Käyttölukko		
22. Avainten ja kulkutunnisteiden hallinta	Vyöhykkeelle tulee nimetä avainvastuu- henkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnistei- den kuittauksista ja jakamattomien avainten säilytyksestä.	Vyöhykkeelle tulee nimetä avainvastuu- henkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnistei- den kuittauksista ja jakamattomien avainten säilytyksestä.	Vyöhykkeelle tulee nimetä avainvastuu- henkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnistei- den kuittauksista ja jakamattomien avainten säilytyksestä.	Vyöhykkeelle tulee nimetä avainvastuu- henkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnistei- den kuittauksista ja jakamattomien avainten säilytyksestä.		
23. Yleisavaimen hallinta	Yleisavainta on säilytettävä turvallisesti vastuuhenkilön hallinnoimana.	Tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Vyöhykkeen yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty, mikä on huomioitava kiinteistöhuollon sopimuksissa.	Tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Vyöhykkeen yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty, mikä on huomioitava kiinteistöhuollon sopimuksissa.	Tilaan ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Vyöhykkeen yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty, mikä on huomioitava kiinteistöhuollon sopimuksissa.		

24. Vartiohenkilöstön avainhallinta	Ei erillisvaatimuksia	Vartiointihenkilöstölle jaettavat avaimet tulee olla sinetöityinä poikkeuksellisia tilanteita varten. Järjestely on huomioitava vartiointipalvelusopimuksissa.	Vartiointihenkilöstölle jaettavat avaimet tulee olla sinetöityinä poikkeuksellisia tilanteita varten. Järjestely on huomioitava vartiointipalvelusopimuksissa.	Vartiointihenkilöstölle jaettavat avaimet tulee olla sinetöityinä poikkeuksellisia tilanteita varten. Hälytystilanteissa korkean tason tilaan edellytetään saapuvan kaksi henkilöä samanaikaisesti. Järjestely on huomioitava vartiointipalvelusopimuksissa.		
25. Vieraiden pääsynhallinta	Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan.	Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Vierasta valvotaan.	Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Vierasta valvotaan.	Vieraan tuominen tilaan edellyttää ennakko-ilmoitusta ja turvallisuusvastaavan hyväksyntää. Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Vierasta valvotaan.		
26. Huoltohenkilöstön pääsynhallinta	Huoltohenkilö tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan.	Huoltohenkilö tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Huolehditaan siitä, että huoltohenkilö ei pääse näkemään suojaustason III tietoa. Vierasta valvotaan.	Huoltohenkilö tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan*. Huolehditaan siitä, että huoltohenkilö ei pääse näkemään turvallisuusluokiteltua tietoa. Vierasta valvotaan.	Huoltohenkilön tuominen tilaan edellyttää ennakko-ilmoitusta ja turvallisuusvastaavan hyväksyntää. Huoltohenkilö tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Huolehditaan siitä, että huoltohenkilö ei pääse näkemään salassa pidettävää tietoa. Vierasta valvotaan.		
27. Siivoushenkilöstön hallinta	Siivoushenkilö tunnistetaan ja varustetaan vieraskortilla.	Siivoushenkilö tunnistetaan ja varustetaan vieraskortilla.	Siivoushenkilöstä vaaditaan etukäteen turvallisuus-	Siivoushenkilöstä vaaditaan etukäteen turvallisuus-		

	Vierailu kirjataan.	Vierailu kirjataan. Huolehditaan siitä, että siivoushenkilö ei pääse näkemään suojaustason III tietoa.	selvitys. Hänet tunnistetaan aina erikseen ja varustetaan vieraskortilla. Vierailu kirjataan. Huolehditaan siitä, että siivoushenkilö ei pääse näkemään turvallisuusluokiteltua tietoa.	selvitys. Hänet tunnistetaan aina erikseen ja varustetaan vieraskortilla. Vierailu kirjataan. Huolehditaan siitä, että siivoushenkilö ei pääse näkemään salassa pidettävää tietoa. Siivoustyötä valvotaan.		
28. LVIS-varmistukset	Toimintavaatimusten mukaisesti.	Toimintavaatimusten mukaisesti.	LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. Kriittiset laitteistot on tunnistettu ja varmennettu.	LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. Kriittiset laitteistot on tunnistettu ja varmennettu.		
29. LVI-automaation etäkäyttö	Ei vaatimuksia.	Ei vaatimuksia.	Tilan riskianalyysissä kiinnitettävä huomiota LVI-etäkäytön riskeihin.	Jos tilassa on palvelimia tai muita olosuhteille herkkiä laitteita, ei tilan LVI-järjestelmää saa ohjata etäkäyttöisesti.		
30. Hissit	Ei vaatimuksia.	Ei vaatimuksia.	Hissin käyttöä on ohjattava kulunvalvonnalla.	Hissin käyttöä on ohjattava kulunvalvonnalla, hissikuilu valvottava.		
C: VALVONTAJÄRJESTELYT						
31. Kulunvalvontajärjestelmä*	Järjestelmän käyttöönottoa harkitaan riskianalyysiin perustuen.	Vyöhykkeen rajalla on käytettävä kulunvalvontaa.	Vyöhykkeen rajalla on käytettävä kulunvalvontaa.	Vyöhykkeen rajalla on käytettävä kulunvalvontaa. Sisään mentäessä käytettävä kaksoistunnistusta (esimerkiksi pääsykoodi ja sähköinen tunniste). Poistuttaessa tilasta tulee käyttää kulunvalvontatunnistetta.		

32. Kulunvalvonta-järjestelmän hallinnointi	Ei vaatimuksia.	Ei vaatimuksia.	Kulkuoikeuksien hallinnointi on oltava viranomaisen hallinnassa tai jos se on ulkoistettu, vaaditaan ulkoistuksen kohteen kanssa turvallisuus-sopimusta.	Kulun-valvonnassa käytetään aluevalvontaa. Kulkuoikeuksien hallinnointi on oltava tilan haltijalla.		
33. Tunkeutumisen ilmaisinjärjestelmä*	Jos tilassa säilytetään suojaustason IV tietoa, tila varustetaan tunkeutumisen ilmaisulla (vähintään FK 3-luokka) tai tieto säilytetään vaatimukset täyttävässä kassakaapissa.	Vyöhykkeen raja valvottava tunkeutumisen ilmaisulla (vähintään FK 3-luokka).	Ovet, aukot, ikkunat ja tilat valvottava tunkeutumisen ilmaisulla (vähintään FK 3-luokka), suositellaan kuoren valvontaa.	Ovet, aukot, ikkunat ja tilat valvottava tunkeutumisen ilmaisulla (vähintään FK 3-luokka), suositellaan kuoren valvontaa.		
34. Tunkeutumisen ilmaisinjärjestelmän testaus	Turvallisuus-dokumentaation mukaisesti	Turvallisuus-dokumentaation mukaisesti	Turvallisuus-dokumentaation mukaisesti	Kerran kuukaudessa		
35. Tunkeutumisen ilmaisinjärjestelmän hallinnointi	Turvallisuus-dokumentaation mukaisesti	Turvallisuus-dokumentaation mukaisesti	Turvallisuus-dokumentaation mukaisesti	Tunkeutumisen ilmaisu-järjestelmän hallinnointi on oltava tilan haltijalla.		
36. Kameravalvonta-järjestelmä	Vyöhykettä tai sitä ympäröivää aluetta valvotaan kamera-valvonnalla.	Vyöhykettä tai sitä ympäröivää aluetta valvotaan tallentavalla kamera-valvonnalla.	Vyöhykettä tai sitä ympäröivää aluetta valvotaan tallentavalla kamera-valvonnalla.	Turvallisuus-vyöhykettä tai tilaa on valvottava tallentavalla kamera-valvonnalla.*		
37. Palvelintilan kameravalvonta	Palvelintilaa tai sitä ympäröivää aluetta voidaan valvoa tallentavalla kamera-valvonnalla.	Palvelintilaa tai sitä ympäröivää aluetta voidaan valvoa tallentavalla kamera-valvonnalla.	Palvelintilaa tai sitä ympäröivää aluetta suositellaan valvottavan tallentavalla kamera-valvonnalla.	Laite- ja palvelintilat on varustettava tallentavalla kamera-valvonnalla*.		
38. Vartiointi	Mahdollisen vartiointin vasteajan on	Vartiointin vasteajan on oltava sellainen,	Vartiointin vasteajan on oltava sellainen,	Ilmoitus hälytyksestä heti tilan omistajalle.		

	oltava sellainen, että kiinnijäämis-riski on merkittävä.	että kiinnijäämis-riski on merkittävä. Vasteaika tulee testata vähintään vuosittain. Testin tulos dokumentoidaan.	että kiinnijäämis-riski on merkittävä. Vasteaika tulee testata vähintään vuosittain. Testin tulos dokumentoidaan.	Vartioinnin vasteajan on oltava sellainen, että kiinnijäämis-riski on merkittävä. Vasteaika tulee testata vähintään vuosittain. Testin tulos dokumentoidaan.		
D: TIETOTEKNISET LAITETILAT						
39. Kaapelointi	täsmentyy					
40. Palo-osastointi	täsmentyy					
41. Lämpö	täsmentyy					
42. Savu	täsmentyy					
43. Vesivahinko	täsmentyy					
44. Pöly ja puhtaus	täsmentyy					
45. Laiteauriot	täsmentyy					
46. UPS	täsmentyy					
47. Olosuhdehälytys	täsmentyy					
48. Varavoima	täsmentyy					
49. Tärinä ja värähtely	täsmentyy					
50. Kemikaalit	täsmentyy					
51. Räjähdeet	täsmentyy					
52. Polttoaineet	täsmentyy					
53. Valmiussuunnitel.	täsmentyy					
54. Sammutuslaitteet	täsmentyy					
55. Varatilat	täsmentyy					
56. EMP ja hajasäteily	täsmentyy					
57. HPM	täsmentyy					

VAATIMUSTEN TÄSMENNYKSIÄ JA TOTEUTUSSUOSITUKSIA

3. AIDAT

Mikäli kohdetta ympäröi valmis aita, sen estearvoa voidaan usein nostaa asettamalla aidan päälle matala piikkilankaeste. Mikäli aidan estetiikkaarvot ovat merkityksellinen, piikkilankaeste voidaan toteuttaa matalana, mutta koko aidan päälliosan peittävänä mattona.

Uudisrakentaminen tapauksissa, joissa aidan ulkonäölle ei ole asetettu erityisiä vaatimuksia:

- aidan h = min 2,40 m
- 2 piikkilankaa (sinkitty teräs 2x1,6mm) ylhäällä, 1 alhaalla.
- silmäkoko max 40x40mm, lanka min 3,0 mm.
- alareuna max. 5cm maan pinnasta.

KELTAINEN ja SININEN turvallisuusvyöhyke: Pylväät halkaisijaltaan 70 mm alumiiniprofiilia (vast.), pylväiden väli enintään 3,00 m, metalliverkon kiinnitysruuvin (vast.) tulee olla aidalla suljetun alueen sisäpuolella.

5. AJOESTEET

Puomia käytettäessä tulee kulkuaukko olla suljettavissa myös portilla.

11. LATTIA- JA KATTORAKENTEET

Olemassa olevissa toimitiloissa: katto-, välipohja- ja lattiarakenne vahvistetaan viranomaisten erillisvaatimusten mukaisesti (esim. erillinen pintavalu lattiassa), mikäli kohteen riskiarviointi tätä edellyttää (seinänaapureiden ja toimintaympäristön arviointi jne.). Riskiarvioinnissa huomioidaan ympäristötekijöiden lisäksi oman toiminnan luonne; onko uhkana esimerkiksi omaisuusrikollinen vai kenties valtiollinen tiedustelupalvelu. Edellistä vastaan riittää kevyempi suojarakentaminen kuin jälkimmäistä vastaan. Yksiselitteisiä rakennevaatimuksia ei anneta julkisessa ohjeessa rikostorjunnallisista syistä.

12. IKKUNAT

Murtosuojakalvoa parempana ratkaisuna voidaan pitää lasirikkoilmaisinta.

16. HALLI-OVET TAI AJO-OVET

KELTAINEN ja SININEN turvallisuusvyöhyke: Ovirakenteen vahvennuksen voi toteuttaa esim. teräspuomilla (12*50 mm lattateräs, tukipisteet seinissä ja keskellä ovissa, FK:n (Finanssialan keskusliitto) varmuusluokan riippulukko) tai ajonestopollarilla. Nosto-oviaukot on varustettava aina myös teräspuomilla tai kalteriovella. Äänieristys riskitason mukaisesti.

Hyväksytyt rullakalterit: SFS-ENV 1627, luokka 2.

17. MUUT AUKOT

Terässäleikköä ei saa voida irrottaa ulkoapäin.

19. ASIAKIRJAN SÄILYTYSVAATIMUKSET

Oleellista on, että kassakaappi ankkuroidaan vahvaan ympäröivään rakenteeseen (ankkurointi ≥ 100 mm). Riskiarvioinnin osoittaessa erityisen korkeaa riskiä, on kassakaappia lisäksi valvottava sensoreilla (esim. inertia, seisminen tai kamera).

Pisteytys, KELTAINEN turvallisuusvyöhyke: kassakaapista, joka ei täytä asetettua vaatimusta saa puolet ao. pisteistä.

20. LUKITUS VYÖHYKKEEN RAJALLA

Käyttölukon tulee olla FK:n hyväksymää mallia tai SFS 7020-standardiin perustuen hyväksytty käyttölukko. Varmuuslukon tulee olla FK:n hyväksymää mallia tai SFS 7020-standardiin perustuen hyväksytty varmuuslukko.

26. HUOLTOHENKILÖSTÖN PÄÄSYNHALLINTA

KELTAINEN turvallisuusvyöhyke: Työajan ulkopuolella tapahtuvien huoltokäyntien on kirjauduttava sähköiseen kulunvalvontalokiin.

27. SIIVOUSHENKILÖSTÖN HALLINTA

KELTAINEN ja SININEN turvallisuusvyöhyke: mikäli turvallisuusselvitys tai Personal Security Clearance tasolle CONFIDENTIAL on mahdotonta toteuttaa, siivoushenkilöstön työskentelyä valvotaan korostetusti isäntien toimesta.

31. KULUNVALVONTAJÄRJESTELMÄ

Kulunvalvontalukijoiden sijoitus vyöhykkeen rajalle.

33. TUNKEUTUMISEN ILMAISINJÄRJESTELMÄ

Ilmaisimet vyöhykkeen rajalla olevissa ovissa, vyöhykkeellä kulkuväylillä, neuvottelutiloissa sekä harkinnan mukaan muissa huonetiloissa.

36. KAMERAVALVONTAJÄRJESTELMÄ

SININEN turvallisuusvyöhyke: kameravalvonnan tallennus on liitettävä tunkeutumisen ilmaisujärjestelmään tai tallentimen liiketunnistukseen.

37. PALVELINTILAN KAMERAVALVONTA

SININEN turvallisuusvyöhyke: kameravalvonnan tallennus on liitettävä tunkeutumisen ilmaisujärjestelmään tai tallentimen liiketunnistukseen.

Liite 2: Valtionhallinnon toimitilarakentamisen turvallisuussopimusmallit

Tässä liitteessä esitetään turvallisuussopimusmallit seuraaviin käyttötarkoituksiin:

- rakentamispalvelut (liite 2.1)
- suunnittelu ja konsultointi (liite 2.2)
- kiinteistöpalvelut (liite 2.3)

VAHTI 2/2013 liite 2.1

**RAKENTAMISPALVELUN
TURVALLISUUSSOPIMUS**

(LUONNOS)

2.11.2012

[ASIAKAS]

JA

[TOIMITTAJA]

(Ohje: Tämä sopimus malli, joka pitää aina muokata organisaatio- ja hankintakohtaisesti kulloinkin hankittavana olevan kohteen mukaan. Malli on tarkoitettu käytettäväksi rakentamispalveluhankinnoissa yksityiseltä palveluntuottajalta (rakennusurakat).

Sisällys

1 SOPIJAPUOLET	37
2 MÄÄRITELMÄT.....	37
3 SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS.....	38
4 TURVALLISUUSOPIMUKSEN TAUSTA JA TARKOITUS	38
5 LUOTTAMUKSELLISUUS JA SALASSAPITO	39
6 PÄÄSY TILOIHIN	40
7 PÄÄSY JÄRJESTELMIIN JA TIETOIHIN	41
8 VAITIOLOSITOUUMUS.....	41
9 TURVALLISUUSSELVITYKSET	43
10 TIETOTURVALLISUUS	43
11 ALIHANKKIJAT	44
12 TARKASTUKSET JA RAPORTOINTI	44
13 SOPIMUSSAKKO JA VAHINGONKORVAUS	45
14 SOPIMUSMUUTOKSET.....	47
15 SOPIMUKSEN IRTISANOMINEN [JA PURKAMINEN].....	47
16 SOPIMUKSEN VOIMASSAOLO.....	47
17 SOVELLETTAVA LAKI JA ERIKESKISYYKSIEN RATKAISEMINEN.....	48
18 SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET	48

SOPIJAPUOLET

1.1 Sopijapuolet ovat:

1. [nimi] (jäljempänä "Asiakas")

Osoite

Y-tunnus

2. [nimi] (jäljempänä "Toimittaja")

Osoite

Y-tunnus

MÄÄRITELMÄT

- 2.1 **Palvelu** tarkoittaa sitä uudis- tai korjausrakentamiseen liittyvää rakentamispalvelua, josta Asiakas ja Toimittaja ovat sopineet Pääsopimuksessa. Mitä tässä Turvallisuussopimuksessa on sovittu Palvelusta, sovelletaan soveltuvin osin myös Pääsopimuksessa sovittuun tavarahankintaan.
- 2.2 **Pääsopimus** tarkoittaa Toimittajan ja Asiakkaan välistä sopimusta nro [0000], jolla sopijapuolet ovat sopineet [sopimuksen kohteesta].
- 2.3 **Salassa pidettävä tieto** tarkoittaa kaikkea sellaista Asiakkaan Toimittajalle luovuttamaa tai Toimittajalla olevaa Asiakkaan asiakirjamuotoista tai muuta tietoa, joka on määritelty salassa pidettäväksi laissa viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä "julkisuuslaki") tai muussa lainsäädännössä, ja jonka Asiakas on tällaiseksi tiedoksi merkinnyt tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin. Salassa pidettäväksi tiedoksi katsotaan myös julkisuuslaissa tarkoitetun ei vielä julkisen asiakirjan sisältämä tieto. Lisäksi kaikki Asiakkaan luovuttamat henkilötiedot katsotaan Salassa pidettäväksi tiedoksi. Salassa pidettäväksi tiedoksi ei katsota sellaista tietoa, joka on julkisesti saatavilla tai jonka sopijapuoli on saanut tietoonsa laillisella tavalla kolmannelta osapuolelta ilman sitä koskevaa salassapitovelvoitetta.
- 2.4 **Turvallisuussopimus** tarkoittaa tätä sopimusasiakirjaa liitteineen.
- 2.5 **Asiakkaan Tilat** tarkoittavat sellaisia Asiakkaan käytössä olevia tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja tai joissa liikkumista on muutoin turvallisuussyistä syytä rajoittaa. Rakenteilla tai korjausrakentamisen kohteena olevat Asiakkaan käyttöön tulevat tilat katsotaan tällaiseksi tilaksi, kun niiden toteutus on edennyt sellaiseen vaiheeseen, että tiloissa liikkumalla voi saada tietoa, jonka tulee pysyä salassa.
- 2.6 **Toimittajan Tilat** tarkoittavat sellaisia Toimittajan tai sen alihankkijan tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja.
- 2.7 **Rakennustyömaalla** tarkoitetaan rakentamispalvelun toteuttamiseksi määriteltyä työma- aluetta, jolla liikkuminen edellyttää asianmukaista työmaakohtaista kulkulupaa.
- 2.8 **Työmaarakennuksella** tarkoitetaan rakennustyömaalla sijaitsevia parakkeja tai vastaavia tiloja, joissa voidaan säilyttää, käyttää tai muutoin käsitellä Palveluun liittyviä Salassa pidettäviä tietoja.

SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS

3.1 Tämä Turvallisuussopimus muodostuu tästä sopimusasiakirjasta ja seuraavista liitteistä:

- Liite 1 Turvallisuussopimuksen yhteyshenkilöt
- Liite 2 Ohje Salassa pidettävien tietojen käsittelystä ja säilyttämisestä
- Liite 3 Henkilöstön vaitiolositoumusmalli

(Ohje: Vaitiolovelvollisuus tulee suoraan laista, Julkl 23 §. Sitoumuksella henkilöstöön kuuluva ilmoittaa saaneensa tiedon tietojen salassapidosta ja siitä, että niiden ilmaiseminen tai luovuttaminen ilman lupaa on kiellettyä. Samaan asiakirjaan voi laittaa myös käsittelyvelvoitteita koskevan lauseen.)

Liite 4 Toimittajan turvallisuudenhallinnan kuvaus [/Selvitys Palveluun liittyvistä tietoturvamenettelyistä]

[Liite 5 Palveluun sovellettava valtionhallinnon tietoturvallisuustaso, tietoturvallisuusvaatimukset, Asiakkaan tilojen turvallisuusluokitukset, Palveluun liittyvien tietojen luokitus suojaustasoille]

3.2 Asiakas ja Toimittaja vastaavat omalta osaltaan liitteen 1 ylläpidosta.

3.3 Liitteessä 2 on esitetty Asiakkaan hyväksymät menettelyt ja ohjeet eri suojaustasoluokkiin kuuluvan tiedon, asiakirjojen ja muun tietoaineiston käsittelystä. Asiakas vastaa liitteen ylläpidosta. *[Ohje: Ohjeiden tulisi olla sisällöltään yhdenmukaiset tietoturvallisuusasetuksen ja sen täytäntöönpanosta annetun VAHTI-ohjeen 2/2010 luokittelu- ja käsittelyohjeiden kanssa.]*

3.4 Toimittaja vastaa liitteen 4 ylläpidosta. Liitteen tulee vastata voimassa olevaa tilannetta.

[3.5 Asiakas vastaa liitteen 5 ylläpidosta]

TURVALLISUUSSOPIMUKSEN TAUSTA JA TARKOITUS

4.1 Toimittaja ja Asiakas ovat tehneet Pääsopimuksen nro [xxx] [sopimuksen kohde] [pvm].

4.2 Tässä Turvallisuussopimuksessa sovitaan Asiakkaan ja Toimittajan välillä noudatettavista turvallisuusjärjestelyistä ja Salassa pidettävää tietoa koskevista järjestelyistä edellä mainitun Pääsopimuksen sisältämien Palveluiden tuottamisessa sekä kaikessa Pääsopimukseen liittyvässä Asiakkaan ja Toimittajan välisessä yhteistyössä.

