VALTIOVARAINMINISTERIÖ

Toimitilojen tietoturvaohje

2/2013 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Toimitilojen tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä

2/2013 VAHTI

441 729
Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila /VM-julkaisutiimi

ISSN 1455-2566 (nid.)
ISBN 978-952-251-460-8 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-461-5 (PDF)

Juvenes Print - Suomen Yliopistopaino Oy, 2013

VALTIOVARAINMINISTERIÖ

Ohje

VM/1041/00.00.00/2013

17.5.2013

Ministeriöille, virastoille ja laitoksille

Toimitilojen tietoturvaohje

Toimitilojen tietoturvaohjeen (VAHTI 2/2013) tarkoituksena on osaltaan tukea tietoturvallisuudesta valtionhallinnossa annetun asetuksen (681/2010) täytäntöönpanoa.

Ohje antaa suuntaviivoja sekä rakentamissuunnittelulle, että olemassa olevien toimitilojen turvallisuutta parantaville ratkaisuille. Ohje edistää salassa pidettävän tiedon säädösten ja linjausten mukaista käsittelyä ja säilytystä valtionhallinnossa. Ohje vahvistaa osaltaan valtionhallinnon tietoturvallisuuden kehittämisestä annetun valtioneuvoston periaatepäätöksen (26.11.2009) toimeenpanoa ja antaa lisäksi perusteita virastokohtaisten sovellusohjeiden laatimiselle.

Ohje on valmisteltu valtiovarainministeriön asettaman ja johtaman Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) toimeksiannosta ja ohjauksessa. Ohje tukee ja täydentää laajaa olemassa olevaa VAHTI-ohjeistoa. Ohje korvaa Tietoteknisten laitetilojen turvallisuussuosituksen (VAHTI 1/2002).

Ohje auttaa organisaatioita ottamaan huomioon lakisääteiset ja kansainvälisten turvallisuussäännöstöjen asettamat toimitilaturvallisuuden vaatimukset. Organisaatioita pyydetään käyttämään ohjetta hyväksi erityisesti toimitilojen muutostilanteissa.

Lisätietoja antaa tietoturvallisuusasiantuntija Aku Hilve, JulkICT-toiminto.

Hallinto- ja kuntaministeri — Henna Virkkunen

Yksikön päällikkö — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: *Toimitilojen tietoturvaohje (VAHTI 2/2013)*

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

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 ja kyberturvallisuuden linjaukset. 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 tulosohjausta.

VAHTI edistää hallitusohjelman ja hallituksen muiden keskeisten linjausten, Yhteiskunnan turvallisuusstrategian (YTS), Julkisen hallinnon ICT-strategian, Suomen kyberturvallisuusstrategian, valtioneuvoston huoltovarmuuspäätöksen sekä valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä 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 tietoturvaohjeisto (www.vm.fi/vahti).

Tiivistelmä

Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) edellytetään 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. Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttää, että Suomi valtiona noudattaa toiminnassaan niitä turvallisuusvelvoitteita, joihin se kansainvälisen yhteistyön myötä on sitoutunut. Velvoitepohjana toimivat näissä tapauksissa tyypillisesti joko tietoturvallisuutta säätävät valtiosopimukset tai Suomen valtiona muilla tavoin hyväksymät kansainväliset turvallisuussäännöstöt.

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 arvioi elinkeinonharjoittajan turvallisuustason. Tätä tarkoitusta varten on laadittu viranomaisten ja elinkeinoelämän yhteistyönä kansallinen turvallisuusauditointikriteeristö (KATAKRI), jonka ylläpidosta vastaa sisäasiainministeriö. Auditointikriteeristö sisältää yksityiskohtaisia toimitilaturvallisuusvelvoitteita, joiden sisältö on mahdollisimman pitkälle otettu huomioon myös tässä ohjeessa.

Ohjetta laadittaessa on huomioitu VAHTI:n vuonna 2012 julkaisema ICT-varautumisen vaatimukset ohje, jonka sisältöä tämä ohje täydentää yksityiskohtaisemmilla vaatimuksilla. Osa valtionhallinnon toimijoista on laatinut hallinnonalakohtaisia fyysisen turvallisuuden tai toimitilaturvallisuuden vaatimusasiakirjoja. Näiden asiakirjojen vähimmäisvaatimukset on pyritty ottamaan huomioon tätä ohjetta laadittaessa. Salassa pidettävän tiedon siirtyessä valtionhallinnon toimijalta toiselle yhteisillä turvallisuusvaatimuksilla varmistetaan tiedon suojaustason mukainen oikea käsittely.

Tämän ohjeen sisältämät linjaukset on suositeltavaa ottaa käyttöön hallinnonaloja ja virastoja koskevina soveltamisohjeina sekä suunniteltaessa uusia tietoteknisiä laitetiloja. Tietoteknisten laitetilojen 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, Aku Hilve (puheenjohtaja), 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, Isto Turpeinen, Iina Vuorialho, Erkki Väätäinen ja Juha Åberg. Työssä käytettiin konsulttina Kesec Ky:tä.

Sisältö

1 Yleistä

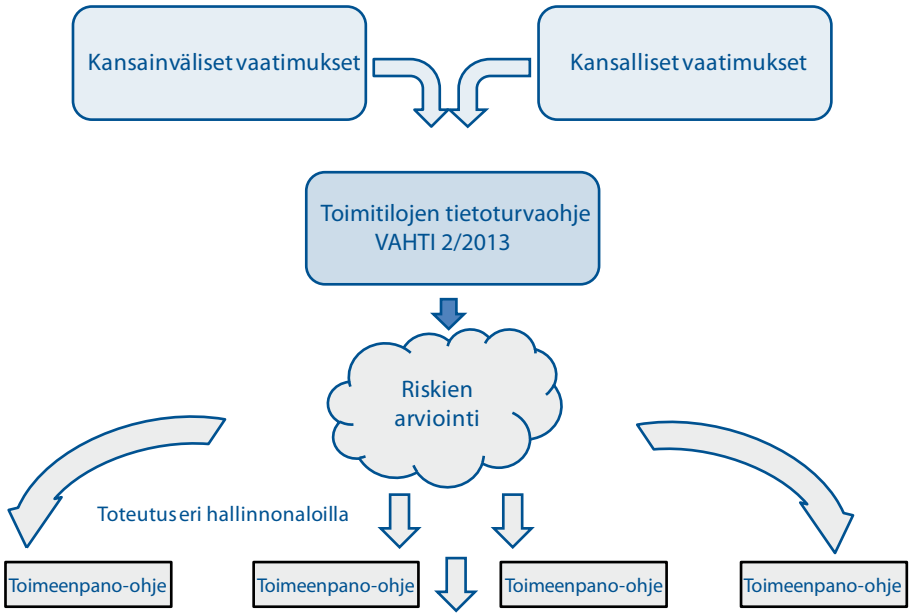
1.1 Ohjeen tausta, tarkoitus ja tavoite

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. Tässä ohjeessa keskitytään toimitilojen tietoturvavaatimuksiin, eikä esim. henkilö- ja rakenneturvallisuuden vaatimuksiin, jotka määräytyvät eri lakien, määräysten ja ohjeiden mukaisesti. Kyseiset vaatimukset on kuitenkin syytä huomioida myös turvallisuusrakentamisessa osana rakenne- ja rakennussuunnittelun perusteita.

Ohjetta laadittaessa on pyritty ottamaan huomioon ratkaisujen kustannustehokkuus ja vakioitujen toimintamallien ja rakenneratkaisujen avulla toivottavasti saavutettavat säästöt. Toimitilojen turvallisuus on keskeinen tekijä useiden tietoturvavaatimusten täyttymiseksi. Lähtökohtana ohjeen soveltamiselle on, että viranomainen on luokitellut tietonsa oikein. Väärä luokitus voi johtaa huomattaviin lisäkustannuksiin.

Tässä ohjeessa ja sen liitteissä esitetään kaikkien valtionhallinnon toimitilojen fyysisen turvallisuuden yleiset vaatimukset. Pääpaino ohjeessa on salassa pidettävien tietojen suojaustasojen IV, III ja II mukaisten tietojen käsittelyn ja säilytyksen asianmukaisessa toteuttamisessa. Vastuuviranomaiset esittävät erikseen vaatimukset niiden toimitilojen turvallisuudesta, joissa käsitellään muutoin kuin satunnaisesti suojaustasoon I kuuluvia tietoja.

Toimitilojen tietoturvaohjeen sovellusperiaate



2 Lainsäädäntö 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 8.

2.1 Lait

Viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999; jäljempänä julkisuuslaki) on julkisuusperiaatteen lisäksi säännökset yleisimmin sovellettavista salassapitosäännöksistä. Salassapitovelvollisuus merkitsee paitsi kieltoa antaa tietoaineistoista tietoa sivullisille ja ilman laissa olevaa oikeutta, myös velvollisuutta ennalta ehkäistä aineistoihin kohdistuvat väärinkäytökset. Viranomaisen on toiminnassaan noudatettava hyvää tiedonhallintatapaa huolehtimalla tietoaineistojensa saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä (18 §). Laissa on säädetty valtioneuvostolle oikeus säätää tietoturvallisuusvaatimuksista mukaan lukien toimitilojen turvallisuutta koskevat vaatimukset.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) koskee turvallisuusluokiteltuja tietoaineistoja, jotka Suomen viranomainen on saanut Suomea sitovan kansainvälisen tietoturvallisuussopimuksen tai kansainvälisen säädöksen (esim. EU-asetus) perusteella. Tällaiset tiedot on pidettävä aina salassa. Laissa on myös säännökset yhteisöturvallisuusselvityksestä, joka nykyisin kuitenkin voidaan tehdä vain ulkomaan viranomaisen pyynnöstä tai kun on kyse julkisista puolustus- ja turvallisuushankinnoista annetussa laissa 1531/2011 tarkoitetuista hankinnoista. Puolustus- ja turvallisuushankinnan tapauksessa yhteisöturvallisuusselvitysmenettelyssä voidaan selvittää esimerkiksi sopimuskumppanin toimitilojen tietoturvallisuutta. Lain mukaisia tehtäviä hoitavat kansallinen turvallisuusviranomainen (NSA[1]), joka toimii ulkoasiainministeriössä sekä määrätyt turvallisuusviranomaiset (suojelupoliisi, Pääesikunta, puolustusministeriö ja Viestintävirasto).

Laki turvallisuusselvityksistä (177/2002) sisältää säännöksen henkilön taustan selvittämisestä hänen luotettavuutensa arvioimiseksi. Lakia ollaan uudistamassa ja uuden turvallisuusselvityslain on suunnitelmien mukaan tarkoitus tulla voimaan kesäkuussa 2014.

[1] National Security Authority

2.2 Tietoturvallisuusasetus

Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Tietoturvallisuusasetuksen mukaan tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava muun muassa siitä, että asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja. Yleiset tietoturvallisuusvelvoitteet koskevat valtionhallinnon viranomaisia siinäkin tapauksessa, että ne eivät luokittele tietoaineistojaan. Tietoturvallisuuden perustasoa koskeva 5 § on siis kaikkia valtionhallinnon viranomaisia velvoittava säädös.

2.3 Ohjeet

2.3.1 Ohje tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)

Tietoturva-asetuksen täytäntöönpanoa edistää ja tukee VAHTI-ohje 2/2010 (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta), joka konkretisoi toimitilaturvallisuuden perusteita. Ohje kiinnittää lisäksi huomiota valvonta- ja kiinteistöautomaatiojärjestelmien tietoturvallisuuteen, tilojen äänieristykseen sekä sähkömagneettisen hajasäteilyn haittojen eliminoimiseen (luku 4.4).

Tämä VAHTI 2/2013-ohje täydentää VAHTI 2/2010 –ohjeen fyysisen turvallisuuden vaatimusmäärittelyjä.

2.3.2 Sisäverkko-ohje (VAHTI 3/2010)

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

2.3.3 ICT-varautumisen vaatimukset (VAHTI 2/2012)

Tietoteknisten ympäristöjen varautumista ja jatkuvuuden hallintaa ohjaamaan laadittu VAHTI-ohje 2/2012 kuvaa erityisesti varautumisen tueksi laadittuja ICT-vaatimusperusteita. Ohje antaa strategisia suuntaviivoja myös fyysisen turvallisuuden vaatimuksille.

2.3.4 Kansallinen turvallisuusauditointikriteeristö (2011)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on laadittu elinkeinonharjoittajien turvallisuustason tarkastamista varten silloin, kun viranomainen joutuu todentamaan vaaditun tason 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 tietoturvallisuusvelvoitteen 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.

Tässä VAHTI-ohjeessa esitetyt vaatimukset on laadittu mahdollisimman yhdenmukaisiksi KATAKRI:ssa esitettävien viranomaisvaatimusten kanssa. Mikäli ristiriitaisuuksia esiintyy, vaatimusten tulkinnasta on syytä keskustella toteuttavan ja (mahdollisen) tarkastavan tahon välillä etukäteen. Tämä ohje palvelee turvallisuusauditoinnin vaatimusperusteiden muodostamisessa siltä osin, kun auditointi kohdistuu valtionhallinnon toimitiloihin. On huomattava, että KATAKRI kattaa myös muita turvallisuuden osa-alueita.

2.3.5 Ohjeiden merkityksestä

Edellä kuvatut ja nyt annettava ohje eivät ole oikeudellisesti sellaisenaan sitovia, vaan niiden on tarkoitus ohjata viranomaisia niiden toteuttaessaan laissa ja asetuksissa säädettyjä velvoitteita.

Ohjeiden tarkoituksena on luoda yhdenmukaiset menettelyt valtionhallinnossa, mikä osaltaan myös yksinkertaistaa ja helpottaa viranomaisten välistä salassa pidettävien tietojen vaihtoa.

2.4 Euroopan unionin turvallisuusregiimi (2011)

Euroopan unionin neuvosto on antanut päätöksen turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2011/292/EU). Neuvostossa kokoontuneiden EU:n jäsenvaltioiden välillä on tehty sopimus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta. Sopimus on hyväksytty eduskunnassa ja sopimuksen määräysten täytäntöön panemiseksi on säädetty laki (224/2012).

Edellä mainitut säännöstöt on syytä tuntea viranomaisissa, joissa EU:n luokiteltua tietoa käsitellään.

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).

2.5 Naton turvallisuussäännöstö (2002)

Suomi on tehnyt Naton kanssa tietoturvallisuussopimuksen vuonna 1994 ja sitä täydentävän järjestelyn vuonna 2012[2]. Suomi noudattaa kumppanuusyhteistyössä järjestelyssä olevia määräyksiä sekä Naton tietoturvallisuusvaatimuksia niiltä osin kuin niitä sovelletaan kumppanimaihin.

2.6 Muu tausta-aineisto

Valtionhallinnon toimitilojen tietoturvaturvaohjetta laadittaessa on käytetty hyväksi edellä mainittujen säädösten ja säännöstöjen lisäksi 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.

[2] sopimussarja 7-8/2013

3 Turvallisuusvyöhykkeet

Turvallisuusvyöhykkeet ovat rajattuja alueita, joiden ulkokuoriin ja niiden aukkojen turvallisuuteen kohdistuu erityisiä vaatimuksia.

Viranomaisten käytössä oleviin toimitiloihin voi sisältyä myös julkisia tiloja (esimerkiksi aula- ja yleisöpalvelutilat). Näihin tiloihin ei kohdistu erityisiä turvallisuusvaatimuksia.

3.1 Määräytymisperusteet

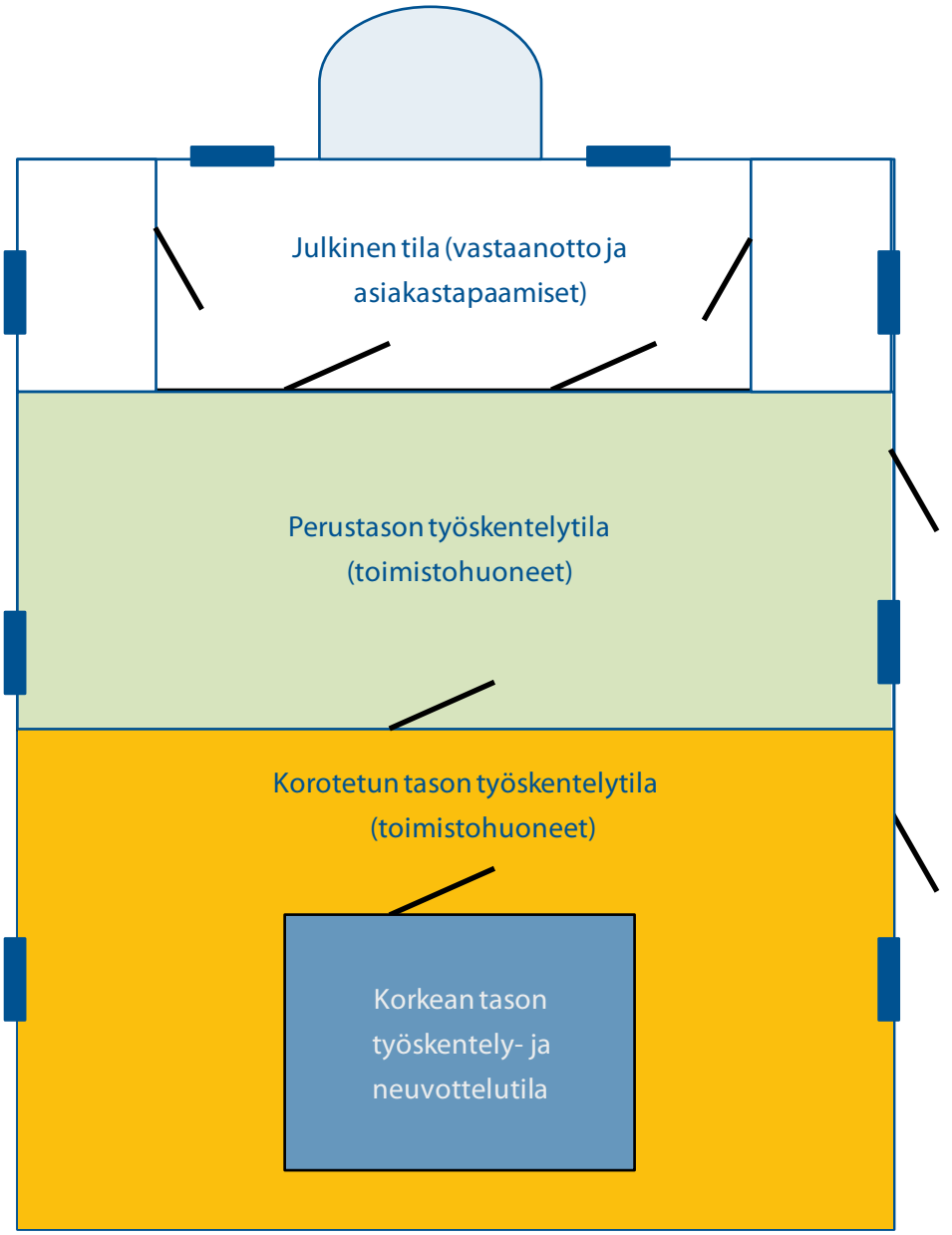
Turvallisuusvyöhykejako perustuu sekä kansalliseen lainsäädäntöön (TTA 14 §) että kansainvälisten velvoitteiden toteuttamiseen[3]. Vyöhykemäärittelyyn vaikuttavat oleellisesti riskianalyysin pohjalta tehdyt uhka-arviot, salassa pidettävän tiedon suojaustaso ja se, kuinka tietoa käsitellään (sähköisesti/paperiasiakirjoina/suullisesti) sekä jätetäänkö tieto tilaan säilytykseen vai ei.

Organisaation tulee analysoida toimintaympäristöönsä kohdistuvat riskit, jotta normeissa ja muissa säännöstöissä kuvatut turvallisuusvyöhykkeet saadaan nimettyä. Sen tulee myös arvioida minkä suojaustason asiakirjoja milläkin vyöhykkeellä käsitellään ja/tai säilytetään. On myös arvioitava miten kunkin 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 voidaan 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 on syytä huomioida **erityisesti uudiskohteiden suunnittelussa ja rakentamisessa**. Liitteessä 6 on esitetty projektikaavio siitä, miten toimitilaturvallisuus uudisrakennushankkeessa tulisi huomioida. Liitteeseen 3 on koottu joitakin esimerkkejä valtionhallinnon toimitilojen turvallisuusvyöhykejaotteluista. Rakennussuunnitteluvaiheessa on kustannustehokasta jättää kunkin turvallisuusvyöhykkeen sisään toiminnan luonteen mukaisesti kohtuulliseksi katsottava laajennusvara.

[3] kansainväliset tietoturvallisuussopimukset, ks. FINLEX

Esimerkki toimipisteen turvallisuusvyöhykekartasta



3.1.1 Tilojen luokittelu suojaustasoihin

Turvallisuusvyöhykejako johdetaan tiedon luokitteluperusteista ottaen huomioon organisaation toiminnan mukanaan tuomat muut tilaturvallisuuteen liittyvät vaatimukset. Julkisuuslain 24 §:ssä on määritelty, mitkä asiakirjat ovat salassa pidettäviä. Tietoturvallisuusasetuksen 8 §:ssä on säännökset salassa pidettävien asiakirjojen ja tietojen luokituksen perusteista. Suojaustasoluokittelun perusteet on esitetty 9 §:ssä. Asetuksen 11§:ssä säädetään, missä tapauksissa suojaustasoluokiteltuun asiakirjaan voidaan tehdä turvallisuusluokkaa osoittava merkintä (ks. liite 9).

3.1.2 Valtionhallinnon toimitilojen turvallisuusvyöhykejako

Valtionhallinnon toimitilat jaetaan turvallisuusvyöhykkeisiin käsiteltävän ja säilytettävän tiedon turvaamiseksi asiakirjojen suojaustasoluokittelun perusteella. Julkisten asiakirjojen käsittely ei edellytä käsittely-ympäristöltään erityisiä turvallisuustoimia. Sama pätee myös suojaustason IV tietojen satunnaiseen käsittelyyn. Käsitteellä ”tila” tarkoitetaan tässä ohjeessa joko yksittäistä huonetta tai niistä muodostuvaa kokonaisuutta.

Mikäli tilassa käsitellään tai säilytetään muutoin kuin satunnaisesti suojaustason IV tietoja, on toimitilojen syytä täyttää liitteessä 1 esitetyt VIHREÄN turvallisuusvyöhykkeen vaatimukset.

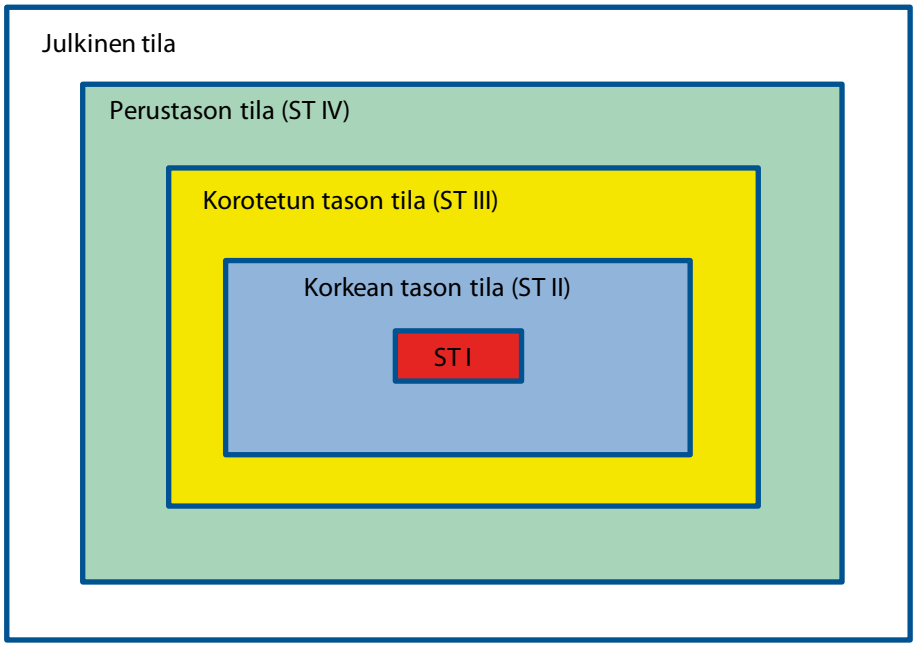
Toimitilojen, joissa muutoin kuin satunnaisesti käsitellään tai säilytetään suojaustasoon III luokiteltuja tietoja, on syytä täyttää liitteessä 1 esitetyt KELTAISEN turvallisuusvyöhykkeen vaatimukset.

Toimitilassa, jossa muutoin kuin satunnaisesti käsitellään suojaustasoon II luokiteltuja tietoja, on syytä täyttää liitteessä 1 esitetyt SINISEN turvallisuusvyöhykkeen vaatimukset.

Toimitilan, jossa muutoin kuin satunnaisesti käsitellään suojaustasoon I luokiteltuja tietoja, tulee täyttää viranomaisten 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

Rakentamista 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. Rakenteilla olevaa kohdetta on syytä käsitellä turvallisuusvaatimusmielessä tilana silloin, kun tavoitteena on käsitellä tulevissa tiloissa salassa pidettävää tietoa ja tilojen toteutus on edennyt sellaiseen vaiheeseen, että oikeudettomien liikkuminen tiloissa vaarantaa tiedon salassa pysymisen.

Turvallisuusvyöhykkeiden hallinnassa hyödynnetään tarvittaessa valtionhallinnon tilahallinnan tietojärjestelmää (HTH), ottaen kuitenkin huomioon ne lainalaisuudet (suojaustasot), jotka turvallisuusvyöhykemerkinnät sisältävien pohjapiirrosten käsittelylle asetetaan.

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 turvallisuusauditointikriteeristössä (KATAKRI) esitetään huomattavasti yksityiskohtaisempia vaatimuksia. Hallinnonalojen sisäiset tilaturvallisuusvaatimukset menevät osin KATAKRI:akin tarkemmalle tasolle.

Tilojen lukitus, kulunvalvonta ja henkilöstön valvonta

Tilojen lukituksen yksityiskohdat on määritelty ainoastaan kansallisissa vaatimuksissa. Vaatimuksena on, että tilojen lukituksen pitää olla järjestetty siten, ettei tilaan pääse oikeudettomia. Lukitusta käytetään yhtenä kulunvalvonnan elementtinä ja se on keskeisin vyöhykejaon mahdollistava tekijä.

Korotetun tai korkean tason käsittelytiloihin ei tule päästä ilman myönnettyä oikeutta ja sähköistä kulunvalvontaa. Vieraat tai huolto- ja siivoushenkilöstö eivät saa liikkua korotetun tai korkean tason tiloissa ilman valvontaa.

Henkilöiden tunnistus

Asiattomien pääsy työtiloihin tulee estää. Turvallisuusvyöhykkeelle saapuvan henkilön tunnistamista edellytetään perustasolta lähtien. Korkeammilla turvallisuustasoilla henkilön liikkumista turvallisuusvyöhykkeellä valvotaan lokikirjauksilla.

