Turvallisuusviranomaisten käsikirja yrityksille

Yrityksiin kohdistuvat tietoturvallisuusvaatimukset turvallisuusluokiteltua tietoa sisältävissä hankinnoissa

31.7.2015

1 Johdanto

Käsikirja on tarkoitettu ohjeistukseksi niille yrityksille, jotka osallistuvat tai suunnittelevat osallistuvansa hankintoihin, joiden yhteydessä yritys saa viranomaisen turvallisuusluokiteltua tietoa. Tällaisiin hankintoihin liittyy yleensä turvallisuusvaatimuksia, joiden avulla viranomainen pyrkii varmistumaan siitä, että turvallisuusluokiteltua tietoa suojataan hankinnan aikana asianmukaisesti.

Käsikirjassa kuvataan kotimaisten ja kansainvälisten hankintojen tyypillisimpiä turvallisuusvaatimuksia. Käsikirja toimii apuna hankintamenettelyn eri vaiheissa sekä käytännön oppaana hankkeen edetessä. Yritykset voivat ottaa käsikirjan ohjeistuksen huomioon myös sisäisessä turvallisuussuunnittelussaan.

Johdantoa seuraavissa luvuissa 2 ja 3 esitetään keskeinen tietoturvallisuutta koskeva lainsäädäntö ja toimivaltaiset turvallisuusviranomaiset. Luvuissa 4 ja 5 kuvataan tietoturvallisuusnäkökulmasta keskeinen hankintalainsäädäntö ja hankintojen tyypilliset tietoturvallisuusvaatimukset. Luvut 6 ja 7 koskevat turvallisuusselvityksiä ja luku 8 vierailulupakäytäntöjä. Luvussa 9 kuvataan yrityksen tyypillisiä turvallisuusvelvoitteita hankintoihin liittyen.

2 Turvallisuusluokitellun tiedon suojaamista koskeva lainsäädäntö

2.1 Julkisuuslaki ja tietoturvallisuusasetus

Viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999), jäljempänä julkisuuslaki, säädetään muun muassa viranomaisen asiakirjojen julkisuudesta ja salassapidosta ja asiakirjojen käsittelyn periaatteista.

Tietoturvallisuusasetuksessa (681/2010) säädetään valtionhallinnon viranomaisia koskevista tietoturvallisuuden yleisistä vaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista käsittelyssä noudatettavista vaatimuksista.

Viranomaisen luovuttaessa salassa pidettäviä asiakirjoja toimeksiantotehtävän hoitamista varten, viranomaisen on ennakolta varmistuttava siitä, että tietojen salassa pidosta ja suojaamisesta huolehditaan asianmukaisesti.

2.2 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) säädetään toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Kansainvälisillä tietoturvallisuusvelvoitteilla tarkoitetaan Suomen tekemän tietoturvallisuussopimuksen (General Security Agreement, GSA) määräyksiä erityissuojattavan tietoaineiston suojaamisesta. Erityissuojattavalla tietoaineistolla tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, joihin toinen valtio tai kansainvälinen järjestö on tietoturvallisuussopimuksen mukaisesti tehnyt turvallisuusluokkaa koskevan merkinnän.

Kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia sovelletaan myös yritykseen ja sen työntekijöihin silloin, kun yritys on sopimuspuolena tai alihankkijana turvallisuusluokitellussa hankkeessa tai osallistuu tällaista sopimusta edeltävään tarjouskilpailuun. Näin ollen erityissuojattavan tietoaineiston suojaamista koskevat velvoitteet sitovat myös yritystä.

2.3 Suomen tekemät tietoturvallisuussopimukset

Suomi on tehnyt tietoturvallisuussopimuksia useiden maiden ja eräiden kansainvälisten järjestöjen kanssa. Tietoturvallisuussopimusten tarkoituksena on suojata sellaista valtioiden tai kansainvälisten järjestöjen turvallisuusluokiteltua tietoa, jota sopimuspuolet vaihtavat suoraan keskenään tai jota vaihdetaan niiden lainkäyttövaltaan kuuluvien julkis- tai yksityisoikeudellisten oikeushenkilöiden tai luonnollisten henkilöiden kesken. Esimerkiksi yrityssalaisuudet tai yrityksen sensitiiviset asiakirjat eivät näin ollen kuulu sopimusten suojan piiriin. Ajantasainen lista voimassa olevista tietoturvallisuussopimuksista löytyy NSA:n sivuilta.

Tietoturvallisuussopimuksessa on määräyksiä turvallisuusluokitellun tiedon suojaamisesta ja käsittelystä, turvallisuusselvityksistä, turvallisuusluokitelluista sopimuksista (*classified contracts*), vierailuista (*visits*) sekä turvallisuusrikkomuksista. Tietoturvallisuussopimus muodostaa perustan kansainvälisille hankinnoille ja sen määräykset koskevat soveltuvin osin myös yrityksiä. Hankintaa koskevissa turvallisuusasiakirjoissa on usein viittaus tietoturvallisuussopimukseen.

Sellaisessa hankinnassa, jossa suomalainen yritys saa pääsyn toisen valtion turvallisuusluokiteltuun tietoon, edellytetään pääsääntöisesti voimassaolevaa tietoturvallisuussopimusta. Turvallisuusluokitellun tiedon suojaamisesta sopiminen Suomen ja vieraan valtion taikka Suomen ja kansainvälisen järjestön välillä edellyttää valtiosopimusta. Kansainväliset turvallisuussopimukset hyväksyy Suomessa eduskunta ja niiden velvoitteet saatetaan voimaan lailla. Prosessi kestää yhdestä kolmeen vuotta. Sopimustarpeesta voi ilmoittaa Ulkoasiainministeriössä toimivalle kansalliselle turvallisuusviranomaiselle (National Security Authority, NSA), joka harkintansa mukaan ryhtyy toimenpiteisiin.

3 Toimivaltaiset viranomaiset

3.1 Kansallinen turvallisuusviranomainen

Suomessa kansallisena turvallisuusviranomaisena (National Security Authority, NSA) toimii ulkoasiainministeriö. NSA:n tehtävänä on erityisesti ohjata ja valvoa, että kansainväliset turvallisuusluokitellut tietoaineistot suojataan ja niitä käsitellään asianmukaisesti sekä viranomaisissa että yrityksissä. NSA myöntää kansainvälisten tietoturvallisuusvelvoitteiden edellyttämät henkilö- ja yritysturvallisuustodistukset. Lisäksi NSA koordinoi määrättyjen turvallisuusviranomaisten toimintaa ja edustaa Suomea kansainvälisissä turvallisuuskomiteoissa ja –työryhmissä sekä johtaa kahden- ja monenvälisten tietoturvallisuussopimusten neuvotteluja. NSA huolehtii myös kansainväliseen turvallisuusluokiteltuun tietoon kohdistuvien tietoturvallisuusrikkomusten selvittämisestä.

3.2 Suojelupoliisi

Suojelupoliisi on turvallisuusselvityslaissa (726/2014) tarkoitettu toimivaltainen viranomainen, jolla on yleinen toimivalta päättää turvallisuusselvitysten tekemisestä. Suojelupoliisi päättää henkilöturvallisuusselvityksen ja yritysturvallisuusselvityksen laatimisesta, ellei tehtävä kuulu Pääesikunnalle.

Suojelupoliisi toimii myös määrättynä turvallisuusviranomaisena (Designated Security Authority, DSA) ja kansallisen turvallisuusviranomaisen asiantuntijana kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa erityisesti henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa.

3.3 Pääesikunta

Pääesikunta päättää yritysturvallisuusselvityksen tekemisestä yrityksestä, jonka on tarkoitus hoitaa puolustusvoimien tehtävää taikka yrityksestä, joka liittyy puolustusvoimien hankintoihin. Pääesikunta päättää henkilöturvallisuusselvityksen tekemisestä silloin, kun selvityksen kohteen on tarkoitus toimia puolustusvoimissa tai hoitaa puolustusvoimien antamaan tehtävää taikka jos turvallisuusselvitys liittyy puolustusvoimien toimintaan tai hankintoihin.

Pääesikunta toimii lisäksi Suojelupoliisin tapaan määrättynä turvallisuusviranomaisena (Designated Security Authority, DSA) kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa.

3.4 Viestintävirasto

Viestintävirasto voi laatia yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.

Viestintävirasto toimii kansallisena tieto- ja tietoliikenneturvallisuudesta vastaavana viranomaisena (National Communications Security Authority, NCSA). NCSA:n tehtäviin kuuluu kansainvälistä turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä (Security Accreditation Authority, SAA). Viestintävirasto toimii kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuutta koskevissa asioissa.

3.5 Puolustusministeriö

Puolustusministeriö toimii määrättynä turvallisuusviranomaisena (Designated Security Authority, DSA) ja osallistuu kansainväliseen yhteistyöhön NSA:n asiantuntijana. Lisäksi puolustusministeriö hyväksyy kansainvälisten hankkeiden turvallisuusasiakirjat ja ohjeistaa niiden laatimisessa hallinnonalallaan.