4.3 Sopijapuolet tiedostavat, että Pääsopimuksen perusteella toimitettaviin Palveluihin sisältyy sellaista tietoa, jonka salassa pysyminen on *[esimerkki, tarkennetaan hankintakohtaisesti: yhteiskunnan häiriöttömän toimintakyvyn ja valtion sekä yksilöiden turvallisuuden kannalta kriittistä]*. Palvelun tuottamisen yhteydessä Toimittajan ja sen alihankkijan henkilöstöllä on pääsy Asiakkaan Tiloihin, joissa liikkumista on turvallisuussyistä syytä rajoittaa. Tällä Turvallisuussopimuksella sopijapuolet pyrkivät varmistamaan, että Salassa pidettävät tiedot pysyvät salassa.

4.4 Huolimatta siitä, mitä muissa Asiakkaan ja Toimittajan välisissä sopimuksissa on mahdollisesti sovittu tämän Turvallisuussopimuksen piiriin kuuluvista asioista tai niihin

liittyvistä vastuista taikka sopimusten keskinäisestä pätemisjärjestyksestä, tätä Turvallisuus sopimusta sovelletaan aina ensisijaisesti tämän Turvallisuussopimuksen piiriin kuuluvissa asioissa. Tähän Turvallisuussopimukseen tai sen perusteella syntyviin vastuisiin ei sovelleta muissa sopijapuolten välisissä sopimuksissa mahdollisesti sovittuja vastuunrajoituksia.

(Ohje: Jos otat tämän Turvallisuussopimuksen Pääsopimuksen liitteeksi, huomaa soveltamisjärjestyksen vaikutus tämän ehdon sanamuotoon.)

LUOTTAMUKSELLISUUS JA SALASSAPITO

- 5.1 Tässä Turvallisuussopimuksessa kuvattuja turvallisuusjärjestelyjä noudatetaan aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa.
- 5.2 Asiakas noudattaa julkisyhteisönä julkisuuslaissa, valtioneuvoston asetuksessa tietoturvallisuudesta valtiorahallinnossa (681/2010; jäljempänä tietoturvallisuusasetus) sekä muussa lainsäädännössä olevia salassapitoa ja julkisuutta koskevia säännöksiä. Sopimuksella ei voida poiketa lainsäädännön Asiakkaalle asettamista pakottavista velvoitteista.
(Ohje: Poista/muokkaa, jos Asiakas ei kuulu julkisuuslain tai tietoturvallisuusasetuksen soveltamisalaan.)
- 5.3 Toimittaja sitoutuu pitämään salassa kaikki Asiakkaan sille luovuttamat tai sillä olevat tai toimeksiannon toteuttamisessa syntyneet Salassa pidettävät tiedot, ottaen lisäksi huomioon kohdassa 5.7 sovitun. Salassa pidettäviä tietoja ei myöskään saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi.
- 5.4 Toimittajan tulee käsitellä Salassa pidettäviä tietoja vain Palvelun tuottamisen edellyttämässä laajuudessa. Toimittaja antaa Salassa pidettäviä tietoja vain niille henkilöille, jotka tarvitsevat Salassa pidettäviä tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Toimittaja sitoutuu saattamaan Turvallisuussopimuksen vaikutusalaan kuuluvat henkilöt tietoiseksi tähän Turvallisuussopimukseen liittyvistä velvoitteista ja antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Salassa pidettävien tietojen asianmukaisesta käsittelystä henkilöille, joilla on pääsy näihin tietoihin. Toimittaja sitoutuu valvomaan, että edellä tarkoitetut henkilöt noudattavat Turvallisuussopimusta.
- 5.5 Toimittaja sitoutuu säilyttämään ja käsittelemään Salassa pidettäviä tietoja siten, että ne pysyvät vain niiden henkilöiden hallussa, joilla on oikeus Salassa pidettäviin tietoihin, eivätkä ne joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon. Asiakkaan antama tarkempi ohjeistus Salassa pidettävien tietojen käsittelystä ja säilyttämisestä, jota Toimittaja sitoutuu noudattamaan, on liitteessä 2.
- 5.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille saattaa olla rikoslain mukaan rangaistava teko.
- 5.7 Tiedon antamisesta asiakirjasta, joka on saatu Asiakkaalta tai laadittu Asiakkaan toimeksiantotehtävää suoritettaessa, päättää Asiakas, jollei toimeksiannosta muuta johdu.
- 5.8 Toimittaja vastaa siitä, ettei Asiakkaan kohteiden tai toiminnan turvallisuus vaarannu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Turvallisuussopimuksen tai Pääsopimuksen vastaisen toiminnan johdosta.

- 5.9 Toimittaja ja sen alihankkijat saavat mainita referenssinä tehneensä työtä Asiakkaalle vain, jos asiasta on erikseen kirjallisesti sovittu.
- 5.10 Mikäli Salassa pidettäviä asiakirjoja tai tietoja käsitellään Asiakkaantoimitilojen ulko-puolella, on Toimittajan noudatettava Asiakkaan antamia toimintaohjeita ja erityisesti huolehdittava siitä, ettei tietoaineistojen turvallisuus vaarannu.
- 5.11 Tässä Turvallisuuksopimuksessa kuvattujen menettelyjen lisäksi Asiakkaalla on oikeus tarvittaessa antaa turvallisuuteen liittyviä käytännön toimintaohjeita, joita Toimittajan tulee noudattaa.

PÄÄSY TILOIHIN

- 6.1 Toimittaja vastaa siitä, että pääsy Asiakkaan korotetun tai korkean turvallisuustason Tiloihin (vyöhykkeet ORANSSI (ST III), KELTAINEN (TL III) tai SININEN (ST II)) annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 10 tarkoitettu turvallisuus selvitys ja jotka ovat tietoisia tämän Turvallisuuksopimuksen velvoitteista ja Tiloissa liikkumisesta annetuista ohjeista.
- Henkilöt, joille ei ole annettu oikeutta päästä mainittuihin Asiakkaan Tiloihin, saavat oleskella tiloissa ainoastaan Asiakkaan luvalla ja valvonnan alaisina.
- 6.2 Toimittaja vastaa siitä, että pääsy Asiakkaan turvallisuuden perustason Tiloihin (vyöhyke 4) tai rakennustyömaalle annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen ja jotka ovat tietoisia tämän Turvallisuuksopimuksen velvoitteista ja Tiloissa tai rakennustyömaalla liikkumisesta annetuista ohjeista. Henkilöt, joille ei ole annettu edellä tarkoitettulla tavalla oikeutta päästä mainittuihin Asiakkaan Tiloihin tai rakennustyömaalle, saavat oleskella niissä ainoastaan Asiakkaan luvalla ja valvonnan alaisina. Henkilöiden pääsy mainittuihin Tiloihin tai rakennustyömaalle ei lähtökohtaisesti edellytä henkilöiden turvallisuus selvittämistä. Asiakkaalla on kuitenkin oikeus edellyttää luvussa 10 tarkoitettun turvallisuus selvityksen tekemistä myös mainittuihin Tiloihin tai rakennustyömaalle pääsevien henkilöiden osalta, mikäli selvitysten tekemiselle laissa asetetut edellytykset täyttyvät.
- 6.3 Henkilöiden, joilla on pääsy Asiakkaan Tiloihin tai rakennustyömaalle, tulee olla tunnistettavissa. Henkilöillä on oltava Asiakkaan Tiloissa tai rakennustyömaalla liikkuessaan näkyvillä Asiakkaan kanssa sovittu kuvallinen henkilötunniste.
- 6.4 Toimittajan ja sen alihankkijan Tilojen tulee olla Tiloissa käsiteltävien Salassa pidettävien tietojen luokitustaso n asettamat vaatimukset huomioon ottaen asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi Tiloihin ja siellä oleviin Salassa pidettäviin tietoihin. Tiloille asetettavia vaatimuksia ja niiden täyttymistä arvioidaan voimassa olevan [Kansallisen turvallisuus auditointikriteeristön (KATAKRI)] mukaisesti.
- 6.5 Mikäli Palvelu suoritetaan tai Salassa pidettäviä tietoja käsitellään Toimittajan tai sen alihankkijan Tiloissa, Toimittajan tulee varmistaa Tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms.

erityistilanteiden varalta. Asiakas ja Toimittaja sopivat tarvittaessa Palveluun liittyvistä tarkemmista vaatimuksista.

- 6.6 Henkilöt, joille ei ole myönnetty oikeutta Salassa pidettäviin tietoihin tai niitä sisältäviin järjestelmiin luvun 7 mukaisesti, saavat oleskella Toimittajan tai sen alihankkijan Tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli Salassa pidettäviä tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.
- 6.7 Henkilöiden, joilla on pääsy Toimittajan tai alihankkijan Tiloihin, tulee olla tunnistettavissa.
- 6.8 [Asiakkaalla on oikeus vaatia luvussa 10 tarkoitetun turvallisuusselvityksen hakemista henkilöistä, joilla on oikeus päästä [tiettyihin yksilöityihin] Toimittajan tai sen alihankkijan Tiloihin, joissa käsitellään suojaustasolle II tai III luokiteltuja Salassa pidettäviä tietoja. Toimittajan tulee myös hyväksyttää henkilö Asiakkaalla ennen kuin henkilölle voidaan myöntää pääsy [tiettyihin yksilöityihin] Tiloihin.]
- 6.9 [Toimittaja pitää ja/tai velvoittaa tarvittaessa alihankkijansa osaltaan pitämään luetteloa henkilöistä, joille Palveluun liittyen on annettu oikeus päästä kohdassa [valitaan sopiva vaihtoehto: 6.1, 6.2, 6.8] tarkoitettuihin Tiloihin tai rakennustyömaalle, huolehtii luettelon ajantasaisuudesta ja toimittaa sen [sovituin määrävälein tai pyynnöstä] Asiakkaalle.]

PÄÄSY JÄRJESTELMIIN JA TIETOIHIN

- 7.1 Toimittaja vastaa siitä, että suojaustasolle II tai III luokiteltuja Salassa pidettäviä tietoja annetaan tai pääsy sellaisia tietoja sisältäviin järjestelmiin sallitaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 10 tarkoitettu turvallisuusselvitys ja joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin. Asiakkaalla on kuitenkin tarvittaessa oikeus edellyttää edellä tarkoitetun menettelyn noudattamista myös suojaustasolle IV luokiteltuihin Salassa pidettäviin tietoihin tai sellaisia tietoja sisältäviin järjestelmiin pääsevien henkilöiden osalta, mikäli turvallisuusselvityksille laissa asetetut edellytykset täyttyvät. Oikeuden päästä Asiakkaan järjestelmiin, jotka sisältävät Salassa pidettäviä tietoja, antaa Asiakas.
- 7.2 Toimittaja vastaa siitä, että Salassa pidettävien tietojen käsittelyyn osallistuvat Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt sekä henkilöt, joilla on pääsy Toimittajan tai Asiakkaan järjestelmiin, joissa säilytetään Salassa pidettäviä tietoja, ovat tietoisia salassapitoa koskevista velvoitteistaan ja noudattavat tätä Turvallisuussopimusta.
- 7.3 [Toimittaja pitää ja/tai velvoittaa tarvittaessa alihankkijansa osaltaan pitämään luetteloa henkilöistä, jotka Palveluun liittyen käsittelevät suojaustasolle [valitaan sopivat vaihtoehdot: II, III, IV] luokiteltuja Salassa pidettäviä tietoja tai joilla on pääsy sellaisia tietoja sisältäviin järjestelmiin, huolehtii luettelon ajantasaisuudesta ja toimittaa sen [sovituin määrävälein tai pyynnöstä] Asiakkaalle.]

RAKENNUSTYÖMAA JA TYÖMAARAKENNUKSET

[Ohje: Alla esitetyt vaatimukset ovat esimerkinomaisia ja ne tulee muokata tapauskohtaisesti tarpeeseen sopiviksi.]

- 8.1 Toimittaja vastaa siitä, että rakennustyömaa aidataan ja sinne kulkeminen toteutetaan valvotusti ja kontrolloidusti kulkupisteiden kautta. Rakennustyömaalla tulee olla työmaatoimisto kulkupisteen läheisyydessä. Toimittaja järjestää rakennustyömaalle tallentavan [kulun]valvontajärjestelmän.
- 8.2 Päivittäisenä työaikana erityistä rakennustyömaan vartiointia ei edellytetä. Toimittaja järjestää kustannuksellaan työajan ulkopuolella rakennustyömaalle piirivartiointin ja tallentavan kameravalvonnan.
- 8.3 Toimittaja ilmoittaa työajan ulkopuolella rakennustyömaalla ilman lupaa tavatuista henkilöistä poliisille ja raportoi Asiakkaan yhteyshenkilölle.
- 8.4 Toimittaja vastaa siitä, että työmaarakennusten, joissa käsitellään Salassa pidettäviä tietoja, ikkunat varustetaan murtosuojakaltereilla ja sisäänkäyntiovet salparaudoilla. Lukitukset on tehtävä [Suomen vakuutusyhtiöiden keskusliiton] hyväksymillä turvalukoilla. Työmaarakennusten avaimia saa luovuttaa vain niiden hallussapitoon oikeutetuille henkilöille kuittausta vastaan. Työmaarakennukset, joissa säilytetään Salassa pidettäviä asiakirjoja, on varustettava [Finanssialan keskusliiton julkaiseman ”Murtohälytysjärjestelmät ja –palvelut 2008” määrittelemän tason 3 mukaisella] rikosilmoitusjärjestelmällä.
- 8.5 Rakennustyömaa-alueella valokuvaaminen ja/tai muu kuvataallentaminen on sallittua ainoastaan Palvelun dokumentoinnin edellyttämässä suppeassa laajuudessa [suunnittelijoiden, Toimittajan työnjohdon ja valvojien toimesta]. Muuhun kuvaamiseen tarvitaan Asiakkaan antama erillinen lupa.

VAITIOLOSITOUS

- 9.1 Toimittaja vastaa siitä, että henkilö, joka käsittelee Salassa pidettäviä tietoja ja/tai jolla on pääsy järjestelmiin, joissa Salassa pidettäviä tietoja säilytetään, tekee vaitiolositoumuksen Asiakkaan hyväksymälle lomakkeelle (liite 3) ennen kuin hän saa aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin.
- 9.2 Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijan henkilökuntaan kuuluva henkilö, jolla on pääsy Asiakkaan kohdassa 6.1 tarkoitettuihin tiloihin, tekee vaitiolositoumuksen Asiakkaan hyväksymälle lomakkeelle (liite 3) ennen kuin hän saa oikeuden päästä mainittuihin tiloihin. Asiakkaalla on tarvittaessa oikeus edellyttää vaitiolositoumusta myös henkilöiltä, joilla on pääsy [kohdassa 6.2 tarkoitettuihin perusturvallisuustason tiloihin ja/tai rakennustyömaalle].

TURVALLISUUSSELVITYKSET

- 10.1 Jollei toisin sovita, jotta henkilö saa kohdassa 7.1 tarkoitetulla tavalla oikeuden käsitellä sellaisia Salassa pidettäviä tietoja, joiden salassapito on välttämätöntä turvallisuusselvityksistä annetun lain (177/2002) 2 §:ssä mainittujen etujen suojaamiseksi, ja/tai päästä järjestelmiin, jotka sisältävät sellaisia Salassa pidettäviä tietoja, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettu perusmuotoinen turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys. Jotta henkilö saa oikeuden päästä Asiakkaan kohdassa 6.1 [ja 6.2] tarkoitettuihin Tiloihin, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettujen edellytysten täyttyessä suppea turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys. [Kohdassa 6.8 tarkoitettuihin tiloihin pääsevästä henkilöstä tehdään suppea turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys.]
- 10.2 Jollei toisin sovita, tasoltaan vastaavaksi ulkomaiseksi turvallisuusselvitykseksi voidaan katsoa ainoastaan ulkomaisen kansallisen turvallisuusviranomaisen (esim. General Security Agreement:in eli GSA:n mukainen National Security Authority, NSA) tekemä turvallisuusselvitys (Personal Security Clearance, PSC). Jollei toisin sovita, PSC-selvitys edellytetään tehtäväksi henkilöstä, joka on ulkomaan kansalainen ja jolla on ollut pysyvä asuinpaikka Suomessa vähemmän kuin [5] vuotta.
- 10.3 Mikäli Toimittaja käyttää Palvelun toteutuksessa sellaista alihankkijaa, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee alihankkijasta tarvittaessa hakea yhteisöturvallisuusselvitys (Facility Security Clearance, FSC) ja tietojen käsittelyyn osallistuvista henkilöistä henkilöturvallisuusselvitys (Personal Security Clearance, PSC), jollei toisin sovita.
- 10.4 Asiakkaan tehtävänä on hakea kaikkia tässä luvussa tarkoitettuja turvallisuusselvityksiä.
- 10.5 Asiakas vastaa kohdissa 10.1-10.3 tarkoitettujen turvallisuusselvitysten kustannuksista. Mikäli turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan tai Toimittajan alihankkijan henkilöstössä tapahtuu vaihdos tai Asiakkaasta riippumaton lisäys, Toimittaja vastaa uuden henkilön turvallisuusselvityksen kustannuksista.
- 10.6 Toimittajan tulee toimittaa kansallisen turvallisuusselvityksen kohteena olevan henkilön täyttämä ja allekirjoittama turvallisuusselvityshakemuslomake Asiakkaalle turvallisuusselvityksen teettämistä varten. Lomakkeen tulee sisältää selvityksen kohteena olevan henkilön suostumus turvallisuusselvityksen tekemiseen. Jos turvallisuusselvitys tulee tehtäväksi sellaisessa valtiossa, jonka lainsäädännön mukaan kyseessä olevan selvityksen tekeminen ei edellytä selvityksen kohteena olevan henkilön suostumusta, Toimittajan ei myöskään [tämän kohdan nojalla] tarvitse pyytää henkilöltä edellä mainittua suostumusta.
- 10.7 Asiakkaalla on perustellusta turvallisuuteen liittyvästä syystä oikeus kieltää Toimittajan tai sen alihankkijan henkilön osallistuminen Palvelun suorittamiseen.

TIETOTURVALLISUUS

- 11.1 Toimittaja noudattaa julkisuuslaissa tarkoitettua hyvää tiedonhallintatapaa sekä henkilö-tietolain (523/1999) edellyttämää hyvää tietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä sekä muuta tietosuoja koskevaa lainsäädäntöä Pääsopimukseen liittyvän Palvelun tuottamisessa.

- 11.2 *[Vaihtoehto 1]*
Asiakas luokittelee Salassa pidettäviä tietojaan tietoturvallisuusasetuksen mukaisiin suojaustasoihin. [Tietojen luokitus eri suojaustasolle ilmenee sopimuksen liitteestä 5.] Toimittaja sitoutuu noudattamaan Salassa pidettäviä tietoja käsitellessään edellä mainitun asetuksen ja Asiakkaan ohjeistuksen kyseiselle suojaustasolle asettamia vaatimuksia.
- 11.2 *[Vaihtoehto 2]*
Asiakas ei luokittele Salassa pidettäviä tietoja tietoturvallisuusasetuksen mukaisiin suojaustasoihin. Toimittaja sitoutuu noudattamaan perustason tietoturvallisuutta ja Asiakkaan ohjeistusta Salassa pidettäviä tietoja käsitellessään.
- 11.3 Asiakas on määrittänyt Palvelun hankinnan yhteydessä Palveluun sovellettavan valtionhallinnon tietoturvataso ja Palveluun liittyvät konkreettiset tietoturvavaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esitetty [Pääsopimuksen liitteessä x/tämän Turvallisuussopimuksen liitteessä 5.]

ALIHANKKIJAT

- 12.1 Toimittajan tulee hyväksyttää Asiakkaalla sellainen alihankkija, jota se aikoo käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai siellä oleviin työmaarakennuksiin. Tässä Turvallisuussopimuksessa alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai työmaarakennuksiin.
- 12.2 Mitä tässä Turvallisuussopimuksessa on sovittu Toimittajan henkilöstöstä, sovelletaan myös alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön.
- 12.3 Toimittajan tulee huolehtia siitä, että se pystyy noudattamaan tätä Turvallisuussopimusta myös käyttäessään alihankkijoita. Toimittaja on tietoinen ja sen on tiedotettava alihankkijalleen, että turvallisuusjärjestelyiden saattamisesta tämän Turvallisuussopimuksen edellyttämälle tasolle saattaa syntyä kustannuksia. Asiakas ei vastaa näistä kustannuksista.
- 12.4 Toimittaja vastaa alihankkijoiden toiminnasta kuin omastaan ja siitä, että alihankkijat toimivat tämän Turvallisuussopimuksen ehtojen mukaisesti.
- 12.5 Ellei toisin sovita, Toimittajan tulee tehdä tämän Turvallisuussopimuksen ehtoja vastaava sopimus kohdassa 12.1 tarkoitetun alihankkijansa kanssa ja Toimittajan on asetettava alihankkijalleen vastaava velvollisuus tämän käyttämän alihankkijan osalta. [Sopimus on hyväksyttävä Asiakkaalla ennen sen allekirjoittamista.]