Ulkoisten palveluntuottajien satunnaista henkilöstöä käsitellään kuten vieraita. Palveluntuottajien säännöllinen kiinteistönhoito-, -huolto- ja siivoushenkilöstö hyväksytetään etukäteen yksikön turvallisuusvastaavalla, joka käynnistää tarvittaessa henkilön taustaselvityksen hakemisen vastuuviranomaiselta. Vakituinen henkilöstö käyttää kuvallista henkilötunnistetta ja vihreälle turvallisuusvyöhykkeelle saapuessaan henkilökohtaista kulkutunnistetta tai avainta. Itsenäinen pääsy ylemmille turvallisuusvyöhykkeille ratkaistaan toimitilakohtaisesti ja kirjataan yksikön turvallisuusohjeistukseen (hyväksyntä ja allekirjoitus). Sinisen turvallisuusvyöhykkeen kulkutunnisteita tai avaimia ei luovuteta vierailleeikä palveluntuottajien henkilöstölle (ns. ovikelloperiaate).

Tietojen ja asiakirjojen säilytys

Tietojen ja asiakirjojen säilytysmenetelmiin kohdistuu suoria kansainvälisiä ja kansallisia vaatimuksia[4]. Suojaustason IV tietoa voidaan säilyttää lukitussa kaapissa tai laatikossa, kun tila on muuten riittävästi valvottu. Suojaustasoon III kuuluva tieto vaatii säilytyspaikakseen vaatimusten mukaisen kassakaapin tai holvin[5]. Sama vaatimus pätee suojaustason II tietoon.

Hajasäteily

Sähkömagneettisen hajasäteilyn uhka on kansainvälisten vaatimusten mukaisesti otettava huomioon jo korotetun tason tiedonkäsittely-ympäristöissä. Kansallinen ohjeistus antaa 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 viran-

[4] arkistolaki, ks. liite 8

[5] ks. liite 1, kohta 19

omaisena Viestintäviraston NCSA-FI -yksikkö. Hajasäteilyn vastatoimet voidaan jakaa karkeasti kahteen menetelmään: laitteiden suojaaminen metallikoteloinnilla tai työskentelytilan suojaaminen rakenteellisilla ratkaisuilla. Tavoitteena on, ettei salassa pidettävää tietoa pääse vuotamaan tilasta ulos sähkömagneettisen säteilyn välityksellä 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 esimerkiksi kameravalvonnasta. Tiiviissä kaupunkiympäristössä aidan rakentaminen on usein mahdotonta. Tällöin on syytä kiinnittää entistäkin suurempaa huomiota organisaation ulkokuoren suojaamiseen.

3.3 Tietotekniset laitetilat

Tietoteknisiä laitetiloja[6] koskevat yleisellä tasolla samat vaatimukset kuin vastaavan tasoiseksi määritettyä normaalia toimitilaa. Laitetilojen turvallisuusrakentamisessa on syytä painottaa tiedon käytettävyyteen tähtääviä toimia enemmän kuin muissa toimitiloissa Tietoteknisille laitetiloille asetettavat erillisvaatimukset on tuotu yksityiskohtaisesti esille liitteessä 4. Liitteeseen 1 on koottu tärkeimmät teknisten laitetilojen turvallisuusvaatimukset (vaatimukset 38-56).

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 mahdolliselle yhteiselle turvallisuusvyöhykkeelle. Yhteiskäyttötilojen ominaisuuksista ja tilojen turvallisuusvaatimuksista sovitaan – esimerkiksi vuokrauksen yhteydessä – ennen käyttöönottoon tähtäävien muutostöiden aloittamista. On toivottavaa ja kustannustehokasta pyrkiä ryhmittelemään perustasoa korkeammat tilat erilliseksi tilaryhmäksi[7].

---

[6] määritelmä: ks. liite 9

[7] Asiakaspalvelu 2014 –hankkeen (Hallinnon ja aluekehityksen ministerityöryhmä) linjausten huomioiminen soveltuvilta osin

3.5 Merkitseminen

Turvallisuusvyöhykkeet voidaan erottaa toisistaan esimerkiksi työntekijöiden tunnistamin värikoodein (ks. 3.1.2). Turvallisuusvyöhykkeiden merkitsemisessä merkintöjen fyysinen näkyvyys ei ole itseisarvo. Turvallisuusvyöhykkeiden 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 yhdessä organisaationsa kanssa 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 asianmukaisesti huomioon ottaen ilman erillisiä fyysisiä turvallisuustoimia. Mikäli vähintään suojaustasoon III kuuluvaa aineistoa käsitellään tai säilytetään organisaation toimitilojen ulkopuolella, ei kyseisen tilan turvallisuustoimia voida mitoittaa satunnaistyöskentelyn mukaisiksi. Mahdolliset jäännösriskit täytyy hyväksyä tapauskohtaisesti ja kirjallisesti työyksikön turvallisuusohjeistuksessa kuvatulla menettelyllä. Kuljetettaessa luokiteltuja tietoja pääasiallisen toimipisteen ja etätyöpisteen välillä, on huolehdittava tietoaineiston turvallisuudesta joko kuriiritoiminnan keinoin tai esimerkiksi salassa pidettävää tietoaineistoa sisältävien muistimedioiden asianmukaisella salauksella[8].

3.7 Liikkuva työ

Liikkuvaan työhön liittyy korostunut ja jatkuva uhka-arviointitarve. Käsiteltäessä vähintään suojaustasoon III luokiteltuja tietoja liikkuvassa työympäristössä[9], tulee hallinnonalan tai organisaation itsensä antaa asiasta erilliset fyysisen turvallisuuden soveltamisohjeet, jotka tähtäävät jäännösriskien minimoimiseen.

[8] toimivaltaisen viranomaisen (Viestintäviraston NCSA-FI) hyväksymät ratkaisut

[9] esim. poliisiautossa

3.8 Työturvallisuus

Tässä ohjeessa esitettyjä fyysisen turvallisuuden toimenpiteitä toteutettaessa tulee huolehtia siitä, etteivät tiedon turvaamiseen tähtäävät ratkaisut aiheuta henkilöturvallisuusriskejä. Toimitilojen turvallisuusvyöhykesuunnittelussa on syytä huomioida pelastusviranomaisten näkemykset kuitenkin siten, etteivät poistumisreitit ja savuntuuletuslohkot mahdollista oikeudetonta pääsyä alemmalta turvallisuusvyöhykkeeltä ylemmälle vyöhykkeelle.

3.9 Tilaturvallisuusjärjestelyjen toteutusvaihtoehtoja

Tietoturvallisuuden kokonaishallinnan kannalta on oleellista saavuttaa sellainen turvallinen työympäristö, joka vastaa keskeisiltä osiltaan tunnistettuihin uhkiin. Mikäli jokin vaatimuksista jää täyttymättä, voidaan puute monesti paikata jollakin korvaavalla järjestelyllä. Esimerkiksi ympäröivän alueen varustaminen kameravalvonnalla ja muilla ilmaisimilla antaa mahdollisuuden suurempaan vasteaikaan luvatonta tunkeutumista vastaan. Näin itse toimitiloihin kohdistuu vähemmän suojausvaatimuksia. Korvaavilla menettelyillä voidaan joissakin tapauksissa saavuttaa merkittäviä kustannussäästöjä. Turvallisuusauditoijan ammattitaidon yksi mittapuu onkin tällaisten, kenties kokonaan kirjattujen vaatimusten ulkopuolisten lisäkontrollien tuoman kokonaishyödyn tunnistaminen ja arviointi osana turvallisuustason kokonaisvaatimusten täyttymistä.

Toimitilavyöhykkeitä määritettäessä on syytä ottaa huomioon työyksikön toiminnan luonne, muutenkin kuin riski- ja uhka-arvioihin perustuen. Onko salassa pidettävää tietoa tarpeen käsitellä kaikissa tiloissa? Voidaanko työprosessien muutoksilla poistaa kokonaan joidenkin turvallisuusvaatimusten toteutustarve? Onko työntekijän päästävä lukemaan esimerkiksi suojaustason II asiakirja suoraan tietojärjestelmästä, vai voidaanko asiakirjasta ottaa paperikopio, jolloin hänen työtilaansa ei ehkä kohdistuisi vaatimuksia sähkömagneettiselta hajasäteilyltä suojautumiseksi? Vaatimusten toteuttamiseksi on usein löydettävissä vaihtoehtoisia ratkaisumalleja.

4 Rakenteelliset turvallisuusvaatimukset

Yksityiskohtaiset alueen ja rakenteiden turvallisuusvaatimukset on esitetty liitteessä 1 (aluetta koskevat vaatimukset 1-6, rakenteita koskevat vaatimukset 7-21).

4.1 Alue

Sen lisäksi, mitä alaluvussa 3.2 on esitetty, on tämän ohjeen perusteella laadittavassa työyksikön turvallisuusdokumentaatiossa syytä ottaa huomioon toimitilaa ympäröivän alueen turvallisuuteen liittyen seuraavaa:

- uhka-arvioon perustuen liikkumista alueella voidaan rajata aidoilla, porteilla ja ajoesteillä
- uhka-arviossa esille tulleet kriittiset kohteet on syytä kattaa 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 seikat kuin edellisessä kohdassa.

4.2 Ulkopinnat

Toimitilarakennuksen ulkopinnan, ala- ja yläpohja mukaan lukien, tulee olla vahvuudeltaan sellainen, ettei siitä pääse havaitsematta tunkeutumaan läpi toimipaikan turvallisuusdokumentaatiossa määritettynä vasteaikana. Vahvana rakenteena voidaan pitää teräsbetoniseinää tai metallilevyillä päällystettyä betonivaluharkkoseinää. Seinäelementtejä ei saa voida irrottaa tilan ulkopuolelta. Työmenetelmiä valittaessa on huomattava, että esimerkiksi oikein raudoitettu valuharkkoseinä antaa paremman suojan, kuin metallilevyllä päällystetty vääriä menetelmiä käyttäen tehty tavanomainen valuharkkoseinä. Turvallisuusviranomaiset antavat tarvittaessa lisätietoa hyväksyttävistä rakenneratkaisuista.

4.3 Sisäseinät

Sisäseinien rakennevaatimukset riippuvat ratkaisevasti muusta turvallisuustoteutuksesta. Mikäli sisäseinä toimii yleisen tilan ja korotetun tai korkean (KELTAINEN/SININEN) tason tilan jakajana, sen rakenteelle asetetaan suuremmat vaatimukset kuin valvottujen turvallisuusvyöhykkeiden väliselle sisäseinälle. Seinän rakenteessa on oleellista riittävän (kumulatiivisen) vasteajan[10] muodostuminen tai sen osana toimiminen.

Äänieristys on merkittävä seikka 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. Salassa pidettävät asiat eivät saa suusanallisen keskustelun välityksellä kulkeutua ymmärrettävinä turvallisuusvyöhykkeen ulkopuolelle. Myös tällaisen tilan ilmanvaihto- ja kaapelikanavat on varustettava puheääntä tehokkaasti vaimentavilla ääniloukuilla, joita on kaupallisesti yleisesti saatavilla.

4.4 Ala- ja yläpohjat

Ala- ja yläpohjan rakenteisiin pätee sama kuin sisäseinän rakenteisiin; rakennevaatimuksiin vaikuttaa ylä- ja alapuolisen tilan kuuluminen tai kuulumattomuus kohteen oman valvonnan piiriin. Niiden tilojen, joissa käsitellään enemmän kuin satunnaisesti suojaustasojen II tai I tietoja, lattiarakenteessa suositellaan käytettävän esimerkiksi erillistä pintavalua tyypillisen 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, mikäli kuilut ulottuvat tiloihin, joissa käsitellään suojaustasojen II tai I tietoja useammin kuin satunnaisesti.

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 vähintään samanlaisen vasteajan kuin turvallisuusvyöhykkeen muu ympäröivä rakennekehä (seinät, ylä- ja alapohja).

[10] määritelmä: ks. liite 9

4.5.1 Materiaalivaatimukset

Tilat, joissa rutiininomaisesti käsitellään suojaustason III 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 halliovissa, on vaatimuksena sankaa suojaava rakenne.

Lukkojen sarjoitus tulee suunnitella kohteen käyttötarkoituksen mukaisesti. Avainten ja kulkutunnisteiden 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 poistumistiereitit. Pelastuslaitoksen pääsy kohteelle on sovittava pelastusviranomaisen kanssa. Pelastuslaitoksen reittiavaimet säilytetään valvotuissa putkilukoissa. Kiinteistön ulkopuolella olevalla reittiavaimella ei saa päästä suoraan korotetun tai korkean vyöhykkeen (KELTAINEN/SININEN) tiloihin, vaan suunnitellun hyökkäysreitin varrelle, kiinteistön sisälle järjestetään toinen valvottu putkilukko, joka mahdollistaa palokunnan pääsyn korotetun tai korkean vyöhykkeen tiloihin.

KELTAISELLE tai SINISELLE turvallisuusvyöhykkeille johtavat ovet on varustettava sähköisellä kulunvalvonnalla.

KELTAISELLE tai SINISELLE turvallisuusvyöhykkeelle johtavat, turvallisuusvyöhykkeiden väliset luukut tai hätäpoistumistiet on varustettava avattavin kalterein ja valvottava tunkeutumisen ilmaisujärjestelmillä. Toteutus ei saa estää luukun tai hätäpoistumistien toimintaa.

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 sekä karmien lujuuden ja lukituksen osalta niin kestäviä, että ne antavat turvallisuuden kokonaisjärjestelyt huomioon ottaen riittävän pitkän vasteajan tunkeutumisyritystä vastaan. Turvallisuusviranomaiset antavat tarvittaessa asiasta yksityiskohtaisia lisätietoja.

4.6.1 Turvalasit ja kalvot

Tavallinen huonekorkeus on noin kolme metriä, mistä syystä toisen 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 tietoa, tulee ikkuna-aukkojen osalta varustaa kaltereilla tai vaaditut normit täyttävällä turvalasilla (liite 1). Tilojen, joissa säilytetään suojaustason IV tietoa, ikkunat voidaan varustaa riskianalyysin tuloksiin perustuen joko turvalasilla tai turvallisuusluokan 2 turvakalvolla.

4.6.2 Karmit ja kiinnitys

Ikkunoiden kiinnitys karmiin ja karmin kiinnitys ympäröivään seinärakenteeseen on ratkaisevaa ikkuna-aukkojen kautta tapahtuvan tunkeutumisen estämiseksi. Ikkunan lukituksen ja salpojen tulee olla vahvat. Jos tilassa käsitellään enemmän kuin satunnaisesti vähintään suojaustason III tietoa, ikkuna-aukon karmirakenteen tulee olla sellainen, ettei turvalasia pystytä irrottamaan karmista eikä karmia pystytä kevyillä käsityökaluilla irrottamaan seinärakenteesta. Yleensä tämä vaatimus saavutetaan käytettäessä teräsbetoniseinään vahvasti kiinnitettävää teräskarmia.

4.6.3 Erillisvaatimukset

Ikkunapinnat tulee peittää verhoilla tai kaihtimilla silloin, kun tilassa käsitellään turvallisuusluokiteltua tietoa ja on mahdollista, että asiattomat voivat nähdä tilaan sisälle. Tietokoneiden näytöt on asetettava sellaiseen työskentelyasentoon, ettei käsiteltävä informaatio näy ulos.

Jos tilassa käsitellään vähintään suojaustason II salassa pidettävää tietoa, sinne johtavat ikkuna-aukot tulee rakentaa edellisessä kohdassa mainituin menetelmin vaikka tilaan johtava ikkuna-aukko sijaitsisi yli neljän metrin korkeudessa. Ikkunapinnoissa suositellaan lisäksi käytettävän tunkeutumisilmaisinta (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 kätketyt tallentimet tai salakuuntelulähettimet pyritään paikantamaan.

Valvontajärjestelyille asetettavat yksityiskohtaiset vaatimukset on esitetty liitteessä 1 (vaatimukset 30-37), jota on syytä käyttää yhdessä tässä luvussa esitettyjen täsmennysten ja kuvausten kera.

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 taulukon mukaisista vaatimuksista sen mukaisesti, mitä viranomaisten vasteaika-arvot kullekin suojauselementille (aita/seinä/ovi/ikkuna/kassakaappi) määrittävät. Vasteaika-arvot eivät ole julkista tietoa, mutta ne toimitetaan pyynnöstä niille viranomaisille, jotka päätyvät vasteaikalaskelmien käyttämiseen liitteessä 1 esitetyn pisteytysmallin sijasta. Käytettäessä vaatimusten tulkinnassa pisteytysmallia on huomattava, että mikäli reagoivan vasteen saapumisaika on kovin pitkä, on kokonaisratkaisussa käytettävä tätä epäkohtaa kompensoivia turvallisuusratkaisuja.

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 SINISEN turvallisuusvyöhykkeen turvallisuusvalvontaa täydentää tallentavalla kameravalvonnalla, joka on liitetty joko tunkeutumisen ilmaisujärjestelmään tai kuvan analyysiin perustuvaan ilmaisujärjestelmään. Kamerat on sijoitettava siten, ettei niiden kuvan 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[11]. Tapauskohtaisesti kameravalvonta saattaa edellyttää rekisteriselostemenettelyä[12]. Ennen kameravalvonnan käyttöönottoa on syytä huomioida mitä laki yksityisyyden suojasta työelämässä (759/2004) säätää kameravalvonnan osalta (5 luku). Valvontajärjestelyjen osalta on syytä ottaa huomioon lisäksi yksityisistä turvallisuuspalveluista annetun lain (282/2002) säännökset.

Korotetun ja korkean tason tilat (KELTAINEN tai SININEN turvallisuusvyöhyke) on varustettava kulunvalvonnalla siten, että vain oikeutetut henkilöt pääsevät turvallisuusvyöhykkeen sisälle ja heidän kulkunsa turvallisuusvyöhykkeelle ja sieltä ulos voidaan myöhemmin todentaa lokitietojen avulla. Korkean tason turvallisuusvyöhykkeelle mentäessä tulee käyttää kaksoistunnistusta (esimerkiksi pääsykoodi ja sähköinen tunniste). Korkeammalle turvallisuusvyöhykkeelle johtavan kulunvalvotun oven ovipäätteen tai ovea ohjaavan keskittimen tai väyläohjaimen ei pidä sijaita alemman turvallisuusvyöhykkeen alueella ilman riittäväksi katsottavaa laitesuojausta. Turvallisuusvyöhykkeiden pääsyoikeuksia, tunkeutumisen ilmaisujärjestelmien tai talotekniikan järjestelmiä ei saa hallinnoida julkisista tiloista.

Tunkeutumisen ilmaisujärjestelmä vaaditaan jo perustason turvallisuusvyöhykkeelle mikäli siellä käsitellään suojaustason IV tietoja, eikä tietoja säilytetä vaatimukset täyttävässä kassakaapissa tai holvissa. Perustasolla (VIHREÄ turvallisuusvyöhyke) vaatimuksena on luokan 2 tunkeutumisen ilmaisujärjestelmä[13] (voi olla langaton). Ylemmillä tasoilla edellytetään luokan 3 järjestelmää, jolla valvotaan ovet, aukot, ikkunat, työtilat ja kuori.

Tunkeutumisen ilmaisujärjestelmän toimivuus tulee testata työyksikön turvallisuusohjeistossa kuvatuin väliajoin.

5.3 Vartiointi

Vartioinnin järjestelyt täydentävät alueen ja tilojen valvontaa. Muu kuin valtionhallinnon omaan henkilöstöön kuuluva, turvallisuusselvitetty vartiointihenkilöstö ei saa viedä korotetun tason (KELTAISEN) turvallisuusvyöhykkeen avaimia julkiseen tilaan. Avaimia säilytetään tilan haltijan toimesta sinetöidyssä kuoressa hyväksytyssä kassakaapissa[14] tai lukitussa, käyttäjän yksilöivässä avainturvakaapissa. Avainten käyttöperiaatteet kuvataan selkeästi työyksikön turvallisuusohjeistossa.

---

11 RikosL 24 luku

12 Henkilötietolaki 2 luku

13 FK:n varmuusluokittelu

14 liite 1, vaatimus 19.

6 Toimeenpano ja ohjeistaminen

Tämä ohje otetaan käyttöön tietoturvallisuusasetuksen velvoitteiden toimeenpanemiseksi valtionhallinnossa. Näitä velvoitteita ovat:

- tietojenkäsittelyn perustason turvallisuusvaatimusten saavuttaminen viimeistään 30.9.2013,
- luokiteltujen asiakirjojen käsittelyvaatimusten täyttyminen viiden vuoden kuluessa luokittelupäätöksestä,
- 1.10.2010 käytössä olleiden sekä ennen 1.10.2012 käyttöön otettujen toimitilojen turvallisuuden saattaminen vastaamaan toimitiloissa käsiteltävän korkeimman tiedon suojaustasoa 1.10.2015 mennessä.

Ohjetta käytetään uudisrakentamisen turvallisuusperusteiden muodostamiseksi.

Liiteluettelo

Liite 1. Turvallisuusvaatimustaulukko

Tässä liitteessä on esitetty valtionhallinnon toimitilaturvallisuusvaatimukset eri tietoturvatasoille. Liitettä on tarkoituksenmukaista lukea yhdessä ohjeen luvuissa 4 ja 5 esitettyjen yleistulkintojen kanssa.

Tilaturvallisuussuunnittelu on syytä toteuttaa kiinteänä osana hankesuunnittelua.

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

Taulukon jatkeeksi on koottu joitakin yksittäisiä toteutussuosituksia, joihin viitataan vaatimussarakkeessa asteriskilla*. Koska valtionhallinnon työpisteiden toimintaympäristö vaihtelee suuresti, ennen toteutuksia vaatimuksenmukaisuus on syytä varmistaa oman työyksikön 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 perustuvalle tasoarvioinnille. Vasteaikamallia käytetään kyseisten viranomaisten ilmoittamaan laskentakaavaan perustuen. Vasteaikamallin kuvaamisen sijasta tässä liitteessä keskitytään vaatimuskohtaiseen pisteytysmalliin.

Pisteytysmalli

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 työyksikön johdon kirjallista ja perusteltua erillispäätöstä. Pisteiden antoperusteet ovat:

1 miinuspiste = vakava poikkeama vaatimuksesta
0 pistettä = poikkeama vaatimuksesta
1 pluspiste = lievä poikkeama vaatimuksesta
2 pluspistettä = vaatimukset täyttävä.

Vaatimustaulukon osa-alueiden A-D (ALUE+RAKENTEET+TILAHALLINTA+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.

Osa-alueen E, TIETOTEKNISET LAITETILAT, pisteytys toimii edellä mainitun periaatteen mukaisesti, mutta toimivaltaiset viranomaiset voivat antaa asiasta tarkentavia tulkintaohjeita.

Mikäli tavoitetason mukaisessa vaatimussarakkeessa lukee ”ei vaatimusta/ei erillisvaatimusta”, 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 miinuspisteitä.

VAATIMUS	PERUSTASO Turvallisuus-vyöhyke VIHREÄ	KOROTETTU TASO Turvallisuus-vyöhyke KELTAINEN	KORKEA TASO Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
KOHDE:					
Kohteelle määritetty riskitaso (matala/keskimääräinen/korkea):					
OSA-ALUE A: ALUE					
1. Pysäköintipaikat	Ei vaatimusta	Uhka-arvion niin osoittaessa vaatimukset kuten korkealla tasolla.	Huomioitava elektronisen tiedustelun uhka. Pysäköinti on sallittu alueen haltijan luvalla merkityille paikoille.		
2. Lastaus/purkausalueet	Ei vaatimusta	Ei vaatimusta	Huomioitava elektronisen tiedustelun uhka.		
3. Aidat*	Ei vaatimusta	Kyllä	Kyllä		
4. Portit	Ei vaatimusta	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		
6. Aluevalvonta (kohderakennusta välittömästi ympäröivä alue).	Ei vaatimusta	Ei vaatimusta	Valvonta riskiarvion mukaisesti, mikäli korkean tason vyöhyke rakennuksen ulkopintana.		

VAATIMUS	PERUSTASO Turvallisuus-vyöhyke VIHREÄ	KOROTETTU TASO Turvallisuus-vyöhyke KELTAINEN	KORKEA TASO Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
OSA-ALUE B: RAKENTEET					
7. Seinärakenne	Normaalit seinärakenteet	Ulkoseinät: Luja betoni tai muu vastaavan lujuuden omaava rakenne. Väliseinät (silloin kun turvallisuus-vyöhyke rajoittuu väliseinään): Normaali toimistokäytössä hyväksytty harkko- tai levyseinärakenne vahvistettuna viranomaisten erillisvaatimusten mukaisesti. Seinärakenteita ei saa voida irrottaa tilan ulkopuolelta.	Vyöhykettä rajaavien seinien tulee olla teräsbetonia, vahvistettua tiilirakennetta, tai vahvistettua seinärakennetta. 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. Ääniloukut ilmastointi- ja kaapelikanaviin, mikäli äänen kantautuminen pitää huomioida riskiarvioon perustuen.	Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. Ääniloukut ilmastointi- ja kaapelikanaviin, mikäli äänen kantautuminen pitää huomioida riskiarvioon perustuen.		
9. Salakuuntelun estäminen	1) Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan salassa pidettävistä asioista. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella salassa pidettävistä asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa salassa pidettävistä asioista. 4) Monimuotoisessa työympäristössä tulee keskustelut salassa pidettävistä asioista käydä riittävästi äänieristetyssä tilassa.	1) Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella salassa pidettävistä asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa salassa pidettävistä asioista. 4) Monimuotoisessa työympäristössä tulee keskustelut salassa pidettävistä asioista käydä riittävästi äänieristetyssä tilassa.	1) Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella salassa pidettävistä asioista. 3) Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa salassa pidettävistä asioista. 4) Monimuotoisessa työympäristössä tulee keskustelut salassa pidettävistä asioista käydä riittävästi äänieristetyssä tilassa.		
10. Hajasäteilyn estäminen	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: Vastatoimet riskianalyysiin pohjautuen. EU: vasta-toimet riski-analyysiin pohjautuen EU CONFIDENTIAL – tasolta alkaen.	