4 Viranomaisen turvallisuusluokiteltuja tietoja sisältävät hankinnat

4.1 Hankintoja koskeva lainsäädäntö

Hankintoja säädellään kansallisesti hankintalailla (348/2007), erityisalojen hankintalailla (349/2007) sekä lailla julkisista puolustus- ja turvallisuushankinnoista (1531/2011). Viimeksi mainittua lakia sovelletaan silloin, kun hankinnan kohde (tavara, palvelu tai rakennusurakka) on suunniteltu tai sovitettu käytettäväksi puolustus- tai turvallisuustarkoituksiin. Turvallisuushankintojen osalta lisäedellytyksenä on, että hankinnan toteuttamiseksi annetaan, laaditaan tai käsitellään turvallisuusluokiteltuja asiakirjoja. Muissa tapauksissa sovelletaan kahta ensiksi mainittua lakia.

Hankintalaki tai erityisalojen hankintalaki ei sisällä erityisiä tietoturvallisuutta koskevia säännöksiä. Myös näihin hankintoihin voi sisältyä salassa pidettävää tietoa, jonka suojaamiseksi hankinnassa hankintayksikkö asettaa erityisiä vaatimuksia. Näistä vaatimuksista hankintayksikön on ilmoitettava hankinta-asiakirjoissa (tarjouspyyntö). Valtioneuvoston asetuksessa julkisista hankinnoista (614/2007) on eräitä tietoturvallisuuteen liittyviä säännöksiä.

Tietyt hankinnat on suljettu pois edellä mainituista laeista. Tämän ohjeen kannalta oleellisia ovat erityisesti säännökset[1], joiden mukaan lakia ei sovelleta hankintoihin, jotka ovat salassa pidettäviä tai joiden toteuttaminen edellyttää erityisiä lakiin perustuvia turvatoimenpiteitä.

Julkisia hankintoja koskeva lainsäädäntö mukaan lukien puolustus- ja turvallisuushankinnoista annettu laki lähtee tarjouskilpailun avoimuuden ja syrjimättömyyden vaatimuksista, joista poikkeamiselle on osoitettava lainsäädäntöön perustuva syy. Tietojen salassapitoon, tietoturvaan ja valtion turvallisuusetuihin liittyvät näkökohdat on listattu lainsäädännössä tietyin edellytyksin perustelluiksi poikkeuksiksi avoimuuden vaatimuksesta. Hankintayksiköt voivat usein varmistaa tietoturvallisuuden riittävän tason asettamalla tätä koskevia erityisvaatimuksia joko tarjouskilpailun aikana tai hankinnan sopimuskaudella. Mikäli tietojen salassapitoa, tietoturvaa tai valtion turvallisuusetuja koskevat vaatimukset ovat erityisen korkealla tasolla, ei avoimeen viestintään perustuvaa tarjouskilpailua voida lainkaan järjestää, jolloin hankintalainsäädännön nojalla voidaan poikkeuksellisesti jättää soveltamatta puolustus- ja turvallisuushankintalain säännöksiä.

[1] Hankintalain 7 § ja erityisalojen hankintalain 17 §.

Julkiset puolustus- ja turvallisuushankinnat

Yritysturvallisuuden ja salassa pidettävyyden näkökulmasta erityisen merkittävä on 1.1.2012 voimaan tullut laki julkisista puolustus- ja turvallisuushankinnoista (1531/2011). Laissa säädetään niistä menettelyistä, joita tulee noudattaa, kun hankitaan tavaroita, palveluja tai rakennusurakoita puolustus- tai turvallisuustarkoituksiin[2].

Puolustus- ja turvallisuushankintalaissa on huomioitu puolustus- ja turvallisuussektorin erityispiirteet. Yksi näistä on ko. sektorin hankintoihin usein olennaisesti liittyvät tietoturvallisuutta koskevat vaatimukset. Tietoturvallisuutta koskevilla vaatimuksilla hankintayksikkö voi pyrkiä varmistamaan, että hankintaan liittyvät turvallisuusluokitellut asiakirjat ja tiedot saavat riittävän suojan asiattomia ulkopuolisia vastaan. Käytännössä tämä tarkoittaa, että hankintayksikkö asettaa ehdokkaalle tai tarjoajalle – ja tarvittaessa myös tämän käyttämälle alihankkijalle – sellaisia tietojen salassa pitoon liittyviä vaatimuksia, joiden se katsoo olevan tarkoituksenmukaisia ja/tai välttämättömiä hankinnan toteuttamisessa.

Puolustus- ja turvallisuushankintalaissa pääsääntöisinä hankintamenettelyinä ovat rajoitettu menettely sekä neuvottelumenettely. Lisäksi hankintayksikön on mahdollista toteuttaa hankinta kilpailullisessa neuvottelumenettelyssä tai suorahankintana laissa määriteltyjen edellytysten täyttyessä. Suorahankinnan käyttöperusteet on rajattu pitkälti siviilihankintoja vastaaviksi kuitenkin siten, että puolustus- ja turvallisuussektorin hankintoihin liittyvät erityispiirteet on huomioitu.

Puolustus- ja turvallisuushankintalain 7 ja 8 §:ssä säädetään niistä hankinnoista, jotka ovat poissuljettuja lain soveltamisalasta. Lakia ei sovelleta hankintoihin, joissa lain soveltaminen velvoittaisi hankintayksikköä toimittamaan sellaisia tietoja, joiden julkistaminen olisi vastoin valtion keskeisiä turvallisuusetuja. Edellä mainitulla perusteella lain soveltamisalan ulkopuolelle jäävät salassa pidettävät hankinnat. Tällaisesta on kyse, kun koko hankinnan olemassaolo on salassa pidettävää tietoa.

Lakia ei myöskään sovelleta seuraavissa tapauksissa:

- tiedusteluun liittyvät hankinnat
- viranomaisten väliset hankinnat
- kansainvälisten menettelysääntöjen nojalla tehtävät hankinnat
- laissa määritellyin edellytyksin tutkimukseen ja kehitykseen liittyvät hankinnat
- eräät muut lain 7 ja 8 §:ssä määritetyt hankinnat

Puolustus- ja turvallisuushankintalaissa tietoturvallisuutta koskevat vaatimukset voivat koskea joko jo hankintakilpailun aikaa tai vasta sopimuksen täytäntöönpanoa[3]. Käytännössä hankintakilpailuun osallistuva yritys voi kohdata tietojen suojaamista koskevan vaatimuksen jo hankintailmoituksessa, jossa ilmoitetaan, mitä edellytyksiä

[2] Lain soveltamisala, ks. 5 §.
[3] Hankintakilpailun aikaiset vaatimukset ks. 54 §, sopimuksen täytäntöönpanon aikaiset vaatimukset, ks. 41 §.

yrityksen tulee täyttää, jotta se pääsee mukaan varsinaiseen kilpailuun ja saa esimerkiksi rajoitetussa menettelyssä tarjouspyynnön.

Hankintayksikön tietoturvallisuutta koskevia vaatimuksia ei määritellä laissa erikseen. Nämä vaatimukset voivat liittyä esimerkiksi turvallisuusluokiteltujen tietojen käsittelyyn, säilyttämiseen, tuhoamiseen sekä luovuttamiseen. Vaatimuksia voidaan myös asettaa niiden tilojen turvajärjestelyille, joissa turvallisuusluokiteltuja tietoja käsitellään tai säilytetään. Hankintayksikkö voi lisäksi vaatia, että kyseiset asiakirjat ja tieto on turvattava sekä koko hankintasopimuksen voimassaoloaikana, mutta myös sen jälkeen.

Tietoturvallisuutta koskevien vaatimusten tulee koskea lähtökohtaisesti yhtä lailla kaikkia potentiaalisia tarjoajia. Kansallisuuteen perustuva syrjintä ei ole sallittua, vaan esimerkiksi mahdolliset tiloihin kohdistuvat turvallisuusvaatimukset tulee asettaa yhtä lailla suomalaisille kuin ulkomaisille yrityksille. Samalla tapaa hankintayksikön tulee vaatimuksia asettaessaan ottaa huomioon hankinnan luonne ja koko ja noudattaa vaatimusten asetannassa suhteellisuusperiaatetta.

4.2 Hankintojen erityispiirteitä

4.2.1 Puolustusvoimien hankinnat

Puolustusvoimat on valtion virastona saman hankintasääntelyn piirissä kuin muutkin virastot. Johtuen puolustusvoimien tehtävistä ja toiminnan luonteesta, sen tekemät hankinnat, erityisesti puolustusmateriaalihankinnat, ovat muita virastoja useammin luvussa 4.1 kuvatun, julkisista puolustus- ja turvallisuushankinnoista säätävän lain (1531/2011) alaisia, tai salassa pidettäviä. Ulkomailta tehtävissä puolustusmateriaalihankinnoissa salassapidon menettelyjä sääntelevät yleensä aina myös toimittajan asettamat ehdot.