TARKASTUKSET JA RAPORTOINTI

- 13.1 Asiakkaalla tai Asiakkaan määräämällä kolmannella taholla (joka ei ole Toimittajan suoranainen kilpailija) on oikeus tarkastaa omalla kustannuksellaan etukäteen ilmoitettuna ajankohtana Toimittajan ja sen alihankkijoiden turvallisuusjärjestelyt tätä Turvallisuussopimusta sekä Pääsopimusta koskevilta osin. Asiakkaan on ilmoitettava tahdostaan suorittaa tarkastus viimeistään kolmekymmentä (30) päivää ennen ehdotettua tarkastuspäivää. Toimittaja voi ehdottaa uutta päivää tarkastukselle. Uusi ajankohta ei kuitenkaan saa olla myöhemmin kuin kymmenen (10) päivää Asiakkaan ehdottaman päivän jälkeen. Tarkastus saadaan suorittaa kuitenkin enintään kaksi kertaa vuodessa, ellei ole erityisen painavia syitä useammille tarkastuksille tai toisin sovita. Haavoittuvuuskannauksia

voidaan kuitenkin tehdä edellä mainituista määräajoista riippumatta erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tai sen alihankkijoiden tieto turvallisuutta tai Toimittajan tai sen alihankkijoiden salassapitovelvoitteita muita asiakkaita kohtaan. Asiakkaalla on edellä tarkoitetun tarkastusoikeuden lisäksi oikeus suorittaa Tiloissaan ja rakennustyömaalla jatkuvaa valvontaa ja tehdä näissä ennalta ilmoittamatta turvallisuustarkastuksia tässä Turvallisuussopimuksessa asetettujen velvoitteiden täyttymisen arvioimiseksi.

- 13.2 Toimittajan tulee huolehtia sopimusjärjestelyin siitä, että Asiakkaalla on mahdollisuus tarkastaa myös Toimittajan sellaisen alihankkijan turvallisuusjärjestelyt, joka osallistuu Salassa pidettävien tietojen käsittelyyn tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai siellä oleviin työmaarakennuksiin.
- 13.3 Mikäli tarkastuksessa havaitaan merkittäviä puutteita turvallisuusjärjestelyissä, Toimittaja korvaa Asiakkaalle tarkastuksesta aiheutuneet kustannukset.
- 13.4 Toimittajan tulee korjata tarkastuksessa tai muussa valvonnassa havaitut puutteet viivytyksettä Asiakkaan kirjallisesta ilmoituksesta. Erityisiä korjaavia toimenpiteitä vaativat puutteet on korjattava viimeistään 30 vuorokauden kuluessa Asiakkaan kirjallisesta ilmoituksesta, ellei siitä ole Asiakkaan ja Toimittajan välillä erikseen toisin sovittu. Olennaiset puutteet, jotka muodostavat ilmeisen uhkan tietoturvallisuudelle, on kuitenkin korjattava heti. Asiakas ei vastaa edellä mainituista korjauksista aiheutuvista kuluista ja kustannuksista.
- 13.5 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, jos Toimittajan tai sen alihankkijan tämän Turvallisuussopimuksen kannalta keskeisissä toiminnoissa tai henkilöstö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai jos Toimittajan tai sen alihankkijan omistussuhteissa tapahtuu merkittäviä muutoksia.
- 13.6 Toimittaja valvoo tämän Turvallisuussopimuksen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Asiakkaalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Asiakas seuraa Palvelun turvallisuustason toteutumista yhteistyössä Toimittajan kanssa.
- 13.7 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, mikäli Toimittajaan tai sen alihankkijaan kohdistuu Asiakasta mahdollisesti uhkaavia yhteydenottoja. Toimittaja on velvollinen ilmoittamaan Asiakkaalle sopimuksen vastaisesta tietovuodosta, tietomurtoyrityksestä tai muusta turvallisuutta vaarantavasta tapahtumasta tai seikasta. Ilmoitukset tulee tehdä viipymättä ja kirjallisesti.
- 13.8 Asiakkaalla on oikeus luovuttaa viranomaisille tai muille valtion yksiköille tieto siitä, että tämän luvun mukainen tarkastus on suoritettu, mutta Asiakkaalla ei kuitenkaan ilman Toimittajan lupaa ole oikeutta luovuttaa näille tietoa tarkastuksen tuloksista ellei pakottavasta lainsäädännöstä muuta johdu.

[SOPIMUSSAKKO JA] VAHINGONKORVAUS

(Ohje: Muokkaa koko luku hankinnan kohteeseen ja siihen liittyviin riskeihin soveltuvaksi. Harkitse tarvetta sopimussakkoa koskeviin ehtoihin ja vertaa niitä Pääsopimuksen mahdollisiin sopimussakkoehdoin. Vaihtoehto A:ssa sopimussakkoa maksetaan kaikista turvallisuussopimuksen rikkomuksista, vaihtoehto B:ssä salassapitovelvollisuuden rikkomuksista. Vaihtoehto C:ssä edellä mainituille rikkomuksille voidaan määritellä erisuuruinen sopimussakko.)

[A Vaihtoehto

- 14.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Turvallisuussopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Sopimussakko ei koske kohdassa 5.7 sovitun velvollisuuden rikkomista, mikäli kyseessä ei ole Salassa pidettävä tieto.*
- 14.2 *Sopimussakon määrä jokaista rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta, kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa].*

B Vaihtoehto

- 14.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista salassapitovelvollisuuden rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa.*
- 14.2 *Sopimussakon määrä jokaista rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa].*

C Vaihtoehto

- 14.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Turvallisuussopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Sopimussakko ei koske kohdassa 5.7 sovitun velvollisuuden rikkomista, mikäli kyseessä ei ole Salassa pidettävä tieto.*
- 14.2 *Sopimussakon määrä jokaista salassapitovelvollisuuden rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa]. Muiden tämän Turvallisuussopimuksen rikkomusten osalta sopimussakon määrä on [10.000 euroa]. Mikäli Toimittaja muun kuin salassapitovelvollisuuden rikkomuksen ollessa kyseessä korjaa rikkomuksen [14] vuorokauden kuluessa siitä, kun se on havainnut rikkomuksen, Asiakkaalla ei ole oikeutta saada sopimussakkoa, mikäli rikkomus on luonteeltaan sellainen, että siitä ei ole voinut aiheutua Asiakkaalle vahinkoa.*
- 14.3 *Jos Toimittaja samalla teolla rikkoo useita tämän Turvallisuussopimuksen velvoitteita, se katsotaan kuitenkin vain yhdeksi sopimussakkoon oikeuttavaksi rikkomukseksi.*
- 14.4 *Ennen sopimussakon perimistä Asiakkaan tulee ilmoittaa Toimittajalle kirjallisesti tämän Turvallisuussopimuksen rikkomuksesta. Jos Toimittaja sitä kirjallisesti pyytää, käsitellään rikkomus lisäksi Asiakkaan ja Toimittajan välisessä tapaamisessa.*
- 14.5 *Kohdissa 14.1-14.4 tarkoitettu sopimussakko ei rajoita Asiakkaan oikeutta saada Toimittajalta vahingonkorvausta siltä osin kuin rikkomuksista Asiakkaalle aiheutunut vahinko ylittää sopimussakon määrän.]*
- 14.6 *Asiakkaalla on oikeus saada korvaus kaikista niistä välittömistä vahingoista sekä kuluista ja kustannuksista, jotka sille ovat aiheutuneet Toimittajan tähän Turvallisuussopimukseen*

kohdistuvasta sopimusrikkomuksista, ellei rikkomus ole aiheutunut Pääsopimuksen kohdassa [x] tarkoitetusta ylivoimaisesta esteestä.

- 14.7 Lisäksi Asiakkaalla on oikeus saada korvaus myös kaikista välillisistä vahingoista, mikäli vahinko on aiheutettu tahallisesti tai törkeällä tuottamuksella taikka salassapitovelvollisuutta rikkoen.

SOPIMUSMUUTOKSET

- 15.1 Turvallisuussopimuksen yhteyshenkilöt (liite 1) vastaavat tämän Turvallisuussopimuksen päivittämistarpeen seuraamisesta. Päivittämistarve arvioidaan yhteyshenkilöiden kesken vähintään kahden vuoden välein.
- 15.2 Tähän Turvallisuussopimukseen tai sen liitteisiin tehtävät muutokset tulee tehdä kirjallisesti ja molempien sopijapuolten vahvistaa allekirjoituksellaan. Tämän Turvallisuussopimuksen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

SOPIMUKSEN IRTISANOMINEN [JA PURKAMINEN]

- 16.1 Sopijapuoli voi irtisanoa tämän Turvallisuussopimuksen päättymään kuuden (6) kuukauden irtisanomisajalla kirjallisesta ilmoituksesta lukien, ottaen kuitenkin huomioon mitä kohdassa 17.1 on sanottu. Irtisanominen ei poista velvollisuutta täyttää ennen irtisanomista syntyneet velvoitteet.
- 16.2 Jos Toimittaja irtisanoo tämän Turvallisuussopimuksen, Asiakkaalla on oikeus irtisanoa se Pääsopimus, johon tämä Turvallisuussopimus perustuu.
- 16.3 Asiakas on oikeutettu irtisanomaan välittömästi päättymään [*tai purkamaan*] tämän Turvallisuussopimuksen ja sen Pääsopimuksen, johon tämä Turvallisuussopimus perustuu, mikäli Toimittaja rikkoo tähän Turvallisuussopimukseen perustuvia sopimusvelvoitteitaan niin olennaisesti, ettei Asiakkaan voida kohtuudella edellyttää jatkavan sopimussuhdetta edes irtisanomisajan pituista aikaa. Irtisanominen ja purkaminen tulee tehdä kirjallisesti. [Lisäksi jos Toimittaja on rikkonut tätä Turvallisuussopimusta vähintään kolme kertaa siten, että Asiakkaalle on syntynyt oikeus vaatia luvussa 14 tarkoitettua sopimussakkoa, Asiakkaalla on aina oikeus irtisanoa välittömästi päättymään [*tai purkaa*] tämä Turvallisuussopimus ja se Pääsopimus, johon tämä Turvallisuussopimus perustuu.]
- 16.4 Tämän Turvallisuussopimuksen päättymisestä huolimatta Toimittajan on maksettava päättymisen perusteena olevista rikkomuksista tämän Turvallisuussopimuksen mukaiset sanktiot.

SOPIMUKSEN VOIMASSAOLO

- 17.1 Tämä Turvallisuussopimus on voimassa niin kauan kuin Asiakkaan ja Toimittajan välinen Pääsopimus on voimassa.
- 17.2 Tämä Turvallisuussopimus tulee voimaan, kun kumpikin sopijapuoli on sen allekirjoittanut.

- 17.3 Tämän Turvallisuussopimuksen mukainen salassapitovelvollisuus on voimassa myös sen jälkeen kuin Asiakkaan ja Toimittajan välinen Pääsopimus on päättynyt.
- 17.4 Pääsopimuksen päätyttyä Toimittaja mahdollisine alihankkijoineen palauttaa kaikki Asiakkaan Salassa pidettäviä tietoja sisältävät dokumentit, tallenteet ja muun materiaalin. Erikseen kirjallisesti niin sovittaessa Toimittaja mahdollisine alihankkijoineen voi myös tuhota edellä mainitun materiaalin Asiakkaan ohjeistuksen mukaisella tavalla.

SOVELLETTAVA LAKI JA ERIMIELISYYKSIEN RATKAISEMINEN

- 18.1 Tähän Turvallisuussopimukseen sovelletaan Suomen lakia, lukuun ottamatta lainvalintasäännöksiä.
- 18.2 Tästä Turvallisuussopimuksesta aiheutuvat erimielisyydet pyritään ensisijaisesti ratkaista sopijapuolten välisin neuvotteluin. Mikäli sopijapuolet eivät pääse sovinnolliseen ratkaisuun, erimielisyydet ratkotaan ensi asteessa [Helsingin käräjäoikeudessa].

SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET

- 19.1 Tämä Turvallisuussopimus on laadittu kahtena (2) samasanaaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]

[paikka ja aika]

[ASIAKAS]

[TOIMITTAJA]

[allekirjoittaja]

[allekirjoittaja]

[allekirjoittaja]

RAKENTAMISEEN LIITTYVIEN SUUNNITTELU- JA KONSULTTIPALVELUJEN TURVALLISUUSSOPIMUS

(LUONNOS)

2.11.2012

[ASIAKAS]

JA

[TOIMITTAJA]

Teksti pohjautuu soveltuvin osin ICT-hankintojen tietoturvaa koskevassa VAHTI-ohjeessa 3/2011 liitteenä olevaan turvallisuussopimusmalliin.. Tekstiin tehdyt muokkaukset on merkitty vihreällä värillä.

(Ohje: Tämä sopimus malli, joka pitää aina muokata organisaatio- ja hankintakohtaisesti kulloinkin hankittavana olevan kohteen mukaan. Malli on tarkoitettu käytettäväksi rakentamiseen liittyvissä suunnittelu- ja konsultointipalveluhankinnoissa yksityiseltä palveluntuottajalta.

Sisällys

1 SOPIJAPUOLET	51
2 MÄÄRITELMÄT	51
3 SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS.....	52
4 TURVALLISUUSSOPIMUKSEN TAUSTA JA TARKOITUS	52
5 LUOTTAMUKSELLISUUS JA SALASSAPITO	53
6 PÄÄSY TILOIHIN	54
7 PÄÄSY JÄRJESTELMIIN JA TIETOIHIN	55
8 VAITIOLOSITOUUMUS.....	55
9 TURVALLISUUSSELVITYKSET	56
10 TIETOTURVALLISUUS	56
11 ALIHANKKIJAT	57
12 TARKASTUKSET JA RAPORTOINTI	57
13 [SOPIMUSSAKKO JA] VAHINGONKORVAUS.....	58
14 SOPIMUSMUUTOKSET.....	60
15 SOPIMUKSEN IRTISANOMINEN [JA PURKAMINEN].....	60
16 SOPIMUKSEN VOIMASSAOLO.....	60
17 SOVELLETTAVA LAKI JA ERIKESKISYYKSIEN RATKAISEMINEN.....	61
18 SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET	61

SOPIJAPUOLET

1.1 Sopijapuolet ovat:

1. [nimi] (jäljempänä "Asiakas")

Osoite

Y-tunnus

2. [nimi] (jäljempänä "Toimittaja")

Osoite

Y-tunnus

MÄÄRITELMÄT

- 2.1 **Palvelu** tarkoittaa sitä uudis- tai korjausrakentamiseen liittyvää suunnittelu- tai konsultointipalvelua, josta Asiakas ja Toimittaja ovat sopineet Pääsopimuksessa. Mitä tässä Turvallisuuksopimuksessa on sovittu Palvelusta, sovelletaan soveltuvin osin myös Pääsopimuksessa sovittuun tavarahankintaan.
- 2.2 **Pääsopimus** tarkoittaa Toimittajan ja Asiakkaan välistä sopimusta nro [0000], jolla sopijapuolet ovat sopineet [sopimuksen kohteesta].
- 2.3 **Salassa pidettävä tieto** tarkoittaa kaikkea sellaista Asiakkaan Toimittajalle luovuttamaa tai Toimittajalla olevaa Asiakkaan asiakirjamuotoista tai muuta tietoa, joka on määritelty salassa pidettäväksi laissa viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä "julkisuuslaki") tai muussa lainsäädännössä, ja jonka Asiakas on tällaiseksi tiedoksi merkinnyt tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin. Salassa pidettäväksi tiedoksi katsotaan myös julkisuuslaissa tarkoitetun, ei vielä julkisen asiakirjan sisältämä tieto. Lisäksi kaikki Asiakkaan luovuttamat henkilötiedot katsotaan Salassa pidettäväksi tiedoksi. Salassa pidettäväksi tiedoksi ei katsota sellaista tietoa, joka on julkisesti saatavilla tai jonka sopijapuoli on saanut tietoonsa laillisella tavalla kolmannelta osapuolelta ilman sitä koskevaa salassapitovelvoitetta.
- 2.4 **Turvallisuuksopimus** tarkoittaa tätä sopimusasiakirjaa liitteineen.
- 2.5 **Asiakkaan Tilat** tarkoittavat sellaisia Asiakkaan käytössä olevia tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja tai joissa liikkumista on muutoin turvallisuuksyistä syytä rajoittaa. Rakenteilla tai korjausrakentamisen kohteena olevat Asiakkaan käyttöön tulevat tilat katsotaan tällaiseksi tilaksi, kun niiden toteutus on edennyt sellaiseen vaiheeseen, että tiloissa liikkumalla voi saada tietoa, jonka tulee pysyä salassa.
- 2.6 **Toimittajan Tilat** tarkoittavat sellaisia Toimittajan tai sen alihankkijan tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja.
- 2.7 **Rakennustyömaalla** tarkoitetaan rakentamispalvelun toteuttamiseksi määriteltyä työ- tai maa-aluetta, jolla liikkuminen edellyttää asianmukaista työmaakohtaista kulkulupaa.
- 2.8 **Työmaarakennuksella** tarkoitetaan rakennustyömaalla sijaitsevia parakkeja tai vastaavia tiloja, joissa voidaan säilyttää, käyttää tai muutoin käsitellä Palveluun liittyviä Salassa pidettäviä tietoja.

SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS

3.1 Tämä Turvallisuussopimus muodostuu tästä sopimusasiakirjasta ja seuraavista liitteistä:

Liite 1	Turvallisuussopimuksen yhteyshenkilöt
Liite 2	Ohje Salassa pidettävien tietojen käsittelystä ja säilyttämisestä
Liite 3	Henkilöstön vaitiolositoumusmalli

(Ohje: Vaitiolovelvollisuus tulee suoraan laista, Julkl 23 §. Sitoumuksella henkilöstöön kuuluva ilmoittaa saaneensa tiedon tietojen salassapidosta ja siitä, että niiden ilmaiseminen tai luovuttaminen ilman lupaa on kiellettyä. Samaan asiakirjaan voi laittaa myös käsittelyvelvoitteita koskevan lauseen.)

Liite 4	Toimittajan turvallisuudenhallinnan kuvaus [/Selvitys Palveluun liittyvistä tietoturvameneettelyistä]
---------	---

[Liite 5 Palveluun sovellettava valtionhallinnon tietoturvaluustaso, tietoturvaluusvaatimukset, Asiakkaan tilojen turvallisuusluokitukset, Palveluun liittyvien tietojen luokitus suojaustasoille]

3.2 Asiakas ja Toimittaja vastaavat omalta osaltaan liitteen 1 ylläpidosta.

3.3 Liitteessä 2 on esitetty Asiakkaan hyväksymät menettelyt, ja ohjeet eri suojaustasoluokkiin kuuluvan tiedon, asiakirjojen ja muun tietoaineiston käsittelystä. Asiakas vastaa liitteen ylläpidosta. *[Ohje: Ohjeiden tulisi olla sisällöltään yhdenmukaiset tietoturvaluusasetuksen ja sen täytäntöönpanosta annetun VAHTI-ohjeen 2/2010 luokittelu- ja käsittelyohjeiden kanssa.]*

3.4 Toimittaja vastaa liitteen 4 ylläpidosta. Liitteen tulee vastata voimassa olevaa tilannetta.

[3.5 Asiakas vastaa liitteen 5 ylläpidosta]

TURVALLISUUSSOPIMUKSEN TAUSTA JA TARKOITUS

4.1 Toimittaja ja Asiakas ovat tehneet Pääsopimuksen nro [xxx] [sopimuksen kohde] [pvm].

4.2 Tässä Turvallisuussopimuksessa sovitaan Asiakkaan ja Toimittajan välillä noudatettavista turvallisuusjärjestelyistä ja Salassa pidettävää tietoa koskevista järjestelyistä edellä mainitun Pääsopimuksen sisältämien Palveluiden tuottamisessa sekä kaikessa Pääsopimukseen liittyvässä Asiakkaan ja Toimittajan välisessä yhteistyössä.

4.3 Sopijapuolet tiedostavat, että Pääsopimuksen perusteella toimitettaviin Palveluihin sisältyy sellaista tietoa, jonka salassa pysyminen on *[esimerkki, tarkennetaan hankintakohtaisesti: yhteiskunnan häiriöttömän toimintakyvyn ja valtion sekä yksilöiden turvallisuuden kannalta kriittistä]*. Palvelun tuottamisen yhteydessä Toimittajan ja sen alihankkijan henkilöstöllä on pääsy Asiakkaan Tiloihin, joissa liikkumista on turvallisuussyistä syytä rajoittaa. Tällä Turvallisuussopimuksella sopijapuolet pyrkivät varmistamaan, että Salassa pidettävät tiedot pysyvät salassa.

4.4 Huolimatta siitä, mitä muissa Asiakkaan ja Toimittajan välisissä sopimuksissa on mahdollisesti sovittu tämän Turvallisuussopimuksen piiriin kuuluvista asioista tai niihin liittyvistä vastuista taikka

sopimusten keskinäisestä pätemisjärjestyksestä, tätä Turvallisuussopimusta sovelletaan aina ensisijaisesti tämän Turvallisuussopimuksen piiriin kuuluvissa asioissa. Tähän Turvallisuussopimukseen tai sen perusteella syntyviin vastuisiin ei sovelleta muissa sopijapuolten välisissä sopimuksissa mahdollisesti sovittuja vastuunrajoituksia.

(Ohje: Jos otat tämän Turvallisuussopimuksen Pääsopimuksen liitteeksi, huomaa soveltamisjärjestyksen vaikutus tämän ehdon sanamuotoon.)

LUOTTAMUKSELLISUUS JA SALASSAPITO

- 5.1 Tässä Turvallisuussopimuksessa kuvattuja turvallisuusjärjestelyjä noudatetaan aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa.
- 5.2 Asiakas noudattaa julkisyhteisönä julkisuuslaissa, valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010; jäljempänä tietoturvallisuusasetus) sekä muussa lainsäädännössä olevia salassapitoa ja julkisuutta koskevia säännöksiä. Sopimuksella ei voida poiketa lainsäädännön Asiakkaalle asettamista pakottavista velvoitteista.

(Ohje: Poista/muokkaa, jos Asiakas ei kuulu julkisuuslain tai tietoturvallisuusasetuksen soveltamisalaan.)