VAATIMUS	PERUSTASO Turvallisuus-vyöhyke VIHREÄ	KOROTETTU TASO Turvallisuus-vyöhyke KELTAINEN	KORKEA TASO Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
11. Lattia- ja kattorakenteet*	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 murtosuojakalvolla*.	Alle 4 m korkeudessa maatasosta, tai alemman kerroksen kattotasanteelta, olevissa ikkunoissa tulee olla standardin SFS-EN 356 P6B mukainen suojalasitus. Suojalasitus tulee asentaa murtautumisyrityksen kestävään karmiin. Alle 4 metrin korkeudessa olevien ikkunoiden tulee olla sellaisia, ettei niitä pysty avaamaan. Yli 4 m korkeudessa olevat ikkunat voidaan vahvistaa tarpeen mukaan.	Pyrittävä ikkunattomiin ratkaisuihin. Mikäli kuitenkin joudutaan käyttämään ikkunoita, ikkunoissa tulee olla standardin SFS-EN 356 P6B mukainen suojalasitus, joka ei saa välittää äänivärähtelyjä uloimpaa lasiin. Lisäksi on huomioitava karmin kiinnitys ympäröivään seinään, saranoiden ja lukituksen rakenne sekä lasin kiinnitys karmirakenteeseen siten, ettei 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.	NATO: 5m	
13. Kattoikkunat	Kuten muutkin ikkunat.	Kuten muutkin ikkunat.	Ei kattoikkunoita.		
14. Salakatselun estäminen	Huomioitava turvallisuus-ohjeistuksessa.	Ikkunoissa tulee olla sälekaihtimet.	Ikkunoissa tulee olla sälekaihtimet.		
15. Ovet	Normaali ovirakenne.	Vyöhykkeen rajalla oltava turvaovi (standardi SFS EN 1627-luokka 3) tai viranomaisten erillisvaatimusten mukaisesti vahvistettu, vastaavan murtosuojan antava palo-ovi. Oven tulee täyttää myös tilan käyttötarkoituksen mukaiset äänieristysvaatimukset. EI30-luokan palo-ovi hyväksytään, mikäli ympäröivä tila kuuluu VIHREÄÄN vyöykkeeseen ja on varustettu em. luokan 3 turvaovella.	Vyöhykkeen (tai keltaisen 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.		

VAATIMUS	PERUSTASO Turvallisuusvyöhyke VIHREÄ	KOROTETTU TASO Turvallisuusvyöhyke KELTAINEN	KORKEA TASO Turvallisuusvyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
16. Halliovet tai ajo-ovet, jotka johtavat turvallisuusvyöhykkeen sisään.*	Ei vaatimuksia. Äänieristys huomioitava riskitason mukaisesti.	Vahvennettu, läpiajon estävä erillisrakenne (turvallisuusviranomaisen hyväksyntä).	Vahvennettu, läpiajon estävä erillisrakenne (turvallisuusviranomaisen hyväksyntä).		
17. Muut aukot	Oltava lukittavissa.	Tilan kuoren aukot on valvottava tukeutumisen ilmaisinjärjestelmällä. Aukot on suljettava kalteroinnilla tai vahvoilla terässäleiköillä*.	Tilan kuoren aukot on valvottava tukeutumisen ilmaisinjärjestelmällä. Aukot on suljettava kalteroinnilla tai vahvoilla terässäleiköillä*.		
18. Hätäpoistumistiet **Huom! Lukitus ei saa estää hätäpoistumista.**	Ei erillisvaatimuksia	Alempien turvallisuusvyöhykkeiden hätäpoistumistiet eivät saa kulkea vyöhykkeen kautta.	Alempien turvallisuusvyöhykkeiden 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 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) - yhdistelmäkaappi 60P + 60 Diskette (NT FIRE 017)	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) - yhdistelmäkaappi 60P + 60 Diskette (NT FIRE 017)		
20. Lukitus* vyöhykkeen rajalla	Käyttölukko* heloineen ja vastalevyineen.	Käyttölukko* heloineen ja vastalevyineen. Lisäksi hakateljellä varustettu varmuuslukko* vastalevyineen tai muu saman murto- ja tiirikointilujuuden antava rakenne ja riittävät valvontajärjestelyt.	Käyttölukko* heloineen ja vastalevyineen. Lisäksi hakateljellä varustettu varmuuslukko* vastalevyineen tai muu saman murto- ja tiirikointilujuuden antava rakenne ja riittävät valvontajärjestelyt.		
21. Lukitus vyöhykkeen sisällä	Käyttölukko	Käyttölukko	Käyttölukko		
OSA-ALUE C: TILAHALLINTA					
22. Avainten ja kulkutunnisteiden hallinta	Vyöhykkeelle tulee nimetä avainvastuuhenkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnisteiden kuittauksista ja jakamattomien avainten säilytyksestä.	Vyöhykkeelle tulee nimetä avainvastuuhenkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnisteiden kuittauksista ja jakamattomien avainten säilytyksestä.	Vyöhykkeelle tulee nimetä avainvastuuhenkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnisteiden kuittauksista ja jakamattomien avainten säilytyksestä.		

VAATIMUS	PERUSTASO Turvallisuus-vyöhyke VIHREÄ	KOROTETTU TASO Turvallisuus-vyöhyke KELTAINEN	KORKEA TASO Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
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.		
24. Vartiohenkilöstön avainhallinta* **5.3.**	Ei erillisvaatimuksia	Vartiointihenkilöstölle jaettavat avainten tulee sijaita turvallisessa avainkaapissa tai olla sinetöityinä poikkeuksellisia tilanteita varten. Järjestely on huomioitava vartiointipalvelusopimuksissa.	Vartiointihenkilöstölle jaettavat avaimet tulee olla sinetöityinä poikkeuksellisia tilanteita varten tai sijaita turvallisessa ja käyttäjän yksilöivässä avainkaapissa. Hälytystilanteissa korkean tason tilaan edellytetään saapuvan kaksi henkilöä samanaikaisesti. Järjestely on huomioitava vartiointipalvelusopimuksissa.		
25. Vieraiden pääsynhallinta **3.1.3**	Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan.	Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Huolehditaan siitä, ettei oikeudeton vieras pääse näkemään salassa pidettävää tietoa. Vierailu valvotaan.	Vieraan tuominen tilaan edellyttää ennakkoilmoitusta ja turvallisuusvastaavan hyväksyntää. Vieras tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Vierailu valvotaan.		
26. Palveluntuottajien henkilöstön hallinta (esim. kiinteistönhoito, -huolto ja siivoushenkilöstö)* **3.1.3**	Henkilö tunnistetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Vakiohenkilöstö varustetaan kuvallisella henkilökortilla.	Henkilö tunnistetaan ja varustetaan vieraskortilla. Vakiohenkilöstö varustetaan kuvallisella henkilökortilla. Vierailu kirjataan (lokimenettely, mikäli kulkutunniste). Huolehditaan siitä, että henkilö ei pääse näkemään salassa pidettävää tietoa. Henkilöä valvotaan.	Henkilön tuominen tilaan edellyttää ennakkoilmoitusta ja turvallisuusvastaavan hyväksyntää. Henkilö tunnistetaan ja varustetaan vieraskortilla. Vakiohenkilöstö varustetaan kuvallisella vieraskortilla. Vierailu kirjataan. Huolehditaan siitä, että henkilö ei pääse näkemään salassa pidettävää tietoa. Henkilöä valvotaan korostetusti.		
27. LVIS-varmistukset	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.		
28. LVI-automaation etäkäyttö	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. Tilaolosuhteita ja hälytyksiä voidaan valvoa etänä. Etävalvontaratkaisun tulee olla turvallinen.		

VAATIMUS	PERUSTASO Turvallisuus-vyöhyke VIHREÄ	KOROTETTU TASO Turvallisuus-vyöhyke KELTAINEN	KORKEA TASO Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
29. Hissit	Ei vaatimuksia.	Hissin käyttöä on ohjattava kulunvalvonnalla.	Hissin käyttöä on ohjattava kulunvalvonnalla, hissikuilu valvottava.		
OSA-ALUE D: VALVONTAJÄRJESTELYT					
30. Kulunvalvontajärjestelmä*	Kulunvalvontajärjestelmän käyttöönottosta päätetään riskianalyysiin perustuen.	Vyöhykkeen rajalla on käytettävä sähköistä kulunvalvontaa.	Vyöhykkeen rajalla on käytettävä sähköistä kulunvalvontaa. Sisään mentäessä käytettävä kaksoistunnistusta (esimerkiksi pääsykoodi ja sähköinen tunniste). Poistuttaessa tilasta tulee käyttää kulunvalvontatunnistetta.		
31. Kulunvalvontajärjestelmän hallinnointi	Ei vaatimuksia.	Kulkuoikeuksien hallinnointi on oltava viranomaisen hallinnassa tai jos se on ulkoistettu, vaaditaan ulkoistuksen kohteen kanssa turvallisuussopimusta.	Kulunvalvonnassa käytetään aluevalvontaa. Kulkuoikeuksien hallinnointi on oltava tilan haltijalla.		
32. Tunkeutumisen ilmaisinjärjestelmä*	Jos tilassa säilytetään suojaustason IV tietoa, tila varustetaan tunkeutumisen ilmaisulla (vähintään FK 2-luokka) tai tieto säilytetään vaatimukset täyttävässä kassakaapissa.	Ovet, aukot, ikkunat ja tilat valvottava tunkeutumisen ilmaisulla (vähintään FK 3-luokka). Kuori on valvottava.	Ovet, aukot, ikkunat ja tilat valvottava tunkeutumisen ilmaisulla (vähintään FK 3-luokka). Kuori on valvottava.		
33. Tunkeutumisen ilmaisinjärjestelmän testaus	Turvallisuusdokumentaation mukaisesti	Turvallisuusdokumentaation mukaisesti	Turvallisuusdokumentaation mukaisesti, vähintään kerran kuukaudessa.		
34. Tunkeutumisen ilmaisinjärjestelmän hallinnointi	Turvallisuusdokumentaation mukaisesti	Turvallisuusdokumentaation mukaisesti	Tunkeutumisen ilmaisujärjestelmän hallinnointi on oltava tilan haltijalla.		
35. Kameravalvontajärjestelmä	Turvallisuusvyöhykettä tai sitä ympäröivää aluetta valvotaan kameravalvonnalla.	Turvallisuusvyöhykettä tai sitä ympäröivää aluetta valvotaan tallentavalla kameravalvonnalla.	Turvallisuusvyöhykettä tai tilaa on valvottava tallentavalla kameravalvonnalla.*		
36. Palvelintilan kameravalvonta	Palvelintilaa tai sitä ympäröivää aluetta voidaan valvoa tallentavalla kameravalvonnalla.	Palvelintilaa tai sitä ympäröivää aluetta valvotaan tallentavalla kameravalvonnalla.	Laite- ja palvelintilat on varustettava tallentavalla kameravalvonnalla*.		
37. Vartiointi	Mahdollisen vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä.	Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä. Vasteaika tulee testata viraston turvallisuusohjeen mukaisesti. Testin tulos dokumentoidaan.	Ilmoitus hälytyksestä heti tilan haltijalle. Vartioinnin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä. Vasteaika tulee testata viraston turvallisuusohjeen mukaisesti, vähintään kerran vuodessa. Testin tulos dokumentoidaan.		

VAATIMUS	PERUSTASO Turvallisuusvyöhyke VIHREÄ	KOROTETTU TASO Turvallisuusvyöhyke KELTAINEN	KORKEA TASO Turvallisuusvyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
OSA-ALUE E: TIETOTEKNISET LAITETILAT					
38. Kaapelointi	Ei erillisvaatimuksia	Kaapelit asennetaan pintaan, värikoodein eroteltuina, mikäli uhka-arvio sitä edellyttää.	Kaapelit asennetaan pintaan, värikoodein eroteltuina		
39. Palo-osastointi	IT-laitetila on varustettava paloilmoituslaitteistoilla	IT-laitetila on varustettava paloilmoituslaitteistoilla	IT-laitetila on varustettava paloilmoituslaitteistoilla sekä näytteenottoilmaisimilla ja automaattisella palosammutuslaitteistolla		
40. Lämpö	IT-laitetila on varustettava omalla erillisellä ilmanvaihtojärjestelmällä, jonka koneisto on sijoitettava omaan erilliseen palo-osastoon tai erotettava muusta ilmastoinnista savuilmaisimilla ohjatuilla palonrajoittimilla. Ilmanvaihtohormit on varustettava automaattisesti toimivilla palonrajoittimilla.	IT-laitetila on varustettava omalla erillisellä ilmanvaihtojärjestelmällä, jonka koneisto on sijoitettava omaan erilliseen palo-osastoon. Ilmanvaihtohormit on varustettava automaattisesti toimivilla palonrajoittimilla.	IT-laitetila on varustettava omalla erillisellä ilmanvaihtojärjestelmällä, jonka koneisto on sijoitettava omaan erilliseen palo-osastoon. Ilmanvaihtohormit on varustettava automaattisesti toimivilla palonrajoittimilla.		
41. Savu	Savun kulkeutuminen ilmanvaihtojärjestelmän kautta osastosta toiseen on estettävä.	Savun kulkeutuminen ilmanvaihtojärjestelmän kautta osastosta toiseen on estettävä.	Savun kulkeutuminen ilmanvaihtojärjestelmän kautta osastosta toiseen on estettävä.		
42. Vesivahinko	Laitetilat on rakennettava varustettuna vesivahingosta hälyttävillä antureilla. Rakennettaessa IT-laitetila pohjaveden keskipinnan alapuolelle, tulee tila varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistolaitteella.	Laitetilat on rakennettava varustettuna vesivahingosta hälyttävillä antureilla. Rakennettaessa IT-laitetila pohjaveden keskipinnan alapuolelle, tulee tila varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistolaitteella.	Laitetilat on rakennettava varustettuna vesivahingosta hälyttävillä antureilla. Rakennettaessa IT-laitetila pohjaveden keskipinnan alapuolelle, tulee tila varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistolaitteella.		
43. Pöly ja puhtaus	Rakenteista ei saa irrota pölyä. Tuloilman suodatuksesta on huolehdittava. Asennuslattian alapohja on siivottava säännöllisesti.	Rakenteista ei saa irrota pölyä. Tuloilman suodatuksesta on huolehdittava. Asennuslattian alapohja on siivottava säännöllisesti.	Rakenteista ei saa irrota pölyä. Tuloilman suodatuksesta on huolehdittava. Asennuslattian alapohja on siivottava säännöllisesti.		
44. Laitevauriot	Laitevaurioiden varalta järjestelmä varustetaan automaattisilla laitteistovarmistuksilla.	Laitevaurioiden varalta järjestelmä varustetaan automaattisilla laitteistovarmistuksilla.	Laitevaurioiden varalta järjestelmä varustetaan automaattisilla laitteistovarmistuksilla.		
45. UPS	Sähkön häiriötön saanti on varmistettava katkottoman sähkönsyötön turvaavilla laitteilla.	Sähkön häiriötön saanti on varmistettava katkottoman sähkönsyötön turvaavilla laitteilla. Sähkön saanti on varmistettava myös varavoimageneraattoreilla, joiden toiminta on testattava määräajoin.	Sähkön häiriötön saanti on varmistettava katkottoman sähkönsyötön turvaavilla laitteilla. Sähkön saanti on varmistettava myös varavoimageneraattoreilla, joiden toiminta on testattava määräajoin.		

VAATIMUS	PERUSTASO Turvallisuusvyöhyke VIHREÄ	KOROTETTU TASO Turvallisuusvyöhyke KELTAINEN	KORKEA TASO Turvallisuusvyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
46. Olosuhdehälytys	Järjestelmä on varustettava olosuhteiden (esim. lämpötila, kosteus) muuttumisen ilmaisevalla hälytysjärjestelmällä.	Järjestelmä on varustettava olosuhteiden (esim. lämpötila, kosteus) muuttumisen ilmaisevalla hälytysjärjestelmällä.	Järjestelmä on varustettava olosuhteiden (esim. lämpötila, kosteus) muuttumisen ilmaisevalla hälytysjärjestelmällä.		
47. Varavoima	Varavoimageneraattoreiden käyttämistä suositellaan UPS-laitteiden lisäksi.	Sähkön saanti on varmistettava UPS-laitteiden lisäksi varavoimageneraattoreilla, joiden toiminta on testattava turvallisuusohjeistossa ilmaistuin määräajoin. Varavoimakoneet on sijoitettava omaan palo-osastoonsa, samoin kuin niiden tarvitsema polttoaine	Sähkön saanti on varmistettava UPS-laitteiden lisäksi varavoimageneraattoreilla, joiden toiminta on testattava turvallisuusohjeistossa ilmaistuin määräajoin. Varavoimakoneet on sijoitettava omaan palo-osastoonsa, samoin kuin niiden tarvitsema polttoaine.		
48. Tärinä ja värähtely	Tulee varmistua laitehyllyjen ja –kaappien riittävästä kiinnityksestä ja tärinävaimennuksesta. Laitteen oman vaimentimen liikevara lepoasennon molemmin puolin sekä pysty- että vaakasuunnassa on huomioitava laitevaurioiden välttämiseksi.	Tulee varmistua laitehyllyjen ja –kaappien riittävästä kiinnityksestä ja tärinävaimennuksesta. Laitteen oman vaimentimen liikevara lepoasennon molemmin puolin sekä pysty- että vaakasuunnassa on huomioitava laitevaurioiden välttämiseksi.	Tulee varmistua laitehyllyjen ja –kaappien riittävästä kiinnityksestä ja tärinävaimennuksesta. Laitteen oman vaimentimen liikevara lepoasennon molemmin puolin sekä pysty- että vaakasuunnassa on huomioitava laitevaurioiden välttämiseksi.		
49. Kemialliset vaikutukset	Ilmanvaihtolaitteet on varustettava kaasu- ja hiukkassuodattimilla. Tilat on tiivistettävä ylipaineistusta silmällä pitäen.	Ilmanvaihtolaitteiden suodattimien ja kulkuvien suunnittelussa on huomioitava kriisiaikana mahdollisesti ilmassa olevien kemiallisten aineiden vaikutus suodattimien toimintaan. Ilmanvaihtolaitteet on varustettava kaasu- ja hiukkassuodattimilla. Tilat on tiivistettävä ylipaineistusta silmällä pitäen.	Ilmanvaihtolaitteiden suodattimien ja kulkuvien suunnittelussa on huomioitava kriisiaikana mahdollisesti ilmassa olevien kemiallisten aineiden vaikutus suodattimien toimintaan. Ilmanvaihtolaitteet on varustettava kaasu- ja hiukkassuodattimilla. Tilat on tiivistettävä ylipaineistusta silmällä pitäen.		
50. Räjähteet	Uhka-arvion mukaisesti.	Uhka-arvion mukaisesti.	Tiloissa vierailevien henkilöiden mukanaan tuomat varusteet tarkastetaan sabotaasiyrityksen varalta.		
51. Polttotaisteluaineet	Uhka-arvion mukaisesti.	Uhka-arvion mukaisesti.	Uhka-arvion mukaisesti.		
52. Valmiussuunnitelma	Toteutetaan, mikäli laiteympäristöön kohdistuu valmiudellisia vaatimuksia.	Toteutetaan, mikäli laiteympäristöön kohdistuu valmiudellisia vaatimuksia.	Toteutetaan, mikäli laiteympäristöön kohdistuu valmiudellisia vaatimuksia.		

VAATIMUS	PERUSTASO Turvallisuus-vyöhyke VIHREÄ	KOROTETTU TASO Turvallisuus-vyöhyke KELTAINEN	KORKEA TASO Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	PIST.
53. Sammutuslaitteet	IT-laitetila on aina varustettava paloilmoituslaitteistoilla.	IT-laitetila on aina varustettava paloilmoituslaitteistoilla.	IT-laitetila on aina varustettava paloilmoituslaitteistoilla. Korkean suojaustason laitetiloissa tulee käyttää lisäksi näytteenottoilmaisimia ja automaattista palosammutuslaitteistoa.		
54. Varatilat	Ei erillisvaatimuksia	Ei erillisvaatimuksia	Laitetilojen suunnittelussa on huomioitava mahdollinen tarve jatkaa toimintaa erillisessä varakeskuksessa tai muussa etukäteen valmistellussa varatoimitilassa.		
55. EMP ja hajasäteily	Ei erillisvaatimuksia	Huomioidaan uhka-arvioissa ja toteutetaan tarvittaessa riittävät suojaustoimet.	Säteilypulssikentän vaimentaminen paikallisesti laitteiston ympärillä toteutetaan ympäröimällä suojattava laitteisto yhtenäisellä metalliverhouksella tai metalliverkolla. Suojattavan tilan ulkopuolelle ulottuviin johtoihin kytkeytymistä huononnetaan maadoitetuilla metallivaipoilla, ylijännitesuojilla ja suodattimilla.		
56. HPM	Ei erillisvaatimuksia	Ei erillisvaatimuksia	IT-laitetilojen suunnittelussa on huomioitava uhka-arvioperusteisesti HPM-aseen käyttöä vastaan suojautuminen.		

LIITTEEN 1 VAATIMUSTEN TÄSMENNYKSIÄ JA TOTEUTUSSUOSITUKSIA

3. AIDAT

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

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

- aidan korkeus = min 2,40 m
- 2 piikkilankaa (sinkitty teräs 2x1,6mm) ylhäällä, 1 alhaalla.
- teräsverkon 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 kiinnitysruuvien (vast.) tulee olla aidalla suljetun alueen sisäpuolella.

Suositellaan maaston muotoja seuraavaa, 3 m korkeaa terässäleaitaa, jonka sälelevyt on kiinnitetty terästolppiin suojapuolelta. Vaikka terässäleaita on verkkoaitaa kalliimpi, se on pitkäikäisempi ja antaa merkittävästi paremman estearvon sekä toimii parempana alustana valvontalaitteille. Korotetulla betoniperustalla varustettu terässäleaita toimii myös ajoneuvoesteenä.

Mikäli aitaaminen on mahdotonta, kuten tiiviissä kaupunkiympäristössä, on kiinnitettävä korostetusti huomiota viraston ulkokuoren suojausmekanismeihin esimerkiksi tehostetun valvonnan ja reagoinnin keinoin.

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. Rikostorjunnallisista syistä yksiselitteisiä rakennevaatimuksia ei anneta julkisessa ohjeessa.

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 toteutetaan 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 $\geq$ 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.

24. VARTIOHENKILÖSTÖN AVAINHALLINTA

Avainkuoren sinetöinti voidaan korvata sähköisesti lukittavalla, viranomaisen erillismääräykset täyttävällä avainkaapilla, josta avaimen poistamista edeltää käyttäjän yksilöivä lokitieto.

KELTAISEN tai SINISEN turvallisuusvyöhykkeen avaimia tai kulkutunnisteita ei saa viedä julkisiin tiloihin.

26. PALVELUNTUOTTAJIEN HENKILÖSTÖN HALLINTA

Vakiohenkilöstön pääsy tilaan tapahtuu kulkutunnisteella korkeintaan VIHREÄLLE turvallisuusvyöhykkeelle. Vakiohenkilöstön itsenäinen pääsy kulkutunnisteen avulla KELTAISELLE turvallisuusvyöhykkeelle on mahdollista ainoastaan erilliseen hyväksymismenettelyyn perustuen.

KELTAINEN ja SININEN turvallisuusvyöhyke: työskentely tapahtuu virka-aikana. Palveluntuottajien henkilöstöä valvotaan KELTAISELLA turvallisuusvyöhykkeellä kollektiivisesti (kukin vastaa omalta osaltaan), mutta SINISELLÄ turvallisuusvyöhykkeellä korostetusti (jatkuva valvonta).

KELTAINEN turvallisuusvyöhyke: Sekä työajalla, että työajan ulkopuolella tapahtuvien huoltokäyntien on kirjauduttava sähköiseen kulunvalvontalokiin. Mikäli turvallisuusselvitys on mahdotonta toteuttaa, henkilöstön työskentelyä valvotaan korostetusti isäntien toimesta.

SININEN turvallisuusvyöhyke: tilaan pääsyn edellytyksenä on turvallisuusselvitys.

30. KULUNVALVONTAJÄRJESTELMÄ

Kulunvalvontalukijat sijoitetaan vyöhykkeen rajalle.

32. TUNKEUTUMISEN ILMAISINJÄRJESTELMÄ

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

35. KAMERAVALVONTAJÄRJESTELMÄ

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

36. PALVELINTILAN KAMERAVALVONTA

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

Liite 2. Pohjakuvaesimerkit eri turvallisuusvyöhykkeiden mukaisista työympäristöistä

JULKISET TILAT (VALKOINEN)

Ei aita/portti/ajoestevaatimusta

P

- 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, VIHREÄ TURVALLISUUSVYÖHYKE

Ei aita/portti/ajoestevaatimusta

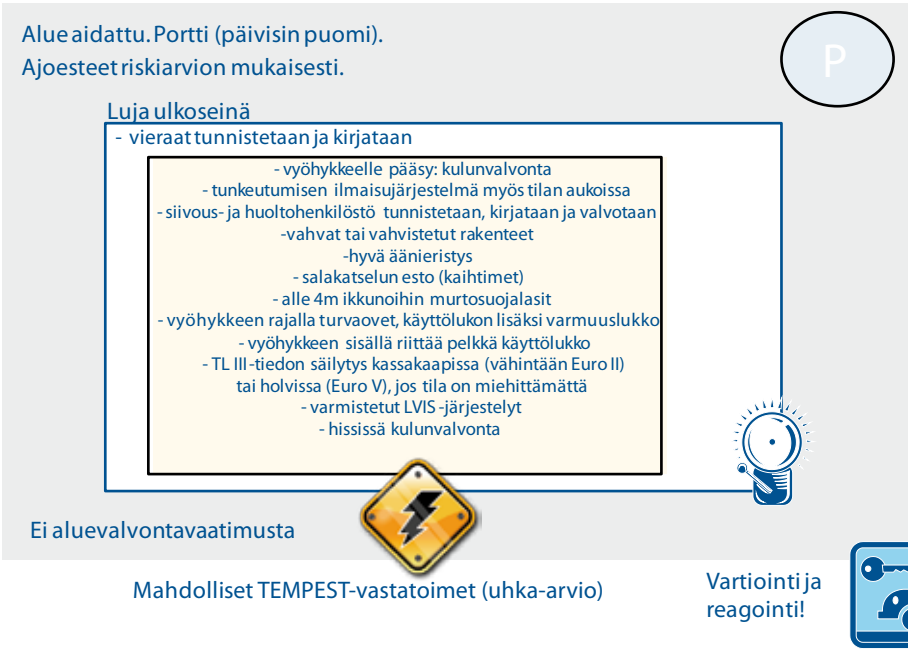
P

- 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, KELTAINEN TURVALLISUUSVYÖHYKE



KORKEA TASO ST II, SININEN TURVALLISUUSVYÖHYKE

Liite 3. 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 riskiympäristö ja tiloissa käsiteltävän tiedon suojaustaso huomioon ottaen.

Kiinteistöosa	Käyttöesimerkki	Turvallisuusvyöhyke			Julkinen tila tai alue	Huom.
		VIHREÄ ST IV	KELTAINEN ST 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				
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		
	Operatiiviset neuvottelutilat		x	x		
	Muut neuvottelutilat	x			x	
	Edustustilat	x			x	
	Erikoiskoulutustilat	x				
	Sosiaalitilat	x			x	
	Palvelinhotellit			x		
	Tietotekniset laitetilat	x	x	x		
	Valtakunnalliset johtamistilat			x		
	Viraston johtamistilat		x	x		
	Alueelliset johtamistilat		x			
	Kulunvalvontapisteet	x				
	Turvallisuusvalvomot		x			
	Kiinteistötekniset tilat	x	x			järjestelmien palvelualueet
	Varavoimakonetilat	x		x		toiminnan kriittisyys
	Arkisto ST III – ST I		x	x		
	Arkisto ST IV - JUL					
	Yleiset varastotilat	x			x	

Liite 4. Tietoteknisten laitetilojen turvallisuussuositukset

1 Johdanto

1.1 Suosituksen tarkoitus ja rajaus

Tämä valtionhallinnon toimitilojen tietoturvaohjeen liite on tarkoitettu apuvälineeksi ja muistilistaksi toteutettaessa tietoteknisten laitetilojen (IT-laitetilat) fyysiseen turvallisuuteen liittyviä erityisvaatimuksia.