4.2.2 EU:n hankkeet ja hankinnat

Suomen julkisia hankintoja koskeva lainsäädäntö ei sovellu EU:n omiin hankintoihin. EU:n toimielinten hankintoihin sovelletaan neuvoston asetusta N:o 1605/2002 Euroopan yhteisöjen yleiseen talousarvioon sovellettavasta varainhoitoasetuksesta.

EU:n neuvoston turvallisuussäännöt[4] luovat perustan EU:n turvallisuusluokitellun tiedon suojaamiseksi. Lisäksi komissiolla, parlamentilla ja Euroopan ulkosuhdehallinnolla on omat neuvoston turvallisuussääntöjä vastaavat turvallisuussääntönsä. Neuvoston turvallisuussäännöissä on yritysturvallisuutta koskeva osio, jossa asetettuja vähimmäisvaatimuksia noudatetaan EU:n hankinnoissa silloin, kun hankinnan yhteydessä

[4] Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi „neuvoston turvallisuussäännöt“ (2013/488/EU).

käsitellään EU:n turvallisuusluokiteltua tietoa. Valmisteilla on myös ohjeasiakirja, jossa on tarkempia suosituksia yritysturvallisuuteen liittyen.

Suomessa ja EU:ssa sovellettavien turvallisuusluokkamerkintöjen vastaavuudet sekä turvallisuusluokkia vastaavat yleiset suojausvaatimukset on esitetty NSA:n ohjeessa ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”.

4.2.3 Horizon 2020

EU rahoittaa tutkimushankkeita Horizon 2020 -ohjelman puitteissa. Pääsääntöisesti vain turvallisuustutkimusta koskevat hanke-esitykset läpikäyvät erityisen turvallisuustarkastelun (Security Scrutiny). Tässä tarkastelussa jäsenvaltioiden turvallisuusviranomaiset käyvät läpi hanke-esitykset siitä näkökulmasta, käsitelläänkö tai tuotetaanko niissä EU:n turvallisuusluokiteltua tietoa (EUCI). Jäsenvaltioiden tekemän yhteisen arvion pohjalta Euroopan komissio päättää hyväksyttyjen hanke-esitysten turvallisuusluokituksen. Mikäli tutkimushankkeelle on määrätty turvallisuusluokka, tiedon suojaamisen osalta noudatetaan vuonna 2015 voimaan tulleita komission turvallisuussääntöjä sekä jäsenvaltioiden säädöksiä.

4.2.4 European Global Navigation Satellite Systems (GNSS)

Suomi osallistuu osaltaan GNSS:ään, jonka näkyvin osa tulee olemaan Galileo-satelliittipaikannusjärjestelmä. Galileoon liittyvän turvallisuusluokitellun tiedon suojaamisessa noudatetaan komission turvallisuussääntöjä ja jäsenvaltioiden kansallista lainsäädäntöä. Hankkeen toteutusvaihetta koskevat tarkentavat turvallisuusluokitellun tiedon suojaamismääräykset on kirjattu hanketurvallisuusohjeeseen (European GNSS PSI = Programme Security Instructions), joka on laadittu yhteistyössä komission, jäsenvaltion turvallisuusviranomaisten (NSA, DSA), EU:n neuvoston ja ESA:n edustajien kesken. Asiakirjaa ylläpitää komissio.

4.2.5 Euroopan puolustusviraston (EDA) hankinnat

Euroopan puolustusviraston (EDA) puitteissa toteutetaan tutkimukseen ja kehittämiseen liittyviä projekteja ja ohjelmia. Näihin liittyy usein hankintoja, joita voivat toteuttaa joko projektiin osallistuvat tai muut yritykset. Näiden hankintojen toteuttamiseen voi sisältyä turvallisuusluokiteltua tietoa, jonka suojaamista koskevat vaatimukset ja määräykset sisältyvät projektisopimukseen tmv. projektin toteuttamista määrittävään asiakirjaan.[5]

[5] Turvallisuusvaatimuksista tarkemmin asiakirjassa “ EDA General Provisions applicable to Ad Hoc Research & Technology Projects and Programmes of the European Defence Agency approved in the Steering Board Decision 2010 No 2010-19”.

4.2.6 Naton hankinnat

Suomi on kumppanimaana tehnyt kahdenvälisen tietoturvallisuussopimuksen Naton kanssa (SopS 7/2013 ja 8/2013). Sopimuksessa on määräykset turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta.

Naton voimassa olevaa turvallisuussäännöstöä[6] ylläpitää Naton turvallisuustoimisto (Nato Office of Security, NOS). Sääntömuutokset hyväksytään sotilaskomiteassa, jossa kaikki jäsenmaat ovat edustettuina. Yritysturvallisuutta ja hankintoja koskee yritysturvallisuusdirektiivi (Industrial Security Directive), jossa on otettu huomioon myös ei-jäsenmaiden mahdollisuus osallistua Naton hankintoihin.

Suomessa ja Natossa sovellettavien turvallisuusluokitusmerkintöjen vastaavuudet sekä turvallisuusluokkia vastaavat yleiset suojausvaatimukset on esitetty Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeessa.

4.2.7 Euroopan Avaruusjärjestön (ESA) hankkeet

Euroopan avaruusjärjestön turvallisuusluokitellun tiedon suojaamisessa noudatetaan ESA:n turvallisuusmääräyksiä (minimivaatimukset) sekä jäsenvaltioiden lainsäädäntöä. Hankkeita koskevat tarkentavat määräykset on kirjattu geneeriseen hanketurvallisuusohjeeseen (ESA Generic PSI), jonka pohjalta laaditaan kulloinkin hankekohtainen turvallisuusohje (Program Specific PSI). Geneerinen PSI on laadittu ESA:n turvallisuustoimiston ja jäsenvaltioiden turvallisuusviranomaisten (NSA, DSA) kesken ja sen hyväksyy ESA:n neuvosto turvallisuuskomitean esityksestä. ESA:n turvallisuuskomitea puolestaan hyväksyy hankekohtaiset PSI:t.

4.2.8 Monenväliset hankkeet

Monenvälisissä hankkeissa on usein tarpeen sovittaa yhteen usean osallistujamaan turvallisuusvaatimukset. Tällöin turvallisuusdokumentaatiosta tulee moniulotteisempi kuin tavanomaisissa hankinnoissa. Turvallisuusliite (yleensä PSI-muotoinen) laaditaan yhteistyössä hankkeeseen osallistuvien jäsenvaltioiden turvallisuusviranomaisten (NSA, DSA) kesken.

[6] Nato Security Policy, NSP (C-M(2002)49).

5 Hankintojen tietoturvallisuusvaatimukset

5.1 Tietoturvallisuusvaatimukset hankintojen eri vaiheissa

Turvallisuusluokiteltua tietoa sisältävä hankinta käynnistyy yleensä siten, että hankintayksikkö ilmoittaa alustavat tiedot hankinnasta. Pääsääntöisesti tämä vaihe ei edellytä turvallisuusluokitellun tiedon luovuttamista mahdollisille tarjoajille.

Seuraavassa vaiheessa hankintayksikkö tekee tarjouspyynnön, josta ilmenee myös hankkeen turvallisuusvaatimukset. Turvallisuusluokitellun tiedon suojaaminen asettaa yritykselle erityisvaatimuksia ja saattaa lisätä hankinnan kustannuksia. Jos tarjouspyyntöasiakirjat sisältävät turvallisuusluokiteltua tietoa, niiden käsittely voi edellyttää käsittelyyn osallistuvan henkilön henkilöturvallisuusselvitystä tai selvityksen perusteella annettavaa henkilöturvallisuusselvitystodistusta (*Personnel Security Clearance Certificate, PSCC*). Mikäli yritys käsittelee turvallisuusluokiteltuja tietoja sisältäviä tarjouspyyntöasiakirjoja tiloissaan, hankintayksikkö voi jo tässä vaiheessa edellyttää myös yrityksestä laadittavaa yritysturvallisuusselvitystä (*Facility Security Clearance, FSC*).

Jos hankinnan turvallisuusvaatimuksissa edellytetään yritysturvallisuusselvitystä, yritysturvallisuusselvitys käynnistetään viimeistään siinä vaiheessa, kun yrityksen osallistuminen turvallisuusluokiteltua tietoa sisältävään hankintaan on varmistunut. Yritysturvallisuusselvityksen hakemisesta ja laatimisesta on tarkemmin luvussa 6.1.

Ennen varsinaisen hankkeen käynnistymistä yritys ja hankintayksikkö tekevät turvallisuusluokiteltua tietoa sisältävää hankintaa koskevan sopimuksen (*Classified Contract*), joka sisältää hankekohtaiset turvallisuusvaatimukset ja -asiakirjat.