- 5.3 Toimittaja sitoutuu pitämään salassa kaikki Asiakkaan sille luovuttamat tai sillä olevat tai toimeksiannon toteuttamisessa syntyneet Salassa pidettävät tiedot, ottaen lisäksi huomioon kohdassa 5.7 sovitun. Salassa pidettäviä tietoja ei myöskään saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi.
- 5.4 Toimittajan tulee käsitellä Salassa pidettäviä tietoja vain Palvelun tuottamisen edellyttämässä laajuudessa. Toimittaja antaa Salassa pidettäviä tietoja vain niille henkilöille, jotka tarvitsevat Salassa pidettäviä tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Toimittaja sitoutuu saattamaan Turvallisuussopimuksen vaikutusalaan kuuluvat henkilöt tietoiseksi tähän Turvallisuussopimukseen liittyvistä velvoitteista ja antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Salassa pidettävien tietojen asianmukaisesta käsittelystä henkilöille, joilla on pääsy näihin tietoihin. Toimittaja sitoutuu valvomaan, että edellä tarkoitetut henkilöt noudattavat Turvallisuussopimusta.
- 5.5 Toimittaja sitoutuu säilyttämään ja käsittelemään Salassa pidettäviä tietoja siten, että ne pysyvät vain niiden henkilöiden hallussa, joilla on oikeus Salassa pidettäviin tietoihin, eivätkä ne joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon. Asiakkaan antama tarkempi ohjeistus Salassa pidettävien tietojen käsittelystä ja säilyttämisestä, jota Toimittaja sitoutuu noudattamaan, on liitteessä 2.
- 5.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille saattaa olla rikoslain mukaan rangaistava teko.
- 5.7 Tiedon antamisesta asiakirjasta, joka on saatu Asiakkaalta tai laadittu Asiakkaan toimeksiantotehtävää suoritettaessa, päättää Asiakas, jollei toimeksiannosta muuta johdu.
- 5.8 Toimittaja vastaa siitä, ettei Asiakkaan kohteiden tai toiminnan turvallisuus vaarannu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Turvallisuussopimuksen tai Pääsopimuksen vastaisen toiminnan johdosta.

- 5.9 Toimittaja ja sen alihankkijat saavat mainita referenssinä tehneensä työtä Asiakkaalle vain, jos asiasta on erikseen kirjallisesti sovittu.
- 5.10 Mikäli Salassa pidettäviä asiakirjoja tai tietoja käsitellään Asiakkaan toimitilojen ulko-puolella, on Toimittajan noudatettava Asiakkaan antamia toimintaohjeita ja erityisesti huolehdittava siitä, ettei tietoaineistojen turvallisuus vaarannu.
- 5.11 Tässä Turvallisuussopimuksessa kuvattujen menettelyjen lisäksi Asiakkaalla on oikeus tarvittaessa antaa turvallisuuteen liittyviä käytännön toimintaohjeita, joita Toimittajan tulee noudattaa.

PÄÄSY TILOIHIN

- 6.1 Toimittaja vastaa siitä, että pääsy Asiakkaan korotetun tai korkean turvallisuustason Tiloihin (vyöhykkeet ORANSSI (ST III), KELTAINEN (TL III) tai SININEN (ST II)) annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 9 tarkoitettu turvallisuusselvitys ja jotka ovat tietoisia tämän Turvallisuussopimuksen velvoitteista ja Tiloissa liikkumisesta annetuista ohjeista. Henkilöt, joille ei ole annettu edellä tarkoitettulla tavalla oikeutta päästä mainittuihin Asiakkaan Tiloihin, saavat oleskella Tiloissa ainoastaan Asiakkaan luvalla ja valvonnan alaisina.
- 6.2 Toimittaja vastaa siitä, että pääsy Asiakkaan turvallisuuden perustason Tiloihin (vyöhyke 4) tai rakennustyömaalle annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen ja jotka ovat tietoisia tämän Turvallisuussopimuksen velvoitteista ja Tiloissa tai rakennustyömaalla liikkumisesta annetuista ohjeista. Henkilöt, joille ei ole annettu edellä tarkoitettulla tavalla oikeutta päästä mainittuihin Asiakkaan Tiloihin tai rakennustyömaalle, saavat oleskella niissä ainoastaan Asiakkaan luvalla ja valvonnan alaisina. Henkilöiden pääsy mainittuihin Tiloihin tai rakennustyömaalle ei lähtökohtaisesti edellytä henkilöiden turvallisuusselvittämistä. Asiakkaalla on kuitenkin oikeus edellyttää luvussa 9 tarkoitettua turvallisuusselvityksen tekemistä myös mainittuihin Tiloihin tai rakennustyömaalle pääsevien henkilöiden osalta, mikäli selvitysten tekemiselle laissa asetetut edellytykset täyttyvät.
- 6.3 Henkilöiden, joilla on pääsy Asiakkaan Tiloihin tai rakennustyömaalle, tulee olla tunnistettavissa. Henkilöillä on oltava Asiakkaan Tiloissa tai rakennustyömaalla liikkueensa näkyvillä Asiakkaan kanssa sovittu kuvallinen henkilötunniste.
- 6.4 Toimittajan ja sen alihankkijan Tilojen tulee olla Tiloissa käsiteltävien Salassa pidettävien tietojen luokitustaso n asettamat vaatimukset huomioon ottaen asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi Tiloihin ja siellä oleviin Salassa pidettäviin tietoihin. Tiloille asetettavia vaatimuksia ja niiden täyttymistä arvioidaan voimassa olevan [Kansallisen turvallisuusauditointikriteeristön (KATAKRI)] mukaisesti.
- 6.5 Mikäli Palvelu suoritetaan tai Salassa pidettäviä tietoja käsitellään Toimittajan tai sen alihankkijan Tiloissa, Toimittajan tulee varmistaa Tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms. erityistilanteiden varalta. Asiakas ja Toimittaja sopivat tarvittaessa Palveluun liittyvistä tarkemmista vaatimuksista.
- 6.6 Henkilöt, joille ei ole myönnetty oikeutta Salassa pidettäviin tietoihin tai niitä sisältäviin järjestelmiin luvun 7 mukaisesti, saavat oleskella Toimittajan tai sen alihankkijan Tiloissa ainoastaan valvonnan

alaisina. Valvontaa ei edellytetä, mikäli Salassa pidettäviä tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

- 6.7 Henkilöiden, joilla on pääsy Toimittajan tai alihankkijan Tiloihin, tulee olla tunnistettavissa.
- 6.8 [Asiakkaalla on oikeus vaatia luvussa 9 tarkoitetun turvallisuusselvityksen hakemista henkilöistä, joilla on oikeus päästä [tiettyihin yksilöityihin] Toimittajan tai sen alihankkijan Tiloihin, joissa käsitellään suojaustasolle II tai III luokiteltuja Salassa pidettäviä tietoja. Toimittajan tulee myös hyväksyttää henkilö Asiakkaalla ennen kuin henkilölle voidaan myöntää pääsy [tiettyihin yksilöityihin] Tiloihin.]
- 6.9 [Toimittaja pitää ja/tai velvoittaa tarvittaessa alihankkijansa osaltaan pitämään luetteloa henkilöistä, joille Palveluun liittyen on annettu oikeus päästä kohdassa [valitaan sopiva vaihtoehto: 6.1, 6.2, 6.8] tarkoitettuihin Tiloihin tai rakennustyömaalle, huolehtii luettelon ajantasaisuudesta ja toimittaa sen [sovituin määrävälein tai pyynnöstä] Asiakkaalle.]

PÄÄSY JÄRJESTELMIIN JA TIETOIHIN

- 7.1 Toimittaja vastaa siitä, että suojaustasolle II tai III luokiteltuja Salassa pidettäviä tietoja annetaan tai pääsy sellaisia tietoja sisältäviin järjestelmiin sallitaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 9 tarkoitettu turvallisuusselvitys ja joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin. Asiakkaalla on kuitenkin tarvittaessa oikeus edellyttää edellä tarkoitetun menettelyn noudattamista myös suojaustasolle IV luokiteltuihin Salassa pidettäviin tietoihin tai sellaisia tietoja sisältäviin järjestelmiin pääsevien henkilöiden osalta, mikäli turvallisuusselvityksille laissa asetetut edellytykset täyttyvät. Oikeuden päästä Asiakkaan järjestelmiin, jotka sisältävät Salassa pidettäviä tietoja, antaa Asiakas.
- 7.2 Toimittaja vastaa siitä, että Salassa pidettävien tietojen käsittelyyn osallistuvat Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt sekä henkilöt, joilla on pääsy Toimittajan tai Asiakkaan järjestelmiin, joissa säilytetään Salassa pidettäviä tietoja, ovat tietoisia salassapitoa koskevista velvoitteistaan ja noudattavat tätä Turvallisuussopimusta.
- [7.3 [Toimittaja pitää ja/tai velvoittaa tarvittaessa alihankkijansa osaltaan pitämään luetteloa henkilöistä, jotka Palveluun liittyen käsittelevät suojaustasolle [valitaan sopivat vaihtoehdot: II, III, IV] luokiteltuja Salassa pidettäviä tietoja tai joilla on pääsy sellaisia tietoja sisältäviin järjestelmiin, huolehtii luettelon ajantasaisuudesta ja toimittaa sen [sovituin määrävälein tai pyynnöstä] Asiakkaalle.]

VAITIOLOSITOUS

- 8.1 Toimittaja vastaa siitä, että henkilö, joka käsittelee Salassa pidettäviä tietoja ja/tai jolla on pääsy järjestelmiin, joissa Salassa pidettäviä tietoja säilytetään, tekee vaitiolositoumuksen Asiakkaan hyväksymälle lomakkeelle (liite 3) ennen kuin hän saa aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin.
- 8.2 Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijan henkilökuntaan kuuluva henkilö, jolla on pääsy Asiakkaan kohdassa 6.1 tarkoitettuihin tiloihin, tekee vaitiolositoumuksen Asiakkaan hyväksymälle lomakkeelle (liite 3) ennen kuin hän saa oikeuden päästä mainittuihin tiloihin. Asiakkaalla on tarvittaessa oikeus edellyttää vaitiolositoumusta myös henkilöiltä, joilla on pääsy [kohdassa 6.2 tarkoitettuihin perusturvallisuustason tiloihin ja/tai rakennustyömaalle].

TURVALLISUUSSELVITYKSET

- 9.1 Jollei toisin sovita, jotta henkilö saa kohdassa 7.1 tarkoitetulla tavalla oikeuden käsitellä sellaisia Salassa pidettäviä tietoja, joiden salassapito on välttämätöntä turvallisuusselvityksistä annetun lain (177/2002) 2 §:ssä mainittujen etujen suojaamiseksi, ja/tai päästä järjestelmiin, jotka sisältävät sellaisia Salassa pidettäviä tietoja, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettu perusmuotoinen turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys. Jotta henkilö saa oikeuden päästä Asiakkaan kohdassa 6.1 [ja 6.2] tarkoitettuihin Tiloihin, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettujen edellytysten täyttyessä suppea turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys. [Kohdassa 6.8 tarkoitettuihin tiloihin pääsevistä henkilöistä tehdään suppea turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys.]
- 9.2 Jollei toisin sovita, tasoltaan vastaavaksi ulkomaiseksi turvallisuusselvitykseksi voidaan katsoa ainoastaan ulkomaisen kansallisen turvallisuusviranomaisen (esim. General Security Agreement:n eli GSA:n mukainen National Security Authority, NSA) tekemä turvallisuusselvitys (Personal Security Clearance, PSC). Jollei toisin sovita, PSC-selvitys edellytetään tehtäväksi henkilöstä, joka on ulkomaan kansalainen ja jolla on ollut pysyvä asuinpaikka Suomessa vähemmän kuin [5] vuotta.
- 9.3 Mikäli Toimittaja käyttää Palvelun toteutuksessa sellaista alihankkijaa, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee alihankkijasta tarvittaessa hakea yhteisöturvallisuusselvitys (Facility Security Clearance, FSC) ja tietojen käsittelyyn osallistuvista henkilöistä henkilöturvallisuusselvitys (Personal Security Clearance, PSC), jollei toisin sovita.
- 9.4 Asiakkaan tehtävänä on hakea kaikkia tässä luvussa tarkoitettuja turvallisuusselvityksiä.
- 9.5 Asiakas vastaa kohdissa 9.1-9.3 tarkoitettujen turvallisuusselvitysten kustannuksista. Mikäli turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan tai Toimittajan alihankkijan henkilöstössä tapahtuu vaihdos tai Asiakkaasta riippumaton lisäys, Toimittaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.
- 9.6 Toimittajan tulee toimittaa turvallisuusselvityksen kohteena olevan henkilön täyttämä ja allekirjoittama turvallisuusselvityshakemuslomake Asiakkaalle turvallisuusselvityksen teettämistä varten. Lomakkeen tulee sisältää selvityksen kohteena olevan henkilön suostumus turvallisuusselvityksen tekemiseen. Jos turvallisuusselvitys tulee tehtäväksi sellaisessa valtiossa, jonka lainsäädännön mukaan kyseessä olevan selvityksen tekeminen ei edellytä selvityksen kohteena olevan henkilön suostumusta, Toimittajan ei myöskään [tämän kohdan nojalla] tarvitse pyytää henkilöltä edellä mainittua suostumusta.
- 9.7 Asiakkaalla on perustellusta turvallisuuteen liittyvästä syystä oikeus kieltää Toimittajan tai sen alihankkijan henkilön osallistuminen Palvelun suorittamiseen.

TIETOTURVALLISUUS

- 10.1 Toimittaja noudattaa julkisuuslaissa tarkoitettua hyvää tiedonhallintatapaa sekä henkilö-tietolain (523/1999) edellyttämää hyvää tietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä sekä muuta tietosuojaa koskevaa lainsäädäntöä Pääsopimukseen liittyvän Palvelun tuottamisessa.

10.2 [Vaihtoehto 1]

Asiakas luokittelee Salassa pidettäviä tietojaan tietoturvallisuusasetuksen mukaisiin suojaustasoihin. [Tietojen luokitus eri suojaustasolle ilmenee sopimuksen liitteestä 5.] Toimittaja sitoutuu noudattamaan Salassa pidettäviä tietoja käsitellessään edellä mainitun asetuksen ja Asiakkaan ohjeistuksen kyseiselle suojaustasolle asettamia vaatimuksia.

10.2 [Vaihtoehto 2]

Asiakas ei luokittele Salassa pidettäviä tietoja, tietoturvallisuusasetuksen mukaisiin suojaustasoihin. Toimittaja sitoutuu noudattamaan perustason tietoturvallisuutta ja Asiakkaan ohjeistusta Salassa pidettäviä tietoja käsitellessään.

- 10.3 Asiakas on määrittänyt Palvelun hankinnan yhteydessä Palveluun sovellettavan valtionhallinnon tietoturvatason ja Palveluun liittyvät konkreettiset tietoturva-vaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esitetty [Pääsopimuksen liitteessä x/tämän Turvallisuussopimuksen liitteessä 5.]

ALIHANKKIJAT

- 11.1 Toimittajan tulee hyväksyttää Asiakkaalla sellainen alihankkija, jota se aikoo käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai siellä oleviin työmaarakennuksiin. Tässä Turvallisuussopimuksessa alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai työmaarakennuksiin.
- 11.2 Mitä tässä Turvallisuussopimuksessa on sovittu Toimittajan henkilöstöstä, sovelletaan myös alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön.
- 11.3 Toimittajan tulee huolehtia siitä, että se pystyy noudattamaan tätä Turvallisuussopimusta myös käyttäessään alihankkijoita. Toimittaja on tietoinen ja sen on tiedotettava alihankkijalleen, että turvallisuusjärjestelyiden saattamisesta tämän Turvallisuussopimuksen edellyttämälle tasolle saattaa syntyä kustannuksia. Asiakas ei vastaa näistä kustannuksista.
- 11.4 Toimittaja vastaa alihankkijoiden toiminnasta kuin omastaan ja siitä, että alihankkijat toimivat tämän Turvallisuussopimuksen ehtojen mukaisesti.
- 11.5 Ellei toisin sovita, Toimittajan tulee tehdä tämän Turvallisuussopimuksen ehtoja vastaava sopimus kohdassa 11.1 tarkoitetun alihankkijansa kanssa ja Toimittajan on asetettava alihankkijalleen vastaava velvollisuus tämän käyttämän alihankkijan osalta. [Sopimus on hyväksyttävä Asiakkaalla ennen sen allekirjoittamista.]

TARKASTUKSET JA RAPORTOINTI

- 12.1 Asiakkaalla tai Asiakkaan määräämällä kolmannella taholla (joka ei ole Toimittajan suoranainen kilpailija) on oikeus tarkastaa omalla kustannuksellaan etukäteen ilmoitettuna ajankohtana Toimittajan ja sen alihankkijoiden turvallisuusjärjestelyt tätä Turvallisuussopimusta sekä Pääsopimusta koskevilta osin. Asiakkaan on ilmoitettava tahdostaan suorittaa tarkastus viimeistään kolmekymmentä (30) päivää ennen ehdotettua tarkastuspäivää. Toimittaja voi ehdottaa uutta päivää tarkastukselle. Uusi ajankohta ei kuitenkaan saa olla myöhemmin kuin kymmenen (10) päivää Asiakkaan ehdottaman päivän jälkeen. Tarkastus saadaan suorittaa kuitenkin enintään kaksi kertaa vuodessa, ellei ole erityisen painavia syitä useammille tarkastuksille tai toisin sovita. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainituista määräajoista riippumatta

erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tai sen alihankkijoiden tietoturvaluottuutta tai Toimittajan tai sen alihankkijoiden salassapitovelvoitteita muita asiakkaita kohtaan. Asiakkaalla on edellä tarkoitettun tarkastusoikeuden lisäksi oikeus suorittaa Tiloissaan ja rakennustyömaalla jatkuvaa valvontaa ja tehdä näissä ennalta ilmoittamatta turvallisuustarkastuksia tässä Turvallisuuksopimuksessa asetettujen velvoitteiden täyttymisen arvioimiseksi.

- 12.2 Toimittajan tulee huolehtia sopimusjärjestelyin siitä, että Asiakkaalla on mahdollisuus tarkastaa myös Toimittajan sellaisen alihankkijan turvallisuusjärjestelyt, joka osallistuu Salassa pidettävien tietojen käsittelyyn tai jolla on pääsy Asiakkaan Tiloihin, rakennus-työmaalle tai siellä oleviin työmaarakennuksiin.
- 12.3 Mikäli tarkastuksessa havaitaan merkittäviä puutteita turvallisuusjärjestelyissä, Toimittaja korvaa Asiakkaalle tarkastuksesta aiheutuneet kustannukset.
- 12.4 Toimittajan tulee korjata tarkastuksessa tai muussa valvonnassa havaitut puutteet viivytyksettä Asiakkaan kirjallisesta ilmoituksesta. Erityisiä korjaavia toimenpiteitä vaativat puutteet on korjattava viimeistään [30 vuorokauden kuluessa] Asiakkaan kirjallisesta ilmoituksesta, ellei siitä ole Asiakkaan ja Toimittajan välillä erikseen toisin sovittu. Olennaiset puutteet, jotka muodostavat ilmeisen uhkan tietoturvaluottuudelle, on kuitenkin korjattava heti. Asiakas ei vastaa edellä mainituista korjauksista aiheutuvista kuluista ja kustannuksista.
- 12.5 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, jos Toimittajan tai sen alihankkijan tämän Turvallisuuksopimuksen kannalta keskeisissä toiminnoissa tai henkilöstö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai jos Toimittajan tai sen alihankkijan omistussuhteissa tapahtuu merkittäviä muutoksia.
- 12.6 Toimittaja valvoo tämän Turvallisuuksopimuksen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poikkeamat ja raportoi ne Asiakkaalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Asiakas seuraa Palvelun turvallisuustason toteutumista yhteistyössä Toimittajan kanssa.
- 12.7 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, mikäli Toimittajaan tai sen alihankkijaan kohdistuu Asiakasta mahdollisesti uhkaavia yhteydenottoja. Toimittaja on velvollinen ilmoittamaan Asiakkaalle sopimuksen vastaisesta tietovuodosta, tietomurtoyrityksestä tai muusta turvallisuutta vaarantavasta tapahtumasta tai seikasta. Ilmoitukset tulee tehdä viipymättä ja kirjallisesti.
- 12.8 Asiakkaalla on oikeus luovuttaa viranomaisille tai muille valtion yksiköille tieto siitä, että tämän luvun mukainen tarkastus on suoritettu, mutta Asiakkaalla ei kuitenkaan ilman Toimittajan lupaa ole oikeutta luovuttaa näille tietoa tarkastuksen tuloksista ellei pakottavasta lainsäädännöstä muuta johdu.

[SOPIMUSSAKKO JA] VAHINGONKORVAUS

(Ohje: Muokkaa koko luku hankinnan kohteeseen ja siihen liittyviin riskeihin soveltuvaksi. Harkitse tarvetta sopimussakkoa koskeviin ehtoihin ja vertaa niitä Pääsopimuksen mahdollisiin sopimussakkoehdoin. Vaihtoehto A:ssa sopimussakkoa maksetaan kaikista Turvallisuuksopimuksen rikkomuksista, vaihtoehto B:ssä salassapitovelvollisuuden rikkomuksista. Vaihtoehto C:ssä edellä mainituille rikkomuksille voidaan määritellä erisuuruinen sopimussakko.)

