NATO OTAN

NORTH ATLANTIC COUNCIL

CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

20. marraskuuta 2020

ASIAKIRJA
C-M(2002)49-REV1

TURVALLISUUS POHJOIS-ATLANTIN LIITOSSA (NATO)

Pääsihteerin ilmoitus

Kesäkuun 17. päivänä 2002 päivätyn asiakirjan C-M(2002)49 ensimmäinen tarkistus

Viite: Asiakirja C-M(2002)49-COR1–COR12 (konsolidoitu toisinto), päivätty 17. kesäkuuta 2002

1. Tämä asiakirja perustuu Naton turvallisuussäännöstön ja sitä tukevien ohjeiden merkittävään ja kokonaisvaltaiseen tarkistukseen sellaisena kuin turvallisuuskomitea on sen hyväksynyt.

2. Asiakirjalla C-M(2002)49-REV1, joka korvaa viitteessä mainitun asiakirjan, tehdään viiteasiakirjaan sekä rakenteellisia että sisällöllisiä muutoksia.

3. Rakennetta on muutettu lisäämällä uusi liite H, jossa käsitellään erikseen turvallisuutta suhteissa Naton ulkopuolisiin toimijoihin. Samaa aihetta käsitellään lisää äskettäin laaditussa Naton ohjeessa turvallisuudesta suhteissa Naton ulkopuolisiin toimijoihin (asiakirja AC/35-D/2006) sekä tätä ohjetta tukevassa Naton ulkopuolisille toimijoille tarkoitetussa tarkistetussa asiakirjassa, joka käsittelee turvallisuutta suhteissa Natoon (asiakirja AC/35-D/1038-REV3).

4. Sisällön osalta tarkistuksella on muutettu osiota "Perusperiaatteet, vähimmäisvaatimukset ja vastuut" (liite B) sekä määräyksiä osioissa "Henkilöstöturvallisuus", "Toimitilaturvallisuus", "Tietoaineistoturvallisuus" ja "Turvallisuus suhteissa Naton ulkopuolisiin toimijoihin" (liitteet B, C, D, E ja H). Tarkistuksella ei ole muutettu asiakirjan C-M(2002)49 liitteitä F ja G.

(Allekirjoitus) Jens Stoltenberg

Liite 1
Liitteen 1 liitteet A, B, C, D, E, F, G, H
Sanasto

TURVALLISUUS POHJOIS-ATLANTIN LIITOSSA (NATO)

JOHDANTO

1. Tässä C-M-asiakirjassa, jonka otsikkona on "Turvallisuus Pohjois-Atlantin liitossa (Nato)", kuvataan ne turvallisuuden perusperiaatteet ja vähimmäisvaatimukset, joita Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten on sovellettava varmistaakseen turvallisuusluokitellun tiedon yhteisen suojaustason. Naton turvallisuusmenettelyt toimivat parhaaksi eduksi vain, jos ne perustuvat niitä tukevaan kansalliseen turvallisuusjärjestelmään, joka on ominaisuuksiltaan näissä periaatteissa määritettyjen ominaisuuksien mukainen tai niitä vastaava. Lisäksi näissä periaatteissa käsitellään Naton sisäisiä turvallisuusrooleja, -tehtäviä ja -vastuita.

2. Tämä periaateasiakirja koostuu liitteessä A olevasta turvallisuussopimuksesta, jonka nimi on "sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta", sekä seuraavista liitteistä:

   a) Liite A – Sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta

   b) Liite B – Perusperiaatteet, vähimmäisvaatimukset ja vastuut

   c) Liite C – Henkilöstöturvallisuus

   d) Liite D – Toimitilaturvallisuus

   e) Liite E – Naton turvallisuusluokitellun tiedon turvallisuus

   f) Liite F – Viestintä- ja tietojärjestelmien turvallisuus

   g) Liite G – Turvallisuusluokiteltujen hankkeiden turvallisuus ja yritysturvallisuus

   h) Liite H – Turvallisuus suhteissa Naton ulkopuolisiin toimijoihin.

3. Tämä periaateasiakirja tukee Naton tiedonhallinnan periaatteita (C-M(2007)0118). Naton turvallisuusluokittelemattoman tiedon hallinnan periaatteita koskevassa asiakirjassa C-M(2002)60 käsitellään niitä perusperiaatteita ja vaatimuksia, joita Naton sotilas- ja siviilielimissä sekä Naton jäsenvaltioissa sovelletaan Naton turvallisuusluokittelemattoman tiedon (NATO UNCLASSIFIED ja julkinen tieto) suojaamiseksi.

TAVOITTEET JA PÄÄMÄÄRÄT

4. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet varmistavat tässä C-M-asiakirjassa kuvattujen perusperiaatteiden ja vähimmäisvaatimusten soveltamisen, jotta Naton turvallisuusluokitellun tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyminen turvataan.

5. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet laativat turvallisuusohjelmat, jotka täyttävät nämä perusperiaatteet ja vähimmäisvaatimukset, jotta Naton turvallisuusluokitellulle tiedolle varmistetaan yhteinen suojaustaso.

