

Heikki Partanen

Pääurakoitsijan toiminta turvallisuusluokiteltua tietoa sisältävässä rakennushankkeessa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Rakennustekniikka

Insinööryö

14.11.2018

Tekijä Otsikko	Heikki Partanen Pääurakoitsijan toiminta turvallisuusluokiteltua tietoa sisältävässä rakennushankkeessa
Sivumäärä Aika	32 sivua + 4 liitettä 14.11.2018
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Rakennustekniikka
Ammatillinen pääaine	Rakennustuotantotekniikka
Ohjaajat	Tuntiopettaja Johan Hellberg Työpäällikkö Juha Korkiakoski
<p>Tämä insinöörityö tehtiin NCC Suomi Oy:n korjausrakointiyksikön toimeksiannosta. Tutkimuksen päätavoite oli selvittää, mitä vaatimuksia pääurakoitsijan työmaatoimintaan aiheutuu siitä, että rakennushankkeessa on turvallisuusluokiteltuja suunnitelma-asiakirjoja ja muita dokumentteja. Lisäksi tavoitteena oli kehittää toimintaohjeet käytännön järjestelyistä, joilla nämä vaatimukset voidaan täyttää ja laatia työturvallisuusosio työmaan perehdytysaineistoon.</p> <p>Tutkimus toteutettiin kirjallisuustutkimuksena. Aineistona käytettiin ajantasaista lainsäädäntöä, valtionhallinnon ohjeita ja aihepiiriä käsitteleviä aiempia tutkimuksia. Lisäksi hyödynnettiin opinnäytetyön tekijän omia kokemuksia luokitelluista rakennushankkeista. Tutkimustuloksia tarkasteltiin korjausrakentamisen näkökulmasta huomioiden siihen liittyvät erityispiirteet.</p> <p>Tutkimustuloksena syntyi turvallisuusluokitellun tietoaineiston aiheuttamat erityisvaatimukset huomioon ottava perehdytysaineisto tietoturvallisuusvaatimuksista työmaaolosuhteissa ja opas työmaajärjestelyiden toteutuksessa huomioitavista asioista.</p> <p>Keskeisiksi huomioitaviksi asioiksi nousivat pääurakoitsijan työmaa-alueella toteuttama henkilöiden, dokumenttien ja työmaa-alueen hallinta. Kaikki ovat toimintoja joita toteutetaan jo tavanomaisella työmaalla, mutta turvallisuusluokitellun aineiston käsittely asettaa toiminnoille korkeammat vaatimukset toteutuksen huolellisuuden ja valvonnan suhteen.</p> <p>Tietoturvallisuusvaatimukset tulee ottaa huomioon mahdollisimman varhaisessa vaiheessa.</p>	
Avainsanat	tietoturvallisuus, turvallisuus selvitys, turvallisuusluokiteltu tieto, turvallisuuspolitiikka

Author Title	Heikki Partanen General contractor's actions in construction project containing classified information
Number of Pages Date	32 pages + 4 appendices 14 November 2018
Degree	Bachelor of Engineering
Degree Programme	Civil Engineering
Professional Major	Construction and Site Management
Instructors	Johan Hellberg, Lecturer Juha Korhikoski, Contract Manager
<p>This Bachelors thesis was commissioned by renovation unit of NCC Finland. The main goal of the study was to find out what requirements for main contractor's construction site activity is posed by project contains classified construction plans and other documents. secondary goals were to develop operational guidelines for practical arrangements to meet these requirements and information security part for the construction site orientation.</p> <p>The study was conducted as a literature study The used material was legislation, state administration guidelines and previous studies about the topic. Also, the author's own experiences of classified construction projects were utilized. The research findings were reviewed from renovation contractors point of view of considering the specific features involved in that field of construction.</p> <p>As the result of the research was created orientation material that takes into account the specific information security requirement and guidance on the issues to be taken into account when founding the construction site.</p> <p>Key issues to be considered were the management of people, documents and work site areas carried out by the main contractor at the construction site. All of these are activities that are already carried out on a regular site, but the handling of classified material introduces higher demands on operations in terms of the care and control of the implementation.</p> <p>Information security requirements must be taken into account as early as possible.</p>	
Keywords	information security, security clearance, classified information, security policy

Sisällys

Lyhenteet ja käsitteet

1	Johdanto	1
1.1	Opinnäytetyön tausta	1
1.2	Tutkimuksen tavoite ja rajaukset	2
1.3	Tutkimuskysymykset	2
1.4	Tutkimusmenetelmät	2
2	Tietoturvallisuuden lainsäädännöllinen tausta	3
2.1	Tietoturvallisuuden määrittely	3
2.2	Julkisuuslaki	4
2.3	Tietoturvallisuusasetus	5
2.4	Turvallisuusselvityslaki ja turvallisuus selvitys prosessi	6
2.5	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI	7
2.6	Katakri 2015	8
3	Salassa pidettävät asiakirjat ja turvallisuusluokittelu	9
3.1	Tiedon suojaustasot rakennushankkeessa	10
3.2	Suunnitelma-asiakirjojen luokittelu	11
3.3	Suunnitelma-asiakirjojen suojaustasot ja suunnittelun ohjaus	12
4	Tietoturvallisuuden toteuttaminen työmaajärjestelyissä	14
4.1	Pääurakoitsijan asema ja vastuut luottamuksellisessa hankkeessa	14
4.2	Henkilöstöturvallisuuden toteutus työmaajärjestelyissä	15
4.2.1	Turvallisuus selvitys ja vaitiolositoumus	15
4.2.2	Henkilöstön perehdytys tietoturvaluuteen	16
4.2.3	Avainten ja kulkutunnisteiden hallinta	16
4.2.4	Valokuvaamisen lupakäytäntö työmaalla	18
4.2.5	Vierailijakäytännöt työmaalla	18
4.3	Asiakirjaturvallisuuden toteutus työmaajärjestelyissä	20
4.3.1	Tiedon vastaanottaminen	20
4.3.2	Tiedon luovuttaminen eteenpäin	20
4.3.3	Tiedon säilytys ja käsittely	21
4.3.4	Tiedon hävittäminen	21

4.4	Tilaturvallisuuden toteutus työmaajärjestelyissä	22
4.4.1	Työmaa-alueen suojaus	23
4.4.2	Työmaatoimiston fyysinen suojaus	27
4.4.3	Korjattavan rakennuskohteen suojaus	28
4.4.4	Korotetun turvallisuustason työmaatilat	29
4.5	Tietoturvallisuusauditointi	30
5	Johtopäätökset	31
	Lähteet	33

Liitteet

Liite 1. Työmaaperehdytyksen tietoturvallisuusaineisto

Liite 2. Turvallisuusselvitys-prosessin hallinnointitaulukko

Liite 3. Turvallisuusselvityksen prosessikaavio

Liite 4. Tietoturvallisuuden arviointi pisteytysmallilla

Lyhenteet ja käsitteet

Katakri	Kansallinen turvallisuusauditointikriteeristö
ST	Suojaustaso
TL	Turvallisuusluokiteltu, turvallisuusluokitus
tursel	Turvallisuus selvitys
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä

1 Johdanto

1.1 Opinnäytetyön tausta

Rakennusliikkeet joutuvat toiminnassaan ottamaan huomioon monenlaiset tilaajien vaatimukset ja ehdot. Yleensä ehdot ovat luonteeltaan kaupallisia ja koskevat esimerkiksi maksuehtoja, toimitusaikaa jne. Nämä menettelytavat on määritetty rakennusalan yleisissä sopimusehdoissa, kohdekohtaisessa urakkaohjelmassa ja siihen rinnastettavissa asiakirjoissa. Tällaiset ehdot ovat rakennusalalla ammattimaisesti toimiville itsensänselvyyksiä ja niiden vaikutus työmaatoteutukseen on vakiintunutta ja tunnettua.

Toisinaan tilaajana on jokin viranomaistaho, jonka toiminnan luonteen takia tarjouslaskennasta alkaen joudutaan käsittelemään salassa pidettäviä asiakirjoja, kun suunnitelma-asiakirjoilla on jonkin asteinen turvallisuusluokitus.

Tarjouslaskentavaiheen aikana asia on vielä hallittavissa ilman mittavia järjestelyjä, koska tässä vaiheessa tilaaja on yleensä rajannut tarjouslaskenta-aineiston salassa pidettävän osuuden tarjouskilpailun ja hinnanmuodostuksen kannalta välttämättömälle minimitasolle. Tässä vaiheessa TL-aineistoa käsittelee yrityksessä korkeintaan muutama henkilö. Lisäksi laskentavaihe on ajalliselta kestoaltaan suhteellisen lyhyt, tyypillisesti korkeintaan muutamia kuukausia.

Rakentamisvaiheessa vaatimukset ja haasteet lisääntyvät huomattavasti, kun hankkeen TL-aineiston määrä lisääntyy ja kyseessä olevaa aineistoa käsittelevien henkilöiden ja sidosryhmien lukumäärä kasvaa. Mikäli rakennusliike ei ole riittävästi varautunut tähän haasteeseen esimerkiksi henkilöresurssien osalta, edessä on suuria ongelmia, kun tavanomaisen rakentamisprosessin lisäksi joudutaan huolehtimaan tietoturvalisuusvaatimuksista.

Opinnäytetyön toimeksiantaja on NCC Suomi Oy:n korjausurakointiyksikkö. Tutkimuksella selvitetään mitä haasteita rakennushankkeen päätoteuttajan toimintaan aiheutuu siitä, että hanke sisältää turvaluokiteltua tietoa ja millaisilla käytännön toimilla ja järjestelyillä haasteisiin vastataan.

1.2 Tutkimuksen tavoite ja rajaukset

Keskeisenä tutkimustavoitteena on tunnistaa turvaluokitellun tiedon vaatimat toimenpiteet työmaajärjestelyissä ja kehittää toimintamalli ja -ohjeet helpottamaan rakennushankkeeseen osallistuvien pääurakoitsijan työmaatoimihenkilöiden työskentelyä.

Tutkimus rajataan käsittelemään isoja korjausurakointi hankkeita, jotka toteutetaan projektinjohtomuotoisena. Tarkastelun kohteeksi rajataan suojaustason IV turvallisuusluokitellun tietoaineiston suojaamiseksi vaadittavat työmaajärjestelyt.

Tutkimuksen ulkopuolelle rajataan myös asiakirjojen käsittelyn tietotekniset vaatimukset ja järjestelyt.