[A Vaihtoehto

- 13.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Turvallisuussopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Sopimussakko ei koske kohdassa 5.7 sovitun velvollisuuden rikkomista, mikäli kyseessä ei ole Salassa pidettävä tieto.*
- 13.2 *Sopimussakon määrä jokaista rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa].*

B Vaihtoehto

- 13.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista salassapitovelvollisuuden rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa.*
- 13.2 *Sopimussakon määrä jokaista rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa].*

C Vaihtoehto

- 13.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Turvallisuus-sopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Sopimussakko ei koske kohdassa 5.7 sovitun velvollisuuden rikkomista, mikäli kyseessä ei ole Salassa pidettävä tieto.*
- 13.2 *Sopimussakon määrä jokaista salassapitovelvollisuuden rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa]. Muiden tämän Turvallisuussopimuksen rikkomusten osalta sopimussakon määrä on [10.000 euroa]. Mikäli Toimittaja muun kuin salassapitovelvollisuuden rikkomuksen ollessa kyseessä korjaa rikkomuksen [14] vuorokauden kuluessa siitä, kun se on havainnut rikkomuksen, Asiakkaalla ei ole oikeutta saada sopimussakkoa, mikäli rikkomus on luonteeltaan sellainen, että siitä ei ole voinut aiheutua Asiakkaalle vahinkoa.]*
- 13.3 *Jos Toimittaja samalla teolla rikkoo useita tämän Turvallisuussopimuksen velvoitteita, se katsotaan kuitenkin vain yhdeksi sopimussakkoon oikeuttavaksi rikkomukseksi.*
- 13.4 *Ennen sopimussakon perimistä Asiakkaan tulee ilmoittaa Toimittajalle kirjallisesti tämän Turvallisuussopimuksen rikkomuksesta. Jos Toimittaja sitä kirjallisesti pyytää, käsitellään rikkomus lisäksi Asiakkaan ja Toimittajan välisessä tapaamisessa.*
- 13.5 *Kohdissa 13.1-13.4 tarkoitettu sopimussakko ei rajoita Asiakkaan oikeutta saada Toimittajalta vahingonkorvausta siltä osin kuin rikkomuksista Asiakkaalle aiheutunut vahinko ylittää sopimussakon määrän.]*
- 13.6 *Asiakkaalla on oikeus saada korvaus kaikista niistä välittömistä vahingoista sekä kuluista ja kustannuksista, jotka sille ovat aiheutuneet Toimittajan tähän Turvallisuussopimukseen kohdistuvasta sopimusrikkomuksista, ellei rikkomus ole aiheutunut Pääsopimuksen kohdassa [x] tarkoitetusta ylivoimaisesta esteestä.*
- 13.7 *Lisäksi Asiakkaalla on oikeus saada korvaus myös kaikista välillisistä vahingoista, mikäli vahinko on aiheutettu tahallisesti tai törkeällä tuottamuksella taikka salassapitovelvollisuutta rikkoen.*

SOPIMUSMUUTOKSET

- 14.1 Turvallisuussopimuksen yhteyshenkilöt (liite 1) vastaavat tämän Turvallisuussopimuksen päivittämistarpeen seuraamisesta. Päivittämistarve arvioidaan yhteyshenkilöiden kesken vähintään kahden vuoden välein.
- 14.2 Tähän Turvallisuussopimukseen tai sen liitteisiin tehtävät muutokset tulee tehdä kirjallisesti ja molempien sopijapuolten vahvistaa allekirjoituksellaan. Tämän Turvallisuussopimuksen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

SOPIMUKSEN IRTISANOMINEN [JA PURKAMINEN]

- 15.1 Sopijapuoli voi irtisanoa tämän Turvallisuussopimuksen päättymään kuuden (6) kuukauden irtisanomisajalla kirjallisesta ilmoituksesta lukien, ottaen kuitenkin huomioon mitä kohdassa 16.1 on sanottu. Irtisanominen ei poista velvollisuutta täyttää ennen irtisanomista syntyneet velvoitteet.
- 15.2 Jos Toimittaja irtisanoa tämän Turvallisuussopimuksen, Asiakkaalla on oikeus irtisanoa se Pääsopimus, johon tämä Turvallisuussopimus perustuu.
- 15.3 Asiakas on oikeutettu irtisanomaan välittömästi päättymään [*tai purkamaan*] tämän Turvallisuussopimuksen ja sen Pääsopimuksen, johon tämä Turvallisuussopimus perustuu, mikäli Toimittaja rikkoo tähän Turvallisuussopimukseen perustuvia sopimusvelvoitteitaan niin olennaisesti, ettei Asiakkaan voida kohtuudella edellyttää jatkavan sopimussuhdetta edes irtisanomisajan pituista aikaa. Irtisanominen ja purkaminen tulee tehdä kirjallisesti. [Lisäksi jos Toimittaja on rikkonut tätä Turvallisuussopimusta vähintään kolme kertaa siten, että Asiakkaalle on syntynyt oikeus vaatia luvussa 13 tarkoitettua sopimussakkoa, Asiakkaalla on aina oikeus irtisanoa välittömästi päättymään [*tai purkaa*] tämä Turvallisuussopimus ja se Pääsopimus, johon tämä Turvallisuussopimus perustuu.]
- 15.4 Tämän Turvallisuussopimuksen päättymisestä huolimatta Toimittajan on maksettava päättymisen perusteena olevista rikkomuksista tämän Turvallisuussopimuksen mukaiset sanktiot.

SOPIMUKSEN VOIMASSAOLO

- 16.1 Tämä Turvallisuussopimus on voimassa niin kauan kuin Asiakkaan ja Toimittajan välinen Pääsopimus on voimassa.
- 16.2 Tämä Turvallisuussopimus tulee voimaan, kun kumpikin sopijapuoli on sen allekirjoittanut.
- 16.3 Tämän Turvallisuussopimuksen mukainen salassapitovelvollisuus on voimassa myös sen jälkeen kuin Asiakkaan ja Toimittajan välinen Pääsopimus on päättynyt.
- 16.4 Pääsopimuksen päättyttyä Toimittaja mahdollisine alihankkijoineen palauttaa kaikki Asiakkaan Salassa pidettäviä tietoja sisältävät dokumentit, tallenteet ja muun materiaalin. Erikseen kirjallisesti niin sovittaessa Toimittaja mahdollisine alihankkijoineen voi myös tuhota edellä mainitun materiaalin Asiakkaan ohjeistuksen mukaisella tavalla.

SOVELLETTAVA LAKI JA ERIMIELISYYKSIEN RATKAISEMINEN

- 17.1 Tähän Turvallisuuksopimukseen sovelletaan Suomen lakia, lukuun ottamatta lainvalintasäännöksiä.
- 17.2 Tästä Turvallisuuksopimuksesta aiheutuvat erimielisyydet pyritään ensisijaisesti ratkaisemaan sopijapuolten välisin neuvotteluin. Mikäli sopijapuolet eivät pääse sovinnolliseen ratkaisuun, erimielisyydet ratkotaan ensi asteessa [Helsingin käräjäoikeudessa].

SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET

- 18.1 Tämä Turvallisuuksopimus on laadittu kahtena (2) samasanaaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]

[paikka ja aika]

[ASIAKAS]

[TOIMITTAJA]

[allekirjoittaja]

[allekirjoittaja]

[allekirjoittaja]

**KIINTEISTÖPALVELUJEN
TURVALLISUUSSOPIMUS**

(LUONNOS)

2.11.2012

[ASIAKAS]

JA

[TOIMITTAJA]

Teksti pohjautuu ICT-hankintojen tietoturvaa koskevassa VAHTI-ohjeessa 3/2011 liitteenä olevaan turvallisuussopimusmalliin.

(Ohje: Tämä sopimus malli, joka pitää aina muokata organisaatio- ja hankintakohtaisesti kulloinkin hankittavana olevan kohteen mukaan. Malli on tarkoitettu käytettäväksi kiinteistöihin liittyvissä palveluhankinnoissa yksityiseltä palveluntuottajalta (esim. kiinteistöhoito- ja käyttäjäpalveluhankinnat).

Sisällys

1 SOPIJAPUOLET	64
2 MÄÄRITELMÄT	64
3 SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS	65
4 TURVALLISUUSOPIMUKSEN TAUSTA JA TARKOITUS	65
5 LUOTTAMUKSELLISUUS JA SALASSAPITO	66
6 PÄÄSY TILOIHIN	67
7 PÄÄSY JÄRJESTELMIIN JA TIETOIHIN	68
8 VAITIOLOSITOUS	69
9 TURVALLISUUSSELVITYKSET	69
10 TIETOTURVALLISUUS	70
11 ALIHANKKIJAT	70
12 TARKASTUKSET JA RAPORTOINTI	71
13 SOPIMUSSAKKO JA VAHINGONKORVAUS	72
14 SOPIMUSMUUTOKSET	73
15 SOPIMUKSEN IRTISANOMINEN [JA PURKAMINEN]	73
16 SOPIMUKSEN VOIMASSAOLO	74
17 SOVELLETTAVA LAKI JA ERIMIELISYYKSIEN RATKAISEMINEN	74
18 SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET	74

SOPIJAPUOLET

- 1.1 Sopijapuolet ovat:
- 1. [nimi] (jäljempänä "Asiakas")
Osoite
Y-tunnus
 - 2. [nimi] (jäljempänä "Toimittaja")
Osoite
Y-tunnus

MÄÄRITELMÄT

- 2.1 **Palvelu** tarkoittaa sitä palvelua, josta Asiakas ja Toimittaja ovat sopineet Pääsopimuksessa. Mitä tässä Turvallisuussopimuksessa on sovittu Palvelusta, sovelletaan soveltuvien osin myös Pääsopimuksessa sovittuun tavarahankintaan.
- 2.2 **Pääsopimus** tarkoittaa Toimittajan ja Asiakkaan välistä sopimusta nro [0000], jolla sopijapuolet ovat sopineet [sopimuksen kohteesta].
- 2.3 **Salassa pidettävä tieto** tarkoittaa kaikkea sellaista Asiakkaan Toimittajalle luovuttamaa tai Toimittajalla olevaa Asiakkaan asiakirjamuotoista tai muuta tietoa, joka on määritelty salassa pidettäväksi laissa viranomaisen toiminnan julkisuudesta (621/1999, jäljempänä "julkisuuslaki") tai muussa lainsäädännössä, ja jonka Asiakas on tällaiseksi tiedoksi merkinnyt tai jonka Toimittaja tiesi tai olisi pitänyt tietää kuuluvan tällaisiin tietoihin. Salassa pidettäväksi tiedoksi katsotaan myös julkisuuslaissa tarkoitetun ei vielä julkisen asiakirjan sisältämä tieto. Lisäksi kaikki Asiakkaan luovuttamat henkilötiedot katsotaan Salassa pidettäväksi tiedoksi. Salassa pidettäväksi tiedoksi ei katsota sellaista tietoa, joka on julkisesti saatavilla tai jonka sopijapuoli on saanut tietoonsa laillisella tavalla kolmannelta osapuolelta ilman sitä koskevaa salassapitovelvoitetta.
- 2.4 **Turvallisuussopimus** tarkoittaa tätä sopimusasiakirjaa liitteineen.
- 2.5 **Asiakkaan Tilat** tarkoittavat sellaisia Asiakkaan käytössä olevia tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja tai joissa liikkumista on muutoin turvallisuussyistä syytä rajoittaa.
- 2.6 **Toimittajan Tilat** tarkoittavat sellaisia Toimittajan tai sen alihankkijan tiloja, joissa säilytetään, käytetään tai muutoin käsitellään Salassa pidettäviä tietoja.

SOPIMUSASIAKIRJAT JA NIIDEN PÄTEMISJÄRJESTYS

3.1 Tämä Turvallisuussopimus muodostuu tästä sopimusasiakirjasta ja seuraavista liitteistä:

- Liite 1 Turvallisuussopimuksen yhteyshenkilöt
- Liite 2 Ohje Salassa pidettävien tietojen käsittelystä ja säilyttämisestä
- Liite 3 Henkilöstön vaitiolositoumukset vaitiolositoumusmalli
(*Ohje: Vaitiolovelvollisuus tulee suoraan laista, Julkl 23 §. Sitoumuksella henkilöstöön kuuluva ilmoittaa saaneensa tiedon tietojen salassapidosta ja siitä, että niiden ilmaiseminen tai luovuttaminen ilman lupaa on kiellettyä. Samaan asiakirjaan voi laittaa myös käsittelyvelvoitteita koskevan lauseen.*)
- Liite 4 Toimittajan turvallisuudenhallinnan kuvaus [/Selvitys Palveluun liittyvistä tietoturvamenettelyistä]
- [Liite 5 Palveluun sovellettava valtionhallinnon tietoturvallisuustaso, tietoturvallisuusvaatimukset, Asiakkaan tilojen turvallisuusluokitukset, Palveluun liittyvien tietojen luokitus suojaustasoille]

3.2 Asiakas ja Toimittaja vastaavat omalta osaltaan liitteen 1 ylläpidosta.

3.3 Liitteessä 2 on esitetty Asiakkaan hyväksymät menettelyt, mukaan lukien Tiloja ja järjestelmiä koskevat määräykset ja ohjeet eri suojaustasoluokkiin kuuluvan tiedon, asiakirjojen ja muun tietoaineiston käsittelystä. Asiakas vastaa liitteen ylläpidosta. *[Ohje: Ohjeiden tulisi olla sisällöltään yhdenmukaiset tietoturvallisuusasetuksen ja sen täytäntöönpanosta annetun VAHTI-ohjeen 2/2010 luokittelu- ja käsittelyohjeiden kanssa.]*

3.4 Toimittaja vastaa liitteen 4 ylläpidosta. Liitteen tulee vastata voimassa olevaa tilannetta.

[3.5 Asiakas vastaa liitteen 5 ylläpidosta]

TURVALLISUUSSOPIMUKSEN TAUSTA JA TARKOITUS

4.1 Toimittaja ja Asiakas ovat tehneet Pääsopimuksen nro [xxx] [sopimuksen kohde] [pvm].

4.2 Tässä Turvallisuussopimuksessa sovitaan Asiakkaan ja Toimittajan välillä noudatettavista turvallisuusjärjestelyistä ja Salassa pidettävää tietoa koskevista järjestelyistä edellä mainitun Pääsopimuksen sisältämien Palveluiden tuottamisessa sekä kaikessa Pääsopimukseen liittyvässä Asiakkaan ja Toimittajan välisessä yhteistyössä.

4.3 Sopijapuolet tiedostavat, että Pääsopimuksen perusteella toimitettaviin Palveluihin sisältyy sellaista tietoa, jonka salassa pysyminen on *[esimerkki, tarkennetaan hankintakohtaisesti: yhteiskunnan häiriöttömän toimintakyvyn ja valtion sekä yksilöiden turvallisuuden kannalta kriittistä]*. Palvelun tuottamisen yhteydessä Toimittajan ja sen alihankkijan henkilöstöllä on pääsy Asiakkaan Tiloihin, joissa liikkumista on turvallisuussyistä syytä rajoittaa. Tällä Turvallisuussopimuksella sopijapuolet pyrkivät varmistamaan, että Salassa pidettävät tiedot pysyvät salassa.

- 4.4 Huolimatta siitä, mitä muissa Asiakkaan ja Toimittajan välisissä sopimuksissa on mahdollisesti sovittu tämän Turvallisuussopimuksen piiriin kuuluvista asioista tai niihin liittyvistä vastuista taikka sopimusten keskinäisestä pätemisjärjestyksestä, tätä Turvallisuussopimusta sovelletaan aina ensisijaisesti tämän Turvallisuussopimuksen piiriin kuuluvissa asioissa. Tähän Turvallisuussopimukseen tai sen perusteella syntyviin vastuihin ei sovelleta muissa sopijapuolten välisissä sopimuksissa mahdollisesti sovittuja vastuunrajoituksia.
(Ohje: Jos otat tämän Turvallisuussopimuksen Pääsopimuksen liitteeksi, huomaa soveltamisjärjestyksen vaikutus tämän ehdon sanamuotoon.)

LUOTTAMUKSELLISUUS JA SALASSAPITO

- 5.1 Tässä Turvallisuussopimuksessa kuvattuja turvallisuusjärjestelyjä noudatetaan aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa.
- 5.2 Asiakas noudattaa julkisyhteisönä julkisuuslaissa, valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010; jäljempänä tietoturvallisuusasetus) sekä muussa lainsäädännössä olevia salassapitoa ja julkisuutta koskevia säännöksiä. Sopimuksella ei voida poiketa lainsäädännön Asiakkaalle asettamista pakottavista velvoitteista.
(Ohje: Poista/muokkaa, jos Asiakas ei kuulu julkisuuslain tai tietoturvallisuusasetuksen soveltamisalaan.)
- 5.3 Toimittaja sitoutuu pitämään salassa kaikki Asiakkaan sille luovuttamat tai sillä olevat tai toimeksiannon toteuttamisessa syntyneet Salassa pidettävät tiedot, ottaen lisäksi huomioon kohdassa 5.7 sovitun. Salassa pidettäviä tietoja ei myöskään saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi.
- 5.4 Toimittajan tulee käsitellä Salassa pidettäviä tietoja vain Palvelun tuottamisen edellyttämässä laajuudessa. Toimittaja antaa Salassa pidettäviä tietoja vain niille henkilöille, jotka tarvitsevat Salassa pidettäviä tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Toimittaja sitoutuu saattamaan Turvallisuussopimuksen vaikutusalaan kuuluvat henkilöt tietoiseksi tähän Turvallisuussopimukseen liittyvistä velvoitteista ja antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Salassa pidettävien tietojen asianmukaisesta käsittelystä henkilöille, joilla on pääsy näihin tietoihin. Toimittaja sitoutuu valvomaan, että edellä tarkoitetut henkilöt noudattavat Turvallisuussopimusta.
- 5.5 Toimittaja sitoutuu säilyttämään ja käsittelemään Salassa pidettäviä tietoja siten, että ne pysyvät vain niiden henkilöiden hallussa, joilla on oikeus Salassa pidettäviin tietoihin, eivätkä ne joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon. Asiakkaan antama tarkempi ohjeistus Salassa pidettävien tietojen käsittelystä ja säilyttämisestä, jota Toimittaja sitoutuu noudattamaan, on liitteessä 2.
- 5.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille saattaa olla rikoslain mukaan rangaistava teko.
- 5.7 Tiedon antamisesta asiakirjasta, joka on saatu Asiakkaalta tai laadittu Asiakkaan toimeksiantotehtävää suoritettaessa, päättää Asiakas, jollei toimeksiannosta muuta johdu.

- 5.8 Toimittaja vastaa siitä, ettei Asiakkaan kohteiden tai toiminnan turvallisuus vaarannu Toimittajan henkilöstön huolimattomuuden, virheellisten työtapojen tai muun tämän Turvallisuuksopimuksen tai Pääsopimuksen vastaisen toiminnan johdosta.
- 5.9 Toimittaja ja sen alihankkijat saavat mainita referenssinä tehneensä työtä Asiakkaalle vain, jos asiasta on erikseen kirjallisesti sovittu.
- 5.10 Mikäli Salassa pidettäviä asiakirjoja tai tietoja käsitellään Asiakkaan toimitilojen ulkopuolella, on Toimittajan noudatettava Asiakkaan antamia toimintaohjeita ja erityisesti huolehdittava siitä, ettei tietoaineistojen turvallisuus vaarannu.
- 5.11 Tässä Turvallisuuksopimuksessa kuvattujen menettelyjen lisäksi Asiakkaalla on oikeus tarvittaessa antaa turvallisuuteen liittyviä käytännön toimintaohjeita, joita Toimittajan tulee noudattaa.

PÄÄSY TILOIHIN

- 6.1 Toimittaja vastaa siitä, että pääsy Asiakkaan korotetun tai korkean turvallisuustason Tiloihin (vyöhykkeet ORANSSI (ST III), KELTAINEN (TL III) tai SININEN (ST II)) annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 9 tarkoitettu turvallisuusselvitys ja jotka ovat tietoisia tämän Turvallisuuksopimuksen velvoitteista ja Tiloissa liikkumisesta annetuista ohjeista. Henkilöt, joille ei ole annettu edellä tarkoitettulla tavalla oikeutta päästä mainittuihin Asiakkaan tiloihin, saavat oleskella Tiloissa ainoastaan Asiakkaan luvalla ja valvonnan alaisina.
- 6.2 Toimittaja vastaa siitä, että pääsy Asiakkaan turvallisuuden perustason tiloihin (vyöhyke 4) annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen ja jotka ovat tietoisia tämän Turvallisuuksopimuksen velvoitteista ja Tiloissa liikkumisesta annetuista ohjeista. Henkilöt, joille ei ole annettu edellä tarkoitettulla tavalla oikeutta päästä mainittuihin Asiakkaan Tiloihin, saavat oleskella niissä ainoastaan Asiakkaan luvalla ja valvonnan alaisina. Henkilöiden pääsy mainittuihin Tiloihin ei lähtökohtaisesti edellytä henkilöiden turvallisuusselvittämistä. Asiakkaalla on kuitenkin oikeus edellyttää luvussa 9 tarkoitetun turvallisuusselvityksen tekemistä myös mainittuihin Tiloihin pääsevien henkilöiden osalta, mikäli selvitysten tekemiselle laissa asetetut edellytykset täyttyvät.
- 6.3 Henkilöiden, joilla on pääsy Asiakkaan Tiloihin, tulee olla tunnistettavissa. Henkilöillä on oltava Asiakkaan Tiloissa liikkueensa näkyvillä Asiakkaan kanssa sovittu kuvallinen henkilötunniste.
- 6.4 Toimittajan ja sen alihankkijan Tilojen tulee olla Tiloissa käsiteltävien Salassa pidettävien tietojen luokitusasteen asettamat vaatimukset huomioon ottaen asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi Tiloihin ja siellä oleviin Salassa pidettäviin tietoihin. Tiloille asetettavia vaatimuksia ja niiden täyttymistä arvioidaan voimassa olevan [Kansallisen turvallisuusauditointikriteeristön (KATAKRI)] mukaisesti.

- 6.5 Mikäli Palvelu suoritetaan tai Salassa pidettäviä tietoja käsitellään Toimittajan tai sen alihankkijan Tiloissa, Toimittajan tulee varmistaa Tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms. erityistilanteiden varalta. Asiakas ja Toimittaja sopivat tarvittaessa Palveluun liittyvistä tarkemmista vaatimuksista.
- 6.6 Henkilöt, joille ei ole myönnetty oikeutta Salassa pidettäviin tietoihin tai niitä sisältäviin järjestelmiin luvun 7 mukaisesti, saavat oleskella Toimittajan tai sen alihankkijan Tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli Salassa pidettäviä tieto- ja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.
- 6.7 Henkilöiden, joilla on pääsy Toimittajan tai alihankkijan Tiloihin, tulee olla tunnistettavissa.
- 6.8 [Asiakkaalla on oikeus vaatia luvussa [x] tarkoitetun turvallisuusselvityksen hakemista henkilöistä, joilla on oikeus päästä [tiettyihin yksilöityihin] Tiloihin. Toimittajan tulee myös hyväksyttää henkilö Asiakkaalla ennen kuin henkilölle voidaan myöntää pääsy [tiettyihin yksilöityihin] Tiloihin.]
- [6.8 Toimittaja pitää ja/tai velvoittaa tarvittaessa alihankkijansa osaltaan pitämään luetteloa henkilöistä, joille Palveluun liittyen on annettu oikeus päästä kohdassa [*valitaan sopiva vaihtoehto*: 6.1, 6.2] tarkoitettuihin Asiakkaan Tiloihin, huolehtii luettelon ajantasaisuudesta ja toimittaa sen [sovituin määrävälein tai pyynnöstä] Asiakkaalle.]