SOVELTAMISALA

6. Näitä perusperiaatteita ja vähimmäisvaatimuksia sovelletaan seuraaviin:

   a) Natosta peräisin oleva turvallisuusluokiteltu tieto;

b) Naton jäsenvaltiosta peräisin oleva turvallisuusluokiteltu tieto, joka annetaan Natolle tai toiselle Naton jäsenvaltiolle Naton ohjelman, hankkeen tai sopimuksen tueksi;

c) Naton ja Naton ulkopuolisten toimijoiden[1] välillä vaihdettava turvallisuusluokiteltu tieto; ja

d) hallituksen (tai Naton sotilas- tai siviilielimen) ulkopuolisille luonnollisille henkilöille ja organisaatioille, kuten konsulteille, yrityksille ja yliopistoille, annettava turvallisuusluokiteltu tieto.

7. ATOMAL-tietoon pääsyyn ja sen suojaamiseen sovelletaan sopimusta Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä (C-M(64)39). Jotta varmistetaan asianmukainen ATOMAL-tietoon pääsyn valvonta sekä tämän tiedon asianmukainen käsittely ja suojaaminen, sovelletaan hallinnollisia järjestelyjä ydinpuolustustietoja koskevasta yhteistyöstä tehdyn Pohjois-Atlantin sopimuksen osapuolten välisen sopimuksen täytäntöön panemiseksi (C-M(68)41).

8. Yhdysvaltojen yhteistä operaatiosuunnitelmaa (US-SIOP) koskevaan tietoon pääsyyn ja sen suojaamiseen sovelletaan määräyksiä, jotka on annettu asiakirjassa C-M(71)27 (uudistettu) erityismenettelyistä Yhdysvaltojen yhteistä operaatiosuunnitelmaa (US-SIOP) koskevan tiedon käsittelemiseksi Natossa.

9. Signaalitiedusteluun (SIGINT) liittyvien tietojen, toimintojen, lähteiden ja menetelmien arkaluonteisuuden vuoksi on sovellettava tiukkoja turvallisuusmääräyksiä ja -menettelyjä, jotka usein menevät tämän C-M-asiakirjan määräyksiä ja menettelyjä pidemmälle. Siksi SIGINT-tietoihin, -toimintoihin, -lähteisiin ja -menetelmiin pääsyyn ja niiden suojaamiseen sovelletaan kansallisia määräyksiä sekä asiakirjan MC 101 (Naton signaalitiedustelun periaatteet) ja siihen liittyvän liittokunnan yhteisen AJP-julkaisun sekä Naton signaalitiedustelun neuvoa-antavan komitean (NACSI) SIGINT-hallinnon ja -menettelyjen oppaan määräyksiä.

ASEMA

10. Pohjois-Atlantin neuvosto (NAC) on hyväksynyt tämän asiakirjan, jolla pannaan täytäntöön sopimus Pohjois-Atlantin sopimuksen osapuolten välillä tietoturvallisuudesta (liitteenä A) ja siten vahvistetaan Naton turvallisuusperiaatteet.[2]

[1] Naton ulkopuoliset valtiot ja muut Naton ulkopuoliset elimet (esim. kansainväliset järjestöt), mukaan lukien näitä valtioita ja elimiä edustavat luonnolliset henkilöt.

[2] Turvallisuuskomitean työjärjestyksen (C-M(2015)0002) mukaan Naton turvallisuusperiaatteet koostuvat asiakirjoista C-M(2002)49 ja C-M(2002)50.

LIITE B

PERUSPERIAATTEET, VÄHIMMÄISVAATIMUKSET JA VASTUUT

PERUSPERIAATTEET

1. Sovelletaan seuraavia perusperiaatteita:

   a) Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet varmistavat tässä C-M-asiakirjassa sovittujen vähimmäisvaatimusten noudattamisen, jotta osapuolten kesken vaihdettavalle turvallisuusluokitellulle tiedolle varmistetaan yhteinen suojaustaso.

   b) Yhteisen vastuun tunnustaen turvallisuusluokiteltua tietoa jaetaan ainoastaan tiedonsaantitarpeen[1] periaatteen perusteella henkilöille, joille on selostettu sovellettavat turvallisuusmenettelyt.

   c) Ainoastaan asianmukaisesti turvallisuusselvitetyille henkilöille annetaan pääsy turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun tietoon.

   d) Turvallisuusselvitystodistuksen antamista ei katsota viimeiseksi vaiheeksi arvioitaessa henkilön kelpoisuutta päästä turvallisuusluokiteltuun tietoon, vaan otetaan käyttöön jatkuvat turvallisuusmenettelyt seurantatoimina, jotta voidaan huomioida sisäpiiriuhan hallinta[2].

   e) Naton turvallisuustoimisto (NOS) koordinoi sisäpiiriuhan hallintaa yhdessä toimivaltaisten kansallisten viranomaisten sekä Naton sotilas- ja siviilielinten kanssa.