1.3 Tutkimuskysymykset

Tutkimuksen pääkysymys:

- Miten pääurakoitsijan toimintaan työmaajärjestelyissä vaikuttaa turvaluokitellun tiedon käsittely?

Tutkimuksen alakysymykset:

- Miten lait ja asetukset ohjaavat tiedon turvallisuusluokittelua ja siihen liittyviä turvallisuustoimenpiteitä?
- Millaisia ylimääräisiä vaatimuksia pääurakoitsijan toimintaan rakennushankkeessa asettaa se, että siinä käsitellään turvaluokiteltua tietoa?

1.4 Tutkimusmenetelmät

Tutkimusmenetelmänä käytetään kirjallisuustutkimusta. Tutkimuksessa pyritään koamaan kirjallisuusaineiston perusteella vastauksia tutkimuskysymyksiin ja rakentamaan kokonaiskuva viranomaisen salassa pidettävän tietoaineiston käsittelystä rakennushankkeen kontekstissa.

Lähteinä käytetään tietoturvallisuutta käsitteleviä lakeja ja asetuksia, valtionhallinnon julkisia ohjeita sekä aiheesta aiemmin tehtyjä opinnäyte- ja muita tutkielmia.

2 Tietoturvallisuuden lainsäädännöllinen tausta

Suomessa säädökset muodostavat alaspäin tarkentuvan hierarkkisen kokonaisuuden. Ylimmällä ja sisällöltään yleisluoteisimmalla tasolla ovat lait. Seuraavan tason muodostavat asetukset, jotka tarkentavat ja selventävät lakitekstin määräyksiä. Alimmalla tasolla ovat viranomaisohjeet, jotka tarkentavat asetuksella säädettyjä asioita.



Kuva 1. Lainsäädännön hierarkkinen rakenne

2.1 Tietoturvallisuuden määrittely

Kansainvälisen standardin SFS-ISO 27000:2017 mukaan tietoturvallisuus on ensisijaisesti tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämistä ja toissijaisesti tiedon aitouden, kiistämättömyyden ja luotettavuuden säilyttämistä. [1, 2.23.]

Tietoturvallisuuden ensisijaiset käsitteet

- Tiedon luottamuksellisuudella tarkoitetaan sitä, että luvattomilla henkilöillä, tahoilla tai prosesseilla ei ole pääsyä tietoihin eikä tietoja luovuteta tällaisille tahoille. [1, 2.12.]
- Tiedon eheys on ominaisuus, johon sisältyy oikeellisuus ja kattavuus. [1, 2.40.]

- Tiedon saatavuus tarkoittaa, että valtuutetulla taholla on tarvepohjainen pääsy- ja käyttöoikeus kohteeseen. [1, 2.9.]

Tietoturvallisuuden toissijaiset käsitteet

- aitous on tahon ominaisuus olla mitä se väittää olevansa. [1, 2.8.]
- kiistämättömyys on kyky osoittaa, että väitetty tapahtuma tai toimenpide on todella tapahtunut ja että sen väitetty alkuperä pitää paikkansa. [1, 2.54.]
- luotettavuus on ominaisuus, joka tarkoittaa, että aiottu käytös ja tulokset ovat yhdenmukaisia [1, 2.62.]

Tietoturvallisuusasetus määrittelee tietoturvallisuuden seuraavasti:

tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä. [8, § 3.1.5.]

2.2 Julkisuuslaki

Lainsäädännöllinen lähtökohta viranomaistiedon salassapidolle on ”laissa viranomaisen toiminnan julkisuudesta”, josta yleisesti käytetään lyhennystä ”julkisuuslaki” (JulkL).

Julkisuuslain mukaan kaikki viranomaisen tieto on lähtökohtaisesti julkista, ellei toisin määrätä. [20, 1§.]

Julkisuuslaissa on säädetty 32-kohtainen luettelo [20, § 24.1.] viranomaisen asiakirjoista, jotka ovat salassa pidettäviä. Näistä rakentamisen kannalta merkittäviä ovat kohdissa 7 ja 10 määritetyt asiat:

7) henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista

ja

10) asiakirjat, jotka koskevat sotilastiedustelua, puolustusvoimien varustamista, kokoonpanoa, sijoitusta tai käyttöä taikka muuta sotilaallista maanpuolustusta taikka maanpuolustusta palvelevia keksintöjä, rakenteita, laitteita tai järjestelmiä taikka maanpuolustuksen kannalta muutoin merkityksellisiä kohteita taikka puo-

lustusvalmiuteen varautumista, jollei ole ilmeistä, että tiedon antaminen niistä ei vahingoita tai vaaranna maanpuolustuksen etua

Merkille pantavaa on, että lakiin on kirjattu teksti ”jollei ole ilmeistä”. Itsestään selvyyksiä ja yleisessä tiedossa olevia asioita ei tarvitse viranomaisen salata, vaikka ne koskisivatkin sinänsä salassa pidettävää aihealuetta.

2.3 Tietoturvallisuusasetus

Julkisuuslain määräyksiä täsmentää ja tarkentaa ”Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa”, josta yleisesti käytetään lyhennettyä muotoa ”tietoturvallisuusasetus”.

Tietoturvallisuusasetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. [8, § 1.]

Keskeisiä rakennusliikkeen toimintaan hankkeessa vaikuttavia vaatimuksia esitetty asetuksen viidennessä pykälässä, joka on otsikoitu ”Tietoturvallisuuden perustason toteuttaminen”. Kyseisessä pykälässä on 10-kohtainen luettelo, joka alkaa: ”Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:” [8, § 5.1.] Luettelon kohdat 5, 7 ja 8 ovat asioita, joista huolehtimisen rakensipalvelun tilaava viranomainen lähes poikkeuksetta ainakin osittain siirtää rakennushankkeessa sopimusteknisesti pääurakoitsijan vastuulle:

5) asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;

7) asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;

8) henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;

2.4 Turvallisuusselvityslaki ja turvallisuusselvitysprosessi

Tietoturva-asetus velvoittaa viranomaisen varmistamaan asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien henkilöiden luotettavuus turvallisuusselvitysmenettelyn avulla. [8, § 5.1.] Menettelystä säädetään turvallisuusselvityslaisissa (762/2015). [7.]

Turvallisuusselvitys on yksi turvallisuusjärjestelyjä täydentävä keino. Menettelyssä selvitetään laissa määritellyillä tavoilla selvityksen kohteen, eli henkilön taustaa. [4, s.18.]

Menettelyä hakee aina suojattavasta tiedosta vastuussa oleva taho, viranomainen tai eräissä poikkeustapauksissa yritys. Menettelyn kohteena on henkilö, jolle ollaan antamassa pääsy suojattavaan tietoon. [4, s. 13.]

Turvallisuusselvitysmenettelyn prosessikaavio on esitetty liitteessä 3.

Henkilöturvallisuusselvityksiä laaditaan kolmen tasoisena: suppeana, perusmuotoisena ja laajana. Henkilön aiottu tehtävä määrää sen minkä laajuisena selvitys tehdään, selvityksen laajuudesta riippuu mitä tietolähteitä selvityksen tekemiseen käytetään. Lisäksi kaikilla selvityksen tasoilla on mahdollista haastatella selvityksen kohdetta eli henkilöä. [4, s.18.]

Perusmuotoisessa turvallisuusselvityksessä voidaan käyttää kaikkia turvallisuusselvityslain 25 §:ssä mainittuja tietolähteitä, muun muassa poliisiasiain tietojärjestelmä, rikosrekisteri, liiketoimintakieltorekisteri, väestötietojärjestelmä, eri oikeushallinnon tietojärjestelmät, Rajavartiolaitoksen ja Tullin tietojärjestelmät. [9.]

Suppean turvallisuusselvityksen laatiminen voi perustua turvallisuusselvityslain 25 §:n kohtien 1–10 tietolähteisiin - lukuun ottamatta Suojelupoliisin toiminnallista tietojärjestelmää ja pääesikunnan turvallisuustietorekisteriä. Suppean selvityksen ulkopuolelle jää mm. ulosottorekisteristä ja luottotietorekisteristä saatavat tiedot. [7, § 24.]

Laajoja turvallisuusselvityksiä laaditaan suhteellisen harvoin. Kriteerit, joiden perusteella tehtävä kuuluu laajan turvallisuusselvityksen piiriin [7, § 20.], ovat sellaiset, että rakentamisessa ei sellaisia tehtäviä ole kuin hyvin harvoin.

Kokemukseni mukaan turvallisuusselvityksiä rakennushankkeiden yhteydessä hakeville viranomaistahoilla on erilaisia käytäntöjä siitä minkä laajuisena turvallisuusselvitykset rakentamiseen osallistuville teetetään. Pääperiaate lienee arvio siitä, missä laajuudessa työtehtävässä tullaan käsittelemään salassa pidettävää aineistoa, joten lähtökohtaisesti toimihenkilöt selvitetään perusmuotoisena ja työntekijät suppeana.

Turvallisuusluokitellun tiedon yksi merkittävimpiä vaikutuksia pääurakoitsijan toimintaan rakennushankkeessa on tarvittavien turvallisuusselvitysten hakeminen ja niihin kuluva aika: Suojelupoliisin turvallisuusselvitysten odotettavissa oleva käsittelyaika 16.4.2018 oli 25 arkipäivää eli 5 työviikkoa. [10.] Tämä koskee pitkään Suomessa asuneita henkilöitä, pääasiassa Suomen kansalaisia. Mikäli turvaselvitettävä henkilö on asunut ulkomailla, tietoja joudutaan pyytämään ulkomaisilta turvallisuusviranomaisilta. Tällöin käsittelyaika on merkittävästi pidempi, jopa kuukausia.

Turvallisuusselvitysprosessin aikatauluvaikutukset ovat rakennushankkeessa merkittäviä sillä aliurakkahankinnassa täytyy ensin teettää turvallisuusselvitys aliurakoitsijaehdokkaiden laskijoista. Tähän prosessiin täytyy varata 5 viikkoa. Hankintapäätöksen jälkeen valitun aliurakoitsijan työntekijöiden turvallisuusselvitystä odotetaan toiset 5 viikkoa ennen kuin päästään töihin. Näin ollen hankkeessa on varauduttava kokonaisuudessaan 10 viikon ylimääräiseen viiveeseen. Mikäli tietoja joudutaan pyytämään ulkomailta, prosessi kestää merkittävästi pidempään, jopa useita kuukausia.

Aikatauluvaikutusten ohella turvallisuusselvitysten hallinnoinnista aiheutuu merkittäviä henkilöstökustannuksia. Prosessia hoitamaan tarvitaan työmaalle yksi täysipäiväinen toimihenkilö.