PÄÄSY JÄRJESTELMIIN JA TIETOIHIN

- 7.1 Toimittaja vastaa siitä, että suojaustasolle II tai III luokiteltuja Salassa pidettäviä tietoja annetaan tai pääsy sellaisia tietoja sisältäviin järjestelmiin sallitaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henkilöille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 9 tarkoitettu turvallisuusselvitys ja joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin, ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Asiakkaalla on kuitenkin tarvittaessa oikeus edellyttää edellä tarkoitetun menettelyn noudattamista myös suojaustasolle IV luokiteltuihin Salassa pidettäviin tietoihin tai sellaisia tietoja sisältäviin järjestelmiin pääsevien henkilöiden osalta, mikäli turvallisuusselvityksille laissa asetetut edellytykset täyttyvät. Oikeuden päästä Asiakkaan järjestelmiin, jotka sisältävät Salassa pidettäviä tietoja, antaa Asiakas.
- 7.2 Toimittaja vastaa siitä, että Salassa pidettävien tietojen käsittelyyn osallistuvat Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt sekä henkilöt, joilla on pääsy Toimittajan tai Asiakkaan järjestelmiin, joissa säilytetään Salassa pidettäviä tietoja, ovat tietoisia salassapitoa koskevista velvoitteistaan ja noudattavat tätä Turvallisuussopimusta.
- 7.3 [Toimittaja pitää ja/tai velvoittaa tarvittaessa alihankkijansa osaltaan pitämään luetteloa henkilöistä, jotka Palveluun liittyen käsittelevät suojaustasolle [*valitaan sopivat vaihtoehdot*: II, III, IV] luokiteltuja Salassa pidettäviä tietoja tai joilla on pääsy sellaisia tietoja sisältäviin järjestelmiin, huolehtii luettelon ajantasaisuudesta ja toimittaa sen [sovituin määrävälein tai pyynnöstä] Asiakkaalle.]

VAITIOLOSITOUMUS

- 8.1 Toimittaja vastaa siitä, että henkilö, joka käsittelee Salassa pidettäviä tietoja ja/tai jolla on pääsy järjestelmiin, joissa Salassa pidettäviä tietoja säilytetään, tekee vaitiolositoumuksen Asiakkaan hyväksymälle lomakkeelle (liite 3) ennen kuin hän saa aloittaa mainittujen tietojen käsittelyn tai saa pääsyn mainittuihin järjestelmiin.
- 8.2 Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijan henkilökuntaan kuuluva henkilö, jolla on pääsy Asiakkaan kohdassa 6.1 tarkoitettuihin Tiloihin, tekee vaitiolositoumuksen Asiakkaan hyväksymälle lomakkeelle (liite 3) ennen kuin hän saa oikeuden päästä mainittuihin tiloihin. Asiakkaalla on tarvittaessa oikeus edellyttää vaitiolositoumusta myös henkilöiltä, joilla on pääsy kohdassa 6.2 tarkoitettuihin Asiakkaan perusturvallisuustason tiloihin.

TURVALLISUUSSELVITYKSET

- 9.1 Jollei toisin sovita, jotta henkilö saa kohdassa 7.1 tarkoitetulla tavalla oikeuden käsitellä sellaisia Salassa pidettäviä tietoja, joiden salassapito on välttämätöntä turvallisuusselvityksistä annetun lain (177/2002) 2 §:ssä mainittujen etujen suojaamiseksi, ja/tai päästä järjestelmiin, jotka sisältävät sellaisia Salassa pidettäviä tietoja, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettu perusmuotoinen turvallisuusselvitys tai tarvittaessa tasoltaan vastaava ulkomainen turvallisuusselvitys. Toimittajan tulee hankkia turvallisuusselvityksen kohteena olevan henkilön suostumus selvityksen tekemiseen. Jotta henkilö saa oikeuden päästä Asiakkaan kohdassa 6.1 [ja 6.2] tarkoitettuihin Tiloihin, henkilöstä tulee hakea turvallisuusselvityksistä annetussa laissa tarkoitettujen edellytysten täytyessä suppea turvallisuusselvitys tai tasoltaan vastaava ulkomainen turvallisuusselvitys.
- 9.2 Jollei toisin sovita, tasoltaan vastaavaksi ulkomaiseksi turvallisuusselvitykseksi voidaan katsoa ainoastaan ulkomaisen kansallisen turvallisuusviranomaisen (esim. General Security Agreement:in eli GSA:n mukainen National Security Authority, NSA) tekemä turvallisuusselvitys (Personal Security Clearance, PSC). Jollei toisin sovita, PSC-selvitys edellytetään tehtäväksi henkilöstä, joka on ulkomaan kansalainen ja jolla on ollut pysyvä asuinpaikka Suomessa vähemmän kuin [5] vuotta.
- 9.3 Mikäli Toimittaja käyttää Palvelun toteutuksessa sellaista alihankkijaa, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee tästä alihankkijasta tarvittaessa hakea yhteisöturvallisuusselvitys (Facility Security Clearance, FSC) ja tietojen käsittelyyn osallistuvista henkilöistä henkilöturvallisuusselvitys (Personal Security Clearance, PSC), jollei toisin sovita.
- 9.4 Asiakkaan tehtävänä on hakea kaikkia tässä luvussa tarkoitettuja turvallisuusselvityksiä.
- 9.5 Asiakas vastaa kohdissa 9.1-9.3 tarkoitettujen turvallisuusselvitysten kustannuksista. Mikäli turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan tai Toimittajan alihankkijan henkilöstössä tapahtuu vaihdos tai Asiakkaasta riippumaton lisäys, Toimittaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.
- 9.6 Toimittajan tulee toimittaa turvallisuusselvityksen kohteena olevan henkilön täyttämä ja allekirjoittama turvallisuusselvityshakemuslomake Asiakkaalle turvallisuusselvityksen teettämistä varten. Lomakkeen tulee sisältää selvityksen kohteena olevan henkilön suos-

tumus turvallisuusselvityksen tekemiseen. Jos turvallisuusselvitys tulee tehtäväksi sellaisessa valtiossa, jonka lainsäädännön mukaan kyseessä olevan selvityksen tekeminen ei edellytä selvityksen kohteena olevan henkilön suostumusta, Toimittajan ei myöskään [tämän kohdan nojalla] tarvitse pyytää henkilöltä edellä mainittua suostumusta.

- 9.7 Asiakkaalla on perustellusta turvallisuuteen liittyvästä syystä oikeus kieltää Toimittajan tai sen alihankkijan henkilön osallistuminen Palvelun suorittamiseen.

TIETOTURVALLISUUS

- 10.1 Toimittaja noudattaa julkisuuslaissa tarkoitettua hyvää tiedonhallintatapaa sekä henkilötietolain (523/1999) edellyttämää hyvää tietojen käsittelytapaa ja tietojen suojaamista koskevia säännöksiä sekä muuta tietosuojaa koskevaa lainsäädäntöä Pääsopimukseen liittyvän Palvelun tuottamisessa.
- 10.2 *[Vaihtoehto 1]*
Mikäli Asiakas luokittelee Salassa pidettäviä tietojaan tietoturvallisuusasetuksen mukaisiin suojaustasoihin. [Tietojen luokitus eri suojaustasolle ilmenee liitteestä 5]. Toimittaja sitoutuu noudattamaan Salassa pidettäviä tietoja käsitellessään edellä mainitun asetuksen ja Asiakkaan ohjeistuksen kyseiselle suojaustasolle asettamia vaatimuksia. (Ohje: Tämän aiheuttamasta hintavaikutuksesta sovitaan tarkemmin.)
- 10.2 *[Vaihtoehto 2]*
Mikäli Asiakas ei luokittele Salassa pidettäviä tietoja yllä mainituin tavoin, tietoturvallisuusasetuksen mukaisiin suojaustasoihin. Toimittaja sitoutuu noudattamaan perustason tietoturvallisuutta ja Asiakkaan ohjeistusta Salassa pidettäviä tietoja käsitellessään..
- 10.3 Asiakas on määrittänyt Palvelun hankinnan yhteydessä Palveluun sovellettavan valtion hallinnon tietoturvatason ja Palveluun liittyvät konkreettiset tietoturva-vaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esitetty [Pääsopimuksen liitteessä X/tämän Turvallisuussopimuksen liitteessä 2 5.]

ALIHANKKIJAT

- 11.1 Toimittajan tulee hyväksyttää Asiakkaalla sellainen alihankkija, jota se aikoo käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin. Tässä Turvallisuussopimuksessa alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin.
- 11.2 Mitä tässä Turvallisuussopimuksessa on sovittu Toimittajan henkilöstöstä, sovelletaan myös alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön.
- 11.3 Toimittajan tulee huolehtia siitä, että se pystyy noudattamaan tätä Turvallisuussopimusta myös käyttäessään alihankkijoita. Toimittaja on tietoinen ja sen on tiedotettava alihankkijalleen, että turvallisuusjärjestelyiden saattamisesta tämän Turvallisuussopimuksen edellyttämälle tasolle saattaa syntyä kustannuksia. Asiakas ei vastaa näistä kustannuksista.

- 11.4 Toimittaja vastaa alihankkijoiden toiminnasta kuin omastaan ja siitä, että alihankkijat toimivat tämän Turvallisuussopimuksen ehtojen mukaisesti.
- 11.5 Ellei toisin sovita, Toimittajan tulee tehdä tämän Turvallisuussopimuksen ehtoja vastaava sopimus kohdassa 11.1 tarkoitetun alihankkijansa kanssa ja Toimittajan on asetettava alihankkijalleen vastaava velvollisuus tämän käyttämän alihankkijan osalta. [Sopimus on hyväksyttävä Asiakkaalla ennen sen allekirjoittamista.]

TARKASTUKSET JA RAPORTOINTI

- 12.1 Asiakkaalla [julkisen hallinnon palvelukeskuksen omalla asiakkaalla, joka hyödyntää Pääsopimuksessa tarkoitettua palvelua palvelukeskuksen välityksellä] tai Asiakkaan määräämällä kolmannella taholla (joka ei ole Toimittajan suoranainen kilpailija) on oikeus tarkastaa omalla kustannuksellaan etukäteen ilmoitettuna ajankohtana Toimittajan ja sen alihankkijoiden turvallisuusjärjestelyt tätä Turvallisuussopimusta sekä Pääsopimusta koskevilta osin. Asiakkaan on ilmoitettava tahdostaan suorittaa tarkastus viimeistään kolmekymmentä (30) päivää ennen ehdotettua tarkastuspäivää. Toimittaja voi ehdottaa uutta päivää tarkastukselle. Uusi ajankohta ei kuitenkaan saa olla myöhemmin kuin kymmenen (10) päivää Asiakkaan ehdottaman päivän jälkeen. Tarkastus saadaan suorittaa kuitenkin enintään kaksi kertaa vuodessa, ellei ole erityisen painavia syitä useammille tarkastuksille tai toisin sovita. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainituista määräajoista riippumatta erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tai sen alihankkijoiden tieto turvallisuutta tai Toimittajan tai sen alihankkijoiden salassapitovelvoitteita muita asiakkaita kohtaan. Asiakkaalla on edellä tarkoitetun tarkastusoikeuden lisäksi oikeus suorittaa Tiloissaan jatkuvaa valvontaa ja tehdä ennalta ilmoittamatta turvallisuustarkastuksia tässä Turvallisuussopimuksessa asetettujen velvoitteiden täyttymisen arvioimiseksi.
- 12.2 Toimittajan tulee huolehtia sopimusjärjestelyin siitä, että Asiakkaalla on mahdollisuus tarkastaa myös Toimittajan sellaisen alihankkijan turvallisuusjärjestelyt, joka osallistuu Salassa pidettävien tietojen käsittelyyn tai jolla on pääsy Asiakkaan Tiloihin.
- 12.3 Mikäli tarkastuksessa havaitaan merkittäviä puutteita turvallisuusjärjestelyissä, Toimittaja korvaa Asiakkaalle tarkastuksesta aiheutuneet kustannukset.
- 12.4 Toimittajan tulee korjata tarkastuksessa tai muussa valvonnassa havaitut puutteet viivytyksettä Asiakkaan kirjallisesta ilmoituksesta. Erityisiä korjaavia toimenpiteitä vaativat puutteet on korjattava kuitenkin viimeistään [30 vuorokauden kuluessa] Asiakkaan kirjallisesta ilmoituksesta, ellei siitä ole Asiakkaan ja Toimittajan välillä erikseen toisin sovittu. Olennaiset puutteet, jotka muodostavat ilmeisen uhkan tietoturvallisuudelle, on kuitenkin korjattava heti. Asiakas ei vastaa edellä mainituista korjauksista aiheutuvista kuluista ja kustannuksista.
- 12.5 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, jos Toimittajan tai sen alihankkijan tämän Turvallisuussopimuksen kannalta keskeisissä toiminnoissa tai henkilöstö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai jos Toimittajan tai sen alihankkijan omissuhteissa tapahtuu merkittäviä muutoksia.
- 12.6 Toimittaja valvoo tämän Turvallisuussopimuksen edellyttämän turvallisuustason toteutumista toiminnassaan säännöllisesti ja suunnitelmallisesti, kirjaa mahdolliset poik-

keamat ja raportoi ne Asiakkaalle viivytyksettä sekä aloittaa korjaustoimet ensi tilassa. Asiakas seuraa Palvelun turvallisuustason toteutumista yhteistyössä Toimittajan kanssa.

- 12.7 Toimittaja on velvollinen ilmoittamaan Asiakkaalle, mikäli Toimittajaan tai sen alihankkijaan kohdistuu Asiakasta mahdollisesti uhkaavia yhteydenottoja. Toimittaja on velvollinen ilmoittamaan Asiakkaalle sopimuksen vastaisesta tietovuodosta, tietomurtoyrityksestä tai muusta turvallisuutta vaarantavasta tapahtumasta tai seikasta. Ilmoitukset tulee tehdä viipymättä ja kirjallisesti.
- 12.8 Asiakkaalla on oikeus luovuttaa muille viranomaisille tai muille valtion yksiköille tieto siitä, että tämän luvun mukainen tarkastus on suoritettu, mutta Asiakkaalla ei kuitenkaan ilman Toimittajan lupaa ole oikeutta luovuttaa muille viranomaisille näille tietoa tarkastuksen tuloksista ellei pakottavasta lainsäädännöstä muuta johdu.

[SOPIMUSSAKKO JA] VAHINGONKORVAUS

(Ohje: Muokkaa koko luku hankinnan kohteeseen ja siihen liittyviin riskeihin soveltuvaksi. Harkitse tarvetta sopimussakkoa koskeviin ehtoihin ja vertaa niitä Pääsopimuksen mahdollisiin sopimussakkoehdoin. . Vaihtoehto A:ssa sopimussakkoa maksetaan kaikista Turvallisuussopimuksen rikkomuksista, vaihtoehto B:ssä salassapitovelvollisuuden rikkomuksista. Vaihtoehto C:ssä edellä mainituille rikkomuksille voidaan määritellä erisuuruinen sopimussakko.

[A Vaihtoehto

- 13.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Turvallisuussopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Sopimussakko ei koske kohdassa 5.7 sovitun velvollisuuden rikkomista, mikäli kyseessä ei ole Salassa pidettävä tieto.*
- 13.2 *Sopimussakon määrä jokaista rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta (esim. jatkuvan palvelun kuukausiveloituksesta)], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa].*

B Vaihtoehto

- 13.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista salassapitovelvollisuuden rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa.*
- 13.2 *Sopimussakon määrä jokaista rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta (esim. jatkuvan palvelun kuukausiveloituksesta)], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa].*

C Vaihtoehto

- 13.1 *Asiakkaalla on oikeus saada Toimittajalta sopimussakkoa jokaista tämän Turvallisuussopimuksen rikkomusta kohden ilman velvollisuutta näyttää toteen sille rikkomuksesta aiheutunutta vahinkoa. Sopimussakko ei koske kohdassa 5.7 sovitun velvollisuuden rikkomista, mikäli kyseessä ei ole Salassa pidettävä tieto.*

- 13.2 *Sopimussakon määrä jokaista salassapitovelvollisuuden rikkomusta kohden on [5 %] kyseessä olevan Pääsopimuksen kokonaisarvosta/ [tai Pääsopimuksen määritellystä osasta (esim. jatkuvan palvelun kuukausiveloituksesta)], kuitenkin vähintään [10.000 euroa] ja enintään [100.000 euroa]. Muiden tämän Turvallisuussopimuksen rikkomusten osalta sopimussakon määrä on [10.000 euroa]. Mikäli Toimittaja muun kuin salassapitovelvollisuuden rikkomuksen ollessa kyseessä korjaa rikkomuksen [14] vuorokauden kuluessa siitä, kun se on havainnut rikkomuksen, Asiakkaalla ei ole oikeutta saada sopimussakkoa, mikäli rikkomus on luonteeltaan sellainen, että siitä ei ole voinut aiheutua Asiakkaalle vahinkoa.*
- 13.3 Jos Toimittaja samalla teolla rikkoo useita tämän Turvallisuussopimuksen velvoitteita, se katsotaan kuitenkin vain yhdeksi sopimussakkoon oikeuttavaksi rikkomukseksi.
- 13.4 Ennen sopimussakon perimistä Asiakkaan tulee ilmoittaa Toimittajalle kirjallisesti tämän Turvallisuussopimuksen rikkomuksesta. Jos Toimittaja sitä kirjallisesti pyytää, käsitellään rikkomus lisäksi Asiakkaan ja Toimittajan välisessä tapaamisessa.
- 13.5 Kohdissa 13.1-13.4 tarkoitettu sopimussakko ei rajoita Asiakkaan oikeutta saada Toimittajalta vahingonkorvausta siltä osin kuin rikkomuksesta Asiakkaalle aiheutunut vahinko ylittää sopimussakon määrän.]
- 13.6 Asiakkaalla on oikeus saada korvaus kaikista niistä välittömistä vahingoista sekä kuluista ja kustannuksista, jotka sille ovat aiheutuneet Toimittajan tähän Turvallisuussopimukseen kohdistuvasta sopimusrikkomuksista, ellei rikkomus ole aiheutunut Pääsopimuksen kohdassa [x] tarkoitetusta ylivoimaisesta esteestä.
- 13.7 Lisäksi Asiakkaalla on oikeus saada korvaus myös kaikista välillisistä vahingoista, mikäli vahinko on aiheutettu tahallisesti tai törkeällä tuottamuksella taikka salassapitovelvollisuutta rikkoen.

SOPIMUSMUUTOKSET

- 14.1 Turvallisuussopimuksen yhteyshenkilöt (liite 1) vastaavat tämän Turvallisuussopimuksen päivittämistarpeen seuraamisesta. Päivittämistarve arvioidaan yhteyshenkilöiden kesken vähintään kahden vuoden välein.
- 14.2 Tähän Turvallisuussopimukseen tai sen liitteisiin tehtävät muutokset tulee tehdä kirjallisesti ja molempien sopijapuolten vahvistaa allekirjoituksellaan. Tämän Turvallisuussopimuksen muutokseksi ei katsota yhteyshenkilöiden vaihtumista.

SOPIMUKSEN IRTISANOMINEN [JA PURKAMINEN]

- 15.1 Sopijapuoli voi irtisanoa tämän Turvallisuussopimuksen päättymään kuuden (6) kuukauden irtisanomisajalla kirjallisesta ilmoituksesta lukien, ottaen kuitenkin huomioon mitä kohdassa 16.1 on sanottu. Irtisanominen ei poista velvollisuutta täyttää ennen irtisanomista syntyneet velvoitteet.
- 15.2 Jos Toimittaja irtisanoo tämän Turvallisuussopimuksen, Asiakkaalla on oikeus irtisanoa se Pääsopimus, johon tämä Turvallisuussopimus perustuu.

- 15.3 Asiakas on oikeutettu irtisanomaan välittömästi päättymään *[tai purkamaan]* tämän Turvallisuussopimuksen ja sen Pääsopimuksen, johon tämä Turvallisuussopimus perustuu, mikäli Toimittaja rikkoo tähän Turvallisuussopimukseen perustuvia sopimusvelvoitteitaan niin olennaisesti, ettei Asiakkaan voida kohtuudella edellyttää jatkavan sopimussuhdetta edes irtisanomisajan pituista aikaa. Irtisanominen ja purkaminen tulee tehdä kirjallisesti. [Lisäksi jos Toimittaja on rikkonut tätä Turvallisuussopimusta vähintään kolme kertaa siten, että Asiakkaalle on syntynyt oikeus vaatia luvussa 13 tarkoitettua sopimussakkoa, Asiakkaalla on aina oikeus irtisanoa välittömästi päättymään *[tai purkaa]* tämä Turvallisuussopimus ja se Pääsopimus, johon tämä Turvallisuussopimus perustuu.]
- 15.4 Tämän Turvallisuussopimuksen päättymisestä huolimatta Toimittajan on maksettava päättymisen perusteena olevista rikkomuksista tämän Turvallisuussopimuksen mukaiset sanktiot.