   f) Turvallisuusriskien hallintaa[3] suoritetaan pakollisena Naton sotilas- ja siviilielimissä Naton turvallisuusriskien hallintaprosessin (AC/35-D/1035) mukaisesti. Sen soveltaminen Naton jäsenvaltioissa on vapaaehtoista. Riskienhallintaa ei saa käyttää keinona kiertää turvallisuusperiaatteita.

   g) Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet käynnistävät organisaatioissaan turvallisuuskoulutus- ja -tietoisuusohjelmia, joissa käsitellään kaikkia turvallisuusnäkökohtia jäljempänä I kohdassa esitetyllä tavalla.

   h) Kaikista epäillyistä turvallisuusluokiteltuun tietoon kohdistuneista tietoturvaloukkauksista ja tällaisen tiedon vaarantumisista ilmoitetaan viipymättä toimivaltaiselle turvallisuusviranomaiselle.

   i) Alkuperäisten luovuttajien luovuttaessa turvallisuusluokiteltua tietoa Natolle ja Naton jäsenvaltioille Naton ohjelman, hankkeen tai sopimuksen tueksi oletuksena on, että tietoa hallitaan ja suojataan Naton tiedonhallinnan periaatteiden ja Naton turvallisuusperiaatteiden mukaisesti.

   j) Turvallisuusluokiteltuun tietoon sovelletaan alkuperäisen luovuttajan määräysvaltaa[4].

---

[1] Periaate, jonka mukaan tehdään myönteinen päätös, että tiedon mahdollisella vastaanottajalla on tarve päästä tietoon, saada tieto siitä tai saada se haltuunsa pystyäkseen suorittamaan virallisia tehtäviä tai palveluja.

[2] Sisäpiiriuhan aiheuttaa henkilöstö, jolla on erioikeuteen perustuva pääsy Naton turvallisuusluokiteltuun tietoon ja/tai Naton omaisuuteen organisaatiossa hoitamansa tehtävän perusteella ja joka voi myöhemmin käyttää väärin tätä pääsyä hävittääkseen, vahingoittaakseen, poistaakseen tai paljastaakseen Naton turvallisuusluokiteltua tietoa ja/tai Naton omaisuutta joko tahallisesti tai huolimattomuudesta.

[3] Uhkien ja haavoittuvuuksien arviointiin perustuva järjestelmällinen lähestymistapa sen määrittämiseksi, mitä vastatoimia tarvitaan tiedon sekä sitä tukevien palvelujen ja resurssien turvallisuuden suojaamiseksi. Riskienhallintaan sisältyy resurssien suunnittelu, järjestäminen, ohjaaminen ja valvonta, joiden avulla varmistetaan, että riski pysyy hyväksyttävyyden rajoissa.

[4] Periaate, jonka mukaan valtio, Nato tai muu organisaatio, jonka alaisuudessa tieto on luotu, tuotettu tai tuotu

k) Naton turvallisuusluokiteltu tieto luovutetaan vakiintuneiden luovutusmenettelyjen ja -perusteiden mukaisesti, ja kaikissa tapauksissa kaikki luovutettava Naton turvallisuusluokiteltu tieto tulee suojata vähintään samantasoisesti kuin tässä C-M-asiakirjassa ja sitä tukevissa ohjeissa määrätään.

l) Turvallisuusluokiteltu tieto turvataan tasapainoisella turvallisuustoimenpiteiden kokonaisuudella, jolla varmistetaan henkilöstöturvallisuus, toimitilaturvallisuus, tietoturvallisuus sekä viestintä- ja tietojärjestelmien turvallisuus (CIS). Myös silloin, kun turvallisuusluokiteltua tietoa annetaan hankeosapuolille ja luovutetaan Naton ulkopuolisille toimijoille (NNE), se turvataan noudattamalla näissä turvallisuusperiaatteissa kuvattuja menettelyjä. Nämä vaatimukset koskevat kaikkia henkilöitä, joilla on pääsy turvallisuusluokiteltuun tietoon, kaikkia turvallisuusluokiteltua tietoa sisältäviä tietovälineitä ja kaikkia tiloja, joissa on tällaista tietoa.

m) Organisaatiot, joilla on hallussaan Naton turvallisuusluokiteltua tietoa, kehittävät mekanismit ja menettelyt, joilla varmistetaan Naton turvallisuusperiaatteiden vaatimusten soveltaminen poikkeuksellisissa toimintaolosuhteissa, kuten häiriötilojen aikana. Nämä järjestelmät ja menettelyt voidaan esittää joko toiminnan jatkuvuussuunnitelmassa tai palautumissuunnitelmassa, tapahtuman luonteen mukaan.