Tietoteknisillä laitetiloilla tarkoitetaan tässä suosituksessa erityisesti konesalia, palvelinhotellia, viestiasemaa, tietoverkon valvomo- tai hallintatilaa tai muuta erillistä, useita palvelimia sisältävää teknistä tilaa, jonka toimintojen voidaan ajatella olevan kriittisiä valtionhallinnon tietoteknisen ympäristön toimivuuden kannalta ja jossa sijaitsevat elektroniset laitteet vaativat luotettavasti toimiakseen erityisen vakaata ja suojattua toimintaympäristöä. Kerros- tai talojakamoita koskevat tämän suosituksen pääasiakirjan (VAHTI 2/2013) yleiset fyysisen turvallisuuden vaatimukset.

Uudisrakennushankkeiden kyseessä ollessa teknisten laitetilojen suunnittelu on syytä aloittaa heti hankkeen alkuvaiheessa, ottaen huomioon suojattavien tietojen suojaustaso ja tärkeys. Teknisten laitetilojen suunnittelijan tulee olla rakenne- ja materiaaliteknisen ammattitaidon lisäksi hyvin perehtynyt IT-laitetiloille asetettuihin toiminnallisiin ja teknisiin vaatimuksiin sekä hallita fyysisen turvallisuuden perusteet.

Kaikki tässä suosituksessa esitetyt linjaukset eivät tule kyseeseen kaikissa toimintaympäristöissä. Jokainen hallinnonala tai organisaatioyksikkö ratkaisee tarvitsemansa suojauksen tason riskikartoituksen ja uhka-analyysin perusteella. Tietoturvallisuuden nykytilan kartoituksessa on huomioitava myös poikkeusoloihin varautuminen, jotta suunnittelun lähtökohdat voidaan määritellä oikein.

IT-laitetilojen suojauksesta vastaa kukin virasto yhdessä hallinnonalansa tietohallinto- tai tietoturvaorganisaatioiden kanssa. Suojaustoimenpiteiden kustannukset on syytä huomioida budjetissa. Kustannukset muodostuvat laitehankinnoista ja muutostöistä. Suositusliitteen kohderyhmä on valtionhallinnon IT-laitetilojen suunnitteluun, ohjaukseen, toteutukseen ja valvontaan osallistuva henkilöstö, mutta työn tulos soveltunee myös muun julkisen sektorin käyttöön.

1.2 Suosituksen laatiminen

Tämä suositus korvaa valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI:n vuonna 2002 julkaiseman samannimisen suosituksen (VAHTI 1/2002). Uusittu, VAHTI 2/2013 –ohjeen liitteenä julkaistava suositus tukeutuu muodoltaan edeltäjäasiakirjaansa. Päivitettyä suositusta on uudistettu vastaamaan kirjoittamishetken yleisiä vaatimuksia sekä pääasiakirjassa esitettyjä linjauksia. Yksityiskohtaisia, tietoteknisiä laitetiloja erityisesti

koskevia tilaturvallisuusvaatimuksia on koottu pääasiakirjan liitteen 1 taulukkoon (vaatimukset 38-56), jota on syytä lukea rinnan tämän liitteen 4 kanssa.

1.3 Suosituksen kohde

Suositus on tarkoitettu erityisesti organisaatioiden IT-laitetilojen rakenneratkaisuja tekeville suunnittelijoille sekä turvallisuus- ja tietoturvallisuusasiantuntijoille.

Suositusta voivat käyttää uusia, kiinteitä IT-laitetiloja suunnittelevat tai niitä hankkivat organisaatiot, joiden on huomioitava toimintaan mahdollisesti vaikuttavat uhkatekijät ja onnettomuudet normaalioloissa sekä poikkeusolojen erityisvaatimukset. Suositusta voi käyttää myös vaatimusasettelutyökaluna ulkoistettaessa käyttöpalveluja ja kehitettäessä toimintaympäristöä. Organisaatiossa voi olla useita eri IT-laitetiloja, joiden suojauksen ei kuitenkaan tarvitse olla samantasoisia. Suojaustarve riippuu ensi kädessä laitteissa käsiteltävien tietojen luokittelusta sekä tilan uhkaympäristöstä.

1.4 IT-laitetilan toiminnalliset rajaukset

IT-laitetilassa saa tehdä vain tietojärjestelmän asennukseen tai ylläpitoon kuuluvia tehtäviä. IT-laitetila on sijoitettava palonkestävään osastoon riippumatta siitä, sijaitseeko se maanpäällisissä rakenteissa vai maanalaisissa tiloissa. IT-laitetilan poikkeusolojen toimivuuteen ja käytettävyyteen vaikuttavia fyysisiä tekijöitä ovat organisaation sijainti (lähellä lentokenttää, satamaa tai teollisuuslaitosta, vilkkaan liikenteen ympäröimänä, sijoittuminen suhteessa rakennuksen muihin käyttäjiin) ja maaperä, jolle rakennetaan tai jonka päällä rakennus sijaitsee.

1.5 Suosituksen rakenne

Tämä suositus on laadittu luvuittain seuraavasti:

- luvussa yksi esitetään taulukkona erilaiset suojamekanismit.
- luvussa kaksi kuvataan erilaisia IT-laitetilojen uhkia.
- luvussa kolme esitetään, kuinka uhkien toteutumista voidaan välttää.
- luvussa neljä kuvataan poikkeusoloihin varautumista.
- luvussa viisi käsitellään suunnittelussa huomioitavia uhkien ja riskien arviointia, joita organisaation IT-laitetilojen suojaaminen edellyttää.

Suositus on rakennettu tietoturvallisuuden kahdeksan osa-alueen mukaisesti. Korkean tietoturvatason IT-laitetilojen osalta on kiinnitettävä huomiota erilaisten aseiden aiheuttamiin vaikutuksiin.

1.6 Uhkatekijät ja suojaustasotaulukko

Seuraavassa taulukossa on esitetty uhkatekijöiden kannalta suojaustason ja uhkaympäristön välisiä yhteyksiä

Suojaustaso	IV	III	II	I
Turvallisuusvyöhyke	**Vihreä**	**Keltainen**	**Sininen**	**Punainen**
Varkaus	X	X	X	X
Kulunvalvonta	X	X	X	X
Tunkeutuminen	X	X	X	X
Tulipalo	X	X	X	X
Ilkivalta	X	X	X	X
Lämpö	X	X	X	X
Savu	X	X	X	X
Vesivahinko	X	X	X	X
Pöly ja puhtaus	X	X	X	X
Laitevaurio, huolto	X	X	X	X
Koulutus	X	X	X	X
Henkilöstö	X	X	X	X
Ovet ja lukitus	X	X	X	X
Palo-osastointi	X	X	X	X
UPS	X	X	X	X
Olosuhdehälytys		X	X	X
Varavoima		X	X	X
Kameravalvonta		X	X	X
Tärinä ja värähtely		X	X	
Kemikaalit		X	X	X

Erityiskysymykset valtionhallinnon toimipisteille, joiden IT-laitetiloissa käsitellään massamuotoisesti suojaustason III turvallisuusluokiteltua tietoa tai suojaustasoihin II ja I luokiteltua tietoa:

Suojaustaso	IV	III	II	I
Turvallisuusvyöhyke	**Vihreä**	**Keltainen**	**Sininen**	**Punainen**
Rakenneratkaisu		X	X	X
Räjähteet		X	X	X
Polttotaisteluaineet		X	X	X
Valmiussuunnitelma		X	X	X
Sammutuslaitteet		X	X	X
Vierailut ja tiedotus		X	X	X
Turvasopimukset		X	X	X
Varatilat (-keskus)		X	X	X
EMP ja säteily		(X)	X	X
HPM			X	X

2 Suojattavat kohteet ja niitä uhkaavat tekijät

Valtion toimitilojen suojausvaatimukset on aiemmin jaettu neljään eri luokkaan seuraavasti:

Perussuojaus, tehostettu perussuojaus, erityissuojaus ja täyssuojaus[15]. Tässä suosituksessa käytetään edellä mainittujen luokkien sijasta valtionhallinnon tietoturvallisuusasetuksen (9§) ja VAHTI-ohjeen 2/2010 mukaisia suojaus- ja tietoturvatasomäärityksiä.

IT-laitetilat ovat organisaation toiminnan kannalta keskeisiä kohteita. Erityistä suojausta vaativien IT-laitetilojen suunnittelussa on suunnittelun kannalta olennaista tietää, millainen uhka on torjuttava.

Käsiteltävien tietojen luokitus on huomioitava IT-laitetilojen suojauksessa suunniteltaessa tilojen turvallisuusratkaisuja. Turvallisuusjärjestelyjen rakentamisessa on käytettävä harkintaa ylimitoituksen välttämiseksi.

Organisaation tietoturvariskikartoituksen ja eri uhkien määrittelyn perusteella saadaan selville tekijät, jotka ohjaavat IT-laitetilojen rakenteellista suunnittelua ja turvallisuusteknisiä vaatimuksia, joiden perusteella päädytään IT-laitetilojen sijaintiin rakenteissa.

Tietoturvallisuuden kannalta tarkasteltuna tärkeitä toimitilaturvallisuuden tehtäviä ovat:

- tietoaineiston ja erityisesti tietovarastojen turvallinen säilytys sekä suojaaminen palo-, vesi- ja murtovahingoilta
- IT-laitetilojen ja laitteiden suojaaminen sekä olosuhdehälytyksin tapahtuva valvonta.

Hankittaessa tietojenkäsittelypalvelut sopimuksin alihankkijoilta on heidän IT-laitetilojensa täytettävä vaatimukset, joita käsiteltävien tietojen suojaustaso edellyttää.

2.1 IT-laitetilan riskit

IT-laitetilan riskikartoituksessa on etsittävä järjestelmällisesti vaaratekijät, arvioitava niistä mahdollisesti aiheutuvat valtiolliset ja taloudelliset menetykset sekä asetettava riskit tärkeysjärjestykseen.

Uhkien todennäköisyyden perusteella voidaan luokitella riskit.

Kutakin riskiä varten on laadittava vahingontorjuntasuunnitelma ja katastrofiluonteisten vahinkojen varalle toipumissuunnitelma.

[15] "Suositus toimitilaturvallisuuden huomioonottamisesta valtionhallinnossa", VM 1/01/99, 30.12.1998

Tärkeimmät IT-laitetilaa uhkaavat riskit ovat:

- tietoturvaloukkaus, tietovarkaus
- palo ja räjähdys
- vesivahinko, tulva
- sähkökatko
- jännitehäiriö
- laiterikko
- lämpötilan nousu
- laitevarkaus
- inhimillinen erehdys
- vahingonteko
- vaarallisten aineiden kuljetusväylät, varastot, satamat, teollisuuslaitokset
- virus tai muu haittaohjelma
- sovellusohjelmiston omat viat tai puutteet
- EMP:n ja HPM:n aiheuttamat vahingot
- kemiallisten aineiden aiheuttamat vahingot
- säteilyonnettomuus.

Tietoturvallisuuden nykytilan kartoituksessa onkin selvitettävä mm. seuraavat seikat:

1. Miten on hoidettu rakenteellinen suojaus murron, palon, vesivahingon ja sabotaasin varalta?
2. Miten on hoidettu kulunvalvonta, lukitus ja tunkeutumisen ilmaisu sabotaasin, tietovarkauden, teollisuusvakoilun ja omaisuuden varastamisen varalta
3. Miten on hoidettu toiminnan varmistaminen laitteiden vahingoittumisen tai tuhoutumisen, tiedostojen tuhoutumisen tai sähkönsyötön katkeamisen varalta?
4. Miten on hoidettu tietojen suojaus ulkopuolisia, hakkereita ja viruksia vastaan?
5. Miten on estetty laitteiden ja järjestelmien väärinkäyttö?
6. Miten on hoidettu työajan ja ylitöiden valvonta, töiden raportointi, ohjelmamuutosten rekisteröinti sekä ohjelmien säännöllinen kontrollointi?
7. Onko riittävä varahenkilöstöjärjestelmä olemassa?
8. Onko varalaitteistoja saatavilla ja mistä?

2.2 Suojautuminen varkautta ja tunkeutumista vastaan

Asiattomien pääsy IT-laitetiloihin on estettävä. Erikseen määritetyn IT-henkilöstön lisäksi ainoastaan laitteiden huoltohenkilöstö ja siivoojat saavat päästää laitetiloihin ja hekin vasta sen jälkeen, kun he ovat todistaneet henkilöllisyytensä ja käyntinsä tarpeellisuuden. Käynnit suoritetaan valvottuina, ottaen huomioon kohteen tärkeys.

Kulunvalvonta IT-laitetiloihin on järjestettävä siten, ettei kukaan pääse saapumaan tai poistumaan tulematta rekisteröidyksi (sähköinen loki). Laitetilojen osalta on pyrittävä käyttämään erillistä kulunvalvontajärjestelmää, jota toimitiloissa toimiva organisaatio hallinnoi. Erityistä suojausta vaativissa kohteissa voidaan liikkumista rajoittaa siten, että sisään– tai uloskäyntiovista ei saa yhdellä oven avauksella päästä kulkemaan kuin yksi henkilö kerrallaan. IT-laitetilaan johtavien ovien ja niiden lukitusjärjestelyjen tulee täyttää pääasiakirjan liitteessä 1 esitetyt vaatimukset.

2.3 Suojautuminen tulipaloa vastaan

IT-laitetila on aina varustettava paloilmoituslaitteistoilla. Korkean suojaustason laitetiloissa tulisi käyttää lisäksi näytteenottoilmaisimia ja automaattista palosammutuslaitteistoa.

2.4 Suojautuminen sortumaa vastaan

Kellaritiloissa sijaitsevien kiinteiden IT-laitetilojen on kestettävä vähintään päälle sortuneen rakennuksen aiheuttama kuormitus siten, että laitteet eivät vaurioidu. IT-laitetilan katto ja kukin ympärysseinä otaksutaan kuormitetuksi kokonaisuudessaan erikseen edellä tarkoitetulla kuormalla. Lisäksi tilan lujuus huomioiden ovet tarkistetaan otaksumalla kuormien kohdistuvan samanaikaisesti tilan kaikkiin osiin.

Pystysuoraan vaikuttavat kuormitukset on johdettava perustuksiin. Perustuksiin oletetaan johtuvan puolet edellä mainitusta kuormasta. Mitoitettaessa perustuksia paaluille tai maanvaraiseksi on niiden kuormitus tarkastettava tapauskohtaisesti.

Tilojen suunnittelussa ja rakenteissa on kiinnitettävä huomiota riittävään osastointiin.

Kellaritiloissa sijaitsevan IT-laitetilan lattian, kantavien teräsbetonisten väliseinien ja pilareiden sekä kaksikerroksisen laitetilan teräsbetonisen välipohjan mitoituksessa voidaan noudattaa kevyen väestönsuojan teknillisiä määräyksiä.

2.5 Suojautuminen lämpöä ja savua vastaan

IT-laitetila on varustettava omalla erillisellä ilmanvaihtojärjestelmällä, jonka koneisto on sijoitettava omaan erilliseen palo-osastoon. Ilmastointi on järjestettävä siten, että laitetilassa on ympäröiviä tiloja korkeampi paine. Ellei IT-laitetilalle voida toteuttaa täysin erillistä ilmastointijärjestelmää, on IT-laitetilan ilmastointi erotettava muusta ilmastoinnista savuilmaisimilla ohjatuilla palonrajoittimilla. Ilmanvaihtolaitteiden tulee pysähtyä automaattisesti paloilmoitin- tai sammutuslaitteiston alkaessa toimia. Laitteet on voitava pysäyttää myös käsin. Kytkin on sijoitettava samaan paikkaan kuin IT-laitetilojen pääkytkin.

Ilmanvaihtolaitteet on sijoitettava erilliseen ilmanvaihtokonehuoneeseen. Ilmanvaihtohormit on rakennettava syttymättömistä rakennustarvikkeista ja ne on varustettava automaattisesti toimivilla palonrajoittimilla.

Savun kulkeutuminen ilmanvaihtojärjestelmän kautta osastosta toiseen on estettävä.

2.6 Suojautuminen vesivahinkoja vastaan

IT-laitetiloihin ei saa rakentaa putkistoja siten, että ne rikkoontuessaan aiheuttaisivat vesivahingon. Laitetilat on rakennettava varustettuna vesivahingosta hälyttävillä antureilla. Tilat on rakennettava alapohjan päälle tai laitteistot varustettava korotusalustalla. Vaihtoehtoisesti sähkö- ja muiden vesivaurioalttiiden asennusten minimikorkeuden on oltava suurempi kuin vesivuodon hallintaan tarvittava korkeus. Jos laitetiloissa on lattiakaivoja, on ne varustettava takaiskuventtiilillä veden sisääntulon estämiseksi.

Rakennettaessa IT-laitetila pohjaveden keskipinnan alapuolelle, tulee tila varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistolaitteella.

2.7 Suojautuminen pölyä vastaan

Lattian tai seinien pintamateriaali ei saa muodostaa pölyä eikä muistakaan rakenteista saa irrota pölyä, joka mahdollisesti vaikeuttaisi laitteistojen jäähdytystä esimerkiksi tukkimalla laitteiden jäähdytysilmanottoaukkoja tai laitteiden prosessorien tuulettimia. Hävitettäväksi tarkoitettu paperimateriaali on tuhottava IT-laitetilan ulkopuolisella paperinrepijällä päivittäin. Mahdolliset tulostimet tulisi sijoittaa eri palotilaan (pöly, palokuorma).

Tuloilman suodatuksesta on huolehdittava siten, että ulkoilman epäpuhtaudet, kuten hiekkapöly tai muu ilmassa oleva aines ei kulkeudu sisätiloihin. Ilmanvaihtokanavien siivous on hoidettava säännöllisesti, jotta niihin ei pääse muodostumaan pölyä. Siivoustarve huomioidaan vuositarkastuksien yhteydessä. sennuslattian alapohja on siivottava säännöllisesti, esimerkiksi kerran vuodessa.

2.8 Suojautuminen tärinää vastaan

Laitteen oman vaimentimen liikevara lepoasennon molemmin puolin sekä pysty- että vaakasuunnassa on huomioitava laitevaurioiden välttämiseksi. Iskunkestävyys ja tärinäkestävyys ovat kovaan maaperään sijoitettujen IT-laitetilojen kannalta tärkeässä asemassa. Maaperän vavahtelu esimerkiksi erilaisten räjähdysten ja seismisten ilmiöiden johdosta vaikuttavat eri tavalla johtuen maaperän laadusta ja etäisyydestä vavahtelun aiheuttajaan.

Suojauduttaessa tärinää vastaan tulee varmistua laitehyllyjen ja –kaappien riittävästä kiinnityksestä ja tärinävaimennuksesta.

2.9 Suojautuminen kemiallisia vaikutuksia vastaan

Ilmanvaihtolaitteiden suodattimien ja kulkuovien suunnittelussa on huomioitava kriisiaikana mahdollisesti ilmassa olevien kemiallisten aineiden vaikutus suodattimien toimintaan.

Ilmanvaihtolaitteet on varustettava kaasu- ja hiukkassuodattimilla. Tilat on tiivistettävä ylipaineistusta silmällä pitäen. Kaasunilmaisimia on käytettävä tulevan ilman laadun valvontaan silloin, kun ilmaisimien herkkyys sekä reaktioaika ovat sellaisia, että suotimet voidaan kytkeä käyttöön ilmaisimien antaman tiedon perusteella. Tämä pidentää oleelli-

sesti suotimien käyttöikää. Ilmaisinta voidaan käyttää myös ilmaisemaan suodatetun ilman laatua sen turvallisuuden varmistamiseksi.

IT-laitetilan ovet, luukut, laitteet, kanavat, putket ja näiden kannattimet sekä muut syöpymiselle alttiit osat ja varusteet on suojattava tarkoituksenmukaisella tavalla korroosiolta.

2.10 Suojautuminen sähköverkon häiriöitä vastaan

Sähkön häiriötön saanti on varmistettava katkottoman sähkönsyötön turvaavilla laitteilla. Sähkön saanti on varmistettava myös varavoimageneraattoreilla, joiden toiminta on testattava määräajoin. Tilojen suunnittelun yhteydessä suoritettavien kuormituslaskelmien perusteella voidaan arvioida, onko erillinen varavoimalaitteisto tarpeellinen vai riittävätkö UPS-laitteet.

Sähkötilat on osastoitava EI 60-luokan rakennusosin ja kaapelien läpivientien tiivistysten on oltava samaa paloluokkaa kuin seinien. IT-laitetilojen ja niissä olevien laitteistojen suojaamiseen sähköhäiriötä vastaan soveltuvat erotusmuuntajat, verkkosuotimet ja verkkojännitestabilisaattorit sekä katkottoman sähkön saannin turvaavat laitteet. Sähkön saanti on huomioitava myös laitetilan erillisen ilmastoinnin käytössä, sillä mahdollisen sähkökatkon aikana eivät laitetilat voi olla ilman asianmukaista ilmastointia. Laitteistojen häiriöherkkyyteen suoraan vaikuttavia tekijöitä ovat maadoitukset, järjestelmän suunnittelu, toimintanopeus, datayhteydet muihin laitteisiin ja muut sähkölaitteet, joiden läheisyydessä toimitaan.

Sähkönsyöttöhäiriöt ovat vaikutuksiltaan vakavia. IT-laitteet käyttävät maapotentiaalia kaikkien toimintojensa referenssinä eli vertailutasona. Salaman iskun yhteydessä syntyvät voimakkaat magneetti- ja sähkökentät saattavat indusoida jännitteitä johdinsilmukoihin ja aiheuttaa jännite-eroja eri johtimien välillä. Todennäköisyys, että suojaamattomaan yhden neliömetrin silmukkaan salamaniskusta indusoituva sähkömotorisen jännitteen huippuarvo ylittää 50 V on pieni, alle kerran viidessä vuodessa.

2.11 Suojautuminen sähkömagneettista säteilyä vastaan

IT-laitetiloja suunniteltaessa on selvitettävä, onko lähietäisyydellä jo olemassa tai suunnitteilla niin voimakkaita radiolähettimiä, tutkia tai muita laitteita, että niiden aiheuttama kenttävoimakkuus ylittää tietokonelaitteistojen valmistajan määrittelemän suurimman sallitun kenttävoimakkuuden. Jollei valmistaja tällaista arvoa ilmoita, ohjearvona voidaan pitää kenttävoimakkuutta 1 V/m.

Sähkömagneettisen säteilyn tietoliikennelaitteita tuhoava vaikutus perustuu energiapulsseihin, jotka indusoituvat antenneihin tai antenneina toimiviin johtimiin. Vaurion syntymisen herkkyys riippuu laitteiston herkkyydestä, sähkömagneettisen kentän voimakkuudesta ja antennien sekä antenneina toimivien johtimien ominaisuuksista. Tällaisen suurienergisen sähkömagneettisen pulssin voi synnyttää joko korkealla tapahtuva ydinräjähdys (EMP) tai radiotaajuinen ase (konventionaalinen EMP-ase tai suurtehomikroaaltoase, HMP). Sähkömagneettisilta aseilta suojautumisen tarve ratkaistaan uhka-arvion perusteella.

Omien laitteiden osalta sähkömagneettinen hajasäteily tulee huomioida suojaustasolta III alkaen ja tarvittaessa on ryhdyttävä ns. TEMPEST-vastatoimiin toimivaltaisen viranomaisen[16] ohjauksen mukaisesti.

2.12 Suojautuminen laitevauriota vastaan

IT-laitteistojen ja ilmastointilaitteistojen sekä niiden oheislaitteiden vikaantumiseen on varauduttava. Laitevaurioiden varalta järjestelmä varustetaan automaattisilla laitteistovarmistuksilla. On myös suositeltavaa sopimalla valmistajan tai maahantuojan kanssa toiminnan takaava huoltosopimus. Ehkäisevä huolto on tehtävä valmistajan tai maahantuojan ohjeiden mukaan. Kaikista huoltotoimista tulee pitää kirjaa.

2.13 Suojautuminen henkilöstön väärinkäytöksiä vastaan

IT-laitetilat on siivottava ja huollettava vain tilojen ollessa miehitettynä riippumatta siitä, käytetäänkö omia siivoojia, huoltohenkilöitä vai ulkopuolista siivousliikettä tai huoltoyrityksiä. Ulkopuoliset toimijat sidotaan noudattamaan turvallisuusmääräyksiä turvallisuussopimuksilla ja vaitiolositoumuksilla (pääasiakirjan liite 7). Sekä ulkopuolisesta, että omasta henkilöstöstä pyydetään turvallisuusselvitykset turvallisuusselvityslain mukaisesti.

IT-laitetiloissa käyvien omien henkilöiden kulku tulee järjestää siten, että jokaisella on omana työaikanaan pääsy vain niihin tiloihin, joissa hänen työtehtäviensä takia tarvitsee oleskella. Henkilöstön käyntejä on seurattava säännöllisesti kulunvalvontajärjestelmän lokitiedostoista.

Kulunvalvonta varmistuksia sisältäviin tiloihin tulee järjestää siten, että kukaan ei voi päästä sinne ilman, että käynnistä jää merkintä kulunvalvontalokiin.

2.14 Suojautuminen ilkivaltaa vastaan

Murtojen ja sabotaasin estämiseksi on IT-laitetila järkevää sijoittaa alempien turvallisuusvyöhykkeiden sisälle. Rakenteita suunniteltaessa huomioidaan turvallisuusvaatimusten täyttyminen.

Teknisinä apuvälineinä käytetään kulunvalvontajärjestelmää, poikkeavien työaikojen kontrollointia ja poikkeamaraportointia sekä tunkeutumisen ilmaisujärjestelmiä.

Tiloissa vierailevien henkilöiden mukanaan tuomat varusteet tarkastetaan sabotaasiyrityksen varalta (esim. HPM-salkkupommi).

[16] Viestintäviraston NCSA-yksikkö

2.15 Suojautuminen HPM-hyökkäystä vastaan

Kriisitilanteissa tyypillisiä IT-laitetiloja vastaan käytettäviä aseita ovat kranaatit, pommit ja ohjukset; erityisesti miina- ja erikoispommit sekä ns. täsmäaseet. Elektronisen sodankäynnin kehittyessä myös mikroaaltoaseiden käyttö on mahdollista.

Mikroaaltoaseiksi (HPM) kutsutaan laitteita, joiden toimintaperiaatteena on lähettää tuhovaikutuksen aikaansaavaa mikroaaltotaajuista sähkömagneettista säteilyä. Mikroaaltoaseet toimivat yleensä yli 1000 MHz:n taajuudella ja saavutettavat hetkelliset tehot ovat jopa tuhansia megawatteja. Aseen toiminta edellyttää näköyhteyttä kohteeseen.