2.5 Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI

Tietosuoja-asetus on luonteeltaan hyvin yleisluontoinen säädös ja asetetut vaatimukset eivät ole yksiselitteisiä, saati konkreettisia. Niinpä valtionhallinto on julkaissut tarkentavia ohjeita, ehkä merkittävimpana Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) julkaisema ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta”.

VAHTI on valtiovarainministeriön asettama työryhmä. Alkuperäiseltä nimeltään se oli ”Valtionhallinnon tietoturvallisuuden johtoryhmä”, johon lyhennetty nimikin viittaa. Sittemmin nimi on vaihtunut muotoon ”julkisen hallinnon digitaalisen turvallisuuden johtoryhmä”. [14.] Tällä hetkellä (v. 2018) Väestörekisterikeskus vastaa VAHTIn operatiivisesta toiminnasta ja toiminnan kehittämisestä. [14.]

VAHTI on julkaissut lukuisia valtionhallinnon tietoturvallisuuteen liittyviä julkisia ohjeita, jotka tarkentavat lakien ja asetusten vaatimuksia. Ensisijaisesti ohjeet on laadittu valtionhallinnon eri toimialojen käyttöön, mutta ne ovat sovellettavissa myös yritystoimintaan.

Rakennushankkeen pääurakoitsijan kannalta merkityksellisiä VAHTI-ohjeita ovat

- VAHTI 2/2010 ohje tietosuoja-asetuksen täytäntöönpanosta
- VAHTI 9/2008 Hankkeen tietoturvaohje
- VAHTI 2/2013 Toimitilojen tietoturvaohje.

2.6 Katakri 2015

Katakri, alkuperäiseltä nimeltään ”Kansallinen turvallisuusauditointikriteeristö”, on viranomaisten auditointityökalu arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. [5, s. 2.]

Ensimmäinen versio valmistui vuonna 2009 puolustusministeriön johdolla ja sen tekemiseen osallistui viranomaistahojen lisäksi elinkeinoelämän edustajia. [5 s. 2.]

Vuoden 2015 kokonaisuudistuksessa nimi muutettiin muotoon ”Tietoturvallisuuden auditointityökalu viranomaisille”, mutta käyttöön vakiintunut lyhennys ”Katakri” päätettiin säilyttää. Samalla päävastuu ylläpidosta ja hallinnoinnista siirrettiin ulkoministeriössä toimivalle Kansalliselle turvallisuusviranomaiselle (NSA). [5, s. 3)

Katakri on kolmeen osa-alueeseen jaettu kokonaisuus:

- Osa-alue T: turvallisuusjohtaminen
- Osa-alue F: Fyysinen turvallisuus

- Osa-alue I: Tekninen tietoturvallisuus

Näistä Teknisen tietoturvallisuuden osa-alue on rakennushankkeessa pääurakoitsijan kannalta vähemmän merkityksellinen työmaaolosuhteiden järjestämisen kannalta.

Kun verrataan Katakria VAHTI-ohjeisiin, voidaan todeta, että vahtiohjeet kirjoittavat auki lakien ja asetusten tietoturvallisuusvaatimuksia ja ohjeistavat niiden toimenpänemiseen yleisellä tasolla, Katakri taas on työkalu, jonka avulla arvioidaan auditoitavan kohteen yleistä kykyä suojata viranomaisen salassa pidettävää tietoa. [5 s. 4..]

Katakri 2015 viittaa monin paikoin VAHTI-ohjeisiin, samoin VAHTI-ohjeissa on viittauksia Katakriin. Näitä onkin hyvin luontevaa käyttää rinnakkain, kun valmistaudutaan viranomaistahon suorittamaan tietoturvallisuustason auditointiin.

3 Salassa pidettävät asiakirjat ja turvallisuusluokittelu

Viranomaisen salassa pidettävät asiakirjat luokitellaan neljälle suojaustasolle sen mukaan, kuinka vakavia seuraamuksia tiedon oikeudettomasta paljastumisesta tai käytöstä voi aiheutua. Luokittelusta säädetään tietoturvallisuusasetuksessa. [8, § 8-12.]

Asiakirja leimataan erityisellä turvallisuusluokitusmerkinnällä, mikäli salassa pidettävän tiedon oikeudettomasta paljastumisesta tai käytöstä voi aiheutua vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7-10 kohdissa tarkoitetulla tavalla. [8, § 11.1.]

Muut salassa pidettävät asiakirjat leimataan "vain" "SALASSA PIDETTÄVÄ"- leimalla ja suojaustasomerkinnällä. Tällaisia ovat asiakirjat jotka ovat salassa pidettäviä julkisuuslain 24.1 §:n kohdissa 1, 3 - 6 sekä 11 - 32 tai muussa laissa määriteltyä salassa pidettävää tietoa. [11, s. 76.]

Taulukossa 1 on esitetty luokituksen perusteet, suojaustasot sekä vastaavat turvallisuusluokitusmerkinnät.

Taulukko 1. Asiakirjojen turvallisuusluokituksen perusteet [8, § 9-11.]

Seuraamus tiedon paljastumisesta, ”salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa salassapitosäännöksessä tarkoitetulle yleiselle edulle”:	Salassa pidettävien asiakirjojen luokittelussa käytävä suojaustaso:	Turvallisuusluokitusmerkintä:
haittaa	suojaustaso IV	KÄYTTÖ RAJOITETTU
vahinkoa	suojaustaso III	LUOTTAMUKSELLINEN
merkittävää vahinkoa	suojaustaso II	SALAINEN
erityisen suurta vahinkoa	suojaustaso I	ERITTÄIN SALAINEN



Kuva 2. Salassapitoleima ja suojaustasomerkintä



Kuva 3. Turvallisuusluokitusmerkintöjen leimat

3.1 Tiedon suojaustasot rakennushankkeessa

Taulukossa 2 on esitetty, millaisia tietoja rakennushankkeissa voi olla eri suojaustasoille luokiteltuna.

Taulukko 2. Esimerkkejä turvallisuusluokitellusta tiedosta rakennushankkeessa [17.]

Suunnitelman suojaustaso	Esimerkki suunnitelman sisällöstä
ST IV	Turvallisuutta koskevat yleissuunnitelmat.
ST III	Rakennuksia ja niiden turvallisuutta koskevat yksityiskohtaiset tiedot.
ST II	Yksityiskohtaiset suunnitelmat puolustus- ja turvallisuustoimialojen rakennushankkeissa.
ST I	Ei käsitellä rakennushankkeissa, tiedot on rajoitettu vain viranomaiskäyttöön.

3.2 Suunnitelma-asiakirjojen luokittelu

Julkisista lähteistä ei ole saatavilla yksiselitteisiä ohjeita rakennussuunnitelmien luokittelusta suojaustasoille.

Toimitilaohjeen liitteessä 5 on esitetty rakentamisdokumentaation käsittelysuositukset. Rakentamishankkeessa tulee laatia tiedon luokittelumatriisi, jossa on listattu dokumenttikokonaisuuksia, joita rakennushankkeessa käytetään. Luokittelumatriisi tulee aina laatia kohdekohtaiseksi ja pitää ajan tasalla.

Luokittelumatriisin esimerkki on esitetty kuvassa 1. Luokittelumatriisin tarkoitus on varmistaa, että tieto on luokiteltu oikeaan suojaustasoon ja että kaikki, jotka tuottavat tai käsittelevät tietoa, ovat tietoisia siitä, minkä suojaustason tietoa hän on käsittelemässä. [2, s. 76.]

TIEDON LUOKITTELUMATRIISI

Hanke:		Piirustustyyppi	Tiedon omistaja	Julkinen	ST IV	ST III	ST II	Huom.
1	Asemapiirros							
2	Pohjapiirustus							
3	Luolan leikkauskuvat							
4	Asemapiirros	Sähköpiirros						

Kuva 4. Esimerkki tiedon luokittelumatriisista [2, s. 76.]

Tiedon luokittelumatriisi on pääurakoitsijan kannalta äärimmäisen oleellinen asiakirja. Ilman ko. asiakirjaa on olemassa riski, että hankkeeseen tietoa tuottavat tahot (suunnittelijat) luokittelevat laatimansa asiakirjat tarpeettoman korkealle suojaustasolle. Tästä

seuraa aikatauluviivettä ja tarpeettomia kustannuksia. Lisäksi vaarana on, että turvallisuusluokitusmerkinnän arvostus ja kunnioitus kärsii, jos sitä käytetään rutiininomaisesti ”varmuuden vuoksi”. Näin ollen aidosti kriittisen tiedon suojaus vaarantuu.

Vaikka rakennuskohde itsessään olisi turvallisuuden kannalta kriittinen laitos, siellä on aina normaaleja tiloja, joiden suunnitelmat eivät liity turvallisuuteen. Tällaisia ovat esimerkiksi WC- yms. tilojen seinäkaaviot tai kalustekaaviot.

Pääurakoitsijan on syytä varmistaa, että tiedon luokittelumatriisi on laadittu kohdekohtaiseksi ja se on hankkeen sidosryhmille saatavissa esim. projektipankissa. Matriisista on syytä varmistaa seuraavat asiat:

- Onko tiedon luokittelumatriisille nimetty omistaja? (Päivittämisestä ja ylläpitämisestä vastaava henkilö.)
- Onko matriisissa listattu asiakirjoja, jotka eivät selvästi kuulu hankkeeseen?
- Onko hankkeessa asiakirjoja, jotka puuttuvat matriisista?
- Onko matriisi laadittu niin yksityiskohtaiseksi, että jokaisella rivillä on vain yksi suojaustasomerkintä?
- Onko jokaiselle asiakirjalle nimetty omistaja? Onko nimetty omistaja yksilöity luonnollinen henkilö?

Oleellista on, että tiedolle on määritetty omistaja, joka vastaa dokumentin oikeasta suojaustasosta.

3.3 Suunnitelma-asiakirjojen suojaustasot ja suunnittelun ohjaus

Suunnitelma-asiakirjat tulee eriyttää mahdollisimman laajasti julkiseen ja salassa pidettävään osaan. Tällä tarkoitetaan sitä, että esimerkiksi rakennetyypit julkaistaan kahdessa osassa. Turvallisuusjärjestelyistä johtuvat rakennetyypit omana Turvallisuusluokiteltuna vihkona ja tavanomaiset perusrakennetyypit (esim. kipsilevyseinät) julkisena asiakirjana.