5.2 Kansainvälisten hankintojen turvallisuusasiakirjat

Mikäli kansainvälisen hankinnan turvallisuusvaatimukset ovat monitahoiset, hanketta varten laaditaan yleensä kattava hanketurvallisuusohje (*Programme Security Instructions, PSI*). Vaihtoehtoisesti tai PSI:tä täydentävästi voidaan laatia turvallisuutta koskeva lisälauseke (*Security Aspect Letter, SAL*). SAL on yleensä PSI:tä suppeampi asiakirja ja sitä käytetään usein tarjouspyyntövaiheessa. Turvallisuusdokumentaatio sisältää yleensä myös turvallisuusluokitteluohjeen (*Security Classification Guide, SCG*).

5.2.1 Programme Security Instructions (PSI)

Programme Security Instructions eli PSI on kattava hankkeen turvallisuusohje.

Sen tarkoituksena on:

- koota yhteen hankkeen turvallisuusmääräykset
- antaa tarkentavia soveltamisohjeita
- sovittaa yhteen kansalliset eroavaisuudet
- jakaa vastuut turvallisuusvaatimusten toteuttamiseksi
- toimia ohjenuorana ja muistin tukena hankkeen aikana.

Se sisältää yleensä vastaukset seuraaviin kysymyksiin:

- mitkä lait ja säädökset sitovat käsittelijää
- miten käsittelijä saa valtuuden käsitellä tietoa
- minkä tasoista salassa pidettävää tietoa hankkeessa käsitellään
- miten tietoa saa ja pitää kullakin suojaustasolla käsitellä, tallentaa ja siirtää fyysisesti ja/tai teknisesti
- mihin käsittelijä saa käyttää saamaansa tietoa
- miten tieto tulee merkitä ja miten merkintöjä tulkitaan käytännössä (vertailutaulukot tms.)
- kenelle tietoa saa tai ei saa toimittaa ja millä ehdoilla
- mikä on tiedon salassapitoaika
- miten tieto tuhotaan tai palautetaan hankkeen päätyttyä.

PSI:n liitteenä on tavallisesti hankkeen turvallisuusluokitteluohje (*Security Classification Guide*), jossa määritetään projektin eri osien tai projektimateriaalin turvallisuusluokat.

5.2.2 Security Aspects Letter (SAL)

SAL eli turvallisuutta koskeva lisälauseke on PSI:tä vastaava mutta suppeampi turvallisuusasiakirja. SAL yksilöi hankkeen turvallisuusvaatimukset tai ne sopimuksen osat, joiden turvallisuus on suojattava. Se vastaa suppeammin samantyyppisiin kysymyksiin kun edellä on esitetty PSI:n osalta. SAL:ia voidaan käyttää, mikäli hankkeeseen kohdistuvat turvallisuusvaatimukset ovat yksinkertaisia tai sillä täydennetään PSI:tä esim. tietyn alihankkijan osalta.

5.2.3 Security Classification Guide (SCG)

Security Classification Guide (SCG) eli turvallisuusluokitteluohje on tärkeä osa PSI:tä tai SAL:ia. Turvallisuusluokitteluohjeessa kuvataan turvallisuusluokitellun hankkeen osa-alueet ja eritellään sovellettavat turvallisuusluokat yksityiskohtaisesti. Turvallisuusluokitteluohjeen avulla hankkeeseen osallistuvat henkilöt tietävät, mihin turvallisuusluokkaan hankkeen prosessi tai yksittäinen materiaalikomponentti kuuluu.

6 Turvallisuusselvitykset

6.1 Yritysturvallisuusselvitys

Mikäli hankinnan turvallisuusvaatimuksissa edellytetään, turvallisuusluokiteltuja tietoja hankinnan yhteydessä saavasta yrityksestä voidaan tehdä yritysturvallisuusselvitys. Pääsääntöisesti yritysturvallisuusselvitystä voidaan edellyttää, jos yritys käsittelee tiloissaan turvallisuusluokiteltuja asiakirjoja tasolla LUOTTAMUKSELLINEN (TL III) tai SALAINEN (TL II). Kansainvälisen turvallisuusluokitellun tiedon osalta vastaavat tasot ovat CONFIDENTIAL ja SECRET. Alimmalla tasolla KÄYTTÖ RAJOITETTU ei yleensä edellytetä yritysturvallisuusselvitystä. Korkeimmalle luokiteltua tietoa (ERITTÄIN SALAINEN/TOP SECRET) ei pääsääntöisesti luovuteta yrityksille. Yritysturvallisuusselvitys laaditaan siten kuin turvallisuusselvityslaissa (726/2014) säädetään.

6.1.1 Yritysturvallisuusselvityksen hakeminen

Kansallisen turvallisuusluokitellun tiedon suojaamiseksi yritysturvallisuusselvitystä voi hakea vain viranomainen. Yritysturvallisuusselvitys voidaan laatia kansallisen tarpeen perusteella, kun viranomainen tekee hankintasopimusta yrityksen kanssa ja sopimuksen yhteydessä yritykselle annetaan turvallisuusluokiteltuja asiakirjoja. Yritysturvallisuusselvityksen laatimisesta turvallisuusselvityksen tekemisestä päättää pääsääntöisesti Suojelupoliisi ja puolustusvoimien hankinnoissa Pääesikunta.

Kansainvälisten tietoturvallisuusvelvoitteiden edellyttämää yritysturvallisuusselvitystä (*Facility Security Clearance, FSC*) voi pyytää:

- **Suomen viranomainen**, jonka on tarkoitus antaa sopimuksen perusteella yritykselle pääsy toisen valtion tai kansainvälisen järjestön turvallisuusluokiteltuun tietoon tasolla CONFIDENTIAL tai korkeampi. Tällöin selvitystä hakeva viranomainen täydentää yritysturvallisuusselvityshakemuslomakkeen ja toimittaa sen NSA:han, joka edellytysten täyttyessä välittää yritysturvallisuusselvityspyynnön edelleen Suojelupoliisiin tai puolustusvoimien hankinnoissa Pääesikuntaan tehtäväksi.

- **Ulkomaan viranomainen**, jonka on tarkoitus tehdä turvallisuusluokiteltu sopimus (classified contract) suomalaisen yrityksen kanssa tasolla CONFIDENTIAL tai korkeampi. Tällöin ulkomaan viranomainen lähettää oman maansa NSA:n kautta FSC:tä koskevan pyynnön Suomen NSA:lle, joka välittää sen Suojelupoliisiin tehtäväksi. Yritystä pyydetään tällöin täyttämään yritysturvallisuusselvityshakemus ja antamaan suostumuksensa yritysturvallisuusselvityksen tekemiseksi.

- **Suomalainen yritys**, jos se osallistuu sellaiseen kansainväliseen tarjouskilpailuun tai hankintaan, joka edellyttää pääsyä toisen valtion tai kansainvälisen

järjestön turvallisuusluokiteltuun tietoon tasolla CONFIDENTIAL tai korkeampi. Tällöin yritys tekee yritysturvallisuusselvityshakemuksen ja toimittaa sen NSA:han, joka edellytysten täyttyessä välittää hakemuksen Suojelupoliisiin.

Yritysturvallisuusselvityksen hakemiseen on määrämuotoinen hakulomake, joka löytyy Suojelupoliisin sivuilta. Pääesikunnan tekemien yritysturvallisuusselvitysten hakemukset tehdään erikseen ohjeistetulla puolustusvoimien sisäisellä menettelyllä ja lomakkeella.

Ulkomaisen yrityksen yritysturvallisuusselvityksen hakemisesta on tarkempaa ohjeistusta luvussa 7.

6.1.2 Yritysturvallisuusselvityksen tekeminen

Yritysturvallisuusselvityksessä voidaan turvallisuusselvityslain 38 §:n mukaisesti selvittää seuraavat asiat:

1) Tietojen suojaaminen oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä
2) Asiattoman pääsyn estäminen tiloihin, joissa tietoja käsitellään tai joissa harjoitetaan muuta selvityksen perusteena olevaa toimintaa
3) Henkilöstön asianmukainen koulutus ja ohjaaminen.

Yllä mainittujen turvallisuustoimenpiteiden toteutumista voidaan selvittää hakemuksessa esitettyjen tietojen ja turvallisuusselvityslain 37 §:ssä tarkoitettujen tietolähteiden avulla sekä yritykseen ja sen toimitiloihin sekä tietojärjestelmiin kohdistuvan tarkastuksen avulla.