SOPIMUKSEN VOIMASSAOLO

- 16.1 Tämä Turvallisuussopimus on voimassa niin kauan kuin Asiakkaan ja Toimittajan välinen Pääsopimus on voimassa.
- 16.2 Tämä Turvallisuussopimus tulee voimaan, kun kumpikin sopijapuoli on sen allekirjoittanut.
- 16.3 Tämän Turvallisuussopimuksen mukainen salassapitovelvollisuus on voimassa myös sen jälkeen kuin Asiakkaan ja Toimittajan välinen Pääsopimus on päättynyt.
- 16.4 Pääsopimuksen päätyttyä Toimittaja mahdollisine alihankkijoihin palauttaa kaikki Asiakkaan Salassa pidettäviä tietoja sisältävät dokumentit, tallenteet ja muun materiaalin. Erikseen kirjallisesti niin sovittaessa Toimittaja mahdollisine alihankkijoihin voi myös tuhota edellä mainitun materiaalin Asiakkaan ohjeistuksen mukaisella tavalla.

SOVELLETTAVA LAKI JA ERIMIELISYYKSIEN RATKAISEMINEN

- 17.1 Tähän Turvallisuussopimukseen sovelletaan Suomen lakia, lukuun ottamatta lainvalintasäännöksiä.
- 17.2 Tästä Turvallisuussopimuksesta aiheutuvat erimielisyydet pyritään ensisijaisesti ratkaista sopijapuolten välisin neuvotteluihin. Mikäli sopijapuolet eivät pääse sovinnolliseen ratkaisuun, erimielisyydet ratkotaan ensi asteessa [Helsingin käräjäoikeudessa].

SOPIMUSKAPPALEET JA ALLEKIRJOITUKSET

- 18.1 Tämä Turvallisuussopimus on laadittu kahtena (2) samanasaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]

[paikka ja aika]

[ASIAKAS]

[TOIMITTAJA]

[allekirjoittaja]

[allekirjoittaja]

[allekirjoittaja]

Liite 3: Rakentamisdokumentaation käsittelysuositukset

Tähän liitteeseen on koottu suosituksia tiedon käsittelystä rakentamishankkeiden aikana:

- liite 3.1: tiedon luokittelumatriisi
- liite 3.2: tiedon luokitteluohje rakentamishankkeissa
- liite 3.3: turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa

VAHTI 2/2013 Liite 3.1 Tiedon luokittelumatriisi

Alla esitetty tiedon luokittelumatriisi on mallitaulukko, jossa on lueteltu rakennushankkeessa käytettyjä dokumenttikokonaisuuksia. Rakennushankkeessa tai –projektissa käytettävien dokumenttien tyyppi ja laji voivat poiketa esitetystä mallista. Tiedon luokittelumatriisia on tarkoituksenmukaista käyttää ja täydentää hankkeen eri vaiheissa. Kun hankkeessa havaitaan tunnistamaton tieto, lisätään se hanke-, suunnittelu-, tai työmaakokouksessa tiedon luokittelumatriisiin. Tieto luokitellaan oikeaan suojaustasoon sekä määritetään tiedolle omistaja.

Tiedon luokittelumatriisin käytön tarkoituksena on varmistaa, että tieto on luokiteltu sisältönsä mukaan oikeaan suojaustasoon ja ettei kenellekään tietoa tuottavalle tai käsittelevälle henkilölle ole epäselvää, minkä suojaustason tietoa hän käsittelee.

Dokumenttipohjainen luokittelumatriisi päivitetään hankkeen kaikissa vaiheissa vastaamaan tarvittavaa käsittelytasoa (tiedon omistaja vastaa dokumentin oikeasta suojaustasosta).

Hankintapohjainen matriisi pohjautuu tiedon suojaustarpeen osalta edelliseen ja kokoaa erilaisista dokumenttikokonaisuuksista hankintakokonaisuuksia.

TIEDON LUOKITTELUMATRIISI**Pvm:**

Hanke:

	Piirustuksen sisältö	Piirustus- tyyppi	Tiedon omistaja	Julkinen	ST IV	ST III	ST III / TL III	ST II	Huom.
1	Asemapiirros								
2	Pohjapiirustus								
3	Luolan leikkauskuvat								
4	Asemapiirros	Sähköpiirros							
5	Pohjapiirustus	Sähköpiirros							
6	Palopeltien johdotuskaavio	Sähköpiirros							
7	Nousujohtokaavio	Kaavio							
8	Maadoituskaavio	Kaavio							
9	Ohjaus- ja hälytysrunkokaavio	Kaavio							
10	Pääkeskus PK	Pääkaavio							
11	Pääkeskus PK	Piirikaavio							
12	Ryhmäkeskus	Pääkaavio							
13	Pistorasiakeskus	Pääkaavio							
14	Turvavalojärjestelmän johtokaavio	Kaavio							
15	Antennijärjestelmän johtokaavio	Telekaavio							
16	Äänentoistojärjestelmän johtokaavio	Telekaavio							
17	Ajannäyttöjärjestelmän johtokaavio	Telekaavio							
18	AV-kaapelointi	Telekaavio							
19	Merkinantojärjestelmien	Telekaavio							

47.4	Asiakkaan ja omistajan kiinteistön ylläpidon rajapintaliite								
47.5	Asiakkaan ja omistajan turvatekniikan hankintarajat								
48	Projektiohjelma								
49	Hyväksytty asemakaava								
50	Projektisuunnitelma								
51	Sopimukset (konsultti, urakka)								
52	Hankekohtaiset ohjeistukset								
53	Turvallisuusasiakirja								
54	Rakennuslupa								
55	Suunnittelukokouspöytäkirjat								Voi sisältää ST-liitteitä
56	Rakentamisen aikataulut								
57	Työmaakokouspöytäkirjat								Voi sisältää ST-liitteitä
58	Urakoitsijapalaverit								Voi sisältää ST-liitteitä
59	Yhteyshenkilöluettelo								
60	Työmaan valokuvat								Tai luokitus tapauskoht.
61	Laadunvalvontaohje								
62	Laadunvalvontasuunnitelma								
63	Luovutukseen liittyvät dokumentit								Voi sisältää ST-liitteitä
63.1	Jälkitarkastus								Voi sisältää ST-liitteitä
63.2	Vastaanottopöytäkirja								
64	Rakennuttamisen loppuraportti								Voi sisältää ST-liitteitä
65	Poistumistiekaavio								
66	Tarjouspyyntöasiakirjat								Sanitoitava julkisiksi
66.1	Kaapelinvetoluettelo (ilman huoneita)								Sanitoitava julkisiksi
66.2	Massaluettelot								Sanitoitava julkisiksi
67	Palvelinhotellin dokumentit								

VAHTI 2/2013 Liite 3.2 Tiedon luokitteluohje rakentamishankkeissa

Rakennushankkeen tiedot luokitellaan hankkeen luonne huomioiden oikeaan suojaustasoon siten, että luokittelija tunnistaa dokumenteista, mikä tieto on salassa pidettävää ja mitä suojaustasoa se on. Tiedon suojaustason määrittää voimassa olevien säädösten lisäksi kiinteistön ja tilan käyttötarkoitus. Toimintojen suojaamisperusteisiin vaikuttavat rakenne- ja valvontajärjestelmien tiedot sekä itse toiminta ja sen sijoittelu kiinteistössä.

LUOKITTELUOHJE

- **Perustaso** (turvallisuusvyöhyke max. VIHREÄ, ST IV)
 - Pääosa dokumentaatiosta julkista, mm. yleiskaapelointi
 - Perustellut hankintakokonaisuudet ST IV (rikosilmoitus, kulunvalvonta, verkkokuvaukset (muu kuin julkinen verkko))
- **Korotettu taso** (turvallisuusvyöhyke max. KELTAINEN ST III / TL III)
 - Pääosa dokumentaatiosta julkista, mm. yleiskaapelointi
 - Perustellut hankintakokonaisuudet ST IV (turvarakenteet, verkot: rikosilmoitus, kulunvalvonta, verkkokuvaukset (muu kuin julkinen verkko))
- **Korkea taso** (turvallisuusvyöhyke max. SININEN, ST II)
 - Perusteltu osa dokumentaatiosta julkista
 - Muut hankintakokonaisuudet ST IV - III (turvarakenteet, osa tilarakenteista, verkot: rikosilmoitus, kulunvalvonta, verkkokuvaukset (muu kuin julkinen verkko))

VAHTI 2/2013 Liite 3.3 Turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa

”Turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa” -taulukon tarkoituksena on selvittää eri toimijoiden roolit ja vastuut salassa pidettävän tiedon käsittelyssä rakennushankkeen aikana. Taulukon ensimmäisellä vaakarivillä on käsitelty rakennushankkeen päävaiheet ja ensimmäisellä pystyrivillä tyypilliset rakennushankkeen toimijat. Pystysarakkeisiin on määritetty toimijoiden roolit tai vastuut hankkeen eri vaiheissa. Toimijan rooli voi muuttua, riippuen asiakasviranomaisen omasta kyvystä ja toimivaltuuksista.

(Erillinen Excel-liite)

Liite 4: Rakentamishankkeiden turvallisuusaskeleet (esimerkki)

Taulukossa ”Rakentamishankkeiden turvallisuusaskeleet” on kuvattu kronologisesti rakennushankkeen eri vaiheet, huomioiden hankkeen turvallisuuden vaatimat välitoimenpiteet. Taulukon janojen aikamääreet ovat suuntaa antavia ja ne on syytä määrittää jokaisessa hankkeessa erikseen jo hankesuunnitteluvaiheessa sekä päivittää niitä tarvittaessa.

Ennakkotiedusteluvaiheessa pyritään selvittämään mahdollisten tarjoajien kykyä käsitellä ja säilyttää suojaustason IV tarjouspyyntöaineistoa sekä kartoittaa ne tarjoajat, jotka tulevat tutustumaan tarjouspyyntöaineistoon asiakkaan ennalta hyväksymään paikkaan.

(Erillinen Excel-liite)

Liite 5: Pohjakuvaesimerkit eri turvallisuusvyöhykkeiden mukaisista työympäristöistä

JULKISET TILAT (VALKOINEN)

Ei aita/portti/ajoestevaatimusta



- vieraiden tunnistamista tai kirjaamista ei vaadita (suositellaan)

- normaalit rakenteet
- normaali äänieristys
- salakatselun estoa ei vaadita, mutta suositellaan
- ikkunoihin ei kohdistu turvallisuusvaatimuksia
- normaalit ovet ja lukot
- ei asiakirjojen säilytykseen kohdistuvia turvallisuusvaatimuksia
- ei siivous- ja huoltohenkilöstöön kohdistuvia tunnistamis- tai kirjaamisvaatimuksia
- yleisöpalvelutiloissa otettava huomioon toiminnan luonteen mukaiset henkilösuojausvaatimukset

Ei aluevalvontavaatimusta

PERUSTASO ST IV / TL IV (VIHREÄ)

Ei aita/portti/ajoestevaatimusta



- vieraat tunnistetaan ja kirjataan

- normaalit rakenteet
- riittävä äänieristys
- salakatselun esto
- alle 4m ikkunoihin tarvittaessa suojakalvo
- normaalit ovet, käyttölukko
- ST IV:n säilytys lukitussa kaapissa tai kassakaapissa, jos tila ei ole valvottu
- siivous- ja huoltohenkilöstö tunnistetaan ja kirjataan

Ei aluevalvontavaatimusta

KOROTETTU TASO ST III (ORANSSI)

Aita/portti/ajosteet riskiarvion mukaisesti



Luja ulkoseinä

- vieraat tunnistetaan ja kirjataan



- vyöhykkeelle pääsy: kulunvalvonta
- tunkeutumisen ilmaisujärjestelmä
- siivous- ja huoltohenkilöstö tunnistetaan, kirjataan ja valvotaan
 - normaalit rakenteet
 - riittävä äänieristys
 - salakatselun esto
 - alle 4m ikkunoihin suojakalvo
 - normaalit ovet, käyttölukko
- ST III:n säilytys kassakaapissa (ei tasovaatimusta) tai holvissa, jos tila ei ole valvottu

Ei aluevalvontavaatimusta

Vartiointi ja reagointi!



KOROTETTU TASO ST III, turvallisuusluokitellut tiedot (KELTAINEN)

Alue aidattu. Portti (päivisin puomi).

Ajoesteet riskiarvion mukaisesti.



Luja ulkoseinä

- vieraat tunnistetaan ja kirjataan

- vyöhykkeelle pääsy: kulunvalvonta
- tunkeutumisen ilmaisujärjestelmä myös tilan aukoissa
- siivous- ja huoltohenkilöstö tunnistetaan, kirjataan ja valvotaan
- **vahvat tai vahvistetut rakenteet**
 - hyvä äänieristys
 - salakatselun esto (kaihtimet)
 - alle 4m ikkunoihin murtosuojalasit
- **vyöhykkeen rajalla turvaovet**, käyttölukon lisäksi **varmuuslukko**
- vyöhykkeen sisällä riittää pelkkä käyttölukko
- TL III:n säilytys kassakaapissa (vähintään Euro II) tai holvissa (Euro V), jos tila ei ole valvottu
- varmistetut LVIS-järjestelyt
- hissiissä kulunvalvonta



Ei aluevalvontavaatimusta



Mahdolliset TEMPEST-vastatoimet (uhka-arvio)

Vartiointi ja reagointi!



KORKEA TASO ST II/TL II (SININEN)

Pysäköintikontrolli

Alue aidattu. Portti (päivisin puomi).

Ajoesteet riskiarvion mukaisesti.

Luja uloimman vyöhykkeen ulkoseinä

- vieraat hyväksytään etukäteen, tunnistetaan, kirjataan + valvotaan

- vyöhykkeelle pääsy: kulunvalvonta ja **kaksoistunnistus**
 - vyöhykkeeltä **poistuminen**: kulunvalvonta
- tunkeutumisen ilmaisujärjestelmä myös tilan aukoissa
- siivous- ja huoltohenkilöstö tunnistetaan, kirjataan ja valvotaan
- vain sallitut elektroniset laitteet tilaan (**kännykkäparkki** ulkopuolelle)
- **vahvat tai vahvistetut rakenteet**
 - hyvä äänieristys
 - salakatselun esto (kaihtimet)
 - ikkunoihin murtosuoja- ja äänivärähtelyn esto
- **kameravalvonta** (vyöhyke tai tila)
- **vyöhykkeen rajalla turvaovet** ja kulkuannostelija (vast.), käyttölokun lisäksi **varmuuslukko**
 - vyöhykkeen sisällä riittää pelkkä käyttölukko
- TL III:n säilytys kassakaapissa (vähintään Euro II) tai holvissa (Euro V), jos tila ei ole valvottu
- varmistetut LVIS-järjestelyt, rajoitettu etäohjaus
- hisseissä kulunvalvonta, kuulut valvotaan



Aluevalvonta tai kuoren valvonta



Vartiointi ja reagointi!
Testaus!



Mahdolliset TEMPEST-vastatoimet (uhka-arvio)

Liite 6: Tietoteknisten laitetilojen turvallisuussuositukset

Erillinen liiteasiakirja

Liite 7: Määritelmät ja lyhenteet

Asiakirja	<i>Asiakirjalla</i> tarkoitetaan tässä ohjeessa julkisuuslain mukaisesti kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.
Aukkojen suojauslevy	Suojaustasosta riippuen vahva vaneri- tai metallilevy (viite: viranomaisten rakennetietokortisto)
Avain	Oven lukkoa tai kiinteistön lukitusjärjestelmää ohjaava tunnistite, joka voi olla mekaaninen, sähköinen tai biometrinen.
EMP	<i>Electro Magnetic Pulse</i> . Sähkömagneettinen pulssi, joka aikaansaadaan esimerkiksi ydinräjäytyksellä. Pulssi vikaannuttaa suojaamattomat elektroniset laitteet.
FK	Finanssialan keskusliitto. FK on mm. luokitellut turvallisuusvälineistöä ja julkaissut Rakenteelliset murtosuojeluohjeet I – III.
Fyysinen turvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan kaikkia organisaation tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyviä asioita, joilla pyritään estämään organisaation tarvitsemien tietojen sekä fyysisen ja ei-fyysisen ominaisuuden tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin. Fyysinen turvallisuus on myös tietojen käytettävyyden ylläpitoa, siltä osin kuin tilaratkaisut voivat sitä palvella tai mahdollisesti olla esteenä.
Hallinnollinen turvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaatiossa käytettäviä tietoturvallisuuden toimintapoliittikkoja, toiminnan linjauksia, johtamista, organisointia, toimintojen sijoitusta organisaatioon, resursointia sekä vastuiden määrittelyä.
Henkilöstöturvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation tietojen ja tietojenkäsittelyn suojaamista ihmisten aiheuttamilta tahallisilta sekä tahattomilta uhkilta ja ihmisten toimista tietoturvallisuuden varmistajina.
HPM	<i>High Power Microwave</i> . Korkeatehoinen mikroaalto, joka aikaansaadaan tyypillisesti täsmäaseella (esim. salkkupommi tai risteilyohjus) lähietäisyydeltä. Vikaannuttaa elektronisia järjestelmiä.
Ikkunoiden suojauslevy	Suojaustasosta riippuen vahva vaneri- tai metallilevy (viite: viranomaisten rakennetietokortisto)
Iskunkestävä lasi	Lasi, joka on testattu standardin SFS-EN 356 mukaan luokkiin P1A – P5A

Julkisivun ikkunat	Julkisivun ikkunoilla tarkoitetaan rakennuksen tai liiketilan asiakassisääkäynnin puoleisella sivulla olevia ikkunoita.
Käyntiväli	Ovilevyn ja karmin välinen rako lukon kohdalla
Käyttölukko	Kiinteästi oveen asennettava lukko vastalevyineen, joka on standardin SFS-EN 12209 mukaan testattu luokkaan 3 ja standardin SFS 7020 mukaan joko luokkaan 1 tai 2
Käyttöturvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation automaattisen ja manuaalisen tietojenkäsittelyn suojaamiseen liittyviä asioita.
Laitteistoturvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation käyttämien tietojenkäsittely- ja tietoliikennelaitteiden suojaamisasioita.
Lukitus	Lukkojen ja niihin sopivien tunnisteiden muodostama järjestelmä, jolla sallitaan tai rajataan henkilöiden pääsy tiloihin ja liikkuminen niissä.
Lukko	Kiinnittämiseen, sulkemiseen tai käytön estämiseen käytettävä laite, joka voidaan asettaa siten, että se avautuu vain siihen sopivalla tunnisteella tai ohjauslaitteella.
Luokiteltu asiakirja/tieto	Esiintymismuodostaan riippumaton salassa pidettävä tieto, joka on luokiteltu kuuluvaksi tietoturvallisuusasetuksessa määritellyyn suojaustasoon (TTA 9§).
Murronsuojalasi	Lasi, joka on testattu standardin SFS-EN 356 mukaan luokkiin P6B – P8B
Murronsuojaovi	Ovi, joka on testattu standardin SFS-ENV 1630 mukaan luokkiin 2 – 6
Murronsuojaseinä	Seinärakenne joka on testattu normin SSF 1047 mukaan luokkiin 1 – 3 tai standardin SFS- ENV 1630 mukaan vastaaviin luokkiin 2 – 4
Murtosuojatappi	Teräksestä valmistettu tappi, jonka halkaisija on vähintään 6 mm ja ulkonema vähintään 12 mm. Tappi sijoitetaan erilleen saranasta .
Murto	Tunkeutuminen rakenteellisesti suojattuun ja lukittuun säilytystilaan sen rakenteita tai lukkoja vahingoittaen.
Ohjelmistoturvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation käyttämien tietokoneohjelmien suojaamista sekä ohjelmien lisensointia ja rekisteröintiä.
Ovet, ikkunat ja muut aukot	Säilytystilan seinissä, lattiassa ja katossa olevia ovia, ikkunoita ja muita aukkoja.