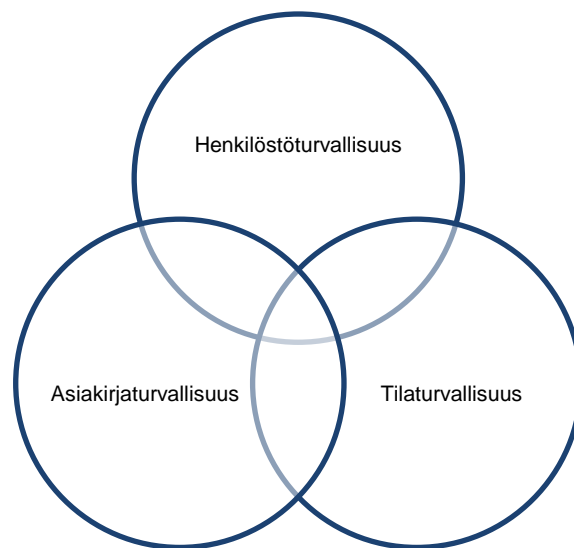
Tähän menettelytapaan pääurakoitsijan tulee ohjata suunnittelijoita heti kun tulee hankkeeseen mukaan, sillä omaksuttuja menettelytapoja on vaikea saada muutettua myöhemmin.

Työpiirustuksia käytetään ja käsitellään työmaalla eri tavalla kuin asiakirjoja yleensä. Esimerkiksi rakennetyypit tai detaljit ovat yleensä A4-kokoinen nidottu vihko, josta työmaaolosuhteissa tulee helposti nippu irtosivuja ja ST-luokitusmerkintä katoaa. Tästä johtuen suunnitelma-asiakirjojen suojaustasoa osoittavissa merkinnöissä, eli leimoissa on syytä noudattaa osittain viranomaisvaatimusta tiukempaa käytäntöä.

Tietosuoja-asetuksen mukaan ST III ja ST IV luokitelluissa asiakirjoissa leima sijoitetaan vain ensimmäisen sivun oikeaan yläkulmaan. [11, s. 86.] Suunnitelma-asiakirjoissa merkintä on syytä tehdä joka sivulle, jotta tieto käsiteltävän tiedon suojaustasosta säilyy koko ajan. Samasta syystä asiakirjan sivut ja sivujen lukumäärä tulee merkitä kaikkiin asiakirjoihin.

4 Tietoturvallisuuden toteuttaminen työmaajärjestelyissä

Tässä luvussa käsitellään käytännön toimenpiteitä työmaajärjestelyissä. Tässä tutkimuksessa työmaan tietoturvaluustoimenpiteet jaetaan henkilöstöturvallisuuden, asiakirjaturvallisuuden ja tilaturvallisuuden osa-alueisiin.



Kuva 5. Työmaan tietoturvallisuuden osa-alueet

Lähtökohtana tietoturvallisuuden suunnittelussa käytetään VAHTI-ohjeita: 2/2010 Ohje tietosuoja-asetuksen täytäntöönpanosta, 2/2013 Toimitilojen tietoturvaohje ja 9/2008 hankkeen tietoturvaohje sekä Katakri 2015. Yleensä hankekohtaisen suunnittelun perustana on rakennuttajan kohteeseen em. asiakirjojen pohjalta laatima turvaohje.

4.1 Pääurakoitsijan asema ja vastuut luottamuksellisessa hankkeessa

Tilaaajana toimiva viranomaistaho tekee pääurakoitsijana toimivan yrityksen kanssa turvallisuussopimuksen, jossa on mm. määritetty sopimussakko ja vahingonkorvaus johon tilaajalla on oikeus, mikäli urakoitsija rikkoo ko. turvallisuussopimuksen ehtoja.

Toimitilaohjeen liitteenä 7.1 on esimerkki rakentamispalvelun turvallisuussopimuksesta, jonka pohjalta turvallisuussopimus laaditaan kohdekohtaiset erityispiirteet huomioiden.

[2, s. 87.] Merkillepantavaa on, että sopimusteksti on muotoiltu niin, että tilaajan oikeus saada toimittajalta sopimussakkoa ei edellytä rikkomuksesta tilaajalle aiheutuneen vahingon toteennäyttämistä. [2, s. 98.] Tämän johdosta turvallisuusjärjestelyihin on kiinnitettävä erityistä huomiota.

Turvallisuussopimuksen mukaan pääurakoitsija vastaa käyttämiensä aliorakoitsijan toimista tilaajalle niin kuin omistaan. Siksi aliorakoitsijaehdokkaiden kanssa on tehtävä saman sisältöinen turvallisuussopimus kuin pääurakassa jo ennen tarjouspyyntöjen lähettämistä. Tätä edellytetään myös turvallisuussopimuksessa. [2, s. 96.]

4.2 Henkilöstöturvallisuuden toteutus työmaajärjestelyissä

Henkilöstöturvallisuus tarkoittaa hankkeessa työskentelevien henkilöiden luotettavuuteen ja soveltuvuuteen sekä oikeuksien hallintaan liittyvien turvallisuustekijöiden hoitamista. [16, liite 1, s. 1.]

Henkilöstöturvallisuuden keinoina rakennushankkeessa käytetään koulutusta ja hallinnollisen turvallisuuden osa-alueita eli turvallisuusselvityksiä, turvallisuussopimuksia ja vaitiolositoumuksia sekä työmaa-alueelle tulevien henkilöiden tunnistamista ja pääsyoikeuksien hallintaa ja rajaamista. [16, s. 9.]

Ihminen on tietoturvallisuusjärjestelyn onnistumisen kannalta heikoin lenkki ja henkilöstöturvallisuuden varmistaminen on tietoturvallisuustoiminnan perusedellytys.

Työmaalla toteutettavia henkilöstöturvallisuuden toimenpiteitä ovat hankehenkilöstölle tehtävät turvallisuusselvitykset, kouluttaminen tietoturvallisuuden vaatimuksista hankkeessa sekä kulkulupien ja -oikeuksien hallinnointi.

4.2.1 Turvallisuusselvitys ja vaitiolositoumus

Lähtökohta henkilöiden hankkeeseen osallistumiseksi on, että henkilö allekirjoittaa vaitiolositoumuksen ja suostumuksen siihen, että hänestä tehdään turvallisuusselvitys viranomaistahon edellyttämällä tavalla. Turvallisuusselvityksen tuloksen perusteella viranomaistaho hyväksyy tai hylkää henkilön osallistumisen hankkeeseen.

Vaitiolositoumuksella henkilö ”ilmoittaa saaneensa tiedon tietojen salassapidosta ja siitä, että niiden ilmaiseminen tai luovuttaminen ilman lupaa on kiellettyä.” [3, s. 89.]

Lähtökohta on, että henkilöt hyväksytään hankkeeseen vain turvallisuusselvityksen perusteella. Toisinaan viranomaisen sallii tähän hankekohtaisia lievennyksiä. On esimerkiksi mahdollista, että henkilöt päästetään hankkeeseen, kun he allekirjoittaneet vaitiolositoumuksen ja turvallisuusselvityshakemuksen. Tällöin on mahdollista, että henkilö poistetaan hankkeesta myöhemmin turvallisuusselvityksen tulosten perusteella.

Liitteessä 2 on asiakirjapohja pääurakoitsijan hankehenkilöstön turvallisuusselvitysprosessin hallinnasta ja dokumentoimisesta.

4.2.2 Henkilöstön perehdytys tietoturvaluuteen

Kaikille hankkeeseen osallistuvilla henkilöillä tulee kouluttaa henkilökohtainen vastuu ja perusasiat salassa pidettävien asiakirjojen käsittelystä ja säilyttämisestä. Koulutus tehdään työmaaperehdytyksen yhteydessä. Perehdytyksen tietoturvaluusaineisto on liitteessä 1.

Henkilöt, jotka työtehtävistään johtuen käsittelevät laajasti ST-aineistoa, koulutetaan erikseen.

4.2.3 Avainten ja kulkutunnusteiden hallinta

Työmaalle nimetään avainvastuuhenkilö, joka huolehtii avainten säilytyksestä ja muusta hallinnoimisesta.

Kaikista työmaalla olevista avaimista ja niihin rinnastettavista kulkutunnusteista laaditaan luettelo. Mikäli avaimessa itsessään ei ole yksilöivää tunnistemerkintää, siihen liitetään merkintä avaimenperällä.



Kuva 6. Avainperät teksti-ikkunalla

Avaimia ja niihin rinnastettavia kulcutunnisteita säilytetään lukitussa, tukevasti seinään kiinnitettyssä avainkaapissa.



Kuva 7. Seinään kiinnitettävä avainkaappi

Avaimia luovutetaan vain todettuun tarpeeseen, henkilökohtaisesti kuittausta vastaan. Kun tarve päättyy, avaimet tulee palauttaa.

Avain- ja kulkulupaluettelot tarkastetaan säännöllisesti, vähintään kolmen kuukauden välein. Henkilöiltä, joiden työskentely hankkeessa on päättynyt, poistetaan kulkuoikeudet ja pyydetään palauttamaan avaimet.

4.2.4 Valokuvaamisen lupakäytäntö työmaalla

Työmaalla on valokuvaaminen kielletty, työmaa-aitoihin ja työmaarakennusten oviin kiinnitetään kiellosta muistuttavat kyltit.

Lähtökohtaisesti valokuvaaminen on sallittua ainoastaan pääurakoitsijan työnjohdon, valvojien tai suunnittelijoiden suorittaman laadunvalvonnan dokumentoimiseksi. Myös muille tahoille voidaan myöntää lupa valokuvaamiseen, mikäli valokuvaamiselle on olemassa perusteltu tarve.

Valokuvausluvut ovat henkilökohtaisia ja myönnettyistä luvista pidetään kirjaa.

Kuvaamiseen käytetään ainoastaan kameraa, joka tallentaa kuvat muistikortilla ja jossa ei ole tietoliikenneyhteyksiä. Valokuvaaminen kännykkäkameroilla on korostetusti kiellettyä.

4.2.5 Vierailijakäytännöt työmaalla

Pääsy työmaalle on vain hankekohtaisen turvallisuus selvitysmenettelyn kautta hyväksytyillä henkilöillä hankkeeseen liittyvien työtehtävien suorittamiseksi. Toisinaan on tarpeellista, että työmaalle tulee henkilöitä tämän prosessin ulkopuolelta. Näin käy viimeistään siinä vaiheessa, kun käyttäjän edustajat tutustuvat uusiin tiloihin.