Yritysturvallisuusselvitys voidaan tehdä tasolle TL II SALAINEN/SECRET tai TL III LUOTTAMUKSELLINEN/CONFIDENTIAL. KÄYTTÖ RAJOITETTU/RESTRICTED -tasolla yritysturvallisuusselvitystä ei pääsääntöisesti tehdä. Selvitykseen kuuluvissa tarkastuksissa voidaan käyttää auditointityökaluna Katakria. Kansainvälisen tietoturvallisuusvelvoitteen perusteella tehtävässä yritysturvallisuusselvityksessä käytetään auditointityökaluna Katakria.

Yrityksen turvallisuustasoa arvioidessaan viranomainen tarkastaa tavallisesti yrityksen henkilöstö- ja hallinnollisen turvallisuuden sekä tilaturvallisuuden. Myös yrityksen tietojärjestelmien turvallisuus voidaan tarkastaa, mikäli yritys käsittelee turvallisuusluokiteltua tietoa tietojärjestelmissään. Tietojärjestelmiin liittyvät tarkastukset tekee Viestintävirasto. Osana yritysturvallisuusselvitystä voidaan laatia henkilöturvallisuusselvitykset yrityksen vastuuhenkilöistä sekä niistä yrityksen työntekijöistä, jotka käsittelevät turvallisuusluokiteltua tietoa tasolla LUOTTAMUKSELLINEN/CONFIDENTIAL tai korkeampi (ks. luku 6.2)

Yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai se on muutoin yritysturvalli-

suusselvityksen tarkoituksen toteuttamiseksi perusteltua. Jos yritykseltä ei edellytetä kykyä suojata turvallisuusluokiteltua tietoa toimitiloissaan (”FSC without safeguards”), arviointi voi kohdistua pelkästään yrityksen henkilöstö- ja hallinnolliseen turvallisuuteen. Jos yritykseltä edellytetään myös kykyä suojata turvallisuusluokiteltuja tietoja yrityksen toimitiloissa (”FSC with safeguards”), arviointi voidaan kohdistaa lisäksi yrityksen toimitiloihin, sekä tekniseen tietoturvallisuuteen soveltuvin osin. Mikäli turvallisuusluokiteltuja tietoja käsitellään myös tietojärjestelmässä (”including CIS”), voidaan arvioida yrityksen tekninen tietoturvallisuus.

Suojelupoliisin tekemät yritysturvallisuusselvitykset ovat maksullisia poliisin maksuasetuksen (1023/2014) mukaisesti. Ajantasaisen hintatiedon saa Suojelupoliisin internet-sivuilta. (http://www.poliisi.fi/supo/yritysturvallisuusselvitys)

Yritysturvallisuusselvityksen prosessi päättyy yrityksen antamaan sitoumukseen, jossa yritys sitoutuu ylläpitämään vaaditun turvallisuustason. Sitoumuksen perusteella yritykselle voidaan myöntää yritysturvallisuusselvitystodistus (ks. luku 6.1.3)

Liitteen 1 kaaviossa on kuvattu yritysturvallisuusselvityksen vaiheet sekä viranomaisen ja yrityksen tehtävät prosessin aikana.

6.1.3 Yritysturvallisuusselvitystodistus (Facility Security Clearance, FSC)

Yrityksen sitouduttua ylläpitämään vaadittu turvallisuustaso sille voidaan myöntää yritysturvallisuusselvitystodistus. *Kansallisen* velvoitteen perusteella tehtävissä yritysturvallisuusselvityksissä yritysturvallisuusselvitystodistuksen myöntää toimivaltainen viranomainen eli Pääesikunta tai Suojelupoliisi. *Kansainvälisen* velvoitteen perusteella tehtävissä selvityksissä FSC-todistuksen myöntää kansallinen turvallisuusviranomainen.

Sitoumuksen ja sen pohjalta myönnettävän todistuksen voimassaoloaikana yritys on velvollinen ilmoittamaan toimivaltaiselle viranomaiselle mikäli yrityksen omistussuhteissa, hankkeeseen liittyvässä henkilöstössä tai turvallisuusjärjestelyissä tapahtuu muutoksia. Turvallisuusselvityslain (726/2014) mukaan todistus on voimassa toistaiseksi, mutta enintään viisi vuotta todistuksen myöntämisestä. Todistusta voidaan käyttää sen osoittamalla tasolla kaikissa hankinnoissa, joihin yritys osallistuu todistuksen voimassaoloaikana.

Yritysturvallisuusselvitystodistus voidaan peruuttaa, jos sen peruste lakkaa olemasta tai jos yrityksen olosuhteissa tapahtuu sellainen muutos, ettei viranomainen voi uusien olosuhteiden vallitessa katsoa turvallisuutta ja luotettavuutta koskevien kriteerien täyttyvän. Peruuttamisesta aiheutuvat mahdolliset taloudelliset seuraukset kantaa yritys. Todistuksen myöntänyt viranomainen informoi todistusta pyytäneelle taholle sitä koskevista muutoksista. Ennen kuin todistus peruutetaan, toimivaltaisen viranomaisen on kuultava selvityksen kohdetta.

6.2 Henkilöturvallisuusselvitys ja –todistus (Personnel Security Clearance, PSC)

Henkilöstä, joka käsittelee hankinnan yhteydessä turvallisuusluokiteltua tietoa, voidaan hankinnan turvallisuusvaatimuksissa edellyttää henkilöturvallisuusselvitystä. *Kansainvälisen* tietoturvallisuusvelvoitteen mukaista henkilöturvallisuusselvitystodistusta (PSC-todistus) edellytetään pääsääntöisesti vain tilanteessa, jossa henkilö saa pääsyn toisen valtion tai kansainvälisen järjestön turvallisuusluokiteltuun tietoon tasolla CONFIDENTIAL tai korkeampi.

Usein henkilöturvallisuusselvitykset tehdään yritysturvallisuusselvityksen yhteydessä, mutta tietyissä tilanteissa pelkkä henkilöturvallisuusselvitys voi riittää hankintaan osallistumiseen. Tämä koskee erityisesti tilannetta, jossa turvallisuusluokiteltuja tietoja käsitellään pelkästään viranomaisen tiloissa. Lisäksi yritysturvallisuusselvityksen osana yrityksen vastuuhenkilöistä voidaan laatia henkilöturvallisuusselvitykset.

Kansallisen turvallisuusluokitellun tiedon osalta turvallisuusselvitystä hakee pääsääntöisesti se viranomainen, jonka turvallisuusluokitellusta tiedosta on kysymys. Tietyin edellytyksin yritys voi tehdä henkilöturvallisuusselvityksen laatimista koskevan hakemuksen myös itse. Tällöin kysymys on kuitenkin yrityksen oman tiedon suojaamisesta esimerkiksi niiden kansantaloudellisen merkittävyyden takia.[7] Turvallisuusselvitystä haetaan vakiomuotoisella lomakkeella.[8]

Kansainvälisen turvallisuusluokitellun tiedon osalta pyyntö turvallisuusselvityksestä PSC-todistuksen saamiseksi tulee pääsääntöisesti Suomen NSA:lle hankinnasta vastaavalta Suomen viranomaiselta tai ulkomaan viranomaiselta. Tietyin edellytyksin yritys voi itse pyytää NSA:lta turvallisuusselvitystä PSC-todistusta varten.

PSC-todistuksen hakemista varten täytetään PSC-hakemuslomake, joka löytyy täyttöohjeineen NSA:n sivuilta. Lomake on tarkoitettu vain Suomen viranomaisten ja yritysten käyttöön haettaessa Suomen NSA:n myöntämää PSC-todistusta. Lomakkeeseen liitetään turvallisuusselvityshakemus ja muut pyydetyt liitteet (erityisesti hakemuksen peruste) ja hakemus toimitetaan NSA:han. NSA toimittaa turvallisuusselvityshakemuksen edelleen Suojelupoliisille arvioituaan, että turvallisuusselvitykselle on kansainvälisen tietoturvallisuusvelvoitteen mukainen peruste. Puolustusvoimien hankintojen osalta noudatetaan puolustusvoimien ohjeistusta.

Henkilöturvallisuusselvitykset tehdään siten kuin turvallisuusselvityslaissa (726/2014)

[7] Turvallisuusselvityslain 22 §:ssä on säännökset yrityksen eräiden muiden tehtävien hyväksymisestä selvitysmenettelyyn.

[8] http://www.poliisi.fi/poliisi/supo60/home.nsf/files/Perusmuotoinen_turvallisuusselvitys_060801b/$file/Perusmuotoinen_turvallisuusselvitys_060801b.pdf.

säädetään. Henkilöturvallisuusselvityksessä toimivaltainen viranomainen,[9] tarkastaa kohteena olevan henkilön taustatiedot laissa säädetyllä menettelyllä. Henkilöturvallisuusselvityksen tekeminen edellyttää kohteena olevan henkilön kirjallista suostumusta, joka annetaan hakulomakkeessa. Lomakkeessa ilmoitetaan myös henkilön työnkuva ja rooli hankkeessa.