KRIITTISIÄ KOHTEITA KOSKEVAN TIEDON SUOJAAMINEN

2. Tiedon julkaiseminen kriittisistä siviilikohteista (esim. puolustusmateriaalivarastoista, energiavarastoista), joilla on sotilaallista merkitystä jännitteiden tai sodan aikana, saattaa edistää kineettistä hyökkäystä tai sabotaasia, koska julkaistun tiedon avulla mahdolliset viholliset tai terroristit voivat pystyä kokoamaan luettelon kriittisistä kohteista ja käyttämään sitä haavoittuvien kohteiden tunnistamiseen hyökkäystä varten. Jotta pystytään estämään vihollisia käyttämästä tällaista tietoa vihamielisiin tarkoituksiin, on toteutettava asianmukaiset toimet, joilla varmistetaan, ettei tätä tietoa ole vapaasti saatavilla julkisesti. Lisäksi tällaisten kohteiden omistajien ja käyttäjien on oltava täysin tietoisia niihin kohdistuvan mainitunlaisen toiminnan vaarasta ja toteutettava tarvittavat toimet näitä kohteita koskevan tiedon suojaamiseksi.

TURVALLISUUDEN VASTUUALUEET

Kansallinen turvallisuusviranomainen (NSA)

3. Kukin Naton jäsenvaltio perustaa kansallisen turvallisuusviranomaisen (NSA), joka vastaa Naton turvallisuusluokitellun tiedon turvallisuudesta. Kansallinen turvallisuusviranomainen toimii Naton turvallisuustoimiston ensisijaisena yhteystahona kaikissa Naton turvallisuuteen liittyvissä asioissa. Kansallinen turvallisuusviranomainen voi ohjata Naton turvallisuustoimiston kääntymään toimivaltaisen määrätyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen puoleen.

4. Kansallisen turvallisuusviranomaisen vastuulla on

a) varmistaa Naton turvallisuusluokitellun tiedon turvallisuus sekä sotilas- että siviilialan kansallisissa virastoissa ja muissa organisaatioissa, sekä kotimaassa että ulkomailla;

b) varmistaa, että kaikissa kansallisissa sekä sotilas- että siviilialan organisaatioissa kaikilla tasoilla tarkastetaan asianmukaisesti määräajoin Naton turvallisuusluokitellun tiedon suojaamiseksi tehdyt turvallisuusjärjestelyt, jotta voidaan todeta, suojataanko

---

Natoon, määrää tämän tiedon käyttöön sovellettavat säännöt ja vaatimukset ja on toimivaltainen tiedon koko elinkaaren aikaisten muutosten suhteen.

tätä tietoa asianmukaisesti. Sellaisissa organisaatioissa, joilla on hallussaan turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa tai ATOMAL-tietoa, tehdään turvallisuustarkastukset vähintään 24 kuukauden välein, jollei Naton turvallisuustoimisto tee näitä tarkastuksia kyseisenä ajanjaksona;

c) varmistaa, että kaikille kansalaisille, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun tietoon, on annettu henkilöturvallisuusselvitystodistus (PSC) Naton turvallisuusperiaatteiden mukaisesti;

d) varmistaa, että on laadittu turvallisuussuunnitelmat, joiden avulla estetään Naton turvallisuusluokiteltua tietoa joutumasta asiattomien tai vihamielisten tahojen haltuun poikkeusolojen aikana; ja

e) auktorisoida kansallisten COSMIC-keskusrekisterien perustaminen tai lakkauttaminen. COSMIC-keskusrekisterien perustamisesta tai lakkauttamisesta on ilmoitettava Naton turvallisuustoimistolle.

Määrätty turvallisuusviranomainen (DSA)

5. Viranomainen, jonka vastuulla on tiedottaa yrityksille ja muille yhteisöille kansallisista periaatteista kaikissa Naton yritysturvallisuuden periaatteita koskevissa asioissa sekä antaa ohjausta ja apua niiden soveltamisessa. Joissakin valtioissa määrätyn turvallisuusviranomaisen tehtävää voi hoitaa kansallinen turvallisuusviranomainen.

Turvallisuuskomitea (SC)

6. Turvallisuuskomitean asettaa Pohjois-Atlantin neuvosto (NAC). Komiteassa on edustajat kunkin Naton jäsenvaltion kansallisesta turvallisuusviranomaisesta / määrätystä turvallisuusviranomaisesta, ja komiteaa tukee tarvittaessa muu Naton jäsenvaltioiden turvallisuushenkilöstö. Kansainvälisen sotilasesikunnan (IMS), strategisten esikuntien sekä tiedonvälityksen, johtamisen ja valvonnan (C3) ohjausryhmän edustajat ovat läsnä turvallisuuskomitean kokouksissa. Myös Naton sotilas- ja siviilielinten edustajia voi olla läsnä käsiteltäessä asioita, joissa näillä elimillä on intressi. Naton turvallisuustoimisto nimeää turvallisuuskomitean puheenjohtajat komitean pääedustajien kokoonpanoa, turvallisuusperiaatteita käsittelevää kokoonpanoa sekä viestintä- ja tietojärjestelmiä käsittelevää kokoonpanoa varten.