Suojautumisen HPM-aseita vastaan tulee lähteä uhan määrittelystä, eli siitä, mitä järjestelmiä vastaan näitä aseita tultaisiin käyttämään ja minkälaista asetta hyökkäyksessä käytettäisiin. Ensin on määriteltävä toimintaympäristön sähkömagneettinen uhka, joka määrittää järjestelmien kestokynnyksen. Tämän perusteella voidaan joko määritellä laitteilta edellytettävä sähkömagneettinen suojataso käyttäen parametrina tilojen suojatasoa, tai määrittää laitetiloille asetettavat vaatimukset laitteiden ympäristönkestokyvyn perusteella.

Korkean tietoturvatason IT-laitetilojen suunnittelussa on olennaista tietää, kuinka etäälle HPM-ase on torjuttava, jottei se kykenisi uhkaamaan elektronisia laitteistoja. Kertakäyttöisillä aseilla voidaan paikallisesti aikaansaada samantyyppinen sähkömagneettinen pulssi, kuin minkä korkealla tapahtuva ydinräjähdys aiheuttaa (EMP).

3 IT-laitetilojen tietoturvallisuustoimenpiteet osa-alueittain

Organisaation tietojärjestelmän sisältämät tiedot ja niiden tärkeys organisaatiolle määrittelevät IT-laitetilojen suojaamisen tason ja mahdollisesti tarvittavan lisäsuojatarpeen.

3.1 Yleiset periaatteet

Organisaation tietoturvariskikartoituksen ja eri uhkien määrittelyn perusteella saadaan selville tekijät, jotka ohjaavat IT-laitetilojen rakenteellista suunnittelua ja turvallisuusteknisiä vaatimuksia. Kartoitusten tuloksia käytetään valittaessa IT-laitetilojen sijaintia rakenteissa sekä olemassa olevien tilojen kehittämissuunnitelmia laadittaessa.

Asiakirjat, joissa käsitellään organisaation tietoturvasuunnitelmaa, -politiikkaa sekä -strategiaa on pidettävä ajan tasalla. Välttämättömäksi katsottavia asiakirjoja ovat tietojen ja tilojen luokitukset sekä tarvittaessa poikkeusolojen turva-, toipumis- ja valmiussuunnitelmat. Asiakirjat tulee säilyttää turvallisesti.

IT-laitetilan turvallisuus- ja palotarkastuksen suorittaa ulkopuolinen taho. IT-laitetilan rakenteisiin ja laitteisiin ei saa tehdä muutoksia ilman tiloista vastaavan henkilön lupaa.

3.2 Fyysinen turvallisuuden toteutuksen erityispiirteitä IT-laitetiloissa

3.2.1 Kulunvalvonta

Kulunvalvonnan järjestelyissä tavoitteena on se, että luvallinen henkilökulku voi tapahtua mahdollisimman joustavasti, mutta luvaton kulku voidaan estää. Kulkuavain ja siihen liittyvä turvakoodi, henkilökortti ja yksityiskohtaiset kirjalliset kulkuohjeet annetaan kuittausta vastaan. Kulkuoikeudet myöntää tilan käytöstä vastaava organisaatio ja ne tarkastetaan sovituin välein.

Kameravalvontajärjestelmän (tallentava) avulla voidaan vartiointipisteestä seurata tapahtumia laitetiloissa sekä kulkua niihin. Kameravalvonnan järjestelyt eivät saa olla sellaisen henkilön vastuulla, joka itse työskentelee IT-laitetilassa. Ennen valvonnan käyttöönottoa henkilöstölle on selvitettävä kameravalvontaan liittyvät lakisääteiset aspektit (ks. pääasiakirja 5.2).

Huolto- ja asennushenkilöstö ilmoittautuu vastaanottopisteessä, jossa heidän henkilöllisyytensä tarkastetaan, jonka jälkeen he saavat esillä pidettävän vierailijakortin. Vieraat noudetaan ja saatetaan vastaanottopisteeseen. Vastaanottopisteessä on oltava lista henkilöistä, jotka saavat hätätapauksissa mennä yksin IT-laitetilaan. IT-laitetiloissa pidetään käynneistä kirjaa, joihin merkitään ajankohdat, vierailija sekä toimenpide mitä varten tiloissa käytiin.

3.2.2 Laite- ja kytkentätilat

Laitetilojen rakentamisen suunnittelussa tulisi huomioida laitetilaa tukevien automaatio-, palo- ja muiden laitteiden sijoittelu. Sijainnin tulisi olla itse laitetilan ulkopuolella, jolloin huoltotoimenpiteiden takia ei tarvitse päästää ylimääräistä henkilöstöä itse laitetilaan.

Osastoivissa seinissä ja välipohjissa olevien kaapeleiden ja putkien läpivientien on oltava samaa paloluokkaa kuin seinien ja välipohjien. Osastoivien ovien ja laitetilojen ovien palonkestoajan tulee olla yhtä pitkä kuin osastoivilta seiniltä vaadittu palonkestoaika.

Kaikkien tilojen seinien, kattojen ja lattioiden pintakerrosten syttymisherkkyysluokan on oltava yksi ja palonleviämisluokan yksi.

Miehittämätön IT-laitetila tulisi pyrkiä sijoittamaan rakennuksen keskelle ikkunattomaan tilaan ja osastoida erilleen muista IT-laitetilan tiloista.

Alas laskettu katto on tehtävä syttymättömistä materiaaleista. Se on kiinnitettävä siten, ettei se tai sen osat pääse putoamaan sammutuslaitteiston laukeamisen yhteydessä.

Asennuslattia rakenteineen on tehtävä syttymättömästä materiaalista. Lattian on oltava puolijohtava ja se on maadoitettava yhden kilo-ohmin vastuksella. Puolijohtavuus on todettava käyttöönottomittauksin. Mittaukset uusitaan määräajoin. PVC:tä sisältäviä pintamateriaaleja ei saa käyttää lattiamattona. Asennuslattian alapohjaan on päästävä helposti esimerkiksi siivousta varten. Lattiamateriaalina voidaan käyttää HPL-laminaattia, joka on antistaattinen. Tilassa liikuttaessa on käytettävä puolijohtavalle lattialle tarkoitettuja jalkineita.

Tilassa on oltava asianmukaiset (pelastusviranomaisten määrittämät) ilmaisimet ja sammutusjärjestelmä. Ilmaisimet tulee kytkeä jatkuvassa reagointivalmiudessa olevaan hälytyskeskukseen.

Laitetiloihin ei saa asentaa muita kuin tietokonelaitteistoihin kuuluvia verkkokaapeleita, sähkökaapeleita, putkistoja tai ilmastointikanavia.

Pelastusyksiköiden toiminnan kannalta voi korkean suojaustason tiloissa olla viranomaisten viestiyhteyttä varten tarvittava laitteisto. IT-laitehuonetta varten tulee olla oma erillinen putkisto. Käytettäessä vuotovesi-ilmaisimia saadaan hälytys mahdollisesta vesivahingosta.

3.2.3 Rakennusmateriaalit

Korkean tietoturvatason IT-laitetilojen rakennesuunnittelussa on huomioitava tämän liitteen 4 ensimmäisessä luvussa esitetyn taulukon erityistekijät. Tämän liitteen luvussa 7 on kuvattu lisäksi erilaisia asevaikutuksia, joilla saattaa tiettyihin riskeihin varauduttaessa olla vaikutusta rakennesuunnitteluun. Organisaatiota kohtaan suunnattuun ilkivallan tekoon (sabotaasi) saatetaan esimerkiksi käyttää helposti saatavia kaupallisia räjähteitä.

IT-laitetila ei saa rajoittua tilaan, jossa on suurempi kuin 1200 MJ/m2 palokuorma. Maanalaisen laitetilan katon ja ympärysseinien tulee olla teräsbetonia tai vastaavasta materiaalista, ja rakennuksen sortuman kestäviä. Myös ovien valinnassa on huomioitava sortuman kuormitus. Betoni- ja teräsbetonirakenteita koskevissa määräyksissä ja ohjeissa (Sisäasiainministeriön määräykset ja Suomen rakentamismääräyskokoelma) on teräsbetonin käytöstä ja raudoituksen murtovenymävaatimuksia koskevia ohjearvoja.

Jos eri IT-laitetilojen ympärysseinät koskettavat toisiaan, on tilojen väliin jätettävä liikuntasauma.

IT-laitetilan sisäiset seinät saavat olla kevytrakenteisia, jollei osastoitavien tilojen käytöstä johdu muuta tietoturvallisuuteen liittyvää vaatimusta. IT-laitetilan huonekorkeuden tulee olla ainakin 2,3 metriä. Vähäisiltä osin, kuten palkkien ja kanavien kohdalla, vapaa korkeus saa olla pienempikin, ei kuitenkaan alle 2,0 metriä. IT-laitetilan ympärysrakenteilla tarkoitetaan tilaan kuuluvia tiloja rajoittavia, kuormituksia vastaanottavia ympärysseiniä, kattoa ja lattiaa.

Kallioon rajoittuvassa IT-laitetilassa on teräsbetoniset ympärysrakenteen osat kiinnitettävä lujasti ja tiiviisti ympäröivään kallioon. Tarvittaessa kalliokatto on lujitettava kiinnijuotettavilla pulteilla, teräsverkolla sekä ruiskubetonikerroksella.

Kallioon rajoittuvan lattian pintakerros voidaan tehdä ympärysrakenteisiin kuulumattomana tavanomaisena maavaraisena lattiana. Tilaan johtavien ovien rakenteen, asennuksen ja lukituksen on oltava järeillä työkaluilla tapahtuvan murron kestäviä.

Kaikkien tilojen seinien, kattojen ja lattioiden pintakerrosten syttymisherkkyysluokan on oltava yksi ja palonleviämisluokan I. Seuraavia rakennustarvikkeita voidaan pitää palamattomina ilman testausta ja erillistä hyväksyntää:

- luonnonkivestä valmistetut tuotteet
- betoni ja betonituotteet
- poltetut savitiilet ja kalkkihiekkatiilet
- keraamiset tuotteet ja lasituotteet
- rakennustarkoitukseen käytettävät teräs ja muut metallituotteet.

Palokuorman laskentaan liittyvät kaavat ja ohjearvot ovat Ympäristöministeriön julkaisemassa oppaassa " Rakennusten paloturvallisuus & Paloturvallisuus korjausrakentamisessa".

3.2.4 Sähkönsyöttö

Määräysten mukaan pienjännitejakelussa on käytettävä TN-S-järjestelmää pääkeskuksesta ähtien. IT-laitteille vedetään oma 5-johtiminen nousujohto pääkeskukselta lähtien ja IT-laitetila varustetaan omalla 5-kiskoisella keskuksella. Muita kuin IT-laitteita varten tulee järjestää oma nousujohto. IT-käyttöön tarkoitetut pistorasiat on merkittävä selvästi muista rasioista erottavalla tavalla.

IT-laitetilaan voidaan järjestää maadoituskisko yhden pisteen maadoitusta varten. Ilmanvaihtolaitteistolle, valaistukselle ja pistorasioille on asennettava kullekin erilliset ryhmäjohdot.

Sähkölaitteet on mitoitettava riittäviksi. PVC-eristeisiä kaapeleita tulee välttää ja niiden asemasta on käytettävä HL- tai FRHL-kaapeleita. IT-laitteistot on voitava saattaa sähköttömiksi sähköturvallisuusmääräysten vaatimusten mukaisesti. Laitteistojen sähkönsyöttö on voitava katkaista varsinaisen laitetilan ulkopuolelta esimerkiksi UPS-keskuksen katkaisijasta. Katkaisinten sijainti on merkittävä ja niiden väärinkäyttö on estettävä.

Kaikkien kaapeleiden läpivientien tiivistysten on oltava samaa paloluokkaa kuin seinien. Sähkötilat on osastoitava EI 60-luokan rakennusosin.

IT-laitetilojen käytön perusteella voidaan rakentaa varmistustasoja seuraavasti:

1. taso yksilinjainen varmistus, ei varalaitteita, N-periaate
2. taso yksilinjainen varmistus, varalaitteet, N+1 periaate
3. taso kaksilinjainen periaate, joista toinen linja on passiivinen, N+1 periaate
4. taso kaksilinjainen periaate, jotka molemmat ovat aktiivisia, N +1 periaate

Neljännen tason järjestelmä soveltuu tärkeisiin jatkuvassa reaaliaikaisessa käytössä oleviin IT-laitetiloihin, joissa tärkeimmät laitteet on varmistettu kaksilla tehoyksiköillä tai laitteistot on kahdennettu.

3.2.5 UPS (keskeytymätön sähkönsaanti)

UPS *(uninterruptible power supply)* suojaa laitteet sähköverkon aiheuttamilta häiriöltä, jännitetransienttivaurioilta ja jännitteen vaihtelulta. UPS-laitteistoja suositellaan käytettäviksi kaikkien IT-laitetilojen katkeamattoman sähkön syötön varmistamisessa.

Sähköverkon yleisimmät häiriöt ovat:

- hetkellinen alijännite
- lyhyt katkos
- maadoitusjännite

- toistuva häiriö
- hetkellinen ylijännite
- 2- tai 4-kertainen nimellistaajuus.

UPS-laitteisto on mitoitettava toimimaan niin pitkään, että häiriö poistuu varavoiman syötön käynnistymisen tai häiriön poistumisen vuoksi. Tämänkin jälkeen UPS toimii suodattimena sähköverkon ja IT-laitteiston välillä. Järjestelmän alasajotoimia on myös harjoiteltava ja UPS:n huolto-ohitukset kirjattava.

IT-laitetilojen hätävalaistus on varmistettava akuilla. Luotettavaan varasähkön saantiin liittyy akkuhuolto.

3.2.6 Varavoima

Varavoimakoneet on sijoitettava omaan palo-osastoonsa, samoin kuin niiden tarvitsema polttoaine. Varavoimakonetila on tyypillisesti suojattava kohde, johon pääsy on rajattava kulunvalvonnallisin keinoin vain niille, joiden työtehtäviin kuuluu varavoimasta huolehtiminen. Polttoainemäärä mitoitetaan riskiarvion mukaiseksi ja sen laatua seurataan säännöllisesti mm. mahdollisen kosteuden syntymisen vuoksi. Laitteistoa tulee koekäyttää ja huoltaa säännöllisesti automaattisen toiminnan varmistamiseksi. Varavoiman on riitettävä teholtaan kaikille IT-laitetilassa sähköä käyttäville laitteistoille, ilmanvaihdolle, jäähdytykselle sekä valaisimille.

3.2.7 EMP (sähkömagneettinen pulssi)

Korkean tietoturvatason mukaisten kiinteiden IT-laitetilojen suunnittelussa on huomioitava EMP:n[17] vaikutusta vastaan suojautuminen. Räjähdyksessä syntyvä EMP voi vaikuttaa satojen, jopa tuhansien kilometrien päässä, kun mekaaniset vaikutukset ovat paikallisia.

Sähkömagneettisen pulssin (EMP) energiasta yli 90 % on alle 10 MHz:n taajuuksilla. Juuri tästä syystä EMP-suojaus ei välttämättä tarjoa suojaa HPM-asetta vastaan. Säteilypulssikentän vaimentaminen paikallisesti laitteiston ympärillä toteutetaan ympäröimällä suojattava laitteisto yhtenäisellä metalliverhouksella tai metalliverkolla. Näin estetään EMP:n kytkeytyminen laitteiden sisäisiin johdotuksiin ja laitekokonaisuutta yhdistäviin kaapeleihin. Suojattavan tilan ulkopuolelle ulottuviin johtoihin kytkeytymistä huononnetaan maadoitetuilla metallivaipoilla, ylijännitesuojilla ja suodattimilla.

Avojohtoihin ja antenneihin indusoituneiden virtojen ja jännitteiden etenemistä suojattuihin laitteisiin estetään ylijännitesuojilla, jotka rajoittavat läpi pääsevän pulssin amplitudia, ja hyötylähteen salliessa suodattimilla, jotka päästävät energiaa lävitseen vain osalla pulssin sisältämästä taajuusalueesta. Laitteistoja voidaan suojata johtoja pitkin tulevilta jännitteiltä ja virroilta myös erottamalla laitteet johdoista esimerkiksi lähetteen siirtoon sopivilla optoeristimillä.

[17] EMP:n tekninen määritelmä: luku 7.

Materiaalivaatimukset johdotetaan teoreettisesta vaimennuksesta, jonka umpinainen homogeeninen pallon muotoinen suoja antaa sitä ympäröivälle magneettikentälle.

Halkaisijaltaan kolmen metrin suojien minimivaimennukset eri materiaaleilla ovat:

Materiaali		**EMP suoja 40 dB**	**EMP suoja 70 dB**
Teräs	0,06 mm	0,3 mm	
Alumiini	0,015 mm	0,5 mm	
Kupari	0,01 mm	0,3 mm	

Materiaalin paksuus määräytyy vaimennusvaatimuksesta 50 kHz:n taajuudella, joka on 70 dB:n ja 40 dB:n vaatimusten alarajataajuus.

Signaalin vieminen sähkömagneettisesti suojattuun tilaan vaatii ylijännitesuojauksen ja suojausvaatimuksen edellyttämän toisiosuojauksen. Häiriöiden kytkeytymistä johtimiin voidaan vaimentaa suojavaipalla. Suojavaippaan kytkeytyvä virta johdetaan suojatun tilan kuoreen ja näin häiriöt eivät pääse kytkeytymään järjestelmän sisälle. Koaksiaalisessa järjestelmässä kaapelin ulkojohdin toimii suojavaippana. Käyttämällä tiivistä ulkojohdinrakennetta, joka liitetään läpiviennissä suojakuoreen, saadaan riittävä suojaus.

Metallivahvistuksia ja -johtimia sisältämättömät valokaapelit ovat tunteettomia sähkömagneettiselle häiriölle.

Suojattaessa IT-laitteet kiinteään EMP-tilaan on huomioitava seuraavat VTT:n tutkimuksissa todetut seikat:

– mikroaaltosäteilyn vaimennus luolatiloihin on noin 110 - 150 dB, mutta ilmastointiputkitus laskee vaimennuksen ilmastointireitillä 40 - 80 dB tasolle.
– maanpäällisissä suojatiloissa seinä- ja ovimateriaalin tuoma vaimennus on 90-130 dB, mutta ilmastointi pudottaa vaimennuksen 50-80 dB tasolle. Alle 12 GHz:n taajuuksilla vaimennus on yli 50 dB, jos ilmastointiverkosto on kohtalaisen pitkä ja mutkikas. Toisaalta pitkäkin verkosto laskee suojauksen 70-80 dB tasolle. Kaapelikuilut ja kaapelit eivät näytä toimivan siirtoteinä alle 12 GHz:n taajuuksilla.

EMP-tilaan johtavat oviaukot toteutetaan siten, ettei sähkömagneettinen suojaympäristö kärsi oven ja karmin välyksen (metallikarmit tiivistetään maadoitusnauhoilla) tai oven käytön takia.

3.2.8 Ylijännitesuojaus

IT-laitteiden sähkönsyötön on täytettävä jännitetason ja taajuuden asettamat vaatimukset. Jännitepiikkien on pysyttävä tietyissä rajoissa, jotteivät laitteistot vaurioidu.

Syöttöjännitteen kestävyyden vaihtelut ovat yleensä – 8 … + 10 % ja syöttötaajuuden vaihtelu +1 %. Massamuistiasemat eivät ole yhtä herkkiä jännitetason vaihteluille kuin keskusyksiköt, mutta sitäkin herkempiä syöttötaajuuden vaihtelulle. Suurin osa hetkellisistä sähköhäiriöistä johtuu omista verkkoon kytketyistä laitteista, muuntajista, sähkömoottoreista ja valaistuksesta. Tästä syystä IT-laitteiden sähkönsyöttö on toteuttava omalla nousujohdolla.

Sähkökaapelit on asennettava erilleen datakaapeleista ja ne tulee johtaa IT-laitetiloihin useammasta kuin yhdestä kohdasta.

3.2.9 Palo-osastointi

IT-laitetilat on osastoitava erilleen muista palotiloista. Rakenteet määräytyvät tilojen palokuorman perusteella.

Viereisen tilan palokuorma	**Käyttötapa, palovaarallisuusluokka**	**Osastointi**
Alle 600 MJ/m^2	Toimistohuone, palovaarallisuusluokka 1-2	EI60
600-1200 MJ/m^2	Suurmyymälä ja teollisuus, palovaarallisuusluokka 3	El120
Yli 1200 MJ/m^2	Teollisuus, palovaarallisuusluokka 4-5	EI240

Miehittämätön IT-laitetila on osastoitava vähintään luokkaan EI120.

3.2.10 Staattiselta sähköltä suojautuminen

Kaikissa IT-laitetiloissa toteutettavissa laitteiden huoltotöissä on käytettävä puolijohtavaa työalustaa ja maadoitusranneketta. Antistaattinen lattiamateriaali varmistaa suojautumisen hankaussähköltä. Myös oikea ilmankosteus (ilmastointi) vähentää staattisen sähkön muodostumista.

3.2.11 HPM-aseelta suojautuminen

Korkean tietoturvatason mukaisten kiinteiden IT-laitetilojen suunnittelussa on huomioitava uhka-arvioperusteisesti HPM-aseen käyttöä vastaan suojautuminen. HPM-ase toimii yli 1 GHz:n taajuuksilla, joten EMP-suoja saattaa olla täysin tehoton HPM-asetta vastaan.

Seinämateriaalin vaimennuksia eri taajuuksilla on kuvattu seuraavassa taulukossa:

Seinämateriaali	**Taajuus**	**Vaimennus**
Lastulevy	2 GHz	4 dB
Lastulevy	60 GHz	5 dB
Betoni	2 GHz	1 dB
Tiili 120 mm	2 GHz	4 dB
Tiili 360 mm	2 GHz	10 dB
Ikkuna	2 GHz	0,5 dB

Teräsbetoniseinän vaimennus eri taajuuksilla on kuvattu seuraavassa taulukossa:

Taajuus GHz	25 cm	16 cm
1	10 dB	8 dB
2	14 dB	11 dB
4	32 dB	17 dB
6	35 dB	31 dB
8	58 dB	32 dB
10	68 dB	32 dB
12	80 dB	32 dB

Betoniseinässä vaikuttaa kaksi tekijää pulssin etenemiseen; matalilla taajuuksilla betonin raudoitus toimii kohtalaisen hyvänä vaimentimena – varsinkin, jos raudoitusverkko on hitsattu yhteen. Säteilyn taajuuden kasvaessa verkon silmäkoko kasvaa säteilyn aallonpituuteen nähden, jolloin verkko ei enää mikroaalto-taajuuksilla toimi vaimentimena.

Luolatilojen suoja mikroaaltosäteilyä vastaan riippuu kulku-, ilmastointi- ja kaapelointireittien rakenteesta, pituudesta, muodosta ja mahdollisista suojarakenteista. Salkkupommin on mahdollista vaikuttaa noin puolen kilometrin etäisyydeltä suojaamatonta elektroniikkaa vastaan ja suojattuakin vastaan, mikäli se saadaan toimitettua noin 50 metrin etäisyydelle kohteesta.

Suojautuminen 100 GW:n lavettiasenteisen HPM-aseen häirinnältä on kuvattu seuraavassa taulukossa. Kyseessä on pahinta mahdollista tilannetta kuvaava malli:

Vaikutusetäisyys	Vaadittu laitetilan suojaustaso	
	Suojattu	Suojaamaton
1000 m	35 dB	55 dB
500 m	40 dB	60 dB
100 m	55 dB	75 dB
50 m	60 dB	80 dB

COTS-laitteiden (kaupalliset tuotteet) HPM-sietokyky on tyypillisesti heikompi kuin MIL-standardien (sotilaskäyttö) vaatimukset täyttävien laitteiden.

3.3 Tietoliikenneturvallisuus

3.3.1 Verkon fyysinen rakenne

Tietoliikenneyhteydet on rakennettava korkean tietoturvatason mukaisissa kohteissa vähintään kahta toisistaan riippumatonta väylää pitkin erillisiin jakamoihin, joiden välillä on mahdollisuus siirtyä käyttämään jompaakumpaa tilanteen mukaan.

Tietoliikenteen suojaamisen tavoitteena on toimivuuden suojaaminen seuraavasti:

- estää luvaton tunkeutuminen tietojärjestelmään
- paljastaa luvattomat tunkeutumisyritykset
- estää siirrettävän tiedon joutuminen sivullisten haltuun ja estää mahdollisesti sivullisten haltuun joutuneen tiedon hyväksikäyttö
- estää väärän tiedon syöttäminen tietojärjestelmään.

IT-laitetilojen tietoliikenneverkon muutoksiin tulee olla tietoliikenteestä tai tietojärjestelmästä vastaavan johdon lupa. Muutokset tulee dokumentoida ja testata ennen käyttöönottoa. Riskejä voidaan hallita jakamalla selkeästi vastuut tietoliikenteen tietoturvan hoitamisesta ja valvomalla, että sovittuja menetelmiä noudatetaan.

3.3.2 Kaapelointimateriaalit

Kaapeloinneissa on käytettävä mahdollisimman paljon valokuituja. Valokuitukaapelit eivät reagoi millään tavoin sähkömagneettiseen säteilyyn ja kestävät melko hyvin palokuormaa.

Valokuidun salakuuntelu on vaikeaa ja edellyttää fyysistä käsiksi pääsyä kaapeliin. Tästä syystä valokuidun kautta välitetyn dataliikenteen salausvaatimus voidaan tapauskohtaisesti omassa hallinnassa olevan tilakokonaisuuden sisällä korvata fyysisen pääsynhallinnan ja – valvonnan menetelmillä. Valokuitukaapelien käyttöä puoltaa myös niiden siirtonopeus, suuri kaistaleveys, kestävyys sekä pieni koko ja paino.

3.4 Laitteistoturvallisuus

3.4.1 Palvelimet

Palvelimet on asennettava tarvittaessa vaativia olosuhteita varten eristysjousien varassa oleviin asennustelineisiin, jotka vaimentavat iskuenergiaa ja tärinää. Käsiteltävien tietojen tärkeyden mukaisesti voidaan käyttää myös lukittavia laitekaappeja, joihin on liitetty aukaisun ilmaiseva valvonta.

Suojaus asennustelineissä voidaan saavuttaa käyttämällä elastisesta aineesta tehtyjä vaimentimia laitteen ja asennusalustan välissä.

Laitehuonetta suunniteltaessa on otettava huomioon ympäristöstä mahdollisesti johtuvan tärinän ja värähtelyn eristäminen. Kallioperään rakennetuissa laitetiloissa saattavat riskejä aiheuttaa lähistöllä suoritettavat louhintatyöt, joissa käytettävien räjähteiden aiheuttama energia vaikuttaa myös ympäristöönsä väliaineena olevan kiven kautta. Tehokas tärinäsuojaus erilaista värähtelyä vastaan saadaan käyttämällä jousipuristimia tai asennusalustan alle sijoitettua lasivillakerrosta tai ilmapusseja.

3.4.2 Asennustelineisiin asennettava kalusto

IT-laitetilojen tilan käyttö pyritään yleisesti optimoimaan, jolloin useita laitteita sijoitetaan tehokkaasti yhden näytön ja näppäimistön avulla hallittaviksi kokonaisuuksiksi laitekaappeihin. Myös varmistuksia suoritetaan robottien tai erillispalvelimien avulla.