Turvallisuusselvitys voidaan tehdä myös suomalaisen yrityksen palveluksessa olevasta ulkomaalaisesta, mutta tällöin on otettava huomioon, että suomalaisilla viranomaisilla voi olla rajalliset mahdollisuudet henkilön taustan selvittämiseen. Turvallisuusselvityslaissa osoitetaan tyhjentävästi turvallisuusselvityksessä käytettävät rekisterit. Toimivaltaisilla viranomaisilla on lain mukaan mahdollisuus tehdä kysely selvityksen kohteena olevan henkilön rekisteritiedoista myös ulkomaan viranomaisille. Kun turvallisuusselvityksen kohteena on ulkomaalainen tai ulkomailla asuva tai asunut suomalainen, ilmoitetaan turvallisuusselvityksen tuloksen yhteydessä se, miltä ajanjaksolta viranomaisilla on ollut tietoa käytössään.

Tarvittaessa Suomen NSA voi ulkomaan kansalaisen osalta pyytää valtioiden välisen tietoturvallisuussopimuksen perustella turvallisuusselvitystä vastaavaa PSC-todistusta henkilön kotimaan NSA:lta (ks. tarkemmin luku 7).

Henkilöturvallisuusselvityksessä Suojelupoliisi tai Pääesikunta ei ota kantaa selvityksen kohteen soveltuvuuteen tehtäväänsä, vaan arvioi rekistereistä ilmi tulevien tietojen perusteella, mitkä tiedot voivat selvityksen tarkoituksen kannalta olla merkityksellisiä. Tällaiset tiedot ilmoitetaan kirjallisesti hakijalle.

Mikäli selvityksen kohteesta haetaan PSC-todistusta, tiedot ilmoitetaan myös NSA:lle joka harkitsee voidaanko PSC-todistus selvityksessä ilmenneiden tietojen perusteella myöntää. NSA välittää tiedon myönnetystä PSC-todistuksesta hakijalle. PSC-todistus voidaan tietyin edellytyksin peruuttaa.

Selvityksen kohteella on turvallisuusselvityksistä annetun lain mukaan oikeus saada tieto siitä, onko hänestä tehty turvallisuusselvitys tiettyä tehtävää varten sekä oikeus saada pyynnöstään turvallisuusselvityksen hänestä sisältämät tiedot. Tätä tiedonsaantioikeutta voi käyttää sopimalla henkilökohtaisen tapaamisajan Suojelupoliisissa tai Pääesikunnassa. On kuitenkin huomattava, että tiedonsaantioikeutta ei ole, jos tieto on peräisin sellaisesta rekisteristä, johon rekisteröidyllä ei ole tarkastusoikeutta (esimerkiksi Suojelupoliisin toiminnallinen tietojärjestelmä). Tällöin selvityksen kohde voi pyytää tietosuojavaltuutettua tarkastamaan tietonsa Suojelupoliisin toiminnallisesta tietojärjestelmästä.

6.3 Tietojärjestelmien hyväksyntä (akkreditointi)

Viestintävirasto voi laatia yritysturvallisuusselvityksen osana tietojärjestelmien ja tie-

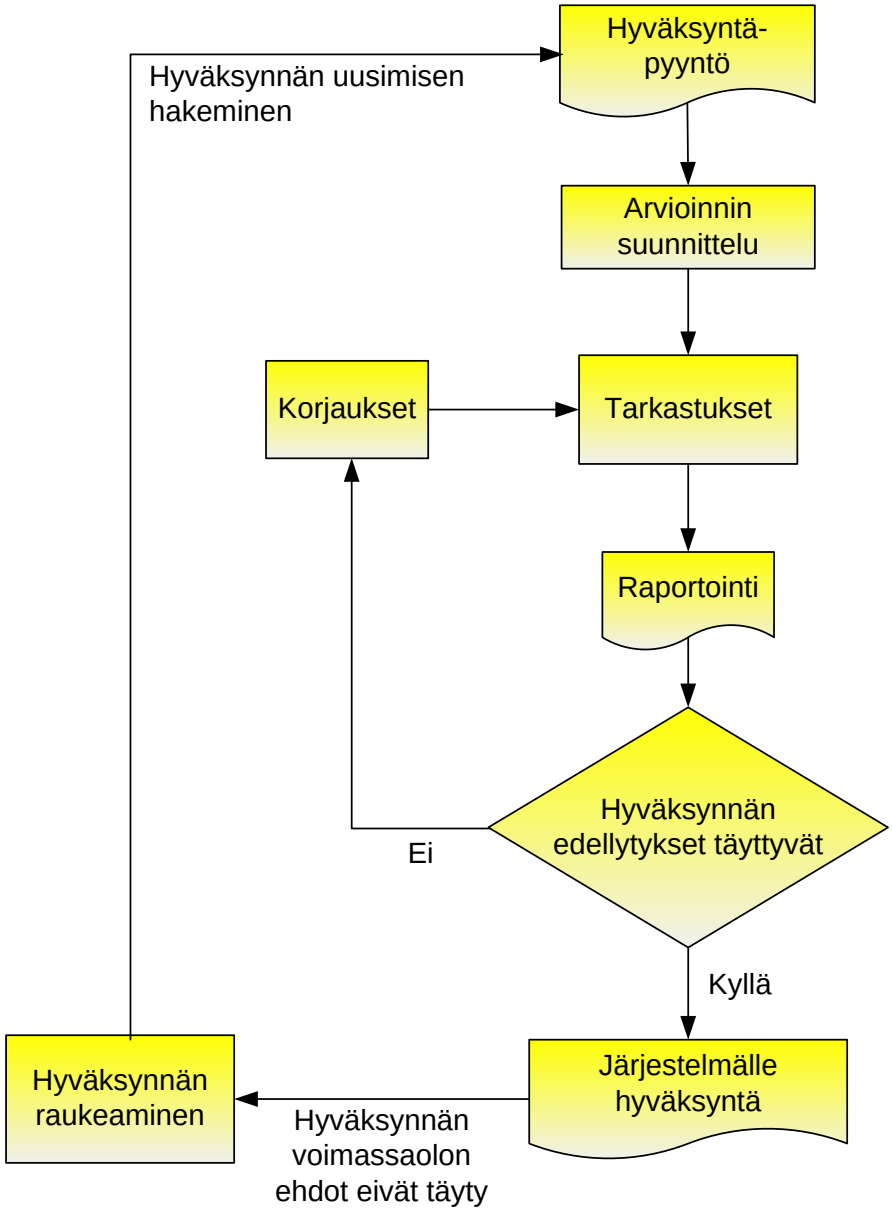
[9] Suppea turvallisuusselvitys: paikallispoliisi, perusmuotoinen tai laaja turvallisuusselvitys: Suojelupoliisi. Puolustusvoimien asioissa aina Pääesikunta.

toliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen. Jos hankintaan liittyvää turvallisuusluokiteltua tietoa käsitellään yrityksen tietojärjestelmässä, on tietojärjestelmä hyväksytettävä hankinnan turvallisuusvaatimuksissa edellytetylle turvallisuustasolle. Hyväksyntä on prosessi, jonka aikana Viestintävirasto määrittää yhdessä tietojärjestelmän omistajan kanssa tietojärjestelmään kohdistuvan riskitason ja hyväksyy sen mukaiset turvallisuusjärjestelyt.

Hyväksyntäprosessissa käytetään auditointityökaluna Katakria. Kansainvälistä luokiteltua hanketta koskevasta sopimuksesta tai muista kansainvälisistä velvoitteista saattaa aiheutua turvallisuusvaatimuksiin tarkentavia määräyksiä.

Hyväksyntäprosessi alkaa, kun Viestintävirastolle toimitetaan hyväksyntäpyyntö. Hyväksyntäprosessin keskeisiä vaiheita ovat arvioinnin suunnittelu, tarkastukset (auditoinnit) sekä raportointi. Mikäli tarkastuksessa havaitaan, että jokin hankkeen turvallisuusvaatimuksista ei täyty, merkitään tämä poikkeamaksi. Havaittujen poikkeamien tulee olla todennetusti korjattuja ennen kuin hyväksyntä voidaan myöntää. Hyväksyntäprosessia on havainnollistettu kuvassa 1. Hyväksyntäprosessi kuvataan yksityiskohtaisemmin ohjeessa "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma"[10].

[10] www.ncsa.fi > Asiakirjat > "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset".



Kuva 1. Hyväksyntäprosessi.