7. Turvallisuuskomitea vastaa suoraan Pohjois-Atlantin neuvostolle seuraavista:

a) (asiakirjoissa C-M(2002)49 ja C-M(2002)50 kuvattujen) Naton turvallisuussääntöjen tarkistaminen ja niiden muuttamista tai hyväksymistä koskevien suositusten antaminen Pohjois-Atlantin neuvostolle;

b) Naton turvallisuussääntöjä koskevien kysymysten käsittely;

c) Naton turvallisuussääntöjen tukemiseksi julkaistavien direktiivien ja ohjausasiakirjojen tarkistaminen ja hyväksyminen[5]; ja

d) sellaisten turvallisuusasioiden käsittely, jotka Pohjois-Atlantin neuvosto, Naton jäsenvaltio, pääsihteeri, sotilaskomitea, tiedonvälityksen, johtamisen ja valvonnan ohjausryhmä tai Naton jonkin sotilas- tai siviilielimen johtaja on saattanut turvallisuuskomitean käsiteltäväksi, sekä asianmukaisten suositusten laatiminen näistä asioista.

Naton turvallisuustoimisto (NOS)

8. Naton turvallisuustoimisto on perustettu Naton kansainväliseen sihteeristöön osana

[5] Naton jäsenvaltio voi pyytää, että myös Pohjois-Atlantin neuvosto hyväksyy turvallisuusperiaatteita tukevan ohjeen.

yhteistä tiedustelu- ja turvallisuusjaostoa. Turvallisuustoimiston henkilöstö on kokenutta sekä sotilas- että siviilialan turvallisuusasioissa. Naton turvallisuustoimisto toimii läheisessä yhteydessä Naton jäsenvaltioiden kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten sekä Naton sotilas- ja siviilielinten kanssa. Turvallisuustoimisto voi myös tarvittaessa pyytää Naton jäsenvaltioita ja Naton sotilas- ja siviilielimiä antamaan turvallisuustoimistolle lisää turvallisuusasiantuntijoita avustamaan sitä osa-aikaisesti, kun kokoaikaisen henkilöstön lisääminen turvallisuustoimistoon ei olisi perusteltua.

9. Naton turvallisuustoimiston vastuulla on

a) käsitellä Naton turvallisuuteen vaikuttavia asioita;

b) määrittää keinot, joilla Naton turvallisuutta voitaisiin parantaa;

c) koordinoida yleisesti turvallisuutta Natossa Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten kesken;

d) varmistaa Naton turvallisuussääntöjen toteuttaminen ja valvonta muun muassa antamalla neuvoja, joita Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet voivat pyytää joko soveltaessaan tässä liitteessä kuvattuja perusperiaatteita ja turvallisuusvaatimuksia tai täyttäessään yksittäisiä turvallisuusvaatimuksia;

e) tiedottaa kulloisenkin tilanteen mukaan turvallisuuskomitealle, pääsihteerille ja sotilaskomitean puheenjohtajalle Naton turvallisuustilanteesta sekä edistymisestä turvallisuutta koskevien Pohjois-Atlantin neuvoston päätösten täytäntöönpanossa;

f) tehdä määräajoin Naton turvallisuusluokitellun tiedon suojaamiseen tarkoitettujen turvallisuusjärjestelmien tarkastuksia Naton jäsenvaltioissa, Naton siviilielimissä, Naton operaatioesikunnassa ja Naton transformaatioesikunnan komentajan johtoesikunnassa[6];

g) tehdä turvallisuutta koskevia selvityksiä sellaisissa Naton ulkopuolisissa toimijoissa, joiden kanssa Nato on tehnyt turvallisuussopimuksen, aluksi varmentamista varten ja sen jälkeen määräajoin Naton turvallisuusperiaatteiden jatkuvan noudattamisen varmistamiseksi;

h) koordinoida kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten ja Naton sotilas- ja siviilielinten kanssa epäiltyyn tai tosiasialliseen Naton turvallisuusluokitellun tiedon katoamiseen tai vaarantumiseen liittyvien asioiden tutkintaa;

i) tiedottaa tarvittaessa kansallisille turvallisuusviranomaisille / määrätyille turvallisuusviranomaisille saamastaan epäedullisesta tiedosta, joka koskee kyseisten valtioiden kansalaisia;

j) suunnitella turvatoimia Brysselissä sijaitsevan Naton päämajan suojaamiseksi ja varmistaa niiden toteuttaminen oikealla tavalla; ja

k) valvoa pääsihteerin johdolla ja puolesta ATOMAL-tietojen suojaamiseksi tarkoitetun Naton turvallisuusohjelman toteuttamista ATOMAL-sopimuksen (C-M(64)39) ja sitä tukevien hallinnollisten järjestelyjen (C-M(68)41) määräysten mukaisesti.