Työmaalla vierailulle on asetettava seuraavat reunaehdot:

- Vierailulla on hankkeeseen liittyvä perusteltu syy.
- Vierailun isäntänä on rakennushankkeen projektiorganisaatiossa toimiva henkilö, joka on perehdytetty työmaa-alueen turvallisuusolosuhteisiin.

- Vierailijat tunnistetaan ja kirjataan vieraskirjaan ainakin seuraavat tiedot: vierailijan nimi ja organisaatio, vierailun syy, vierailijan isäntä ja vierailun ajankohta.

Vierailun isäntä vastaa siitä, että vieras ei pääse näkemään salassa pidettävää tietoa, johon tällä ei ole oikeutta.

4.3 Asiakirjaturvallisuuden toteutus työmaajärjestelyissä

Lähtökohta asiakirjaturvallisuuden järjestämisessä on se, että turvallisuusluokitellun aineiston määrä minimoidaan. Perustyökalu tähän on tiedon luokittelumatriisi, sen pitäminen ajan tasalla ja tietoa tuottavien henkilöiden saatavilla.

4.3.1 Tiedon vastaanottaminen

Salassa pidettävän tiedon vastaanottamisessa korostuu tiedon eheyden ja kiistämättömyyden varmistaminen. Toisin sanoen tietoa vastaanottavan tahon täytyy pystyä luotettavasti todentamaan, että tieto on todella peräisin siltä, joka esiintyy tiedon lähettäjänä ja tieto siirtyy muuttumattomana lähettäjältä vastaanottajalle.

Tällaisia tietoja, joiden eheydestä ja kiistämättömyydestä pääurakoitsijan tulee pystyä vakuuttamaan, ovat muun muassa tiedot henkilöiden turvallisuus selvitysten tuloksista, työmaalle toimitettavat suunnitelma-asiakirjat jne.

Hankekohtaiset tiedon välityksen toimintatavat määrittää tilaaja.

4.3.2 Tiedon luovuttaminen eteenpäin

Lähtökohta turvallisuusluokitellun tiedon suhteen on aina se, että henkilölle annetaan pääsy vain siihen tietoon, jota hän tarvitsee työtehtäviensä suorittamiseksi ja vain siksi aikaa, kun hän suorittaa tätä työtehtävää. [11, s.64.]

Ennen kuin luovutetaan salassa pidettävää tietoa eteenpäin, on varmistettava, että vastaanottavalla taholla on tarve, oikeus ja valmiudet käsitellä ja säilyttää salassa pidettävää tietoa. Tiedonvaihto tilaajan organisaation suuntaan (suunnittelijat, valvojat yms.) on selvä ja se tapahtuu samojen tilaajan määrittämien toimintatapojen mukaan kuin tiedon vastaanottaminen.

Alihankkijoiden osalta vaatimusten täyttymistä on tosiasiallisesti mahdotonta valvoa. Lähtökohtana on, että kaikki luottamuksellinen aineisto säilytetään työmaalla valvotussa ja turvallisissa olosuhteissa.

Poikkeuksen muodostavat eräät turvallisuusratkaisuihin liittyvät urakoitsijat (esim. lukitus- ja turvaurakoitsijat, murtosuojaovien toimittajat jne.), joilla voidaan toimintansa luonteen johdosta katsoa olevan ammattitaitoa tietojen turvalliseen käsittelyyn. Tällöinkin urakoitsijan tietoturvallisuuden taso tulee auditoida ennen tietojen luovuttamista.

4.3.3 Tiedon säilytys ja käsittely

Salassa pidettävä tietoaineisto säilytetään ja käsitellään aina asianmukaisesti suojattuna ja noudattaen ns. puhtaan pöydän periaatetta. Tällä tarkoitetaan sitä, että turvallisuusluokiteltuja asiakirjoja ei säilytetä työpöydällä edes taukojen aikana.

4.3.4 Tiedon hävittäminen

Riippuen dokumentin suojaustasosta, tiedon hävittäminen on sallittu kolmella tavalla: [11, s.95.]

- valvotusti polttamalla
- paperisilppurissa, vaadittu silpun koko vaihtelee suojaaluokan mukaan, ST-IV asiakirjat saa hävittää silppurilla, joka tekee enintään 3,9 x 30 mm kokoista silppua.
- suljettuun astiaan siirrettäväksi polttolaitokseen

Koska rakennustyömaalla ei yleensä ole mahdollisuutta paperien polttamiseen, jäljelle jää kaksi vaihtoehtoa.

Vaivattominta on kerätä hävitettävät asiakirjat lukolliseen tietosuoja-astiaan ja toimittaa ne tuhottavaksi laitokseen. Hävittämisestä tulee vaatia todistus, joka arkistoidaan sovitulla tavalla yrityksen omaan tietojärjestelmään tai projektipankkiin.

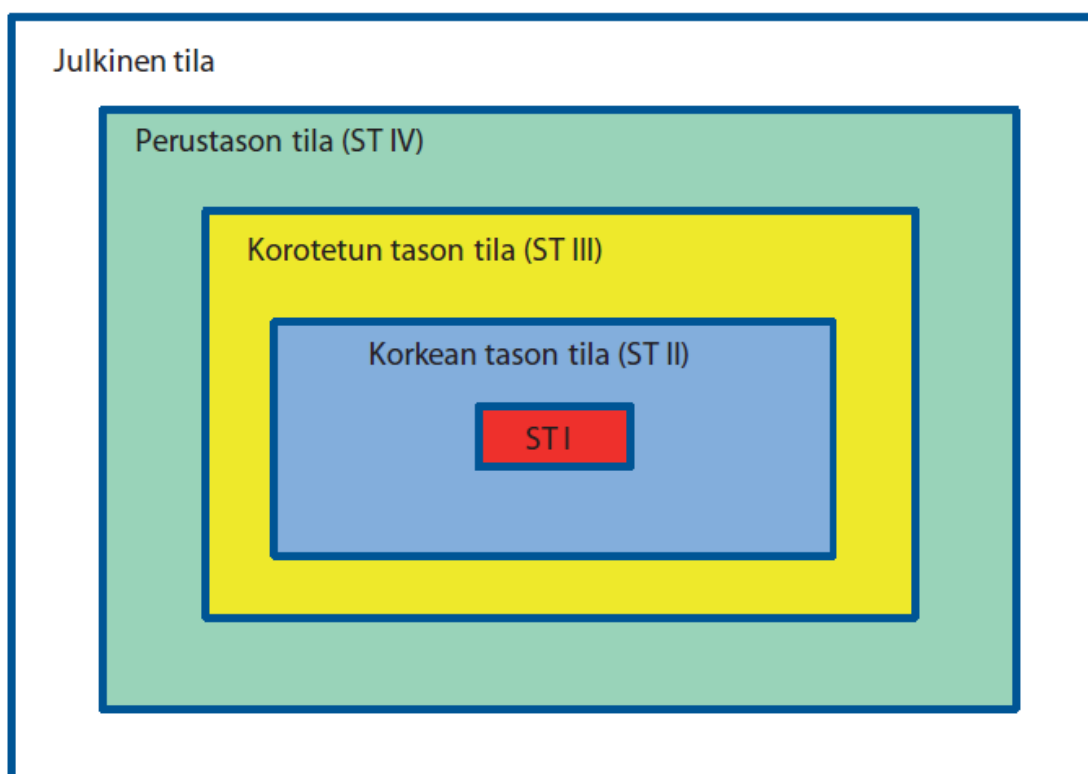
Isolle työmaalle voi olla kannattavaa hankkia paperisilppuri A4-kokoisten asiakirjojen hävittämiseen. Silppuria hankittaessa tulee valita riittävän tehokas silppuri.

4.4 Tilaturvallisuuden toteutus työmaajärjestelyissä

Tilaturvallisuudella tarkoitetaan rakenteellisia ja valvonnallisia järjestelyjä, joilla varmistetaan tilojen pysyminen vain oikeutettujen hallinnassa ja käytössä sekä käyttötarkoituksen edellyttämässä kunnossa. [16, liite 1, s. 2.]

Tilaturvallisuuden toteuttamiseksi suojattava alue jaetaan eritasoisin turvallisuusvyöhykkeisiin sen mukaan, minkä tasoista tietoa tiloissa käsitellään. [2, s. 19.]

Toimitilaohje luokittelee tilat julkiseen tilaan (eräänlainen ”0-taso”) ja neljään sanallisesti nimettyyn turvallisuusvyöhykkeeseen jotka vastaavat suojaustasoja (I-IV). Kuvassa 8 on esitetty periaate turvallisuusvyöhykkeiden sisäkkäisen toteutuksen periaatteesta ja tasoista käytetyistä nimityksistä ja värikoodauksesta.



Kuva 8. Monitasoisen suojaamisen periaate [2, s. 22.]

Rakennustyömaan yhteydessä ei voi puhua julkisesta tilasta, sillä alueelle on lähtökohdaisesti asiattomilta pääsy kielletty, vaikka siellä ei olisi salassa pidettävää tietoa. Työmaa-alue täyttää Katakriin kohdassa F02 hallinnolliselle alueelle asetetut vaatimukset, koska alueella on selkeästi määritellyt rajat ja pääsy ilman saattajaa vain henkilöillä, joilla on lupa tulla alueelle. [5, s. 19.]

4.4.1 Työmaa-alueen suojaus

Rakennustyömaan aluesuojaus toteutetaan hyvälle tasolle jo työturvallisuusvaatimusten takia. Toinen syy aluesuojauksen korkeatasoiseen toteutukseen tavanomaisella rakennustyömaalla on rikosten torjunta. Työmaat vakuutetaan mm. omaisuusrikosten varalta ja vakuutuksen myöntäjä edellyttää toimenpiteitä vakuutetun omaisuuden turvaamiseksi. Finanssialan julkaisussa ”rakennustyömaiden rikostorjunta” on esitetty perusasiat työmaan suojaamiseksi tehtävistä toimenpiteistä. [12.]

Tässä luvussa käsitellään ST-aineiston suojaamiseksi toteutettavia korotetun turvallisuustason toimenpiteitä työmaajärjestelyissä.

Työmaan aitaus

Työmaa-aita on ensimmäinen suojaustaso turvallisuus järjestelyissä. Määräyksissä ja ohjeissa ei anneta täsmällisiä vaatimuksia aitaamisen toteutustasosta. Toimitilaohjeen mukaan aitausta vaaditaan korotetun tason ja sitä ylemmällä vyöhykkeellä. [2, s. 36, kohta 3.] Tällöin aidan tulisi olla vähintään 2,4m korkea. [2, s. 45.]