Laitteistot asennetaan standardikehikkoihin, jotka maadoitetaan keskitetysti ja tärinäeristetään asennuspinnastaan. Tärinävaimennuksen on vaimennettava seismisten ilmiöiden aiheuttamat tärinät sekä mahdolliset kallioperässä tapahtuvat räjähdykset, joita suoritetaan esimerkiksi kallionlouhinnassa.

3.4.3 Jäähdytys ja ilmastointi

Ilmanvaihto on suunniteltava seuraavien periaatteiden mukaisesti:

- IT-laitetilaa varten on oltava oma erillinen ilmanvaihtojärjestelmä
- IT-laitetilassa (palvelintila) tulee olla korkeampi paine kuin ympäröivässä tilassa
- suunnittelussa on huomioitava tarve savu- ja sammutuskaasujen poistoon
- sammutuslaitteiston laukeamisen on pysäytettävä ilmanvaihtolaitteiston toiminta
- savun kulkeminen ilmanvaihtojärjestelmän kautta osastosta toiseen on estettävä.

Jäähdytys- ja ilmastointijärjestelmä tulee sijoittaa erilliseen palo-osastoon.

Jäähdytysjärjestelmä pitää varmistaa ja siitä pitää olla huoltohälytysyhteys siltä varalta, että kapasiteetti laskee vaurion johdosta. Tarvittaessa on oltava käytettävissä varajäähdytysjärjestelmä, jota voidaan käyttää myös huollettaessa varsinaista järjestelmää. Rajalämpötilan minimi on 20 celsiusastetta ja maksimi 26 celsiusastetta. Suhteellisen kosteuden asetusarvo on 50% , hälytysrajaminimi 32 % ja hälytysrajamaksimi 60 %.

Puhallusaukkojen sekä poistokanavien sijainti

Tuloilma johdetaan huonetilaan asennuslattian ilmanvaihtolevyjen kautta. Poistokanavat kiertävät huonetilan yläosassa. Poistoilmakanavassa on säädettävät poistoilmasäleiköt, joita säätämällä saadaan tasainen lämpötila huonetilaan ja ylipaine ympäröiviin tiloihin nähden.

IT-laitteiden kosteus- ja lämpötila-antureiden sijoittamisessa tulee ottaa huomioon puhallusaukkojen sijainti niin, ettei tuloilma vääristä mittaustuloksia. IT-laitetilaan otettava ilma on tarvittaessa voitava tehokkaasti suodattaa. Suodatuksen aikana ilmavirran tulee olla vähintään 0,9 dm3/s varsinaista laitetilan neliömetriä kohden. IT-laitetilassa on voitava ilmanvaihtojärjestelmän avulla ylläpitää ylipainetta silloin, kun ilman saanti tilan ulkopuolelta on mahdollista.

IT-laitetilan ilmanvaihtojärjestelmä käsittää seuraavat osat:

- raitisilmakanava, jolla ilma johdetaan IT-laitetilaan
- ilmanvaihtolaitteisto, jolla ilma otetaan IT-laitetilaan ja tarvittaessa suodatetaan

- jakokanavisto tuloilmaventtiileineen, jolla ilma jaetaan IT-laitetilan eri osiin
- poistoilmaventtiili, jonka kautta ilma poistuu IT-laitetilasta sulkuhuoneeseen, mikäli
- sellainen on IT-laitetilan käytössä
- ylipaineventtiili, jonka kautta ilma poistuu IT-laitetilasta ja joka säätelee tilan ylipainetta
- ylipainemittari, joka osoittaa IT-tilan ja ulkoilman välisen paine-eron.

IT-laitetilan raitisilma tulee ensisijaisesti ottaa rakenteiden sortuma-alueen ulkopuolelta. Ilman ottokohdan korkeus sen alapuolelta olevasta vaakapinnasta on oltava vähintään 80 cm. Ilma on johdettava tulemaan ilmanottoaukkoon alhaaltapäin.

3.5 Tietoaineistoturvallisuus

3.5.1 Varmistukset ja niiden sijoitus

IT-laitetilan tietovälineet säilytetään erillisessä käyttöarkistossa ja varmuusarkistossa, jotka ovat eri tiloissa. Arkistotilojen tulee täyttää pääasiakirjan liitteen 1 mukaiset vaatimukset. Niihin pääsy on rajoitettu käytössä olevan turvallisuusdokumentaation mukaisesti.

Tietojätevaraston tulee sijaita erillisessä palo-osastossa. Poikkeusoloja varten voidaan varautua ottamalla säännöllisesti suojakopiot ja sijoittamalla ne eri tiloihin kuin laitteistot.

3.6 Käyttöturvallisuus

3.6.1 Ohjeet ja hälytykset häiriötilanteissa

Hälytykset ohjataan keskitettyyn valvontapisteeseen tai henkilölle, joka huolehtii tilojen vartioinnista. Hälytyksen vastaanottajalla tulee olla selkeät toimintaohjeet erilaisia hälytyksiä varten.

Kaikki hälytykset ja niistä aiheutuneet toimenpiteet kirjataan tietojärjestelmään. Valvomoihin ohjatuista, kriittisiksi määritellyistä hälytyksistä tulee lisäksi ilmoittaa välittömästi organisaation vastuuhenkilöstölle.

Hälytyksiä tulee testata niiden toimivuuden toteamiseksi sekä kouluttaa henkilöstöä, joka vastaanottaa hälytyksiä.

3.6.2 Varajärjestelyt ja toipuminen

Organisaation toiminnan jatkuvuusvaatimusten mukaisesti organisaatiolla on oltava poikkeusoloja ja –tilanteita varten ajantasaiset tietojenkäsittelyn jatkuvuus-, toipumis- ja valmiussuunnitelmat, joiden mukaisesti toiminta voi jatkua mahdollisesti eri toimipisteessä ja mahdollisesti normaalitilannetta rajoitetummassa mittakaavassa.

3.6.3 Piirustukset ja laiterekisterit

IT-laitetilassa sijaitsevista laitteista on pidettävä laiterekisteriä ja tietoliikenneverkon osalta piirustusten on oltava ajan tasalla.

Piirustusten jakelu on jo suunnitteluvaiheesta alkaen pidettävä mahdollisimman pienenä, jottei ratkaisujen turvallisuus vaarannu. Rakentamisvaiheessa piirretään IT-laitetilojen ristikytkennöistä tarkat kuvat, johdotuskaaviot sekä toistinten, keskittimien ja muiden kytkentälaitteiden porttien kytkentäkaaviot. Jokaisesta lähiverkon segmentistä mainitaan sen pituus ja mitataan impedanssi sekä merkitään segmentin kaapelit.

Mittauspöytäkirja allekirjoitetaan tilojen vastaanottotarkastuksessa ja sitä säilytetään turvakaapissa yhdessä muiden laitetiloja koskevien dokumenttien kanssa.

Kaikki IT-laitteet on dokumentoitava ja kytkentäpiirustukset pidettävä ajan tasalla muutosmerkintöineen. Ristikytkennät ja kaapelit on merkittävä yksiselitteisesti.

3.6.4 Ulkoistetut IT-laitetilat

Monia julkishallinnon tietotekniikkapalveluja on ulkoistettu alihankkijoille oman organisaation ulkopuolisiin tiloihin. Näiden tilojen osalta on sopimuksilla sovittava palvelun

tasosta, auditoinneista ja tietojen varmuuskopioiden säilytyksestä. Sopimuksiin voidaan liittää erillinen kuvaus palveluntarjoajan IT-laitetilojen turvallisuudesta, mikä helpottaa mahdollista auditointia. Pääasiakirjan liitteenä 7 on kolme erilaista turvallisuussopimusmallia.

Tietojärjestelmien ja IT-laitetilojen siirrettävyyden auditoinneilla ja tarkastuksilla voidaan vakuuttua toimintaympäristön riittävästä turvallisuudesta.

4 Poikkeusoloihin varautuminen

Korkean tietoturvatason mukaisten IT-laitetilojen suunnittelussa on huomioitava mahdollinen tarve jatkaa toimintaa erillisessä varakeskuksessa tai muussa etukäteen valmistellussa varatoimitilassa.

4.1 Varakeskukset

Varakeskus on fyysisesti eri paikassa sijaitseva varatoimipiste, jossa toimintaa voidaan jatkaa poikkeusoloissa. Toiminnan käynnistämistä varten pitää olla varattuna henkilöstö sekä ajantasaiset tiedot varajärjestelmissä, joilla toimintaa jatketaan.

Varakeskuksen toimintaan liittyvät myös tarvittavien tietoliikenneyhteyksien varaukset. Toiminta on ohjeistettava ja sitä on harjoiteltava vuosisuunnitelman mukaisesti.

5 Virastokohtaisten erityistoimenpiteiden suunnittelu ja toteutus

IT-laitetilojen sijainti ja niiden erityispiirteet on etukäteen selvitettävä yhteistyössä paikallisten palo- ja pelastusviranomaisten kanssa, ellei tiloihin turvallisuussyistä ole opasteita.

Tietoturvallisuussuunnitelmassa on huomioitava tiedotustarpeet sekä sovittava, mitä asioita IT-laitetilojen tietoturvasta kerrotaan julkisesti, voidaanko tiloihin päästää vierailijoita ja saako tiloissa ottaa valokuvia.

IT-laitetilojen merkitsemistä opaskilpiin ja sisäisiin puhelinluetteloihin on järkevää rajoittaa. Tietoturvallisuuteen liittyvät asiat ovat monelta osin salassa pidettäviä, eivätkä näin ollen aktiivisen tiedottamisen kohde.

Korotetun ja korkean tietoturvatason mukaisten IT-laitetilojen järjestelmähallintaa ei lähtökohtaisesti hoideta etähallintana, jollei järjestelyä ole erikseen hyväksytty toimivaltaisen viranomaisen toimesta.

5.1 Perussuojausvaatimukset

Toimitilaturvallisuuden tärkein yksittäinen toiminto on koko kiinteistön kulunvalvonta. Muita toimitilaturvallisuuden peruselementtejä ovat tunkeutumisen ilmaisu ja siihen reagointi, lukitukset ja kameravalvonta.

Kiinteistö jaetaan toiminnot huomioiden kokonaisuuksiin, joita kutakin voidaan tarkastella turvallisuusvyöhykemallin kannalta. Osakokonaisuuksia ovat alue, rakennus ja tilaryhmä/tila. Tilalla tarkoitetaan rakennuksessa sijaitsevaa huonetta, toimistoa tai niistä koostuvaa kokonaisuutta.

Usein IT-laitetilat ovat hajasijoitetut rakennuksen eri osiin. IT-laitetilan perustason suojauskeinoja ovat varkauksien ehkäisy, tilojen kulunvalvonta, tunkeutumisen estäminen rakenteilla ja turvalukittavilla ovilla, suojautuminen tulipaloa vastaan hälyttymillä sekä suojautuminen ilkivaltaa vastaan valvonnan keinoin. IT-laitetiloissa muodostuva lämpö tai savu on huomioitava ilmastoinnissa ja olosuhdehälytyksissä. Vesivahinko vältetään oikealla LVIS-suunnittelulla sekä rakenteilla, unohtamatta olosuhdehälytyksiä. Säännöllinen siivous takaa, että tilat ovat pölyttömiä ja puhtaita eikä niissä ole ylimääräistä palokuormaa.

IT-laitetilojen palo-osastoinnin ja rakenteiden palonkestävyyden suunnittelussa on huomioitava se, millaisia paloja kohteessa voi syttyä ja millainen alkusammutuskalusto kannattaa hankkia.

Keskeytymätön sähkönsaanti varmistetaan UPS-laitteiden käytöllä ja pitempiaikaisiin sähkökatkoihin varaudutaan varavoimajärjestelyin.

Viestintäverkkojen ja -palvelujen varmistamisesta on annettu Viestintäviraston määräys 54 A/2012. Määräyksessä ilmaistaan teleyrityksille asetettavat vaatimukset tärkeysluokitella viestintäverkon ja palvelun komponentit sekä tätä kautta näitä komponentteja sisältävät laitetilat.

5.2 Uhkien selvitys ja arviointi

IT-laitetiloihin kohdistuvat uhkien selvitys ja arviointi voidaan suorittaa suojattavan tietojärjestelmän kannalta. Uhkat voidaan asettaa erilaisiin todennäköisyysluokkiin esimerkiksi niiden tapahtumatiheyden ja suuruusluokan arvion mukaan. Tällöin yksittäisessä tapauksessa voi alhaisen turvatason laitetilassa olevassa palvelimessa oleva tieto olla tärkeä osatekijä jossain suuremmassa, merkityksellisessä kokonaisuudessa.

Uhkan arvioinnin tarkoituksena on selvittää, millaisia uhkia toimintaan kohdistuu ja millaisiksi riskeiksi ne voivat muodostua. Arvioinnissa pyritään selvittämään riskin todennäköisyys ja aiheutuvan vahingon suuruus. Uhkatekijöiden tunnistaminen ja niistä organisaation toimintaan ja tietojenkäsittelyyn kohdistuvien riskien arviointi ovat perustana kaikille tietoturvallisuustoimenpiteille.

6 Lähteet

Kirjallisuus ja julkaisut

- Suojaus sähkömagneettista pulssia vastaan, VTT, teletekniikan laboratorio, loppuraportti 18.3.1991.
- Viestintäverkkojen ja -palvelujen varmistamisesta, Viestintäviraston määräys 54 A/2012
- Kaapeliasennusten paloturvallisuus, suojeluohje 1992, Suomen Vakuutusyhtiöiden Keskusliitto.
- Rakennusten käyttöturvallisuus, määräykset ja ohjeet 2001 (RakMK F2/2001)
- Suurtehomikroaaltoase (HPM) ja perusteet siltä suojautumiselle, Pääesikunta 14.4.2000.
- Sisäasiainministeriön julkaisu, S1-luokan teräsbetonisuojan teknilliset määräykset, sarja A:39. Määräys 11/91. Voimassa 1.9.1991 – 31.8.2001.
- Sisäasiainministeriön julkaisu, Kevyen väestönsuojan teknilliset määräykset, sarja A:34. Määräys 5/91 1.9.1991 alkaen toistaiseksi.
- Sisäasiainministeriön julkaisu, S1-, S3-, ja S6-luokan kalliosuojien sekä S3-luokan teräsbetonisen suojan teknilliset määräykset, sarja A:55. Määräys 15/95 1.4.1998 alkaen toistaiseksi.
- Suomen rakentamismääräyskokoelma
- Rakennusten paloturvallisuus & Paloturvallisuus korjausrakentamisessa 2012, Ympäristöministeriö.

7 Määritelmiä

Erilaisia asevaikutuksia sekä räjähteiden aiheuttamia vahinkoja.
Miinapommin teho perustuu sen sisältämään räjähdysaineeseen, jota on yleensä 40-60 % kokonaispainosta. Erikoispommeista tärkeimpiä ovat panssaripommi ja FAE-pommi (Fuel Air Explosive). Edellisen teho perustuu sen paksuun kuoreen ja betoniin hyvin tunkeutuvaan muotoiltuun kärkeen. Jälkimmäinen vaikuttaa kohteeseen korkealla ja laajaalaisella ylipaineella.

Raskaan tykistön 155 mm:n sirpalekranaatin (tykistöammus) sirpaleen pysäyttämiseksi tarvitaan suojarakenteissa esimerkiksi puuta 40 cm, terästä 2,6 cm, teräsbetonia 15 cm, tiiliä 30 cm ja säkeissä olevaa hiekkaa 50 cm. Samainen kranaatti tunkeutuu räjähtämättä keskimäärin saveen 12 metriä, moreeniin 4 metriä ja betoniin 80 cm.

Kun kranaatti tai pommi räjähtää suljetussa tilassa tunkeutumisen jälkeen, räjähdysvaikutus ruhjoo lähellä olevia kohteita. Ilmakuljetteinen 500 kg:n miinapommi rikkoo kuivan maan sisässä kahdeksan metrin päästä 20 cm:n paksuisen betoniseinän. Primäärienergiana käytettävän räjähdysaineen energia tilavuusyksikköä kohden on hyvin suuri, 10 GJ/m3 luokkaa.

Polttovaikutukseen perustuva napalm-pommi liimautuu kohteeseen ja palaa noin 2 minuuttia, kehittäen 800 – 1200 celsiusasteen lämpötilan.

Siviiliräjähteet
Siviiliräjähteistä tavanomaisimpia ovat kalliolouhinnassa käytetyt dynamiitti ja aniitti. Avoimessa tilassa tapahtuvan pintaräjähdyksen (dynamiittipötkö) voimasta syntyvä paineaalto riittää noin 10 metrin etäisyydeltä rikkomaan ikkunoiden uloimmat lasit.

Oikosulkuaseet
Oikosulkuaseiden toiminta perustuu ilmassa leijuvaan sähköä johtavaan pölyyn. Pöly kulkeutuu laitteiden ilmastointiin ja sitä kautta edelleen laitteiden tuulettimien ohjaamina piirilevyille, jonne se alkaa kerääntyä aiheuttaen oikosulkuja.

Sähkömagneettinen pulssi
EMP-häiriöllä tarkoitetaan ydinräjähdyksen yhteydessä syntyvää sähkömagneettista säteilyä. Suurin sähkömagneettinen voimakkuus voi olla 50 – 150 kV/m ja suurin magneettikentän voimakkuus 1 – 8 kA/m. Vastaava nousuaika on 20 – 100 ns.

Ydinräjähdyksen kokonaisenergiasta noin puolet vapautuu mekaanisena energiana (paine ja tärinä), noin 35 % lämpösäteilynä ja noin 15 % radioaktiivisena säteilynä.

Liite 5. Rakentamisdokumentaation käsittelysuositukset

Tähän liitteeseen on koottu suosituksia tiedon käsittelystä rakentamishankkeiden aikana:

- liite 5.1: tiedon luokittelumatriisi
- liite 5.2: tiedon luokitteluohje rakentamishankkeissa
- liite 5.3: turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa

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

Hanke:								
Piirustuksen sisältö		Piirustus-tyyppi	Tiedon omistaja	Julkinen	ST IV	ST 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						

Hanke:								
Piirustuksen sisältö		Piirustus-tyyppi	Tiedon omistaja	Julkinen	ST IV	ST III	ST II	Huom.
17	Ajannäyttöjärjestelmän johtokaavio	Telekaavio						
18	AV-kaapelointi	Telekaavio						
19	Merkinantojärjestelmien johto-kaavio	Telekaavio						
20	Palo- ja Savunpoistojärjestelmien johtokaavio	Telekaavio						
21	Ovikaaviot	Telekaavio						
22	Sähköselostus							
23	Sähköurakan yksikköhintaluettelo							
24	Valaisinluettelo							
25	Sähköpisteluettelo							
26	Ovivarustelun urakkarajat							
27	Turvajärjestelmät, pistepiirustus	Turva-piirustus						
28	Tietoliikennejärjestelmät, piste-piirustus	Turva-piirustus						
29	Turvajärjestelmien johtokaaviot	Turvakaavio						
30	Ovikaaviot ovikoodeilla	Turvakaavio						
31	Lukituskaavio							
32	Tietoliikennejärjestelmän johto-kaavio	Turvakaavio						
33	Kerrosjakamoiden kalustus	Turvakaavio						
34	Kaapelinvetoluettelo	Turva						
35	Turvajärjestelmien selostus							
36	Turvaurakan yksikköhintaluettelo							
37	Asiakirjaluettelo	Turva						
38	Yhteiskannatusjärjestelmä	LVI						
39	LVI-laiteluettelo	LVI						
40	Ohjaus- ja toimilaitteiden sijoitus	LVI						
41	Rakennusautomaatio, järjestel-mäkaavio							
42	Ilmakäsittelykone, säätökaavio	LVI-kaavio						
43	Poistoilmakoje, säätökaavio	LVI-kaavio						
44	Palopeltien valvontajärjestelmien, säätökaavio	LVI-kaavio						
45	Lämmönjakokeskus, säätökaavio	LVI-kaavio						
46	Jäähdytyskoneikko, säätökaavio	LVI-kaavio						
47	Hankesuunnitelma							
47.1	Rakennustapaselostus							Sanitoitava julkisiksi
47.2	Huonekortit							
47.3	LVI-työt							Sanitoitava julkisiksi
47.4	Asiakkaan ja omistajan kiinteistön ylläpidon rajapintaliite							
47.5	Asiakkaan ja omistajan turvatekni-kan hankintarajat							

Hanke:								
Piirustuksen sisältö		**Piirustus-tyyppi**	**Tiedon omistaja**	**Julkinen**	**ST IV**	**ST III**	**ST II**	**Huom.**
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							

Liite 5.1 Tiedon luokitteluohje rakentamishankkeissa

Rakennushankkeen tiedot luokitellaan hankkeen luonne huomioon ottaen 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 VIHREÄ, ST IV)
  - Pääosa dokumentaatiosta julkista, mm. yleiskaapelointi
  - Perustellut hankintakokonaisuudet ST IV (tunkeutumisen ilmaisu, kulunvalvonta, verkkokuvaukset (muu kuin julkinen verkko)
- Korotettu taso (turvallisuusvyöhyke KELTAINEN, ST III)
  - Pääosa dokumentaatiosta julkista, mm. yleiskaapelointi
  - Perustellut hankintakokonaisuudet ST IV (turvarakenteet, verkot: tunkeutumisen ilmaisu, kulunvalvonta, verkkokuvaukset (muu kuin julkinen verkko)
- Korkea taso (turvallisuusvyöhyke SININEN, ST II)
  - Perusteltu osa dokumentaatiosta julkista
  - Muut hankintakokonaisuudet ST IV - III (turvarakenteet, osa tilarakenteista, verkot: tunkeutumisen ilmaisu, kulunvalvonta, verkkokuvaukset (muu kuin julkinen verkko)

Liite 5.2 Turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa

”Turvallisuusluokitellun tiedon hallintaprosessi rakentamishankkeissa” -taulukon[18] 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.

[18] Taulukko perustuu Juha Kyllösen (puolustushallinnon rakennuslaitos) laatimaan dokumenttiin ”Turvallisuusluokitellun tiedon hallintaprosessi puolustushallinnon rakentamishankkeissa”.

TURVALLISUUSLUOKITELLUN TIEDON HALLINTAPROSESSI RAKENNUSHANKKEISSA

Toimenpiteiden numerointi osoittaa toteutusjärjestyksen								
	Tarveselvitys	**Hankesuunnitelun valmisteluvaihe**	**Hankesuunnittelu**	**Rakennus-suunnittelu, valmisteluvaihe**	**Rakennus-suunnittelu**	**Rakentamisvaiheen valmisteluvaihe**	**Rakentamisvaihe**	**Käyttöönottovaihe**
Kohteen käyttäjä / tiedon omistaja (rakennuttaja)	1) Määrittää hankkeen suojaustason hanke-suunnitteluvaiheessa (JulkL 621/1999, TTA 681/2010, VAHTI 2/2010) 2) Huolehtii osaltaan tarveselvityksen yhteydessä valtionhallinnon ulkopuolisten sidos-ryhmien henkilöstön turvallisuusselvitysha-kemusten saattamisesta turvallisuusselvitysme-nettelyyn 4a) Selvittää asiakkaalta sidosryhmän käsittely-oikeuden STIII -suojaus-tasolle . 4b) Laatii ja auditoi hankekohtaisen turval-lisuussopimuksen STIV-tason kaupallisen sopi-musasiakirjan tai tilauksen liitteeksi (HE 2012 turvallisuus-selvityslaiksi) 6) Laatii hankekohtaisen turvallisuussopimuksen STIII-tasolle ja tarvit-taessa auditoi hanke-kohtaiset erityisvaati-mukset.	1) Tiedon turvallisuusluo-kitteluohje hankesuun-nitteluvaiheessa (VAHTI 2/2012) 2) Salassa pidettävän tiedon suojaustasovaa-timusten täyttymisen määrittely valtionhal-linnon ulkopuolisissa sidosryhmissä (KATAKRI). Vaatimuksen täyttymät-tä jäämisen määrittää ja siitä vastaa tiedon omistaja. 5) Yritysturvallisuus-selvitys niissä valtion-hallinnon ulkopuolisissa sidosryhmissä, joilla ei ole yritysturvallisuus-todistusta ja joilla on STIII-tason turvallisuus-luokitellun tietoaineis-ton käsittelytarve omissa toimitiloissaan (HE 2012 turvallisuussel-vityslaiksi)"	1) Määrittelee hankkeessa tuotettavien tilojen turval-lisuusvyöhykkeet ja käyt-tötarkoitukset ja sen, missä rakennusvaiheessa tilan turvallisuusvyöhykettä ale-taan toteuttamaan.	1) Tiedon turvallisuus-luokitteluohjeen päivitys rakennussuunnitteluvai-heeseen. 6) Yritysturvallisuus-selvitys niissä valtion-hallinnon ulkopuolisissa sidosryhmissä, joilla ei ole yritysturvallisuustodistusta ja joilla on STIII-tason turvaluokitellun tietoaineiston käsitte-lyoikeus omissa toimiti-loissaan (HE 2012 turvallisuussel-vityslaiksi)"		1) Tiedon turvallisuusluo-kitteluohjeen päivitys ra-kentamisvaihetta varten. 6) Yritysturvallisuus-selvitys niissä sidosryh-missä , joilla ei ole yritys-turvallisuustodistusta ja joilla on STIII -tason turva-luokitellun tietoaineiston käsittelyoikeus omissa toi-mitiloissaan (HE 2012 tur-vallisuusselvityslaiksi)"		