Sotilaskomitea ja Naton sotilaselimet

10. Naton korkeimpana sotilasviranomaisena sotilaskomitea vastaa sotilasasioiden hoitamisesta yleisesti. Sotilaskomitea vastaa siten kaikista Naton sotilasrakenteen turvallisuusasioista, mukaan lukien niiden toimenpiteiden keskitetty kokonaiskäsittely,

[6] Naton jäsenvaltiot voivat Naton turvallisuustoimiston pyynnöstä osallistua sen Naton sotilas- ja siviilielimissä tekemiin tarkastuksiin joko tarkkailijoina tai tarkastusryhmän aktiivisina jäseninä. Tämä ei kuitenkaan ole mahdollista sellaisissa siviilielimissä, joiden perusrakenteissa kaikki Naton jäsenvaltiot eivät ole mukana.

joita tarvitaan Naton turvallisuusluokitellun tiedon siirtämiseen käytettävän salaustekniikan ja -aineiston asianmukaisuuden varmistamiseksi, sekä tämän C-M-asiakirjan liitteessä F määriteltyjen Naton rahoittamien salauslaitteistojen turvallisuushyväksyntä. Aiemmin sovittujen periaatteiden sekä edellä olevien 8 ja 9 kohdan mukaisesti Naton turvallisuustoimisto hoitaa turvallisuuteen liittyviä toimeenpanotehtäviä Naton sotilasrakenteessa ja tiedottaa tästä toiminnasta sotilaskomitean puheenjohtajalle.

11. Sotilaskomitean alaisuuteen perustettujen Naton sotilaselinten johtajat vastaavat kaikista organisaatioidensa turvallisuusasioista. Tähän sisältyy vastuu siitä, että varmistetaan turvallisuusorganisaation perustaminen, asianmukaisten turvallisuustoimenpiteiden ja -menettelyjen suunnittelu ja toteutus Naton turvallisuussääntöjen mukaisesti sekä turvallisuustoimenpiteiden tarkastaminen määräajoin kaikilla komentotasoilla. Sellaisissa organisaatioissa, joilla on hallussaan turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa tai ATOMAL-tietoa, tehdään turvallisuustarkastukset vähintään 24 kuukauden välein, jollei Naton turvallisuustoimisto ole tehnyt tällaista tarkastusta kyseisenä ajanjaksona;

Naton siviilielimet

12. Naton kansainvälinen sihteeristö ja Naton siviilivirastot vastaavat Pohjois-Atlantin neuvostolle turvallisuuden ylläpitämisestä organisaatioissaan. Tähän sisältyy vastuu siitä, että varmistetaan turvallisuusorganisaation perustaminen, turvallisuusohjelmien suunnittelu ja toteutus Naton turvallisuussääntöjen mukaisesti sekä turvallisuustoimenpiteiden tarkastaminen määräajoin kaikilla komentotasoilla. Sellaisissa organisaatioissa, joilla on hallussaan turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa tai ATOMAL-tietoa, tehdään turvallisuustarkastukset vähintään 24 kuukauden välein, jollei Naton turvallisuustoimisto ole tehnyt tällaista tarkastusta kyseisenä ajanjaksona.

TURVALLISUUSVALVONTA OSAAMISKESKUSTEN[7] / YHTEISYMMÄRRYSPÖYTÄKIRJAAN PERUSTUVIEN ELINTEN OSALTA

13. Turvallisuusvalvonnalla tarkoitetaan valvontatehtävää, jolla varmistetaan, että Naton turvallisuusluokiteltua tietoa käsittelevä organisaatio soveltaa Naton turvallisuussääntöjä oikein suojatakseen tätä tietoa. Naton komentorakenteen (NCS) ulkopuolisten elinten turvallisuusvalvonta Naton turvallisuusluokitellun tiedon suojaamisen osalta tapahtuu seuraavasti:

    a) Osallistuvat valtiot vastaavat turvallisuusasioiden hoitamisesta kyseisessä Naton sotilaselimessä (NMB) ja tekevät asianmukaiset järjestelyt sitä varten. Jollei näiden yksiköiden turvallisuusvalvonnan hoitamiseksi ole tehty erillisiä sopimuksia, se valtio, jossa kyseinen yksi tai useampi yksikkö sijaitsee, eli isäntävaltio, johtaa turvallisuusvalvontaa.

    b) Osaamiskeskukset / yhteisymmärryspöytäkirjaan perustuvat elimet voivat olla Naton sotilaselimiä, jos Pohjois-Atlantin neuvosto on tehnyt aktivointipäätöksen asiassa. Tällaisissa tapauksissa sovelletaan Naton turvallisuussääntöjä ja osaamiskeskuksen / yhteisymmärryspöytäkirjaan perustuvan elimen johtaja vastaa kaikista organisaationsa turvallisuusasioista. Osallistuvat valtiot vastaavat turvallisuusvaatimusten käsittelystä osaamiskeskuksessa / yhteisymmärryspöytäkirjaan perustuvassa elimessä ja tekevät tarvittavat järjestelyt sitä varten. Isäntävaltio johtaa turvallisuusvalvontaa, jolleivät osallistuvat valtiot ole sopineet muista järjestelyistä tämän valvonnan suhteen.