Vaatimuksen täyttävä ratkaisu on esimerkiksi Vepe Oy:n Euro3p-aitaelementti korotusosalla korotettuna. Kokonaisuuden korkeus on 2,6 m. Aitaelementit kiinnitetään toisiinsa kiinnikkeillä niin että aita ei ole avattavissa ilman työkaluja.



Kuva 9. Työmaa-aidan korotus

Henkilöliikenne

Vaatus raportoida työmaalla työskentelevien henkilöiden tiedot verottajalle sähköisesti on johtanut siihen, että työmaa pyritään aitaamaan niin, että työmaalle tullaan vain kulunvalvontapisteen kautta. Teknisesti paras ratkaisu tähän on pyöröportti, jonka sisä- ja ulkopuolella on kulunvalvontalukijat, joilla henkilöt kirjataan järjestelmään sisään tai ulos. Tällä järjestelyllä voidaan saada mahdollisimman ajantasoinen tieto työmaalla kullakin hetkellä olevista työntekijöistä.

Kuvassa 9 on esitetty esimerkki työmaan henkilöliikenteen pyöröportin toteutuksesta. Esimerkissä pyöröportin tiivis limittyminen työmaa-aitaan on varmistettu vanerirakenteilla.



Kuva 10. Henkilöportti työmaa-alueelle

Käytetyn kulunvalvontajärjestelmän tulee mahdollistaa kulkuoikeuksien rajaaminen kellonaikojen ja päivien mukaan, niin että työmaalle ei pääse esim. keskellä yötä käytämällä kulkutunnisteita.

Ajoneuvoliikenne

Ajoneuvoliikenne työmaa-alueelle järjestetään kulunvalvotun sähkötoimisen liukuportin kautta. Sähköisesti ohjatun ajoneuvoportin kustannukset ovat n. 10-kertaiset manuaalisesti avattavaan ja suljettavaan, riippulukolla lukittavaan porttiin verrattuna. Kustannus on kuitenkin perusteltu, sillä tällä järjestelyllä voidaan varmistaa, että portti sulkeutuu ja pysyy kiinni.

Kuvassa 10 on esimerkk toteutus työmaan sähköisen liukuportin toteutuksesta.



Kuva 11. Työmaan sähköinen liukuportti ajoneuvoliikenteelle

Piirivartiointi ja kameravalvonta

Yleensä tilaaja edellyttää hankekohtaisessa turvallisuussopimuksessa, että kohteeseen järjestetään työajan ulkopuolella piirivartiointi ja tallentava kameravalvonta

Työmaalla aloitetaan piirivartiointi mahdollisimman pian sen jälkeen, kun pääurakoitsija saa työmaa-alueen hallintaansa. Piirivartijan työmaakerrokseen kuuluu työmaa-alueella olevien suojattavien kohteiden lukituksen tarkastus (työmaaportit, työmaatoimisto, varastokontit ja työmaarakennukset jne.) ja työmaa-alueella tehtävä kierros.

Työmaakerroksella tarkastetaan, että kuorisuoja on ehjä, eikä työmaa-alueella ole mitään epäilyttävää tai asiaankuulumatonta toimintaa.

Mikäli kohdekohtaisesti ei muuta vaadita, niin valvontakamerat on syytä sijoittaa siten, että työmaa-alueelle johtavat portit (henkilö ja ajoneuvoliikenne) valvotaan. Kohdekohtaisen riski- ja uhka-arvion perusteella harkitaan muut valvontakameralla suojattavat kohteet.

Työmaa-alueen ulkovalaistus

Työturvallisuuden takia työmaa-alueen ulkovalaistus on toteutettava riittävälle tasolle vähintään kulku- ja työskentelyalueille.

Alueturvallisuutta täydentävä ulkovalaistus harkitaan kohdekohtaisesti. Ihannetilanteessa koko työmaa-alueen ulkokuori on tehokkaasti valaistu, niin että myös pimeään aikaan alueelle tunkeutuminen jää huomaamatta.

Alueelle tunkeutumista voidaan ehkäistä kustannustehokkaasti esimerkiksi liikkeestä aktivoituvilla valonheittimillä.

4.4.2 Työmaatoimiston fyysinen suojaus

Työmaatoimisto on turva-alue, koska siellä säilytetään ST-aineistoa. Se on tyypillisesti ainoa turva-alue työmaa-alueella.

Työmaatoimisto voidaan sijoittaa olemassa olevaan kiinteistöön tai työmaatiloihin eli ns. parakkeihin.

Hälytysjärjestelmä

Työmaatoimisto suojataan tason 3 murtohälytysjärjestelmällä. Tämä tarkoittaa suojattavan alueen täydellistä kuorisuojausta toteutettuna esimerkiksi ovikoskettimilla ja lasirikkoilmaisimilla sekä liiketunnistimilla toteutettu tilavalvonta joka kattaa kaikki huoneet, joissa säilytetään suojattavaa aineistoa. [13 s. 6.]

Tason 3 hälytysjärjestelmä kytketään päälle ja pois käyttäen henkilökohtaisia vähintään neljä merkkisiä koodeja. Järjestelmään aktivoidaan vain tarpeellinen määrä käyttäjiä. Käyttäjälueetelo tarkistetaan säännöllisesti kulkulupa- ja avainluetteloiden tarkastuksen yhteydessä.

Hälytysjärjestelmä kytketään päälle aina kun viimeinen henkilö poistuu, niin että tyhjä tila on aina suojattu hälytysjärjestelmällä.

Hälytysjärjestelmän käyttöpaneeli sijoitetaan valvottavan työmaatoimiston käyntioven yhteyteen, niin että järjestelmä on aktivoitavissa päälle ja pois alueelle tultaessa ja sieltä poistuttaessa.

Työmaatoimiston lukitus

Työmaatoimiston ulko-oviin asennetaan käyttölukot, jonka avainten kopiointi on estetty patenttisuojalla. [5, s. 21.]

Työmaatoimiston avaimia luovutetaan vain niille henkilöille, joilla on hälytysjärjestelmän käyttökoodit.

ST-aineiston säilytys

Ilman hälytysjärjestelmää säilytykseen käytetään kassakaappia. Kun tilat suojataan murtohälytysjärjestelmällä, ST-IV-tason aineistoa voidaan säilyttää lukituissa kaapeissa. [2, s. 39 kohta 19.]

Säilytysyksikkönä käytettävän lukittavan kaapin hankinnassa täytyy huomioida, että siihen täytyy jäädä murtautumisesta jälki. [5, s. 23.]

4.4.3 Korjattavan rakennuskohteen suojaus

Yleensä korjattavan rakennuskohteen suojaamisessa riittää tavanomaiset omaisuusrikollisuuden torjumiseksi tehtävät työmaan turvallisuusjärjestelyt.

Hälytysjärjestelmä

Kohde suojataan Tason 2 murtohälytysjärjestelmällä. Suojaus toteutetaan rakennuksen pohjakerrokseen sijoitettavilla liiketunnistimilla. Mikäli rakennus on useampikerroksinen, liiketunnistin sijoitetaan porrashuoneen yhteyteen.

Lukitus

Korjattavan rakennuskohteen käyntiovet sarjoitetaan työnaikaiseen sarjaan. Kulku estetään niistä ovista, jotka eivät ole työmaan aikana päivittäisinä käyntiovinä. Toimenpiteet tehdään työturvallisuutta vaarantamatta, niin että poistumistiet toimivat.

4.4.4 Korotetun turvallisuustason työmaatilat

Vaikka tutkimuksen tarkastelu on rajattu suojaustason IV asiakirjojen vaatimukseen, esitelen tässä pääkohdat ST III tietoaaineiston aiheuttamista vaatimuksista.

Seinät, lattia ja katto

Turva-aluetta rajaavien rakenteiden tulee antaa rakenteellisen suoja, niin että alueelle tunkeutuminen on hidasta ja vaikeaa. [5, s. 19.]

Rakenteellisen murtosuojauksen viranomaisvaatimukset eivät ole julkista tietoa, mutta FK:n korkeimman turvatason ohje, *Rakenteellisen murtosuojaus III*, määrää vahvistamaan kevytrakenteiset seinät molemmin puolin 1,0mm metallilevyllä. [14, s. 5.]

Ovet

Turva-alueen oven täytyy olla tyyppihyväksytty luokan 3 murtosuojaoivi. [2, s. 38.]

Lukitus ja kulunvalvonta

Turva-alueen rajalla ovissa tulee olla käyttölukon lisäksi varmuuslukko ja kulunvalvonta. [2, s.41.]

Ikkunat

Alle 4 metrin korkeudella Ikkunoissa tulee olla luokan P6B murtosuojalasisitus kiinnitettyinä murtautumisyrityksen kestävään karmiin ja ikkunat eivät saa olla avattavissa. [2, s.38.]

Säilytysyksikkö

Salassa pidettävä tietoaaineisto on säilytettävä kassakaapissa.

Voidaan todeta, että tietoaaineiston suojaustason nostaminen yhdellä pykälällä aiheuttaa huomattavia kustannuksia, mikäli työmaalle joudutaan rakentamaan vaatimusten mukaiset tilat ja suojausjärjestelmät.

Tästä syystä suunnitelmien luokittelu oikealle suojaustasolle on äärimmäisen tärkeää.

4.5 Tietoturvallisuusauditointi

Tilaaajaorganisaation suorittama tietoturvallisuusauditointi on edellytys sille, että työmaatoiminta pystytään aloittamaan täysimääräisenä. Hyväksytyn auditointituloksen jälkeen työmaalla voidaan käsitellä ja säilyttää myös turvallisuusluokiteltua tietoaineistoa. [16, s.31.]

Auditointiajankohta suunnitellaan työmaan perustamisaikataulussa.

Tietoturvallisuusauditointiin valmistaudutaan noudattaen samoja periaatteita kuin rakennuskohteen luovutukseen valmistauduttaessa. Turvallisuusjärjestelyiden toteutus tarkastetaan ensi itse. Tilaaajaorganisaatiolta pyydetään auditointia vasta sitten kun ollaan itse vakuutettu siitä, että järjestelyt täyttävät vaatimukset.

Liitteessä 4 on tarkastusluettelo tietoturvaluustason arvioimiseksi. Luettelo perustuu VAHTI:n Toimitilaohjeen liitteessä 1 esitettyyn pisteytysmalliin ja Excel-tiedosto laskee syötettyjen tietojen perusteella tarkastuksen tuloksen automaattisesti.