Toimenpiteiden numerointi osoittaa toteutusjärjestyksen								
	Tarveselvitys	**Hankesuunnitelun valmisteluvaihe**	**Hankesuunnittelu**	**Rakennus-suunnittelu, valmisteluvaihe**	**Rakennus-suunnittelu**	**Rakentamisvaiheen valmisteluvaihe**	**Rakentamisvaihe**	**Käyttöönottovaihe**
Suunnittelijat/ muut asiantuntijat			2a) Käsittelee ST III -tason rakennushankkeissa tietoaineistoa DSA-turvallisuusviranomaiselle antamansa sitoumuksen mukaisesti sekä noudattaa hankekohtaista turvallisuussopimusta 2b) Käsittelee ST IV -tason rakennushankkeissa tietoaineistoa hankekohtaisen turvallisuussopimuksen mukaisesti		1a) Käsittelee ST III -tason rakennushankkeissa tietoaineistoa DSA-turvallisuusviranomaiselle antamansa sitoumuksen mukaisesti sekä noudattaa hankekohtaista turvallisuussopimusta 1b) Käsittelee ST IV -tason rakennushankkeissa tietoaineistoa hankekohtaisen turvallisuussopimuksen mukaisesti			3) Toimittaa saamansa ja laatimansa rakennushanketta koskevan dokumentaation ja sähköiset tallennusmediat tuhottavaksi tai toimittaa allekirjoitetun pöytäkirjan suoritetusta tuhoamisesta takuuajan päätyttyä ja turvallisuussopimuksen mukaisesti.
Rakennuttaja-konsultti	3) Osallistuu henkilöturvallisuusselvitysmenettelyyn henkilöstönsä osalta. 5) Osallistuu turvallisuussopimuksen valmisteluun. 7) Allekirjoittaa turvallisuussopimuksen"	3) Huolehtii osaltaan hankesuunnitteluryhmän perustamisvaiheessa valtionhallinnon ulkopuolisten sidosryhmien henkilöstön turvallisuusselvityshakemusten saattamisesta turvallisuusselvitysmenettelyyn. 4a) Selvittää asiakkaalta em. sidosryhmän käsittelyoikeuden STIII -suojaustasolle. 4b) Laatii ja auditoi hankekohtaisen turvallisuussopimuksen STIV -tason kaupallisen sopimusasiakirjan tai tilauksen liitteeksi (HE 2012 turvallisuusselvityslaiksi)		2) Huolehtii asiakkaalle, että tarjouspyyntövaihetta edeltävässä ennakkotiedusteluvaiheessa sidosryhmäehdokkaiden henkilöstön turvallisuusselvityshakemukset saatetaan turvallisuusselvitysmenettelyyn (ml. vaitiolositoumukset) 3) Pyytää sidosryhmältä omistuspohjastaan selvityksen ja 4) Laatii sekä auditoi hankekohtaisen tarjouslaskentavaiheen turvallisuussopimuksen tasolle ST IV.		2) Huolehtii asiakkaalle, että tarjouspyyntövaihetta edeltävässä ennakkotiedusteluvaiheessa sidosryhmäehdokkaiden henkilöstön turvallisuusselvityshakemukset saatetaan turvallisuusselvitysmenettelyyn (ml. vaitiolositoumukset) 3) Pyytää sidosryhmältä omistuspohjastaan selvityksen ja 4) Laatii sekä auditoi hankekohtaisen tarjouslaskentavaiheen turvallisuussopimuksen tasolle ST IV.		4) Säilyttää suojaustason vaatimusten mukaisesti rakennushankkeen loppukuvat

Toimenpiteiden numerointi osoittaa toteutusjärjestyksen								
	Tarveselvitys	**Hankesuunnitelun valmisteluvaihe**	**Hankesuunnittelu**	**Rakennus-suunnittelu, valmisteluvaihe**	**Rakennus-suunnittelu**	**Rakentamisvaiheen valmisteluvaihe**	**Rakentamisvaihe**	**Käyttöönottovaihe**
		6) Laatii hankekohtaisen turvallisuussopimuksen STIII -tasolle ja tarvittaessa auditoi hankekohtaiset erityisvaatimukset.		5a) Tarjouspyyntövaiheen perusteella valittujen sidosryhmien käsittelyoikeus tasolle ST III selvitetään asiakkaalta. 5b) Laatii ja auditoi hankekohtaisen turvallisuussopimuksen tasolle ST IV kaupallisen sopimusasiakirjan tai tilauksen liitteeksi (HE2012 turvallisuusselvityslaiksi) 7) Laatii hankekohtaisen turvallisuussopimuksen tasolle ST III ja tarvittaessa auditoi hankekohtaiset erityisvaatimukset.”		5a) Tarjouspyyntövaiheen perusteella valittujen sidosryhmien käsittelyoikeus tasolle ST III selvitetään asiakkaalta. 5b) Laatii ja auditoi hankekohtaisen turvallisuussopimuksen tasolle ST IV kaupallisen sopimusasiakirjan tai tilauksen liitteeksi (HE2012 turvallisuusselvityslaiksi) 7) Laatii hankekohtaisen turvallisuussopimuksen tasolle ST III ja tarvittaessa auditoi hankekohtaiset erityisvaatimukset.”		
Omistaja	3) Osallistuu henkilöturvallisuusselvitysmenettelyyn henkilöstönsä osalta. 5) Osallistuu turvallisuussopimuksen valmisteluun. 7) Allekirjoittaa turvallisuussopimuksen"		3) Säilyttää suojaustason vaatimusten mukaisesti hankesuunnitelman.	8) Säilyttää suojaustason vaatimusten mukaisesti alkuperäiset kaupalliset asiakirjat		8) Säilyttää suojaustason vaatimusten mukaisesti alkuperäiset kaupalliset asiakirjat		4) Säilyttää suojaustason vaatimusten mukaisesti rakennushankkeen loppukuvat

Toimenpiteiden numerointi osoittaa toteutusjärjestyksen								
	Tarveselvitys	Hankesuunnitelun valmisteluvaihe	Hankesuunnittelu	Rakennus-suunnittelu, valmisteluvaihe	Rakennus-suunnittelu	Rakentamisvaiheen valmisteluvaihe	Rakentamisvaihe	Käyttöönottovaihe
Rakennusvaiheen urakoitsijat							1a) Käsittelee ST III -tason rakennushankkeissa tietoaineistoa DSA-turvallisuusviranomaiselle antamansa sitoumuksen mukaisesti sekä noudattaa hankekohtaista turvallisuussopimusta 1b) Käsittelee ST IV -tason rakennushankkeissa tietoaineistoa hankekohtaisessa turvallisuussopimuksen mukaisesti"	1) Toimittaa saamansa ja/tai laatimansa rakennushanketta koskevan dokumentaation ja sähköiset tallennusmediat tuhottavaksi tai toimittaa allekirjoitetun pöytäkirjan suoritetusta tuhoamisesta turvallisuussopimuksen mukaisesti. 2) Toimittaa takuuaikana tarvitsemansa asiakirjat rakennuttajakonsultille säilytettäväksi"

Liite 6. Rakentamishankkeiden turvallisuusaskeleet (esimerkki)

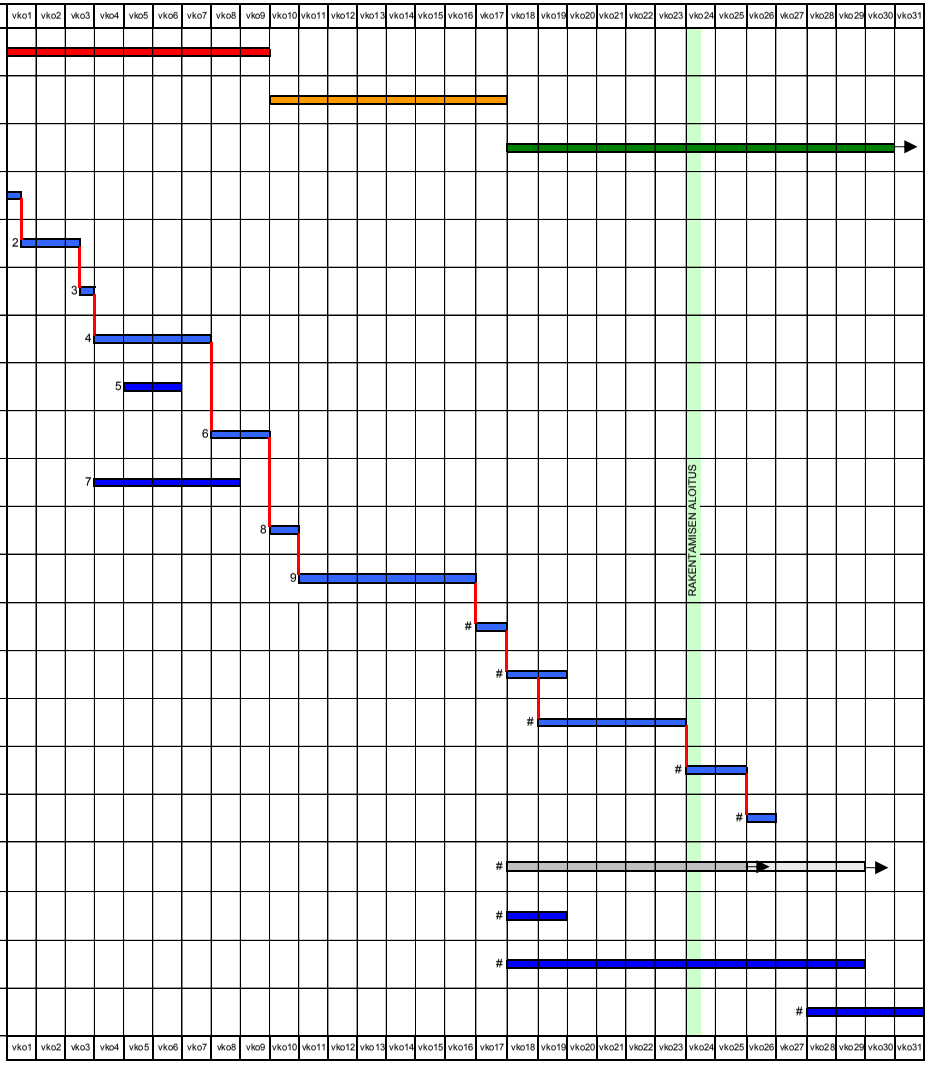
Taulukossa ”Rakentamishankkeiden turvallisuusaskeleet”[19] on kuvattu kronologisesti rakennushankkeen eri vaiheet, huomioiden hankkeen turvallisuuden vaatimat välitoimenpiteet. Taulukon janojen aikamääreet ovat suuntaa antavia ja ne on syytä määrittää jokaisessa hankkeessa erikseen jo hankesuunnitteluvaiheessa sekä päivittää niitä tarvittaessa. Taulukon esimerkki kuvaa korotetun tason hanketta, joka tähtää suojaustason III tiedon käsittelyn mahdollistamiseen rakennettavissa tiloissa.

Ennakkotiedusteluvaiheessa pyritään selvittämään mahdollisten tarjoajien kykyä käsitellä ja säilyttää suojaustason IV tarjouspyyntöaineistoa sekä kartoittaa ne tarjoajat, jotka tulevat tutustumaan tarjouspyyntöaineistoon asiakkaan ennalta hyväksymään paikkaan. Luokiteltu osa tarjouslaskennasta voidaan toteuttaa tilaajan määrittämissä tiloissa ja ympäristössä.

[19] Taulukko perustuu Juha Kyllösen (puolustushallinnon rakennuslaitos) laatimaan dokumenttiin ”Rakennushankkeiden turvallisuusaskeleet”.

Rakentamishankkeiden turvallisuusaskelet (esimerkki)

	TEHTÄVÄ	SUORITTAJA
	ENNAKKOTIEDUSTELUVAIHE	
	TARJOUSLASKENTAVAIHE	
	RAKENNUSVAIHE	
1	ENNAKKOTIEDUSTELUN LAATIMINEN JA POSTITUS URAKOITSIJOILLE	HANKEVASTAAVA/ RAKENNUTTAJA-KONSULTTI
2	ENNAKKOTIEDUSTELUUN VASTAAMINEN	YRITYS
3	ENNAKKOTIEDUSTELUAINEISTON KÄSITTELY JA TURVALLISUUSSELVITYSHAKEMUSTEN TOIMITTAMINEN ASIAKKAALLE	HANKEVASTAAVA/ RAKENNUTTAJA-KONSULTTI
4	ENNAKKOTIEDUSTELUSTA SAATUJEN TARJOUSLASKENTAHENKILÖSTÖN TURVALLISUUSSELVITYSHAKEMUSTEN LUPAHALLINTA	ASIAKAS
5	HANKETTA KOSKEVIEN TURVALLISUUSMÄÄRÄYSTEN LAATIMINEN	HANKEVASTAAVA / ASIAKAS
6	TARJOUSPYYNTÖASIAKIRJOJEN KOPIOINTI JA JÄRJESTELY	HANKEVASTAAVA/ RAKENNUTTAJA-KONSULTTI
7	YRITYSKOHTAINEN TARKASTUS ANNETUN TILATURVALISUUSSELVITYKSEN OIKEELLISUUDESTA (MAHDOLLISUUKSIEN MUKAAN KAIKKI YRITYKSET)	HANKEVASTAAVA / ASIAKAS
8	TARJOUSLASKENTAVAIHEEN TURVALLISUUSKOULUTUS JA TARJOUSPYYNTÖASIAKIRJOJEN LUOVUTTAMINEN	HANKEVASTAAVA / ASIAKAS
9	TARJOUSLASKENTA	YRITYS
10	YRITYSTEN VALINTA RAKENNUSHANKKEEN URAKOITSIJOIKSI	HANKEVASTAAVA / OMISTAJA
11	RAKENNUSHANKKEEN ALOITUSVAIHETTA KOSKEVIEN TURVALLISUUSSELVITYSHAKEMUSTEN TOIMITTAMINEN ASIAKKAALLE ALIURAKOITSIJAT => YRITYS => RAKENNUTTAJAKONSULTTI => ASIAKAS)	(RAKENNUTTAJA-KONSULTTI
12	LUPAHALLINNAN KÄSITTELY	ASIAKAS/ VIRANOMAINEN
13	TYÖMAATILOJEN RAKENTAMINEN (esim. ST III -TASOON)	YRITYS
14	TYÖMAATOIMITILOJEN TARKASTUS	ASIAKAS
15	"HARMAA AIKA", JOLLOIN YRITYKSILLÄ EI OLE MAHDOLLISUUTTA PEREHTYÄ SALASSA PIDETTÄVÄÄN AINEISTOON	
16	RAKENNUSVAIHEEN TURVALLISUUSKOULUTUS	ASIAKAS
17	YRITYKSEN TOIMITILOJEN SAATTAMINEN VAADITULLE TURVALLISUUSTASOLLE. SAKOLLINEN VÄLITAVOITE URAKKASOPIMUKSESSA.	YRITYS
18	YRITYKSEN TOIMITILOJEN LOPPUTARKASTUS => TURVALLISUUSSOPIMUS TAVOITETASOLLE	ASIAKAS



Liite 7. Valtionhallinnon toimitilarakentamisen turvallisuussopimusmallit

Tässä liitteessä esitetään turvallisuussopimusmallit seuraaviin käyttötarkoituksiin:

- rakentamispalvelut (liite 7.1)
- suunnittelu ja konsultointi (liite 7.2)
- kiinteistöpalvelut (liite 7.3)

Liite 7.1

RAKENTAMISPALVELUN TURVALLISUUSSOPIMUS

(ESIMERKKI)

XX.XX.20__

[ASIAKAS]

JA

[TOIMITTAJA]

(Ohje: Tämä on sopimusmalli, joka pitää aina muokata organisaatio- ja hankintakohtaisesti kulloinkin hankittavana olevan kohteen mukaan. Malli on tarkoitettu käytettäväksi rakentamispalveluhankinnoissa yksityiseltä palveluntuottajalta (rakennusurakat), kun tilaajaorganisaatio ei rakentamisen aikana toimi kohteena olevassa tilassa).

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.

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 työmaa-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 liittyvien tietojen luokitus suojaustasoille/Muut turvallisuutta koskevat vaatimukset]

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 2 mukaisten vaatimusten ylläpidosta. Ohje: Ohjeiden tulisi olla sisällöltään yhdenmukaiset tietoturvallisuusasetuksen ja sen täytäntöönpanosta annetun VAHTI-ohjeen 2/2010 luokittelu- ja käsittelyohjeiden kanssa.]

3.4 Toimittaja laatii asiakkaan liitteessä 2 esittämien vaatimusten mukaisesti turvallisuusohjeistuksen (liite 4) palveluun liittyvistä tietoturvamenettelyistä. 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 kaikessa kohdassa 4.2 tarkoitetussa toiminnassa ja aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa ja Toimittajan liikkuessa Asiakkaan Tiloissa.

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 tai Palvelun tuottamisen yhteydessä Toimittajan muuten havainnoimat tai haltuunsa saamat 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 liit-

tyvistä velvoitteista ja antamaan ohjeistusta sekä järjestämään koulutusta erityisesti Salassa pidettävien tietojen asianmukaisesta käsittelystä henkilöille, joilla on pääsy näihin tietoihin sekä turvallisuusjärjestelyistä Palvelun tuottamiseen osallistuville henkilöille. 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. [Tietojen luokitus suojaustasoille/Muut turvallisuutta koskevat määräykset, joita Toimittaja sitoutuu noudattamaan, on määritelty liitteessä 5.]

5.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille on 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 ulkopuolella, on Toimittajan noudatettava Asiakkaan antamia toimintaohjeita ja erityisesti huolehdittava siitä, ettei tietoaineistojen turvallisuus vaarannu. Salassa pidettäviä tietoja sisältävien asiakirjojen tai muun materiaalin valokuvaus, kopiointi tai muistiinpanojen tekeminen Salassa pidettävistä tiedoista on kielletty ilman Asiakkaan erillistä lupaa.

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 KELTAINEN (ST 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 tarkoitetulla tavalla turvallisuusselvitys ja jotka ovat tietoisia tämän Turvallisuussopimuksen 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 VIHREÄ, ST IV) 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 tarkoitetulla tavalla oikeutta päästä mainittuihin Asiakkaan Tiloihin tai rakennustyömaalle, saavat oleskella niissä ainoastaan Asiakkaan luvalla ja valvonnan alaisina. Asiakkaalla on oikeus edellyttää luvussa 10 tarkoitetun turvallisuusselvityksen tekemistä myös mainittuihin Tiloihin tai rakennustyömaalle pääsevien henkilöiden osalta, ottaen huomioon turvallisuusselvitysten tekemiselle laissa asetetut edellytykset.

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 Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt, joilla on pääsy Asiakkaan Tiloihin tai rakennustyömaalle, noudattavat tätä Turvallisuussopimusta.

6.5 Toimittajan ja sen alihankkijan Tilojen tulee olla Tiloissa käsiteltävien Salassa pidettävien tietojen suojaustason 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 [VAHTI-ohjeen 2/2013 ja voimassa olevan Kansallisen turvallisuusauditointikriteeristön (KATAKRI)] mukaisesti.

6.6 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.

6.7 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. Uhka-analyysiin pohjautuen Asiakas ja Toimittaja voivat tapauskohtaisesti erikseen sopia, että em. henkilöstön valvontaa ei edellytetä tapauksissa, joissa Salassa pidettäviä tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

[Ohje: On otettava huomioon, että kyseisillä henkilöillä on mahdollisuus tuoda kyseisiin tiloihin teknisiä laitteita, joiden avulla voidaan saada oikeudettomasti tietoon Salassa pidettäviä tietoja.]

6.8 Henkilöiden, joilla on pääsy Toimittajan tai alihankkijan Tiloihin, tulee olla tunnistettavissa.

6.9 [Asiakkaalla on oikeus vaatia luvussa 10 tarkoitetun turvallisuusselvityksen hakemista henkilöistä, joilla on oikeus päästä [tiettyihin yksilöityihin] Toimittajan tai sen alihankkijan Tiloihin, joissa käsitellään Salassa pidettäviä tietoja. Toimittajan tulee myös hyväksyttää henkilö Asiakkaalla ennen kuin henkilölle voidaan myöntää pääsy [tiettyihin yksilöityihin] Tiloihin.]

6. 10 [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, 6.9] 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, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Toimittaja vastaa siitä, että suojaustasolle IV 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, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Asiakkaalla on tarvittaessa oikeus edellyttää myös näiden henkilöiden turvallisuusselvittämistä ottaen huomioon turvallisuusselvityksille laissa asetetut edellytykset. 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 piirivartioinnin 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 [Finanssialan 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] tunkeutumisen ilmaisinjärjestelmällä. Salassa pidettävän aineiston säilytyksessä noudatetaan liitteen 2 ja VAHTI-ohjeen 2/2013 vaatimuksia.

8.5 Rakennustyömaa-alueella valokuvaaminen ja/tai muu kuvatallentaminen on sallittua ainoastaan Palvelun dokumentoinnin edellyttämässä suppeassa laajuudessa [suunnittelijoiden, Toimittajan työnjohdon ja valvojien toimesta]. Kuvaamiseen tarvitaan Asiakkaan antama lupa.

VAITIOLOSITOUMUS

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, tämän sopimuksen 6 ja 7 luvuissa turvallisuusselvityksellä tarkoitetaan Suomen voimassa olevan turvallisuusselvityslainsäädännön mukaista turvallisuusselvitystä tai sitä vastaavaa, Suomen kansallisen turvallisuusviranomaisen (National Security Authority, NSA) kautta hankittua ulkomaan turvallisuusviranomaisen myöntämää henkilöturvallisuustodistusta.

10.2 Jollei toisin sovita, ulkomaisella Toimittajalla tai alihankkijalla, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee olla yrityksen kotimaan turvallisuusviranomaisen myöntämä yritysturvallisuustodistus (Facility Security Clearance, FSC) sekä salassa pidettävien tietojen käsittelyyn osallistuvilla henkilöillä henkilöturvallisuustodistus (Personnel Security Clearance, PSC). Suomen NSA voi pyytää ulkomaan turvallisuusviranomaisen myöntämän turvallisuustodistuksen koskien niiden maiden yrityksiä ja henkilöstöä, joiden turvallisuusviranomaisten kanssa Suomen NSA tekee yhteistyötä.

10.3 Suomessa tehtävien turvallisuusselvitysten hankkimisesta vastaa Asiakas. Toimittaja on yhteydessä Suomen NSA:han ulkomaisen alihankkijansa turvallisuustodistusten hankkimiseksi. Asiakas on yhteydessä Suomen NSA:han ulkomaisen Toimittajan ja sen ulkomaisen alihankkijan turvallisuustodistuksen hankkimiseksi.

10.4 Asiakas vastaa Suomessa tehtyjen 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. Toimittaja vastaa ulkomaisten turvallisuustodistusten kustannuksista.

10.5 Ulkomaisen tai kansallisen turvallisuusselvityksen tuloksesta riippumatta asiakkaalla on erityisestä perustellusta, turvallisuuteen liittyvästä syystä oikeus kieltää Toimittajan tai sen alihankkijan henkilön osallistuminen Palvelun suorittamiseen.

TIETOTURVALLISUUS

11.1 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.

11.2 *[Vaihtoehto 1]*
Asiakas luokittelee Salassa pidettäviä tietojaan tietoturvallisuusasetuksen mukaisiin suojaustasoihin. [Tietojen luokitus eri suojaustasoille 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 tietoturvallisuuden perustasoa ja Asiakkaan ohjeistusta Salassa pidettäviä tietoja käsitellessään.

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

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 tai järjestelmiin, joissa käsitellään Salassa pidettävää tietoa. Tässä Turvallisuussopimuksessa alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai työmaarakennuksiin tai järjestelmiin, joissa käsitellään Salassa pidettävää tietoa.

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 hyväksytettävä 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 etukäteen tahdostaan suorittaa tarkastus. Toimittaja voi perustellusta syystä ehdottaa uutta päivää tarkastukselle. Haavoittuvuusskannauksia voidaan

kuitenkin tehdä edellä mainitusta 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, järjestelmiin, joissa käsitellään Salassa pidettäviä tietoja, 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 sopimussakkoehtoihin. 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 Kohdissa14.1-14.4 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 ratkaisemaan 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) samasanaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]	[paikka ja aika]
[ASIAKAS]	[TOIMITTAJA]
_____	_____
[allekirjoittaja]	[allekirjoittaja]
_____	_____
[allekirjoittaja]	[allekirjoittaja]

Liite 7.2

RAKENTAMISEEN LIITTYVIEN SUUNNITTELU- JA KONSULTTIPALVELUJEN TURVALLISUUSSOPIMUS

(ESIMERKKI)

XX.XX.20__

[ASIAKAS]

JA

[TOIMITTAJA]

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

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 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.

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 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 tietoturvamenettelyistä]

[Liite 5 Palveluun liittyvien tietojen luokitus suojaustasoille/Muut turvallisuutta koskevat vaatimukset]

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 2 mukaisten vaatimusten ylläpidosta. [Ohje: Ohjeiden tulisi olla sisällöltään yhdenmukaiset tietoturvallisuusasetuksen ja sen täytäntöönpanoa välittömästi täydentävien ohjeiden luokittelu- ja käsittelyohjeiden kanssa.]

3.4 Toimittaja laatii asiakkaan liitteessä 2 esittämien vaatimusten mukaisesti turvallisuusohjeistuksen (liite 4) palveluun liittyvistä tietoturvamenettelyistä. 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 kaikessa kohdassa 4.2 tarkoitetussa toiminnassa ja aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa ja Toimittajan liikkuessa Asiakkaan Tiloissa.

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 tai Palvelun tuottamisen yhteydessä Toimittajan muuten havainnoimat tai haltuunsa saamat 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 liit-

tyvissä 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 sekä turvallisuusjärjestelyistä Palvelun tuottamiseen osallistuville henkilöille. 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. [Tietojen luokitus suojaustasoille/Muut turvallisuutta koskevat määräykset, joita Toimittaja sitoutuu noudattamaan, on määritelty liitteessä 5.]

5.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille on 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 ulkopuolella, on Toimittajan noudatettava Asiakkaan antamia toimintaohjeita ja erityisesti huolehdittava siitä, ettei tietoaineistojen turvallisuus vaarannu. Salassa pidettäviä tietoja sisältävien asiakirjojen tai muun materiaalin valokuvaus, kopiointi tai muistiinpanojen tekeminen Salassa pidettävistä tiedoista on kielletty ilman Asiakkaan erillistä lupaa.

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 KELTAINEN (ST III) tai SININEN (ST II)) annetaan vain nimetyille Toimittajan ja sen alihankkijan henkilöstöön kuuluville henki-

löille, jotka Toimittaja on hyväksyttänyt Asiakkaalla etukäteen, joista on tehty luvussa 9 tarkoitetulla tavalla turvallisuusselvitys ja jotka ovat tietoisia tämän Turvallisuussopimuksen 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 VIHREÄ, ST IV) 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 tarkoitetulla tavalla oikeutta päästä mainittuihin Asiakkaan Tiloihin tai rakennustyömaalle, saavat oleskella niissä ainoastaan Asiakkaan luvalla ja valvonnan alaisina. Asiakkaalla on oikeus edellyttää luvussa 9 tarkoitetun turvallisuusselvityksen tekemistä myös mainittuihin Tiloihin tai rakennustyömaalle pääsevien henkilöiden osalta, ottaen huomioon turvallisuusselvitysten tekemiselle laissa asetetut edellytykset.

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 Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt, joilla on pääsy Asiakkaan Tiloihin tai rakennustyömaalle, noudattavat tätä Turvallisuussopimusta.

6.5 Toimittajan ja sen alihankkijan Tilojen tulee olla Tiloissa käsiteltävien Salassa pidettävien tietojen luokitustason 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 [VAHTI-ohjeen 2/2013 ja voimassa olevan Kansallisen turvallisuusauditointikriteeristön (KATAKRI)] mukaisesti.

6.6 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.

6.7 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. Uhka-analyysiin pohjautuen Asiakas ja Toimittaja voivat tapauskohtaisesti erikseen sopia, että em. henkilöstön valvontaa ei edellytetä tapauksissa, joissa Salassa pidettäviä tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

[Ohje: On otettava huomioon, että kyseisillä henkilöillä on mahdollisuus tuoda kyseisiin tiloihin teknisiä laitteita, joiden avulla voidaan saada oikeudettomasti tietoon Salassa pidettäviä tietoja.]