[7] Osaamiskeskukset, jotka Pohjois-Atlantin neuvosto on hyväksynyt asiakirjan PO(2020)0038 (INV) mukaisesti.

c) Jos osaamiskeskusta / yhteisymmärryspöytäkirjaan perustuvaa elintä ei ole aktivoitu Naton sotilaselimeksi (eikä Pohjois-Atlantin neuvosto siten ole myöntänyt sille kansainvälistä asemaa), mutta se on akkreditoitu Naton osaamiskeskukseksi / yhteisymmärryspöytäkirjaan perustuvaksi elimeksi, sovelletaan Naton turvallisuussääntöjä. Vaikka osallistuvat valtiot vastaavat kaikista osaamiskeskuksen / yhteisymmärryspöytäkirjaan perustuvan elimen turvallisuusasioista, isäntävaltio johtaa turvallisuusvalvontaa, jolleivät osallistuvat valtiot ole sopineet muista järjestelyistä tämän valvonnan suhteen. Osaamiskeskuksen / yhteisymmärryspöytäkirjaan perustuvan elimen perustamista koskevassa yhteisymmärryspöytäkirjassa esitetään, miten tämä toteutetaan osaamiskeskuksessa / yhteisymmärryspöytäkirjaan perustuvassa elimessä.

d) Jos jonkin Naton jäsenvaltion monikansallista yksikköä ei ole akkreditoitu osaamiskeskukseksi eikä aktivoitu Naton sotilaselimeksi, mutta se käyttää Naton turvallisuusluokiteltua tietoa, sovelletaan Naton turvallisuussääntöjä ja osallistuvat valtiot vastaavat turvallisuusasioista. Jos osallistujina on Naton ulkopuolisia valtioita, näiden kanssa on tehtävä turvallisuussopimus ennen kuin turvallisuusluokiteltua tietoa voidaan vaihtaa. Tällaisissa tapauksissa isäntävaltio johtaa turvallisuusvalvontaa, jolleivät osallistuvat valtiot ole sopineet muista järjestelyistä tämän valvonnan suhteen. Monikansallisen yksikön perustamista koskevassa yhteisymmärryspöytäkirjassa esitetään, miten tämä toteutetaan monikansallisessa yksikössä.

TURVALLISUUSKOORDINOINTI

14. Naton jäsenvaltioiden kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten ja Naton sotilas- tai siviilielinten välinen Naton turvallisuusasia, jota ei voida ratkaista, tai Naton turvallisuussääntöjen toteuttamista tai tulkintaa koskeva asia saatetaan Naton turvallisuustoimiston ratkaistavaksi. Jos asian saattavat turvallisuustoimiston ratkaistavaksi sotilasviranomaiset, tämä tehdään komentoketjujen kautta. Ratkaisemattomat erimielisyydet Naton turvallisuustoimisto antaa turvallisuuskomitean käsiteltäväksi.

TURVALLISUUSSÄÄNTÖJEN MUUTTAMINEN

15. Naton jäsenvaltioiden ja Naton sotilas- ja siviilielinten ehdotukset Naton turvallisuussääntöjen muuttamiseksi tulisi toimittaa ensisijaisesti Naton turvallisuustoimiston käsiteltäväksi. Sotilasviranomaisten tekemät ehdotukset välitetään komentoketjujen kautta. Naton turvallisuustoimisto käsittelee ehdotukset, ja tarvittaessa ne esitetään turvallisuuskomitealle jatkokäsittelyä varten. Tämä kohta ei estä Naton jäsenvaltioiden kansallisia turvallisuusviranomaisia / määrättyjä turvallisuusviranomaisia tekemästä virallisesti ehdotuksia turvallisuuskomitealle, jos ne niin tahtovat.

LIITE C

HENKILÖSTÖTURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään henkilöstöturvallisuutta koskevat periaatteet ja vähimmäisvaatimukset. Lisätietoja ja vaatimuksia löytyy Naton turvallisuussääntöjä tukevasta henkilöstöturvallisuusdirektiivistä (AC/35-D/2000).

2. Henkilöstöturvallisuusmenettelyt suunnitellaan sellaisiksi, että niillä pystytään selvittämään, voiko henkilölle hänen lojaalisuutensa, rehellisyytensä ja luotettavuutensa huomioon ottaen myöntää pääsyn turvallisuusluokiteltuun tietoon ilman, että siitä aiheutuu turvallisuusriski, jota ei voida hyväksyä. Tämä edellyttää, että kaikki siviili- ja sotilashenkilöt[1], joiden velvollisuudet tai tehtävät edellyttävät pääsyä turvallisuusluokkaan CONFIDENTIAL[2] ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, on tutkittava asianmukaisesti, jotta saavutetaan riittävä luottamuksen taso heidän edellytyksistään päästä turvallisuusluokiteltuun tietoon, ja heillä on tämän johdosta oltava kansallinen henkilöturvallisuusselvitystodistus (PSC).[3]

3. Saadakseen pääsyn Naton turvallisuusluokkaan NATO CONFIDENTIAL (NC) ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon henkilöllä on oltava voimassa oleva asianmukaisen tason kansallinen henkilöturvallisuusselvitystodistus sekä asianmukaisen kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen vahvistus siitä, että kyseiselle henkilölle voidaan myöntää pääsy Naton turvallisuusluokiteltuun tietoon.