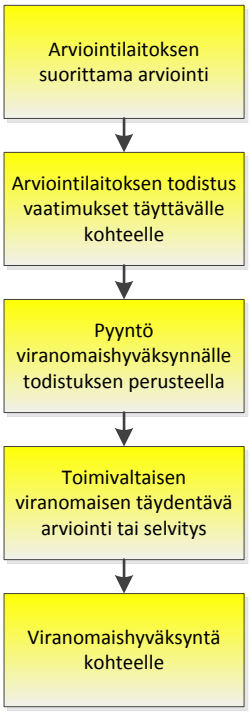
Hyväksynnän myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuustasonsa säilyttämiseen. Hyväksynnän voimassaolo raukeaa, mikäli tarkastetussa kohteessa tapahtuu olennainen sen turvallisuuteen vaikuttava muutos. Näitä voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten esimerkiksi ohjelmistojen turvapäivitysten asennukset, eivät aiheuta hyväksynnän raukeamista. Tapauskohtaiset ehdot hyväksynnän raukeamiselle määritellään hyväksynnän myöntämisen yhteydessä. Merkittävät turvallisuuteen vaikuttavat muutokset tulee hyväksyttää etukäteen Viestintävirastolla.

6.4 Hyväksytyn arviointilaitoksen suorittaman arvioinnin suhde viranomaishyväksyntään

Hyväksytty arviointilaitos on organisaatio (esimerkiksi yritys), jonka Viestintävirasto on erillisessä prosessissa hyväksynyt tekemään turvallisuustarkastuksia määrätylle turvallisuustasolle asti. Ajantasainen tieto Viestintäviraston hyväksymistä arviointilaitoksista löytyy Viestintäviraston verkkosivuilta[11].

Hankkeeseen liittyvän viranomaishyväksynnän tekee aina toimivaltainen turvallisuusviranomainen. Viranomaishyväksyntä voidaan myöntää joko viranomaisen oman tai, eräissä tapauksissa, hyväksytyn arviointilaitoksen tekemän arvioinnin perusteella.

Jos viranomaishyväksyntää haetaan arviointilaitoksen arvion perusteella, keskeisinä hyväksymisehtoina ovat arviointilaitoksen tarkastuksen riittävä laajuus kohteessa sekä viranomaisille toimitettujen arviointiraporttien tietojen riittävyys. Toimivaltainen turvallisuusviranomainen voi hyväksyntää varten suorittaa tarkentavia arviointeja tai pyytää arvioinnin kohteelta lisäselvitystä sen varmistamiseksi, että arvioinnin kohde täyttää sovellettavat tietoturvallisuusvaatimukset. Hyväksymismenettelyä on havainnollistettu kuvassa 2.



Kuva 2. Kohteen hyväksymismenettely.

Yritys voi hyödyntää arviointilaitoksen arviointia myös valmistautuessaan yritysturval-

[11] https://www.viestintavirasto.fi/tietoturva/tietoturvallisuudenarviointilaitokset/hyvaksytytarviointilaitokset.html.

lisuusselvitysprosessiin. Toimivaltaisen viranomaisen hyväksyntäprosessiin arviointilaitoksen arvioinnista on eniten hyötyä, kun yritys on saattanut tietojenkäsittelyympäristönsä kokonaisuudessaan vaatimusten tasolle ja saanut tästä arviointilaitoksen todistuksen. Tietojärjestelmien osalta viranomaishyväksynnän hakemista on kuvattu yksityiskohtaisemmin Viestintäviraston ohjeessa "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma"[12].

7 Ulkomaisten työntekijöiden ja alihankkijoiden turvallisuustodistukset

7.1 Ulkomaiset työntekijät (PSC)

Mikäli ulkomaalaisesta työntekijästä ei voida tehdä Suomen turvallisuusselvityslain mukaista turvallisuusselvitystä, hakija voi olla yhteydessä NSA:han tarvittavan todistuksen (Personnel Security Clearance, PSC) hankkimiseksi ulkomailta. NSA voi pyytää turvallisuusselvitystodistukset niistä maista, joiden kanssa Suomella on tietoturvallisuussopimus. Harkinnanvaraisesti todistuksia voidaan pyytää myös esim. EU- ja Nato –maista. Tietoturvallisuussopimuksissa on pääsääntöisesti sovittu, että PSC-todistus tarvitaan vasta CONFIDENTIAL –tasolta ylöspäin. Turvallisuusselvitysmenettely vaihtelee maittain.

Turvallisuusselvityspyyntöä varten NSA:lle tulee toimittaa seuraavat tiedot:

- tiedot henkilöistä (nimi, syntymäaika, kansalaisuus ja osoite)
- kopio passin henkilötietosivusta tai kopio henkilöllisyystodistuksesta
- mahdollisimman täsmällinen peruste PSC –pyynnölle. Peruste voi olla esimerkiksi henkilöiden osallistuminen kansainväliseen hankkeeseen, jossa henkilöt saavat pääsyn turvallisuusluokiteltuun tietoon tai saavat pääsyn tiloihin, jossa on mahdollisuus päästä käsiksi turvallisuusluokiteltuun tietoon. Perusteesta tulisi käydä ilmi, mitä turvallisuusluokiteltua tietoa hankkeessa käsitellään (Suomen turvaluokiteltu tieto, EU, Nato tai muun maan kansallinen tieto).
- tieto siitä, mille tasolle turvallisuustodistuksia haetaan (*CONFIDENTIAL/SECRET*)

Tiedot voi toimittaa lomakkeella, jonka saa pyydettäessä NSA:sta.

[12] www.ncsa.fi > Asiakirjat > "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset".

Jos ulkomaalainen henkilö on asunut Suomessa riittävän pitkään, turvallisuusselvitys voidaan käynnistää Suomessa samalla tavalla kuin suomalaistenkin työntekijöiden turvallisuusselvitys (ks. luku 6.2)

7.2 Ulkomaiset alihankkijat (FSC)

Jos alihankkija on ulkomaalainen yritys, pääsopimuspuoli voi pyytää Suomen NSA:ta hankkimaan ulkomaalaisesta yrityksestä FSC:n. Suomen NSA välittää pyynnön alihankkijan kotimaan NSA:lle. Edellytyksenä on pääsääntöisesti, että Suomella on kyseessä olevan valtion kanssa tietoturvallisuussopimus. Tietoturvallisuussopimuksissa on yleensä sovittu, että PSC-todistus tarvitaan vasta CONFIDENTIAL –tasolta ylöspäin.

Pyyntöä varten NSA tarvitsee ainakin seuraavat tiedot:

- -tiedot alihankkijayrityksestä (nimi, rekisterinumero ja katuosoite) ja sen yhteyshenkilöstä.

- tieto siitä, riittääkö vastaus FSC:n olemassaolosta/sen puuttumisesta vai onko FSC –menettely tarkoitus käynnistää, jos yrityksellä ei ole FSC:tä.

- -mahdollisimman täsmällinen peruste FSC –pyynnölle. Peruste voi olla esimerkiksi osallistuminen hankkeeseen, jossa käsitellään jonkin valtion turvallisuusluokiteltua tietoa ja jossa ulkomaalaisen yrityksen on tarkoitus toimia suomalaisen yrityksen alihankkijana sekä viittaus hankkeen turvallisuusnormistoon, joka edellyttää alihankkijoilta FSC:tä. Perusteesta tulisi käydä ilmi, mitä luokiteltua tietoa hankkeessa suojataan (Suomen kansallinen turvallisuusluokiteltu tieto, EU, Nato, muun maan kansallinen tieto). Mukaan tulisi liittää ne osat turvallisuusdokumentaatiosta, joista peruste ilmenee.

- -mille tasolle *(CONFIDENTIAL/SECRET)* turvallisuusselvitystä haetaan.

- -tieto siitä, käsitelläänkö tietoja yrityksen tiloissa tai tietojärjestelmissä

Tiedot voi toimittaa lomakkeella, jonka saa pyydettäessä NSA:sta.

8 Vierailulupakäytäntö (Request for Visit, RfV)

Kansainvälisiin turvallisuusluokiteltuihin hankkeisiin liittyy usein vierailuja hanke-osapuolten välillä. Henkilöt, jotka vierailevat sellaisissa ulkomaalaisen viranomaisen tai yrityksen tiloissa, joissa käsitellään turvallisuusluokiteltua tietoa (CONFIDENTIAL tai korkeampi), tarvitsevat vierailuluvan. RESTRICTED –tason vierailut eivät pääsääntöisesti edellytä RfV:tä, vaan vierailusta voidaan sopia suoraan kohteen ja vierailijan välillä.

Vierailulupamenettelyllä varmistetaan, että vierailijalla on voimassa oleva henkilöturvallisuusselvitys (riittävällä tasolla) ja että vierailuun on tarvittava peruste.

Vierailulupapyyntö laaditaan RfV -lomakkeelle, johon merkitään vierailuun ja vierailijoihin liittyvät tiedot. Lomakkeen voi pyytää NSA:sta. Vieraileva yritys toimittaa RfV -lomakkeen kansalliselle turvallisuusviranomaiselle, joka välittää pyynnön edelleen vierailun isäntämaan toimivaltaiselle turvallisuusviranomaiselle.