Pikasalpa	Oven kiintopuolen sulkeva salpalaite, joka on sisäpuolelta painikkeesta avattavissa.
Rakorauta	Huultamattomaan oveen lukon kohdalle kiinnitetty teräksinen tai messinkinen T-profiili, jonka pituus on vähintään 30 cm ja materiaalin paksuus 3 mm .
Riippulukko	Riippulukot ovat standardin SFS-EN 12320 ja SFS 7020 mukaan testattu ja FK:n luetteloima luokkiin 1, 2, 3, 4 tai 5.
Riippulukkokiinnikkeet	Teräksestä valmistettuja riippulukkojen kiinnitykseen tarkoitettuja osia, jotka asennetaan karmiin ja oveen hitsaamalla, ruuvi- tai pulttikiinnityksin siten, ettei niitä saa ulkopuolelta rikkomatta irrotettua.
Rullakalteri	Kalteri, joka on testattu standardin SFS-ENV 1630 mukaan ja FK:n luetteloima luokkiin 2-6.
Säilytystila	Tila, joissa suojattavaa tietoa säilytetään. Säilytystila tulee ympäröidä kiinteillä rakenteilla. Säilytystiloiksi ei lueta rakennuksen ulkopuolisia rakenteita, kuten parvekkeita, katoksia, kuisteja ja lastaussiltoja.
Säilytystilan seinät, lattia ja katto	Säilytystilaa rajoittavia rakenteita, jotka voivat olla rakennuksen ulkopintoja tai muihin sisätiloihin rajoittuvia seiniä, lattiaa tai kattoja.
Telki	Lukon liikkuva osa, joka lukitsee oven karmissa olevaan vastalevyyn
TEMPEST	Sähkömagneettisen hajasäteilyn (EMR, <i>Electro Magnetic Radiation</i>) estävät suoja-toimet määrittelevä NATO-standardi. Standardin sisältö ei ole julkista tietoa. Standardin pohjalta on valmisteltu normi Euroopan Unionin turvallisuusluokitellun tiedon suojaamiseksi.
Teräspuomi	Riippulukkokiinnikkeillä varustettu, teräspuomi-profiilista tai lattateräksestä valmistettu oven, parioven tai suojalevyn lukituslaite. Puomi on kiinnitettävä tai lukittava molemmista päistään seinään tai karmiin. Puomi voidaan valmistaa vähintään 50x30x3 mm ³ :n teräspuomi-profiilista tai vähintään 12x50 mm ² :n lattateräksestä.
Teräsristikot	*Hitsaamalla valmistettu ristikko, jossa teräksen poikkipinta-ala on vähintään 110 mm² (pyöröteräs Ø 12 mm), terästen väli korkeintaan 120 mm ja jänneväli 350 mm *Haitariristikko on FK:n luetteloima kokoontaitettava teräsristikko. *Muototeräsristikko on hitsaamalla valmistettu teräsristikko, jossa teräksen poikkipinta-ala on vähintään 75 mm² (pyöröteräs Ø 10 mm) ja aukkokoko enintään 400 cm²

Teräsverkko	Teräskehikkoon hitsaamalla kiinnitetty verkko, jonka poikkipinta-ala on vähintään 10 mm ² ja aukkoko enintään 22 cm ²
Tietoaineistoturvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan kaikissa eri talletusmuodoissa olevia organisaation päivittäessä toiminnassa tarvitsemia tietoja sekä niiden suojaamiseen liittyviä asioita.
Tietoliikenneturvallisuus	Tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation käyttämien tietoverkkojen ja niissä tapahtuvien tietoliikenteen suojaamiseen liittyviä asioita.
Tietotekninen laitetila	Tyypillisesti konesali, palvelinhotelli tai muu erillinen useita palvelimia sisältävä tekninen tila, jonka toimintojen voidaan ajatella olevan kriittisiä valtionhallinnon tietoteknisen ympäristön toimivuuden kannalta ja joille on esitetty erityisvaatimuksia VAHTI 2/2013 liitteessä 6. Tavallisia kerros- tai talojakamoita koskevat yleiset toimitilaturvallisuusvaatimukset (VAHTI 2/2013 liite 1).
TTA	Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
Tilaturvallisuusjärjestelmät	Yhteisnimitys tilan valvontajärjestelmille, joita käytetään sekä <i>security</i> -, että <i>safety</i> -turvallisuuden varmistamiseksi (sähkölukitus, kulunvalvonta, tunkeutumisen ilmaisu, kameravalvonta, paloilmaisu, sammutusjärjestelmät, äänievakuointi jne.).
Tunkeutumisen ilmaisujärjestelmä	Ovien, ikkuna-aukkojen, käytävätilojen jne. valvontaan tarkoitettu ja ilmaisimiin perustuva tekninen järjestelmä, jonka kautta vartiohenkilöstö saa tiedon luvattomasta tilaan tunkeutumisesta (aiemmin: murtohälytysjärjestelmä). Järjestelmävaatimukset on jaettu Finanssialan keskusliiton toimesta toimintavarmuutta painottaen neljään vaatimusluokkaan.
Turvallisuusluokiteltu asiakirja/tieto	Esiintymismuodostaan riippumaton salassa pidettävä tieto, joka on luokiteltu kuuluvaksi tietoturvallisuusasetuksessa määritellyyn suojaustasoon ja joka on luokitusperusteidensa vuoksi varustettu turvallisuusluokitusmerkinnällä (TTA 11§).
Varmuuslukko	Kiinteästi oveen asennettava lukko vastalevyineen, joka on standardin SFS-EN 12209 mukaan testattu luokkaan 5 ja standardin SFS 7020 mukaan joko luokkaan 3 tai 4.
Vastalevy	Kiinteästi asennettavan lukon osa, joka kiinnitetään ruuveilla karmiin.
Vasteaika	Aika, joka kuluu hälytyksen lähtemisestä vasteen (vartija, poliisi) hälytyspaikalle saapumiseen. Kumulatiivinen vasteaika mittaa eri rakenteiden ja turvallisuusratkaisujen muodostamaa kokonaisaikaa (esim. aita/hälytys - ulko-ovi – sisäseinä - kassakaappi).

Liite 8: Lähdeluettelo

Laki viranomaisten toiminnan julkisuudesta (621/1999)

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

Laki turvallisuus selvityksistä (177/2002)

Arkistolaki (831/1994)

Valtioneuvoston asetus tieturvallisuudesta valtionhallinnossa (681/2010)

Euroopan unionin turvallisuusregiimi (6952/2/11 REV2/1.4.2011)

Naton turvallisuussäännöstö C-M 2002(49), (2002)

NATO AC/35-D/2001 Directive on Physical Security, (rev.2008, NATO UNCLASSIFIED)

Sisäasiainhallinnon tilaturvallisuusmääräys (2011)

Puolustusvoimien tilaturvallisuusmääräys (2011)

Yhteiskunnan turvallisuusstrategia (2010)

Ohje tietoturva-asetuksen täytäntöönpanosta (VAHTI 2/2010)

Sisäverkko-ohje (VAHTI 3/2010)

ICT-varautumisen vaatimukset (VAHTI 1/2012)

Kansallinen turvallisuusauditointikriteeristö (versio II, 2011)

Standardi ISO/IEC 27002:2005

Suomen rakentamismääräyskokoelma (1993–2011)

Rakenteellinen murtosuojaohje I – III (Finanssialan Keskusliitto ry 2011)

Kameravalvontaopas (julkaisija Turva-alan yrittäjät ry 2011)

Liite 9: Viiteaineiston lähdelainaukset

1. Lait

Laki viranomaisten toiminnan julkisuudesta (621/1999) ja valtioneuvoston asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999) määrittelevät yleisellä tasolla, minkä tyyppiset asiakirjat ovat salassa pidettäviä. Salassa pidettävien asiakirjojen suhteen julkisuuslain 6§ todetaan: ”*Salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi.*”

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttää, että Suomi valtiona kunnioittaa kaikessa toiminnassaan kansainvälisen yhteistyön mukaisia turvallisuusvelvoitteita. Velvoitepohjana toimivat kansainvälisessä kanssakäymisessä tyypillisesti joko tietoturvallisuutta säättävät valtiosopimukset tai Suomen muuten hyväksymät kansainväliset turvallisuussäännöstit.

Laki turvallisuuselvityksistä (177/2002) uusiutuu vuoden 2013 kuluessa. Uusi laki on kattavuudeltaan edeltäjänsä laajempi ja sisältää paitsi säädökset henkilöturvallisuuselvitysten toteuttamiseksi, myös säädökset yritysturvallisuuselvitysten hoitamiseksi.

Arkistolaki (831/1994) ottaa kantaa toimitilaturvallisuuden alaan säättämällä, että ”*asiakirjoja on säilytettävä siten, että ne ovat turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä*” (12§). Arkistolain 15§ linjaa lisäksi, että ”*asiakirjoja voidaan lainata vain toiselle viranomaiselle taikka arkistolaitokseen tai muuhun laitokseen, jossa niiden käyttö on valvottua ja säilyttäminen turvallista*”.

2. Tietoturvallisuusasetus

Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) annetaan asiakirjan käsittelylle seuraava määritelmä (3§): ”*...asiakirjan vastaanottamista, laatimista, tallettamista, katselua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, hävittämistä, säilyttämistä ja arkistointia sekä asiakirjaan automaattisen tietojenkäsittelyn, äänen- ja kuvantoistolaitteiden tai muiden apuvälineiden avulla taikka muutoin kohdistuvia toimenpiteitä*”.

Pykälässä 4 normitetaan tietoturvallisuuden suunnittelun perusteet seuraavasti:

”*Valtionhallinnon viranomaisen on pidettävä huolta, että tietoturvallisuuden suunnittelu hyvän tiedonhallintatavan mukaisesti perustuu viranomaisen selvityksiin ja arvioihin sen hallussa olevista asiakirjoista sekä niihin talletettujen tietojen merkityksestä ja että suunnittelussa otetaan huomioon vaatimus hyvän julkisuus- ja salassapitorakenteen toteuttamisesta tietojärjestelmissä ja että tietoturvallisuustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset.*”

Asetuksen viidennessä pykälässä todetaan, että ”*valtionhallinnon viranomaisen on huolehdittava, että ...asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja.*” Kuudes pykälä velvoittaa huolehtimaan siitä, että asiakirjan elinkaaren kaikki vaiheet tulevat otetuiksi huomioon toteutuksessa.

Tietoturvasäätöasetuksen pykälä 14 säättää asiakirjan säilyttämiseen ja käsittelyyn käytettävistä tiloista seuraavasti:

”Valtionhallinnon viranomaisen on pidettävä huolta, että:

- 1) tilat, joissa säilytetään tai muutoin käsitellään luokiteltuja asiakirjoja, suojataan asianmukaisesti lukituksella, kulunvalvonnalla ja muilla toimenpiteillä luvattoman pääsyn estämiseksi tiloihin ja siellä oleviin asiakirjoihin;*
- 2) henkilöt, joille annetaan pääsy tiloihin, joissa säilytetään tai muutoin käsitellään suojaustasoon I tai II kuuluvia asiakirjoja, ovat tunnistettavissa;*
- 3) suojaustasoon I ja II kuuluvat asiakirjat säilytetään sellaisessa kassakaapissa tai muussa lukittavassa kaapissa, holvissa tai tilassa, joka estää luvattoman pääsyn asiakirjaan sisältyviin tietoihin;*
- 4) henkilöt, joille annetaan pääsy arkistoon taikka tietokonekeskukseen tai muihin tietojärjestelmien ylläpidon tai tietoliikenteen toimivuuden kannalta merkityksellisiin tiloihin, joissa säilytetään tai käsitellään suojaustasoon III kuuluvia asiakirjoja taikka suojaustasoon IV kuuluvia valtakunnalliseen henkilörekisteriin talletettuja asiakirjoja, ovat tunnistettavissa.”*

Pykälässä 15 todetaan asiakirjan käsittelystä viranomaisen toimitilojen ulkopuolella:

”Luokiteltuja asiakirjoja ei saa säilyttää tai muutoin käsitellä valtionhallinnon viranomaisetoimitilojen ulkopuolella, ellei viranomaisenluvasta, toimeksiannosta tai antamista ohjeista muuta johdu.”

Elinkaariteemaa sivuavassa pykälässä 21 säädetään asiakirjan arkistoinnista ja hävittämisestä seuraavasti:

”Luokiteltujen asiakirjojen arkistoinnista säädetään arkistolaissa (831/1994). Tarpeettomaksi käyneen suojaustasoon I tai II kuuluvan asiakirjan kopio tulee hävittää, jollei sitä palauteta asiakirjan laatineelle viranomaiselle. Hävittämisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Asiakirjan valmisteluvaiheen versiot voi kuitenkin hävittää ne laatinut henkilö.

Paperimuotoinen asiakirja on tuhottava suojaustasoa vastaavalla tavalla. Sähköisesti talletettu asiakirja on vastaavasti tuhottava laitteesta, tietovälineeltä tai tietojärjestelmästä sekä pidettävä huolta, että tietojärjestelmien käytön yhteydessä syntyneet väliaikaistiedostot poistetaan riittävän usein, jolleivät ne poistu tietojärjestelmästä automaattisesti.”

3. Ohje tietoturvasäätöasetuksen täytäntöönpanosta (VAHTI 2/2010)

Tietoturva-asetuksen toimeenpanoa edesauttava VAHTI-ohje 2/2010 (*Ohje tietoturvasäätöasetuksesta valtionhallinnossa annetun asetuksen täytäntöönpanosta*) linjaa omalta osaltaan toimitilaturvallisuuden perusteita:

”Viranomaisen on huolehdittava kaikessa suunnittelussa ja toimeenpanossa, että henkilöstön käytössä ovat turvalliset työvälineet, tilat ja toiminnot ja että henkilöstö on tietoinen tietotyön riskeistä, tuntee oikeat menettelytavat ja on myötävaikuttamassa omalla asenteellaan korkean tietoturvakulttuurin olemassaoloon” (luku 4).

”Tilaturvallisuuden tarkoituksena on osana fyysistä turvallisuutta suojata henkilöstöä, tietoa ja materiaalia. Tilaturvallisuudella tarkoitetaan kaikkia niitä rakenteellisia ja valvonnallisia järjestelyjä, joilla varmistetaan tilojen pysyminen vain oikeutettujen hallinnassa ja käytössä sekä käyttötarkoituksen edellyttämässä

kunnossa. Rakenteilla tarkoitetaan seiniä, kattoja, ikkunoita, ovia, paloturma- ja kassakaappeja sekä muita mekaanisia ratkaisuja. Valvontajärjestelmillä tarkoitetaan yleensä kulunvalvonta-, tunkeutumisen ilmaisu-, kameravalvonta- ja olosuhdevaroitussjärjestelmiä. Sähköisiin valvontajärjestelmiin kuuluvat myös kiinteistöautomaatiojärjestelmät, joilla valvotaan ja ohjataan tilan käyttöolosuhteita.

Tilaturvallisuuden kokonaisuudesta ei ole olemassa varsinaisia standardeja, mutta kunkin tietoturvaluokituksen mukaiset viranomaisvaatimukset on esitetty yksityiskohtaisesti Kansallisen turvallisuusauditointikriteeristön (KATAKRI) fyysisen turvallisuuden osiossa. Viranomaisen on määriteltävä vastuullaan olevien tilojen turvallisuusratkaisut. Määrittelyssä on huomioitava mm. rakenteelliset ratkaisut, tarvittavat valvontajärjestelmät ja mahdollisesti tilojen käyttöoikeuksiin liittyviä asioita.

Tilaturvallisuutta tulee tarkastella kokonaisuutena. Kokonaisuuteen kuuluvat esim. tietoverkkojen laite- ja ristikytke-tilojen tilaturvallisuuden huomioiminen sekä huolehtiminen siitä, etteivät asiattomat pääse käsiksi mm. aktiivisiin kytkentärasioihin.” (luku 4.4).

Ohje kiinnittää lisäksi huomiota valvonta- ja kiinteistöautomaatiojärjestelmien tietoturvaluokituksen, tilojen äänieristykseen sekä sähkömagneettisen hajasäteilyn haittojen eliminointiin (luku 4.4).

4. Euroopan unionin turvallisuusregiimi (2011)

Euroopan unionin turvallisuusluokittelun tiedon turvaamiseen tähtäävä turvallisuussäädös on laadittu neuvoston pääsihteeristön johdolla ja hyväksytty eduskunnan toimesta noudatettavaksi myös Suomessa niissä tapauksissa, joissa EU:n luokiteltua tietoa käsitellään suomalaisten viranomaisten tai yhteisöjen toimesta. Säädös on syytä tuntea myös silloin, kun suomalaista turvallisuusluokiteltua tietoa harkitaan luovutettavaksi EU-käyttöön.

EU:n turvallisuussäädös sisältää melko yksityiskohtaiset vaatimukset fyysisen turvallisuuden toimenpiteille. Nämä vaatimukset on lähtökohtaisesti otettu huomioon KATAKRI:ssa ja myös tässä ohjeessa niiltä osin, kuin ne kutakin valtionhallinnon toimijaa koskettavat (taulukko 1).

EU-säädöksen mukaisesti toimitilavyöhykkeet, joilla käsitellään turvallisuusluokiteltua tietoa voidaan nimetä

- hallinnolliseksi vyöhykkeeksi,
- turvavyöhykkeeksi,
- teknisesti suojatuksi turvavyöhykkeeksi.

Toimitilat, joissa säilytetään CONFIDENTIEL UE/EU CONFIDENTIAL- tai sitä korkeamman tason EU:n turvallisuusluokiteltuja tietoja, on määriteltävä turvavyöhykkeiksi ja toimivaltaisen turvallisuusviranomaisen on hyväksyttävä ne. RESTREINT UE/EU RESTRICTED -tason turvallisuusluokiteltua tietoa voidaan käsitellä hallinnollisella vyöhykkeellä ja tilapäisesti myös sen ulkopuolella silloin, kun pääsy tietoon pystytään suojaamaan asiattomilta.

CONFIDENTIEL UE/EU CONFIDENTIAL- ja SECRET UE/EU SECRET -tason EU:n turvallisuusluokitellut tiedot on säilytettävä turvavyöhykkeellä kassakaapissa tai holvissa.

5. Naton turvallisuussäännöstö (2002)

Suomi noudattaa Naton kanssaan tekemässään kumppanuusyhteistyössä Naton asettamia tietoturvaluusvaatimuksia (C-M 2002(49)) silloin, kun kyseessä on Naton turvallisuusluokitellun tiedon suojaaminen. Naton turvallisuussäännöstön sisältö on syytä ottaa huomioon myös silloin, kun suomalaista turvallisuusluokiteltua tietoa harkitaan luovutettavaksi Nato-käyttöön.

Naton turvallisuussäännöstö sisältää laajan liiteosion. Liite AC/35-D/2001 (rev.2008) luo suuntaviivoja fyysisen turvallisuuden toteuttamiselle. Liitteen sisältö on otettu huomioon lähtökohtaisesti KATAKRI:ssa, samoin kuin tässä ohjeessa niiltä osin, kuin ne kutakin valtionhallinnon toimijaa koskettavat (taulukko 1).

Natossa toimitilat jaetaan kolmeen eri vyöhykkeeseen:

- hallinnolliset vyöhykkeet,
- luokan II vyöhykkeet,
- luokan I vyöhykkeet.

Luokan I vyöhykkeelle pääsy ja sieltä ulostulo on kontrolloitua ja sallittu vain asianmukaisen henkilöturvallisuustodistuksen omaaville henkilöille sekä erilliseen hyväksyntään perustuen. Luokan II vyöhykkeiden sisään ja ulospääsy on valvottua ja niillä voivat vierailla saatettuina tilapäisesti myös muut kuin pääsyyn kirjallisesti oikeutetut, mutta myös heidän taustansa tulee tätä ennen selvittää⁷. Pääsy hallinnollisille vyöhykkeille ei edellytä turvallisuusselvitystä, ainoastaan pääsyn valvontaa. Hallinnollisilla vyöhykkeillä saa käsitellä korkeintaan NATO RESTRICTED –tasolle luokiteltua tietoa.

Edellä mainittujen vyöhykkeiden lisäksi voidaan tekniset turvatilat muodostaa joko toimitilavyöhykkeen sisään tai erilliseksi kokonaisuudekseen. Osassa Naton luokiteltuja toimitiloja käytetään rajatusta tilasta käsitettä ”System High”. Tämän käsitteen mukaiseen tilaan voidaan myöntää pääsy ainoastaan sellaiselle henkilöstölle, jolla on käsittelyoikeus kaikkeen tilassa käsiteltävään tietoon. Tällaisia tiloja ovat esimerkiksi viesti- ja sanomakeskukset.

6. Suomen rakentamismääräyskokoelma

Rakentamismääräyskokoelman määräykset ovat velvoittavia. Ohjeet sen sijaan eivät ole velvoittavia, vaan muitakin kuin niissä esitettyjä ratkaisuja voidaan käyttää, jos ne täyttävät rakentamiselle asetetut vaatimukset.

Rakentamismääräyskokoelman määräykset koskevat uuden rakennuksen rakentamista. Rakennuksen korjaus- ja muutostyössä määräyksiä sovelletaan, jollei määräyksissä nimenomaisesti määrätä toisin, vain

⁷ PSC, Personal Security Clearance, henkilöturvallisuustodistus

siltä osin kuin toimenpiteen laatu ja laajuus sekä rakennuksen tai sen osan mahdollisesti muutettava käyttötapa edellyttävät.

Rakennustuotteille, joille on asetettu vaatimuksia rakentamismääräyskokoelmassa, voidaan myöntää tyyppihyväksyntä. Tyyppihyväksyntäasetukset julkaistaan omana erillisenä sarjanaan määräyskokoelmassa.

Kokoelman rakenne:

A Yleinen osa

B Rakenteiden lujuus

C Eristykset

D LVI JA energiatalous

E Rakenteellinen paloturvallisuus

F Yleinen rakennussuunnittelu

G Asuntorakentaminen

Eurokoodit (ympäristöministeriön asetus muutoksineen Eurocode-standardien soveltamisesta talonrakentamisessa)

Liite 10: Esimerkkejä valtionhallinnon toimipisteiden turvallisuusvyöhykejaottelusta

Alla olevaan taulukkoon on koottu joitakin tyypillisiä valtionhallinnon toimitilaympäristöjä ja niiden turvallisuusvyöhykejaotteluja. Taulukon esitys on suuntaa antava ja jokaisen ympäristön vyöhykejako on syytä määrittää tapauskohtaisesti riskiympäristön ja tiloissa käsiteltävän tiedon suojaustason huomioon ottaen.

KIINTEISTÖOSA	KÄYTTÖESIMERKKI	TURVALLISUUSVYÖHYKE				JULKINEN TILA TAI ALUE	HUOM.
		VIHREÄ ST IV	ORANSSI ST III	KELTAINEN TL III	SININEN ST II		
SIJOITTUMINEN	Toimitilarakennuksen sijoituspaikka					x	
	Vedenottamo	x					
	Laiturit	x				x	
ALUE	Julkinen alue					x	esim. kulkuväylät, P-paikat
	Huoltopiha	x					
	Poliisin/PV:n piha-alue	x					
	Virka-autojen pysäköinti	x					
	Varusmieskoulutusalueet	x					
	Esikunta-alueet	x				x	
	Teknisesti valvottu alue	x	x				
RAKENNUS	Toimistorakennukset	x				x	
	Varastot	x				x	
	Kasarmirakennukset	x					
	Asuintalot					x	
	Rajavartioasemat, rajanylityspaikat	x					
	Satamat	x				x	
	Polttoaineasemat ja -varastot	x					

TILARYHMÄ	Asiakaspalvelu- ja vastaanottotilat	x				x	
	Yleiset toimistotilat	x					
	Ylimmän johdon neuvottelutilat		x	x	x		
	Operatiiviset neuvottelutilat			x	x		
	Muut neuvottelutilat	x				x	
	Edustustilat	x				x	
	Erikoiskoulutustilat	x	x				
	Sosiaalitilat	x				x	
	Palvelinhotellit				x		
	Tietotekniset laitetilat	x	x	x	x		
	Valtakunnalliset johtamistilat				x		
	Viraston johtamistilat		x	x	x		
	Alueelliset johtamistilat		x	x			
	Kulunvalvontapisteet	x	x				
	Turvallisuusvalvomot		x	x			
	Kiinteistötekniset tilat	x	x	x			järjestelmien palvelu-alueet
	Varavoimakonetilat	x			x		toiminnan kriittisyys
	Arkisto ST III – ST I		x	x	x		
	Arkisto ST IV - JUL		x				
	Yleiset varastotilat	x				x	