5 Johtopäätökset

Opinnäytetyö ja sen tuloksena syntynyt ohje työmaan tietoturvallisuuden toteuttamisesta on tietääkseni ensimmäinen rakennusliikkeen näkökulmasta laadittu katsaus aihepiiriin. Työn aikana vahvistui ennako-oletus aihepiirin arkaluonteisuuden aiheuttamista hankaluuksista, esimerkiksi lähdeaineiston suhteen. Sinänsä lähdeaineistoa löytyi enemmän kuin olin odottanut, mutta tietoaineisto oli odotetusti yleisluontoista ja teoreettista. Konkreettisia ja mitattavissa olevia vaatimuksia löytyi hyvin vähän. Pääasiassa tietoturvallisuustoimenpiteiden vaatimustaso on julkisesti saatavissa asiakirjoissa muodossa ”riittävästi”, ”asianmukaisesti”, ”tarvittaessa” ja niin edelleen.

On ymmärrettävää, että kun käsiteltävä aihe on salassa pidettävän tiedon suojaamistoimenpiteet, niin konkreettisia toimenpiteitä ei voi esittää julkisessa aineistossa. Samasta syystä myös tämän opinnäytetyökirjan tarkkuustasoa päätettiin rajoittaa ja koko opinnäytetyö toteuttaa yleisellä tasolla sitomatta mihinkään erityiseen hankkeeseen. Lukijalle lienee kuitenkin selvää, että työ liittyy läheisesti toimeksiantajayrityksen alka-vaan tai käynnissä olevaan kohteeseen.

Rajan veto yleisen ja yksittäisen tason välillä sekä salassa pidettävän kohdekohtaisen tiedon ja opinnäytetyöhön sisällytettävän julkisen tiedon välillä aiheutti jonkin verran hankaluuksia tutkimuksen toteutukseen. Aikataulusyistä päätös aiheen rajaamisesta oli kuitenkin ehdottoman välttämätön, jotta pystyttiin välttämään ylimääräiset ja aikaa vievät hyväksyttämisprosessit.

Tietoturvallisuussuunnittelu on huomioitava aivan alusta alkaen työmaan tuotannon suunnittelussa, (aluesuunnitelma ja tarkentavat osasuunnitelmat) niin että työmaalle saadaan luotua toimiva tietoturvallisuuskulttuuri ja tietoisuus potentiaalisista ongelmista. Asiaa ei pidä jättää irralliseksi ”myöhemmin tehtäväksi” erilliseksi tehtäväksi. Mallia tähän voidaan ottaa työturvallisuussuunnittelusta, joka on viime vuosina ainakin NCC:llä integroitu kiinteäksi osaksi työmaatoimintaa.

Salassa pidettävä tieto rakennushankkeessa aiheuttaa työmaatoteutukseen aina tietyt perustason vaatimukset joiden täyttämiseen opinnäytetyössä muodostettiin toimintaohjeet. Turvallisuusvaatimuksista johtuvat hankekohtaiset toimenpiteet kannattaa aina käydä läpi tilaajan turvallisuusorganisaation kanssa hyvissä ajoin. Näin saadaan selvil-

le hankekohtaiset poikkeukset ja erityispiirteet. Lisäksi menettelyllä rakennetaan luot-
tamusta tilaajan suuntaan.

Opinnäytetyön tuloksista voidaan tehdä myös johtopäätös, että turvallisuusvaatimukset
aiheuttavat selkeitä lisäkustannuksia rakennushankkeelle. Pelkästään henkilö- ja asia-
kirjahallinnan toteuttamiseen tarvitaan ylimääräisiä henkilöresursseja pienessäkin
hankkeessa.

Turvallisuusluokitellun tiedon vaikutuksia ei ole tutkittu rakennusliikkeen näkökulmasta,
vaikka tarvetta mielestäni olisi. Tämä opinnäytetyö on yleiskatsaus rakennusliikkeen
näkökulmasta. Jatkotutkimuksena voisi tehdä tarkempaa tarkastelua turvallisuusluoki-
tellun hankkeen henkilöstö- ja asiakirjahallinnasta.

Lähteet

- [1] SFS-EN ISO/IEC 27000:2017, Tietoturvallisuuden hallintajärjestelmät. Yleiskäyttö ja sanasto
- [2] Valtionhallinnon tietoturvallisuuden johtoryhmä (2013): *VAHTI 2/2013 Toimitilojen tietoturvaohje*, Valtiovarainministeriö, Juvenes Print - Suomen Yliopistopaino Oy, 141 s. ISBN 978-952-251-460-8, Verkkojulkaisu saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10229, Haettu 10.9.2018
- [3] Valtionhallinnon tietoturvallisuuden johtoryhmä, (2008): *VAHTI 9/2008 Hankkeen tietoturvaohje*, Valtiovarainministeriö, Juvenes Print - Suomen Yliopistopaino Oy, 73 s. ISBN 978-951-804-896-4, Verkkojulkaisu saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=8eaa14ba-bbc3-4775-a6f6-fe413af35c56&groupId=10229, Haettu 10.9.2018
- [4] Oikeusministeriö (2017): *Rikollista tekoa koskevien tietojen arvioinnista turvallisuusselvitysmenettelyssä*, Saatavissa: <http://urn.fi/URN:ISBN:978-952-259-578-2>, Haettu 10.9.2018
- [5] Puolustusministeriö (2015): *Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille*, saatavissa: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf, Haettu 10.9.2018
- [6] Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621 (julkisuuslaki), <https://www.finlex.fi/fi/laki/ajantasa/1999/19990621>
- [7] Turvallisuusselvityslaki 726/2014, <https://www.finlex.fi/fi/laki/ajantasa/2014/20140726>
- [8] Valtioneuvoston asetus tietoturvallisuudesta valtioneuvostossa 1.7.2010/681, <https://www.finlex.fi/fi/laki/ajantasa/2010/20100681>
- [9] Turvallisuusselvitys on ennaltaehkäisevää turvallisuustyötä, Suojelupoliisi, <http://www.supo.fi/turvallisuusselvitykset/henkiloturvallisuusselvitys>, Luettu 9.9.2018.
- [10] Usein kysytyjä kysymyksiä turvallisuusselvityksistä, Suojelupoliisi, https://www.supo.fi/turvallisuusselvitykset/henkiloturvallisuusselvitys/usein_kysytyja, Luettu 8.10.2018.
- [11] Valtionhallinnon tietoturvallisuuden johtoryhmä, (2010): *VAHTI 2/2010 Ohje tietoturvallisuudesta valtioneuvostossa annetun asetuksen täytäntöönpanosta*, Verkkojulkaisu saatavissa:

https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229, haettu 17.10.2018

- [12] Finanssiala ry (2017), Rakennustyömaiden rikostorjunta, Verkkojulkaisu saatavissa: <http://www.finanssiala.fi/vahingontorjunta/dokumentit/Rakennusrikosturvallisuus.pdf>, haettu 15.10.2018
- [13] Finanssiala ry (2017), Murtohälytysjärjestelmät ja -palvelut, Verkkojulkaisu saatavissa: http://www.finanssiala.fi/vahingontorjunta/dokumentit/Murtohalutysjarjestelmat_ja_palvelut_ohje.pdf, haettu 15.10.2018
- [14] Finanssiala ry (2017), Rakenteellinen murtosuojaus III, Verkkojulkaisu saatavissa: <http://www.finanssiala.fi/vahingontorjunta/dokumentit/Rakenteellinen%20murtosuojaus%20III.pdf>, haettu 9.11.2018
- [15] Digitaalisen turvallisuuden palvelut julkishallinnolle, Väestörekisterikeskus, <https://vrk.fi/digiturva>, luettu 9.11.2018
- [16] Saulio, Lauri (2012), *Turvallisuus puolustusvoimien turvaluokiteltua tietoa sisältävissä rakennushankkeissa*. tutkielma, esiupseerikurssi, sotatekniikka, Maanpuolustuskorkeakoulu, Saatavissa: <http://urn.fi/URN:NBN:fi-fe201206186042>, Haettu 15.9.2018
- [17] Senaatti kiinteistöt, *Senaatin palveluntoimittajien turvallisuuskoulutus*, interaktiivinen verkkokoulutus, Saatavissa: <https://senaatti.mmq.fi/>, Haettu 11.11.2018

Työmaaperehdytyksen tietoturvallisuusaineisto

Salassa pidettävät ja turvallisuusluokitellut asiakirjat tunnistetaan suojaustasoa osoittavasta leimasta.



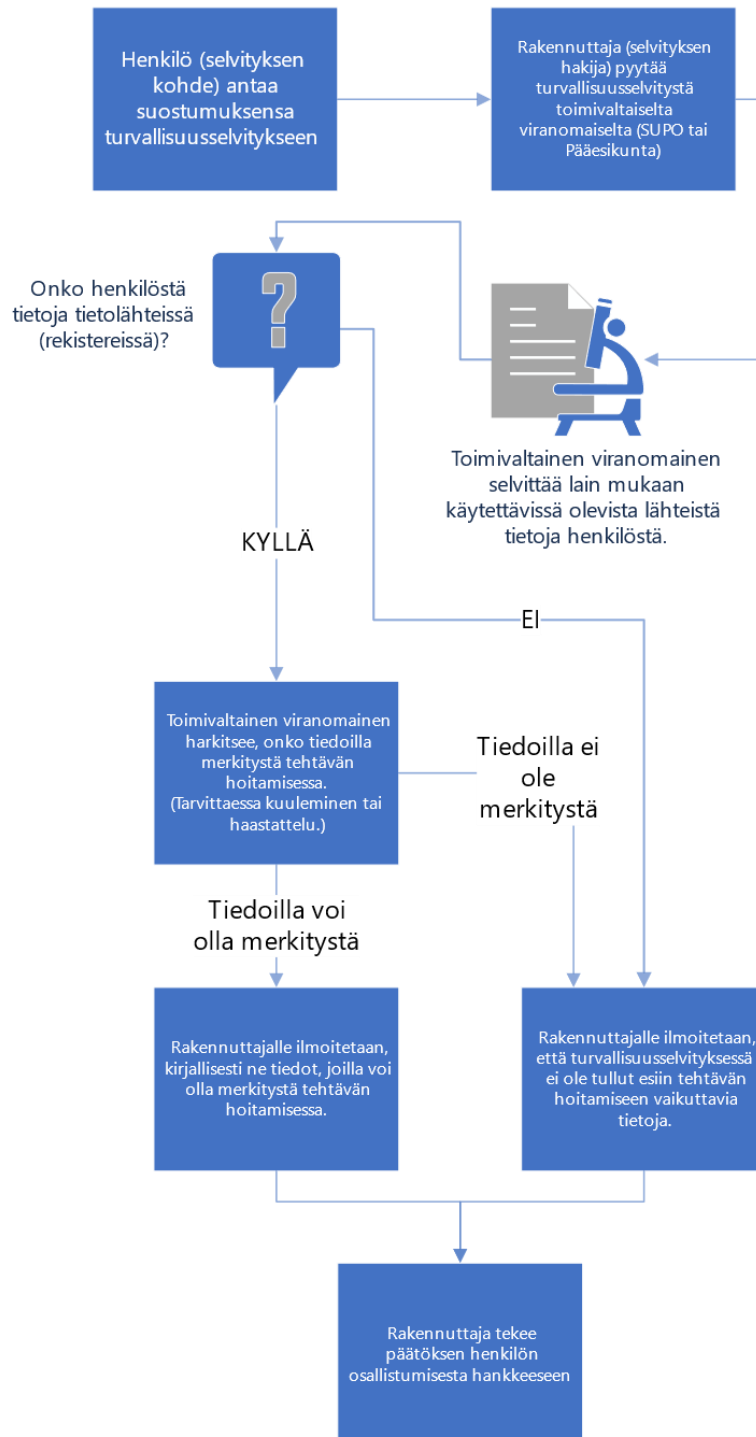
Turvallisuusluokiteltuja asiakirjoja ei saa viedä ilman lupaa työmaa-alueen ulkopuolelle.