9 Yritysten turvallisuusvastuut ja -velvoitteet

9.1 Pääsopijapuolen vastuut

Ennen hankinnan käynnistymistä yrityksen tulisi käynnistää osaltaan alustava riskienhallintaprosessi. Riskianalyysi auttaa selvittämään, miltä osin yritysten turvallisuutta tulisi parantaa. Apuna työssä voidaan käyttää Katakria, johon koottu velvoittavista lähteistä peräisin olevia tietoturvallisuusvaatimuksia.

Hankintaan pääsopijapuolena osallistuvan yrityksen vastuut määritellään turvallisuusluokiteltua hankintaa koskevassa sopimuksessa. Kansainvälisissä hankkeissa tästä sopimuksesta käytetään nimitystä Classified Contract. Hanketta koskevien yleisten sopimusmääräysten lisäksi sopimus sisältää muun turvallisuusdokumentaation (kansainvälisissä hankinnoissa yleensä PSI:n ja/tai SAL:in). Turvallisuusdokumentaatio on yleensä kiinteä osa sopimusta, ja sen asettamat velvoitteet sitovat yritystä samalla tavalla kuin sopimuskin.

Pääsopijapuolena osallistuvan yrityksen käyttämät alihankkijat nimetään usein sopimuksessa ja ne sitoutuvat alihankintasopimuksessa noudattamaan samoja velvoitteita kuin pääsopijapuolikin. Jos hankkeen aikana ilmenee tarve käyttää uusia alihankkijoita, on niiden turvallisuustason varmistamisessa toimittava niin kuin turvallisuusluokiteltua hanketta koskevassa sopimuksessa määrätään. Yleensä tämä merkitsee ainakin viranomaiselle annetun sitoumuksen ja hanketta koskevan turvallisuusdokumentaation päivittämistä. Pääsopijaosapuoli vastaa siitä, ettei se käytä hankkeessa sellaisia alihankkijoita, joita hankintayksikkö ei ole hyväksynyt.

Hankintayksikkö voi asettaa tiettyjä rajoituksia ulkomaalaisten tai ulkomaalaisomistuksessa olevien alihankkijoiden käytölle. Pääsopimuspuolen tulee ottaa nämä rajoitukset huomioon alihankkijoita valitessa.

9.2 Hankkeen turvallisuusvastaavan tehtävät

Turvallisuusdokumentaatiossa nimetään yleensä hankinnan turvallisuudesta vastaava yrityksen edustaja (Facility Security Officer, FSO). Usein kyseessä on yrityksen turvallisuuspäällikkö. Yrityksessä saattaa olla muitakin turvallisuudesta vastaavia henkilöitä, kuten tietoturvallisuusvastaava, mutta vastuu ulkomaiseen hankintayksikköön ja viranomaisiin nähden on aina nimetyllä henkilöllä.

Turvallisuusvastaava on ratkaisevassa roolissa hankkeen turvallisuuden toteutumisessa. Hänen vastuullaan on hankkeen turvallisuusdokumentaation mukaisten vaatimusten käytännön toteuttaminen sekä henkilöstön koulutus ja toiminnan valvonta. Turvallisuusvastaava tai hänen varahenkilönsä ilmoittavat aina myös havaituista turvallisuuspoikkeamista. Hankkeen turvallisuusvastaavat ovat yhteydessä toisiinsa käy-

tännön turvallisuusyhteistyön osalta esimerkiksi vierailulupiin liittyen.

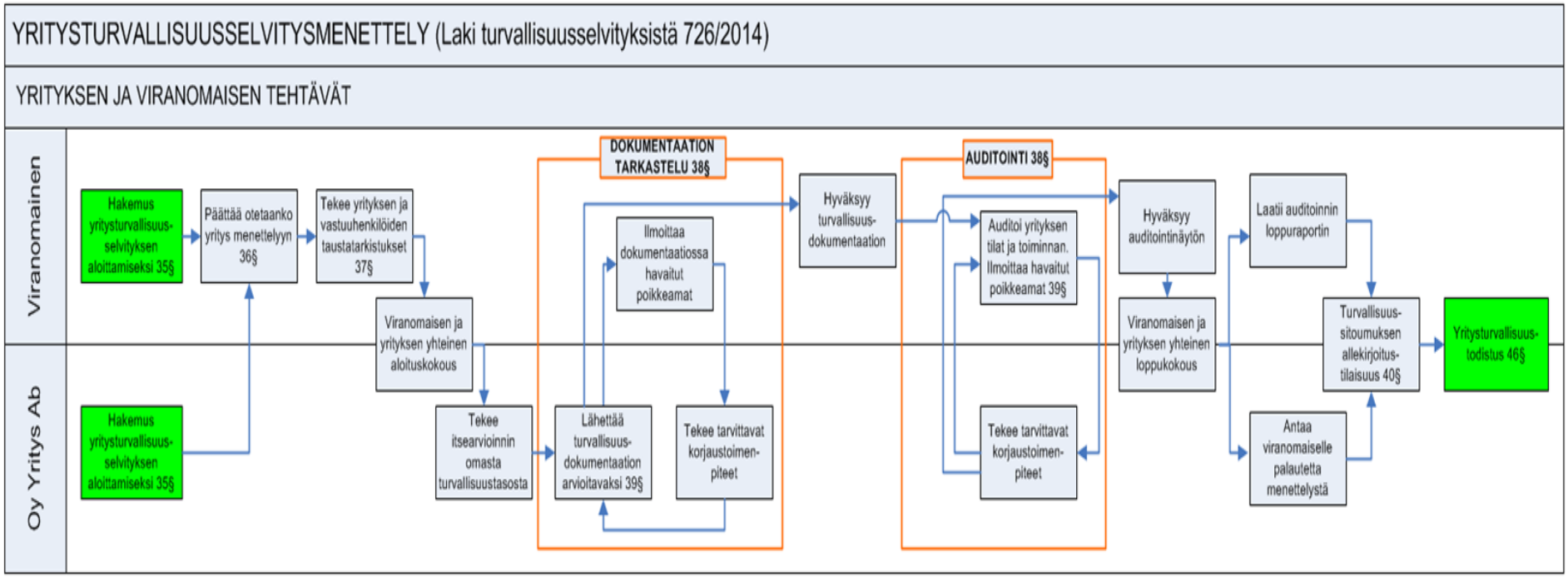
9.3 Turvallisuusrikkomukset ja tiedon vaarantuminen

Kaikista turvallisuusrikkomuksista ja epäillyistä turvallisuusrikkomuksista sekä turvallisuusluokitellun tiedon vaarantumisesta tulee välittömästi ilmoittaa hankkeen turvallisuusdokumentaatiossa määrätyille tahoille. Yleensä turvallisuusdokumentaatio edellyttää ilmoittamista ainakin tiedon luovuttajalle. Kansainvälisen turvallisuusluokitellun tiedon vaarantumisesta ja tiedon suojaamiseen liittyvistä rikkomuksista tulee ilmoittaa myös NSA:lle.

Lisävahingot tulee estää mahdollisuuksien mukaan. Lisäksi on huolehdittava siitä, että ne henkilöt, jotka ovat välittömästi tekemisissä tietoturvallisuusloukkauksen kanssa, eivät tutki asiaa.

NSA ilmoittaa toisen maan turvallisuusviranomaisille tietoonsa tulleista turvallisuusrikkomuksista ja tiedon suojan vaarantumisesta. NSA ryhtyy myös toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syyllistyneen syytteeseen saattamiseksi.

LIITE 1


YRITYSTURVALLISUUSSELVITYSMENETTELY (Laki turvallisuusselvityksistä 726/2014)
YRITYKSEN JA VIRANOMAISEN TEHTÄVÄT
Viranomainen
Oy Yritys Ab
Hakemus yritysturvallisuus-selvityksen aloittamiseksi 35§
Päättää otetaanko yritys menettelyyn 36§
Tekee yrityksen ja vastuuhenkilöiden taustatarkistukset 37§
Viranomaisen ja yrityksen yhteinen aloituskokous
Hakemus yritysturvallisuus-selvityksen aloittamiseksi 35§
Tekee itsearvioinnin omasta turvallisuustasosta
DOKUMENTAATION TARKASTELU 38§
Lähettää turvallisuus-dokumentaation arvioitavaksi 39§
Ilmoittaa dokumentaatiossa havaitut poikkeamat
Tekee tarvittavat korjaustoimen-piteet
Hyväksyy turvallisuus-dokumentaation
AUDITOINTI 38§
Auditoi yrityksen tilat ja toiminnan. Ilmoittaa havaitut poikkeamat 39§
Tekee tarvittavat korjaustoimen-piteet
Hyväksyy auditointinäytön
Viranomaisen ja yrityksen yhteinen loppukokous
Laatii auditoinnin loppuraportin
Antaa viranomaiselle palautetta menettelystä
Turvallisuus-sitoumuksen allekirjoitus-tilaisuus 40§
Yritysturvallisuus-todistus 46§