6.8 Henkilöiden, joilla on pääsy Toimittajan tai alihankkijan Tiloihin, tulee olla tunnistettavissa.

6.9 [Asiakkaalla on oikeus vaatia luvussa 9 tarkoitetun turvallisuusselvityksen hakemista henkilöistä, joilla on oikeus päästä [tiettyihin yksilöityihin] Toimittajan tai sen alihankkijan Tiloihin, joissa käsitellään Salassa pidettäviä tietoja. Toimittajan tulee myös hyväksyttää henkilö Asiakkaalla ennen kuin henkilölle voidaan myöntää pääsy [tiettyihin yksilöityihin] Tiloihin.]

6.10 [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, 6.9] 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 ja joista on tehty luvussa 9 tarkoitettu turvallisuusselvitys, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Toimittaja vastaa siitä, että suojaustasolle IV 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, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Asiakkaalla on tarvittaessa oikeus edellyttää myös näiden henkilöiden turvallisuusselvittämistä , ottaen huomioon turvallisuusselvityksille laissa asetetut edellytykset. 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 perusturvallisuustason tiloihin ja/tai rakennustyömaalle].

TURVALLISUUSSELVITYKSET

9.1 Jollei toisin sovita, tämän sopimuksen 6 ja 7 luvuissa turvallisuusselvityksellä tarkoitetaan Suomen voimassa olevan turvallisuusselvityslainsäädännön mukaista turvallisuusselvitystä tai sitä vastaavaa, Suomen kansallisen turvallisuusviranomaisen (National Security Authority, NSA) kautta hankittua ulkomaan turvallisuusviranomaisen myöntämää henkilöturvallisuustodistusta.

9.2 Jollei toisin sovita, ulkomaisella Toimittajalla tai alihankkijalla, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee olla yrityksen kotimaan turvallisuusviranomaisen myöntämä yritysturvallisuustodistus (Facility Security Clearance, FSC) sekä salassa pidettävien tietojen käsittelyyn osallistuvilla henkilöillä henkilöturvallisuustodistus (Personnel Security Clearance, PSC). Suomen NSA voi pyytää ulkomaan turvallisuusviranomaisen myöntämän turvallisuustodistuksen koskien niiden maiden yrityksiä ja henkilöstöä, joiden turvallisuusviranomaisten kanssa Suomen NSA tekee yhteistyötä.

9.3 Suomessa tehtävien turvallisuusselvitysten hankkimisesta vastaa Asiakas. Toimittaja on yhteydessä Suomen NSA:han ulkomaisen alihankkijansa turvallisuustodistusten hankkimiseksi. Asiakas on yhteydessä Suomen NSA:han ulkomaisen Toimittajan ja sen ulkomaisen alihankkijan turvallisuustodistuksen hankkimiseksi.

9.4 Asiakas vastaa Suomessa tehtyjen turvallisuusselvitysten kustannuksista. Mikäli turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että Toimittajan tai Toimittajan alihankkijan henkilöstössä tapahtuu vaihdos tai Asiakkaasta riippuma-

ton lisäys, Toimittaja vastaa uuden henkilön turvallisuusselvityksen kustannuksista. Toimittaja vastaa ulkomaisten turvallisuustodistusten kustannuksista.

9.5 Ulkomaisen tai kansallisen turvallisuusselvityksen tuloksesta riippumatta asiakkaalla on erityisestä 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]*
Asiakas luokittelee Salassa pidettäviä tietojaan tietoturvallisuusasetuksen mukaisiin suojaustasoihin. [Tietojen luokitus eri suojaustasoille 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 tietoturvavaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esitetty [Pääsopimuksen liitteessä x/tämän Turvallisuussopimuksen liitteessä x.]

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 tai järjestelmiin, joissa käsitellään Salassa pidettävää tietoa. Tässä Turvallisuussopimuksessa alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin, rakennustyömaalle tai työmaarakennuksiin tai järjestelmiin, joissa käsitellään Salassa pidettävää tietoa.

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 hyväksytettävä 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 etukäteen tahdostaan suorittaa tarkastus. Toimittaja voi perustellusta syystä ehdottaa uutta päivää tarkastukselle. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainitusta riippumatta erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tai sen alihankkijoiden tietoturvallisuutta 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.

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, järjestelmiin, joissa käsitellään Salassa pidettäviä tietoja, rakennustyömaalle 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 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 omistussuhteissa tapahtuu merkittäviä muutoksia.

12.6 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.

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 sopimussakkoehtoihin. 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], 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 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], 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 Kohdissa13.1-13.4 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 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 14 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 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 Turvallisuussopimukseen sovelletaan Suomen lakia, lukuun ottamatta lainvalintasäännöksiä.

17.2 Tästä Turvallisuussopimuksesta 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 Turvallisuussopimus on laadittu kahtena (2) samasanaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]	[paikka ja aika]
[ASIAKAS]	[TOIMITTAJA]
_____	_____
[allekirjoittaja]	[allekirjoittaja]
_____	
[allekirjoittaja]	

Liite 7.3

KIINTEISTÖPALVELUJEN TURVALLISUUSSOPIMUS

(ESIMERKKI)

XX.XX.20__

[ASIAKAS]

JA

[TOIMITTAJA]

(Ohje: Tämä on sopimusmalli, 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).

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 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.

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 liittyvien tietojen luokitus suojaustasoille/Muut turvallisuutta koskevat vaatimukset]

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 2 mukaisten vaatimusten ylläpidosta. [Ohje: Ohjeiden tulisi olla sisällöltään yhdenmukaiset tietoturvallisuusasetuksen ja sen täytäntöönpanoa välittömästi täydentävien ohjeiden luokittelu- ja käsittelyohjeiden kanssa.]

3.4 Toimittaja laatii asiakkaan liitteessä 2 esittämien vaatimusten mukaisesti turvallisuusohjeistuksen (liite 4) palveluun liittyvistä tietoturvamenettelyistä. 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 Turval-

lisuussopimuksen 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 kaikessa kohdassa 4.2 tarkoitetussa toiminnassa ja aina Toimittajan käsitellessä Asiakkaaseen tai Palvelun toteutukseen liittyvää tai muuta Asiakkaalta saatua Salassa pidettävää tietoa ja Toimittajan liikkuessa Asiakkaan Tiloissa.

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 tai Palvelun tuottamisen yhteydessä Toimittajan muuten havainnoimat tai haltuunsa saamat 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 sekä turvallisuusjärjestelyistä Palvelun tuottamiseen osallistuville henkilöille. 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. [Tietojen luokitus suojaustasoille/Muut turvallisuutta koskevat määräykset, joita Toimittaja sitoutuu noudattamaan, on määritelty liitteessä 5.]

5.6 Toimittaja tiedostaa, että Salassa pidettävien tietojen paljastaminen ulkopuolisille on 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 ulkopuolella, on Toimittajan noudatettava Asiakkaan antamia toimintaohjeita ja erityisesti huolehdittava siitä, ettei tietoaineistojen turvallisuus vaarannu. Salassa pidettäviä tietoja sisältävien asiakirjojen tai muun materiaalin valokuvaus, kopiointi tai muistiinpanojen tekeminen Salassa pidettävistä tiedoista on kielletty ilman Asiakkaan erillistä lupaa.

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 KELTAINEN (ST 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 tarkoitetulla tavalla turvallisuusselvitys ja jotka ovat tietoisia tämän Turvallisuussopimuksen 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 VIHREÄ, ST IV) 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 liikkumisesta annetuista ohjeista. Henkilöt, joille ei ole annettu edellä tarkoitetulla 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 oikeus edellyttää luvussa 9 tarkoitetun turvallisuus-

selvityksen tekemistä myös mainittuihin Tiloihin pääsevien henkilöiden osalta, ottaen huomioon turvallisuusselvitysten tekemiselle laissa asetetut edellytykset.

6.3 Henkilöiden, joilla on pääsy Asiakkaan Tiloihin, tulee olla tunnistettavissa. Henkilöillä on oltava Asiakkaan Tiloissa liikkuessaan näkyvillä Asiakkaan kanssa sovittu kuvallinen henkilötunniste.

6.4 Toimittaja vastaa siitä, että Toimittajan tai sen alihankkijan henkilöstöön kuuluvat henkilöt, joilla on pääsy Asiakkaan Tiloihin, noudattavat tätä Turvallisuussopimusta.

6.5 Toimittajan ja sen alihankkijan Tilojen tulee olla Tiloissa käsiteltävien Salassa pidettävien tietojen luokitustason 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 [VAHTI-ohjeen 2/2013 ja voimassa olevan Kansallisen turvallisuusauditointikriteeristön (KATAKRI)] mukaisesti.

6.6 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.

6.7 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. Uhka-analyysiin pohjautuen Asiakas ja Toimittaja voivat tapauskohtaisesti erikseen sopia, että em. henkilöstön valvontaa ei edellytetä tapauksissa, joissa Salassa pidettäviä tietoja säilytetään tai käsitellään Tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi.

6.8 Henkilöiden, joilla on pääsy Toimittajan tai alihankkijan Tiloihin, tulee olla tunnistettavissa.

6.9 [Asiakkaalla on oikeus vaatia luvussa 9 tarkoitetun turvallisuusselvityksen hakemista henkilöistä, joilla on oikeus päästä [tiettyihin yksilöityihin] Toimittajan tai sen alihankkijan Tiloihin, joissa käsitellään Salassa pidettäviä tietoja. Toimittajan tulee myös hyväksyttää henkilö Asiakkaalla ennen kuin henkilölle voidaan myöntää pääsy [tiettyihin yksilöityihin] Tiloihin.]

6.10 [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, 6.9] tarkoitettuihin 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 ja joista on tehty luvussa 9 tarkoitettu turvallisuusselvitys, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Toimittaja vastaa siitä, että suojaustasolle IV 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, joille on annettu oikeus päästä kyseisiin järjestelmiin ja/tai tietoihin ja jotka ovat tietoisia salassapitoa koskevista velvoitteistaan. Asiakkaalla on tarvittaessa oikeus edellyttää myös näiden henkilöiden turvallisuusselvittämistä, ottaen huomioon turvallisuusselvityksille laissa asetetut edellytykset. 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 perusturvallisuustason tiloihin].

TURVALLISUUSSELVITYKSET

9.1 Jollei toisin sovita, tämän sopimuksen 6 ja 7 luvuissa turvallisuusselvityksellä tarkoitetaan Suomen voimassa olevan turvallisuusselvityslainsäädännön mukaista turvallisuusselvitystä tai sitä vastaavaa, Suomen kansallisen turvallisuusviranomaisen (NSA) kautta hankittua ulkomaan turvallisuusviranomaisen myöntämää henkilöturvallisuustodistusta.

9.2 Jollei toisin sovita, ulkomaisella Toimittajalla tai alihankkijalla, joka käsittelee tai säilyttää Salassa pidettäviä tietoja Suomen rajojen ulkopuolella, tulee olla yrityksen kotimaan turvallisuusviranomaisen myöntämä yritysturvallisuustodistus (Facility Security Clearance, FSC) sekä salassa pidettävien tietojen käsittelyyn osallistuvilla henkilöillä henkilöturvallisuustodistus (Personnel Security Clearance, PSC). Suomen NSA voi pyytää ulkomaan turvallisuusviranomaisen myöntämän turvallisuustodistuksen koskien niiden maiden yrityksiä ja henkilöstöä, joiden turvallisuusviranomaisten kanssa Suomen NSA tekee yhteistyötä.

9.3 Suomessa tehtävien turvallisuusselvitysten hankkimisesta vastaa Asiakas. Toimittaja on yhteydessä Suomen NSA:han ulkomaisen alihankkijansa turvallisuustodistusten hankkimiseksi. Asiakas on yhteydessä Suomen NSA:han ulkomaisen Toimittajan ja sen ulkomaisen alihankkijan turvallisuustodistuksen hankkimiseksi.

9.4 Asiakas vastaa Suomessa tehtyjen 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. Toimittaja vastaa ulkomaisten turvallisuustodistusten kustannuksista.

9.5 Ulkomaisen tai kansallisen turvallisuusselvityksen tuloksesta riippumatta asiakkaalla on erityisestä 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 suojaustasoille ilmenee liitteestä 5]. Toimittaja sitoutuu noudattamaa. 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 valtionhallinnon tietoturvatason ja Palveluun liittyvät konkreettiset tietoturvavaatimukset, jotka Toimittajan tulee täyttää. Vaatimukset on esitetty [Pääsopimuksen liitteessä X/tämän Turvallisuussopimuksen liitteessä x.]

ALIHANKKIJAT

11.1 Toimittajan tulee hyväksyttää Asiakkaalla sellainen alihankkija, jota se aikoo käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin tai järjestelmiin, joissa käsitellään Salassa pidettävää tietoa. Tässä Turvallisuussopimuksessa alihankkijalla tarkoitetaan ainoastaan sellaista alihankkijaa, jota Toimittaja käyttää Salassa pidettävien tietojen käsittelyssä tai jolla on pääsy Asiakkaan Tiloihin tai järjestelmiin, joissa käsitellään Salassa pidettävää tietoa.

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 hyväksytettävä 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 etukäteen tahdostaan suorittaa tarkastus. Toimittaja voi perustellusta

syystä ehdottaa uutta päivää tarkastukselle. Haavoittuvuusskannauksia voidaan kuitenkin tehdä edellä mainitusta riippumatta erikseen sovittavina ajankohtina. Tarkastukset eivät saa vaarantaa Toimittajan tai sen alihankkijoiden tietoturvallisuutta 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.

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 tai pääsy järjestelmiin, joissa käsitellään Salassa pidettäviä tietoja.

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 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 omistussuhteissa tapahtuu merkittäviä muutoksia.

12.6 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.

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 sopimussakkoehtoihin. 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 salassapitovelvollsuuden 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 useammin kuin kerran 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 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 Turvallisuussopimukseen sovelletaan Suomen lakia, lukuun ottamatta lainvalintasäännöksiä.

17.2 Tästä Turvallisuussopimuksesta 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 Turvallisuussopimus on laadittu kahtena (2) samasanaisena kappaleena, yksi (1) kummallekin sopijapuolelle.

[paikka ja aika]	[paikka ja aika]
[ASIAKAS]	[TOIMITTAJA]
_____	_____
[allekirjoittaja]	[allekirjoittaja]
_____	
[allekirjoittaja]	

Liite 8. Viiteaineiston lähdelainaukset

1. Lait

Viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999; jäljempänä julkisuuslaki) on säännökset yleisimmin sovellettavista salassapitosäännöksistä. Salassapitovelvollisuus merkitsee paitsi kieltoa antaa tietoaineistoista tietoa sivullisille ja ilman laissa olevaa oikeutta, myös velvollisuutta ennalta ehkäistä aineistoihin kohdistuvat väärinkäytökset. Julkisuuslain 22§ toteaa: *”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.”*

Viranomaisen on toiminnassaan noudatettava hyvää tiedonhallintatapaa huolehtimalla tietoaineistojensa saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä (18§). Laissa on säädetty valtioneuvostolle oikeus säätää tietoturvallisuusvaatimuksista mukaan lukien toimitilojen turvallisuutta koskevat vaatimukset.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) koskee turvallisuusluokiteltuja tietoaineistoja, jotka on Suomen viranomainen on saanut Suomea sitovan kansainvälisen tietoturvallisuussopimuksen tai kansainvälisen säädöksen (esim. EU-asetus) perusteella. Tällaiset tiedot on pidettävä aina salassa. Laissa on myös säännökset yhteisöturvallisuusselvityksestä, joka nykyisin kuitenkin voidaan tehdä vain ulkomaan viranomaisen pyynnöstä tai kysymyksen ollessa julkisista puolustus- ja turvallisuushankinnoista annetussa laissa 1531/2011 tarkoitetuista hankinnoista. Yhteisöturvallisuusselvitysmenettelyssä voidaan selvittää esim. sopimuskumppanin toimitilojen tietoturvallisuutta, kun on kysymys puolustus- ja turvallisuushankinnasta.

Laki turvallisuusselvityksistä (177/2002) sisältää säännöksen henkilön taustan selvittämisestä hänen luotettavuutensa arvioimiseksi. Lakia ollaan uudistamassa ja uuden turvallisuusselvityslain on suunnitelmien mukaan tarkoitus tulla voimaan kesäkuussa 2014. Uusi laki on kattavuudeltaan edeltäjäänsä laajempi ja sisältää paitsi säädökset henkilöturvallisuusselvitysten toteuttamiseksi, myös säädökset yritysturvallisuusselvitysten hoitamiseksi.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011); Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaan. Tämä ei estä viranomaisen itsensä suorittamaa arviointia.

Arkistolaki (831/1994) ottaa kantaa toimitilaturvallisuuden alaan säätämällä, 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) säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Asetuksen 2 luvussa on säännökset yleisistä tietoturvallisuusvaatimuksista, kuten säännökset tietoturvallisuuden suunnittelun perusteista ja tietoaineistojen elinkaaren, ts. eri käsittelyvaiheiden huomioon ottamisesta. Tietoturvallisuuden perustason toteuttamista koskevat säännökset ovat 5§:n 1 momentissa. Sen mukaan tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava mm. siitä, että asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja. Yleiset tietoturvallisuusvelvoitteet koskevat valtionhallinnon viranomaisia siinäkin tapauksessa, että ne eivät luokittele tietoaineistojaan. Tietoturvallisuuden perustasoa koskeva 5§ on siis suoraan viranomaisia velvoittava säännös, joka ei ole riippuvainen siitä, millaisia tietoturvallisuutta koskevia ratkaisuja viranomainen tekee.

Viranomaiset ovat velvollisia huolehtimaan vastaavasta suojasta silloinkin kun tietojenkäsittely tapahtuu viranomaisten toimitilojen ulkopuolella, esim. ICT-alan palveluyrityksessä.

Valtionhallinnon viranomainen päättää itse, milloin tietoaineistojen luokitus otetaan käyttöön. Asetuksen avulla yhdenmukaistetaan suojaustasoja. Jos tietoaineisto luokitellaan, luokittelun on määrä johtaa samanlaisiin suojaustoimiin eri viranomaisissa. Asetuksen luokittelun perusteita koskevilla säännöksillä on pyritty luomaan kullekin viranomaiselle parhaiten sopivat luokittelutavat: luokittelu voidaan kohdistaa myös rajoitettuna tiettyihin tietoaineistoihin tai tiettyihin tietoaineistojen käsittelyvaiheisiin sen mukaan, minkälainen tarve suojattavan edun kannalta kulloinkin on. Suojaustasoluokkia on neljä (ST IV – ST I) ; korkein suojaustasoluokka on I.

Sen lisäksi, että tietoaineisto luokitellaan suojaustasoittain, ne voidaan varustaa erityisiin perusteisiin nojaten turvallisuusluokitusmerkinnällä (11§) tapauksissa, joissa asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7—10 kohdassa tarkoitetulla tavalla. Tällöin 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”.”

Asetuksen 14 §:ssä on luokiteltujen asiakirjojen käsittely- ja säilytystiloja koskevat turvallisuusvaatimukset. Sen mukaan 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.*

Luokiteltuja asiakirjoja saisi pääsäännön mukaan käsitellä vain viranomaisen toimitiloissa. Käsittely toimitilojen ulkopuolella edellyttäisi aina viranomaisen lupaa, toimeksiantoa tai ohjeita, joissa asetetaan edellytykset aineistojen käsittelylle (15 §). Jos esim. käsittelytehtävät on annettu palveluyritykselle, asia kirjataan toimeksiantoon tai sen liiteasiakirjoihin.

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 tietoturvallisuusasetuksen täytäntöönpanosta (VAHTI 2/2010)

Tietoturva-asetuksen toimeenpanoa edesauttava VAHTI-ohje 2/2010 (Ohje tietoturvallisuudesta 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, paloturva- ja kassakaappeja sekä muita mekaanisia ratkaisuja. Valvontajärjestelmillä tarkoitetaan yleensä kulunvalvonta-, tunkeutumisen ilmaisu-, kameravalvonta- ja olosuhdevaroitusjärjestelmiä. Sähköisiin valvontajärjestelmiin kuuluvat myös kiinteistöautomaatiojärjestelmät, joilla valvotaan ja ohjataan tilan käyttöolosuhteita.

Tilaturvallisuuden kokonaisuudesta ei ole olemassa varsinaisia standardeja, mutta kunkin tietoturvallisuustason 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 ristikytkentätilojen tilaturvallisuuden huomioiminen sekä huolehtiminen siitä, etteivät asiattomat pääse käsiksi mm. aktiivisiin kytkentärasioihin.” (luku 4.4).

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

4. Euroopan unionin turvallisuusregiimi (2011)

Euroopan unionin neuvosto on antanut päätöksen turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2011/292/EU). Neuvostossa kokoontuneiden EU:n jäsenvaltioiden välillä on tehty sopimus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta. Sopimus on hyväksytty eduskunnassa ja sopimuksen määräysten täytäntöön panemiseksi on säädetty laki (224/2012).

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).

EU-säännöstön 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 on tehnyt Naton kanssa tietoturvallisuussopimuksen vuonna 1994 ja sitä täydentävän järjestelyn vuonna 2012 (sopimussarja 7-8/2013). Suomi noudattaa kumppanuusyhteistyössä järjestelyssä olevia määräyksiä sekä Naton tietoturvallisuusvaatimuksia niiltä osin kuin niitä sovelletaan kumppanimaihin.

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 selvittää [20]. 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 siltä osin kuin toimenpiteen laatu ja laajuus sekä rakennuksen tai sen osan mahdollisesti muutettava käyttötapa edellyttävät.

[20] PSC, Personal Security Clearance, henkilöturvallisuustodistus

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 9. Määritelmät ja lyhenteet

Asiakirja	Asiakirjalla 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 tunniste, joka voi olla mekaaninen, sähköinen tai biometrinen.
DSA	Designated Security Authority, laissa 588/2004 määrätty turvallisuusviranomainen (puolustusministeriö, Pääesikunta, suojelupoliisi).
EMP	Electro Magnetic Pulse. 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 toimintapoliitikkoja, 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	High Power Microwave. 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 asiakassisäänkäynnin puoleisella sivulla olevia ikkunoita.
Kansallinen turvallisuusviranomainen	Laissa 588/2004 määritetty NSA-viranomainen (ks. NSA).
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 määriteltyyn 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.
NCSA	National Communications Security Authority, laissa 588/2004 määritetty kansallinen tietoturvallisuusviranomainen (Viestintäviraston NCSA-FI –yksikkö).
NSA	National Security Authority, laissa 588/2004 määritetty kansallinen turvallisuusviranomainen (ulkoasiainministeriön NSA-yksikkö).
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, lattioita tai kattoja.
Telki	Lukon liikkuva osa, joka lukitsee oven karmissa olevaan vastalevyyn
TEMPEST	Sähkömagneettisen hajasäteilyn (EMR, Electro Magnetic Radiation) estävät suojatoimet määrittelevä NATO-standardi. Standardin sisältö ei ole julkista tietoa. Standardin pohjalta on valmisteltu normi Euroopan Unionin turvallisuusluokitellun tiedon suojaamiseksi.
Teräspuomi	Riippulukkokiinnikkeillä varustettu, teräsputkiprofiilista tai lattateräksestä valmistettu oven, parioven tai suojalevyn lukituslaite. Puomi on kiinnitettävä tai lukittava molemmista päistään seinään tai karmiin. Puomi voidaan valmistaa vähintään 50x30x3 mm3:n teräsputkiprofiilista tai vähintään 12x50 mm2: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 mm^2 (pyöröteräs ø 10 mm) ja aukkokoko enintään 400 cm2
Teräsverkko	Teräskehikkoon hitsaamalla kiinnitetty verkko, jonka poikkipinta-ala on vähintään 10 mm2 ja aukkokoko 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 4. 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 security-, että safety-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, rikosilmoitinjärjestelmä). Järjestelmävaatimukset on jaettu Finanssialan keskusliiton toimesta toimintavarmuutta painottaen neljään vaatimusluokkaan.

Turvallisuusluokiteltu asiakirja/tieto	Esiintymismuodostaan riippumaton salassa pidettävä tieto, joka on luokiteltu kuuluvaksi tietoturvallisuusasetuksessa määriteltyyn suojaustasoon ja joka on luokitusperusteidensa (tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle) vuoksi varustettu turvallisuusluokitusmerkinnällä (ks. 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).
Viranomaisten erillisvaatimukset	Määrättyjen turvallisuusviranomaisten hallussa olevat yksityiskohtaiset rakenteellisen turvallisuuden vaatimukset, jotka perustuvat viranomaisten tekemiin tunkeutumistesteihin ja näistä johdettuihin vasteaikoihin.

Liite 10. Lähdeluettelo

- Arkistolaitoksen määräys ja ohjeet arkistotiloista (KA 1386/40/2007, 21.8.2007)
- Arkistolaki (831/1994)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Euroopan unionin turvallisuusregiimi (6952/2/11 REV2/1.4.2011)
- ICT-varautumisen vaatimukset (VAHTI 1/2012)
- Kameravalvontaopas (julkaisija Turva-alan yrittäjät ry 2011)
- Kansallinen turvallisuusauditointikriteeristö (versio II, 2011)
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- Laki turvallisuusselvityksistä (177/2002)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- NATO AC/35-D/2001 Directive on Physical Security, (rev.2008, NATO UNCLASSIFIED)
- Naton turvallisuussäännöstö C-M 2002(49), (2002)
- Ohje tietoturva-asetuksen täytäntöönpanosta (VAHTI 2/2010)
- Puolustusvoimien tilaturvallisuusmääräys (2011)
- Rakennushankkeiden turvallisuusaskeleet, (Juha Kyllönen, PHRAKL 2012)
- Rakenteellinen murtosuojeluohje I – III (Finanssialan Keskusliitto ry 2011)
- Sisäasiainhallinnon tilaturvallisuusmääräys (2011)
- Sisäverkko-ohje (VAHTI 3/2010)
- Standardi ISO/IEC 27002:2005
- Suomen rakentamismääräyskokoelma (1993–2011)
- Turvallisuusluokitellun tiedon hallintaprosessi puolustushallinnon rakentamishankkeissa (Juha Kyllönen, PHRAKL 2012)
- Valtioneuvoston asetus tieturvallisuudesta valtionhallinnossa (681/2010)
- Yhteiskunnan turvallisuusstrategia (2010)

LIITE 11. Voimassa olevat VAHTI -julkaisut

VAHTI 2/2013	Toimitilojen tietoturvaohje
VAHTI 1/2013	Sovelluskehityksen tietoturvaohje
VAHTI 3/2012	Teknisen ICT-ympäristön tietoturvataso-ohje
VAHTI 2/2012	ICT-varautumisen vaatimukset
VAHTI 1/2012	VAHTIn toimintakertomus vuodelta 2011
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset
VAHTI 5/2009	Effective Information Security
VAHTI 4/2009	Information Security Instructions for Personnel
VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008	Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008	Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys
VAHTI 4/2008	Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007	Älypuhelimien tietoturvallisuus
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 10/2006	Henkilöstön tietoturvaohje
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi

VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006	Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006	Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti-ohjeet

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin 0295 16001
Telefaksi 09 160 33123
www.vm.fi

2/2013
VAHTI
Toukokuu 2013

ISSN 1455-2566 (nid.)
ISBN 978-952-251-460-8 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-461-5 (pdf)