Asiakirjat säilytetään työmaalla NCC:n työnjohton osoittamassa paikassa.

Myös työmaa-alueella havainnoimalla saadut tiedot ovat salassa pidettäviä asioita.

Työmaa-alueen ulkopuolella (esimerkiksi lounasravintolassa) ei saa keskustella salassa pidettävistä asioista.

Salassapito- ja vaitiolovelvollisuuden rikkominen muodostaa pahimmassa tapauksessa rikokseksi katsottavan teon.



Turvallisuusselvityksen prosessikaavio [4, s.17]

Kohde: Esimerkkihanke
 Tarkastettava tila: Työmaatoimistotilat
 Tilan / vyöhykkeen turvallisuustaso: Perustaso, ST IV (vihreä)
 Arvion laatija: Heikki Partanen, NCC Suomi Oy
 Pisteytysmallin tulos (keskiarvo, osat A-D): 2,00
 Johtopäätös: Tilaturvallisuus täyttää KORKEAN riskitason toimintaympäristön vaatimukset.

Alue	#	Arvioitava osa-alue	VAATIMUS	Vaatimusten mukaisuus	Piste
A	1	Pysäköintipaikat	Ei vaatimusta		-
A	2	Lastaus/ purkausalueet	Ei vaatimusta		-
A	3	Aidat*	Ei vaatimusta	Täyttää vaatimukset	2
A	4	Portit	Ei vaatimusta	Täyttää vaatimukset	2
A	5	Ajoesteet*	Ei vaatimusta		-
A	6	Aluevalvonta	Ei vaatimusta		-
B	7	Seinärakenne	Normaalit seinärakenteet	Täyttää vaatimukset	2
B	8	Äänieristys	Äänieristyksen tulee estää asiattomia kuulemasta tilassa käytyjä keskusteluja.	Täyttää vaatimukset	2

Kohde: Esimerkkihanke
 Tarkastettava tila: Työmaatoimistotilat
 Tilan / vyöhykkeen turvallisuustaso: Perustaso, ST IV (vihreä)
 Arvion laatija: Heikki Partanen, NCC Suomi Oy
 Pisteytysmallin tulos (keskiarvo, osat A-D): 2,00
 Johtopäätös: Tilaturvallisuus täyttää KORKEAN riskitason toimintaympäristön vaatimukset.

Alue	#	Arvioitava osa-alue	VAATIMUS	Vaatimusten mukaisuus	Piste
B	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 työ-ympäristössä tulee keskustelut salassa pidettävistä asioista käydä riittävästi äänieristetyssä tilassa.	Täyttää vaatimukset	2
B	10	Hajasäteilyn estäminen	Ei vaatimuksia.		-
B	11	Lattia- ja kattorakenteet*	Normaali katto-, välipohja- ja lattiarakenne.	Täyttää vaatimukset	2
B	12	Ikkunat*	Normaali rakenne. Riskianalyysin tulosten perusteella voidaan alle 4 metrin korkeudessa si-jaitsevien ikkunoiden lasi kalvottaa vähintään SFS-EN 356 P1A murtosuoja-kalvolla*.	Täyttää vaatimukset	2
B	13	Kattoikkunat	Kuten muutkin ikkunat.		-
B	14	Salakatselun estäminen	Huomioitava turvallisuusohjeistuksessa.	Täyttää vaatimukset	2
B	15	Ovet	Normaali ovirakenne.	Täyttää vaatimukset	2

Kohde: Esimerkkihanke
 Tarkastettava tila: Työmaatoimistotilat
 Tilan / vyöhykkeen turvallisuustaso: Perustaso, ST IV (vihreä)
 Arvion laatija: Heikki Partanen, NCC Suomi Oy
 Pisteytysmallin tulos (keskiarvo, osat A-D): 2,00
 Johtopäätös: Tilaturvallisuus täyttää KORKEAN riskitason toimintaympäristön vaatimukset.

Alue	#	Arvioitava osa-alue	VAATIMUS	Vaatimusten mukaisuus	Piste
B	16	Halliovet tai ajoovet, jotka johtavat turvallisuusvyöhykkeen sisään*	Ei vaatimuksia. Äänieristys huomioitava riskitason mukaisesti.		-
B	17	Muut aukot	Oltava lukittavissa.	Täyttää vaatimukset	2
B	18	Hätäpoistumistiet Huom! Lukitus ei saa estää hätäpoistumista	Ei erillisvaatimuksia	Täyttää vaatimukset	2
B	19	Asiakirjan säilytysvaatimukset*	Säilytetään lukitussa paikassa, edellyttäen että tila on valvottu tunkeutumisen ilmaisujärjestelmällä työajan ulkopuolella. Ilman em. järjestelyä säilytys kassakaapissa tai holvissa.	Täyttää vaatimukset	2
B	20	Lukitus* vyöhykkeen rajalla	Käyttölukko* heloineen ja vastalevyineen.	Täyttää vaatimukset	2
B	21	Lukitus vyöhykkeen sisällä	Käyttölukko	Täyttää vaatimukset	2
C	22	Avainten ja kulcutunnisteiden hallinta	Vyöhykkeelle tulee nimetä avainvastuuhenkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulcutunnisteiden kuittauksista ja jakamattomien avainten säilytyksestä.	Täyttää vaatimukset	2

Kohde: Esimerkkihanke
 Tarkastettava tila: Työmaatoimistotilat
 Tilan / vyöhykkeen turvallisuustaso: Perustaso, ST IV (vihreä)
 Arvion laatija: Heikki Partanen, NCC Suomi Oy
 Pisteytysmallin tulos (keskiarvo, osat A-D): 2,00
 Johtopäätös: Tilaturvallisuus täyttää KORKEAN riskitason toimintaympäristön vaatimukset.

Alue	#	Arvioitava osa-alue	VAATIMUS	Vaatimusten mukaisuus	Piste
C	23	Yleisavaimen hallinta	Yleisavainta on säilytettävä turvallisesti vastuuhenkilön hallinnoimana.	Täyttää vaatimukset	2
C	24	Vartiohenkilöstön avainhallinta* 5.3	Ei erillisvaatimuksia	Täyttää vaatimukset	2
C	25	Vieraiden pääsynhallinta 3.1.3	Vieras tunnustetaan ja varustetaan vieraskortilla. Vierailu kirjataan.	Täyttää vaatimukset	2
C	26	Palveluntuottajien henkilöstön hallinta (esim kiinteistön-hoito, -huolto ja siivoushenkilöstö) * 3.1.3	Henkilö tunnustetaan ja varustetaan vieraskortilla. Vierailu kirjataan. Vakiohenkilöstö varustetaan kuvallisella henkilö-kortilla.	Täyttää vaatimukset	2
C	27	LVIS-varmistukset	Toimintavaatimusten mukaisesti.		-
C	28	LVI-automaation etäkäyttö	Ei vaatimuksia.		-
C	29	Hissit	Ei vaatimuksia.		-
D	30	Kulunvalvontajärjestelmä*	Kulunvalvontajärjestelmän käyttöönotosta päätetään riskianalyyysiin perustuen.	Täyttää vaatimukset	2
D	31	Kulunvalvontajärjestelmän hallinnointi	Ei vaatimuksia.	Täyttää vaatimukset	2

Kohde:	Esimerkkihankke
Tarkastettava tila:	Työmaatoimistotilat
Tilan / vyöhykkeen turvallisuustaso:	Perustaso, ST IV (vihreä)
Arvion laatija:	Heikki Partanen, NCC Suomi Oy
Pisteytysmallin tulos (keskiarvo, osat A-D):	2,00
Johtopäätös:	Tilaturvallisuus täyttää KORKEAN riskitason toimintaympäristön vaatimukset.

Alue #	Arvioitava osa-alue	VAATIMUS	Vaatimusten mukaisuus	Piste
D 32	Tunkeutumisen ilmaisjärjestelmä*	Jos tilassa säilytetään suojaustason IV tietoa, tila varustetaan tunkeutumisen ilmaisulla (vähintään FK 2-luokka) tai tieto säilytetään vaatimukset täyttävässä kassakaapissa.	Täyttää vaatimukset	2
D 33	Tunkeutumisen ilmaisjärjestelmän testaus	Turvallisuusdokumentaation mukaisesti		-
D 34	Tunkeutumisen ilmaisjärjestelmän hallinnointi	Turvallisuusdokumentaation mukaisesti		-
D 35	Kameravalvontajärjestelmä	Turvallisuusvyöhykettä tai sitä ympäröivää aluetta valvotaan kameravalvonnalla.	Täyttää vaatimukset	2
D 36	Palvelintilan kameravalvonta	Palvelintilaa tai sitä ympäröivää aluetta voidaan valvoa tallentavalla kameravalvonnalla.		-
D 37	Vartiointi	Mahdollisen vartiointin vasteajan on oltava sellainen, että kiinnijäämisriski on merkittävä.	Täyttää vaatimukset	2