TIEDONSAANTITARPEEN PERIAATTEEN SOVELTAMINEN

4. Naton jäsenvaltioiden ja Naton siviili- ja sotilaselinten henkilöillä on pääsy vain sellaiseen Naton turvallisuusluokiteltuun tietoon, johon heillä on tiedonsaantitarve. Kenelläkään ei ole yksinomaan aseman tai viran tai henkilöturvallisuusselvitystodistuksen perusteella pääsyä Naton turvallisuusluokiteltuun tietoon.

HENKILÖTURVALLISUUSSELVITYSTODISTUKSET (PSC)

5. Naton turvallisuussäännöt eivät edellytä henkilöturvallisuusselvitystodistusta turvallisuusluokkaan NATO RESTRICTED (NR) kuuluvaan tietoon pääsyyn.[4] Henkilöiden, jotka tarvitsevat pääsyn ainoastaan turvallisuusluokkaan NATO RESTRICTED kuuluvaan tietoon, on saatava ohjeistusta heidän turvallisuusvelvoitteistaan Naton turvallisuusluokitellun tiedon[5] suojaamisen osalta, heidän on annettava vakuutuksensa turvallisuutta koskevasta vastuustaan kirjallisesti

---

[1] Poikkeuksena ne valtion ylimpien tehtävien haltijat, joihin viitataan tämän liitteen kohdassa 7.

[2] Jotkin Naton jäsenvaltiot edellyttävät kansallisten säädösten ja määräysten mukaisesti henkilöturvallisuusselvityksen turvallisuusluokkaan RESTRICTED tai vastaavaan kansalliseen turvallisuusluokkaan kuuluvaan tietoon pääsyä varten.

[3] Henkilöturvallisuusselvitys (PSC) on kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen tai muun toimivaltaisen turvallisuusviranomaisen myönteinen arvio, jolla tunnustetaan luonnollisen henkilön kelpoisuus päästä turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon ottaen huomion henkilön lojaalius, rehellisyys ja luotettavuus.

[4] Jotkin Naton jäsenvaltiot voivat kansallisten säädöstensä ja määräystensä mukaisesti vaatia henkilöturvallisuusselvitystä turvallisuusluokkaan NATO RESTRICTED kuuluvaan tietoon pääsyä varten.

[5] Jäsenvaltiot voivat käyttää joko Naton omaa ohjeistusta tai vastaavaa kansallista ohjeistusta, jos jälkimmäisessä korostetaan näiden kahden turvallisuuskehyksen vaatimusten eroja.

tai vastaavalla kiistämättömyyden varmistavalla tavalla ja heillä on oltava myös tiedonsaantitarve.

6. Asianmukainen henkilöturvallisuusselvitystodistus tarvitaan silloin, kun henkilöt tehtäviään suorittaessaan pääsevät tai saattavat päästä turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon. Lisäksi henkilöiltä edellytetään:

   a) tiedonsaantitarvetta;

   b) saatua ohjeistusta turvallisuusvelvoitteistaan Naton turvallisuusluokitellun tiedon suojaamisen osalta;

   c) vakuutuksen antamista turvallisuutta koskevasta vastuustaan joko kirjallisesti tai vastaavalla kiistämättömyyden varmistavalla tavalla.

7. Edellä olevista 5 ja 6 kohdasta poiketen valtion ylimpien tehtävien haltijoiden (esimerkiksi valtion- ja hallitusten päämiehet, ministerit, kansanedustajat, oikeuslaitoksen jäsenet) pääsy Naton turvallisuusluokiteltuun tietoon perustuu kansallisiin säädöksiin ja määräyksiin; tällaisia henkilöitä on ohjeistettava heidän turvallisuusvelvoitteistaan, ja heillä on oltava tiedonsaantitarve.

8. Vaadittavan henkilöturvallisuusselvitystodistuksen taso ja siten tehtyjen turvallisuusselvitysmenettelyjen laajuus määräytyvät sen perusteella, mihin turvallisuusluokkaan kuuluvaan Naton turvallisuusluokiteltuun tietoon henkilön on saatava pääsy. Naton turvallisuusluokiteltuun tietoon pääsyn saaneiden henkilöiden tai virantoimituksessaan tai tehtävissään tietoon mahdollisesti pääsevien henkilöiden edellytyksistä on oltava sovittu luottamuksen taso.

9. Henkilöturvallisuusselvitystodistuksen myöntämistä ei tule pitää henkilöstöturvallisuusmenettelyn viimeisenä vaiheena; vaatimuksena on varmistaa henkilön jatkuvat edellytykset päästä Naton turvallisuusluokiteltuun tietoon. Tämä saavutetaan, kun turvallisuusviranomaiset ja -johtajat osallistavat henkilöitä tehokkaasti ja arvioivat heitä säännöllisesti. Tähän sisältyy sellaisten henkilön olosuhteissa tai käyttäytymisessä tapahtuvien muutosten arviointi, joilla voi olla turvallisuusvaikutuksia. Lisäksi, turvallisuuskoulutus- ja tietoisuusohjelmien tehokkaalla käytöllä muistutetaan henkilöitä heidän turvallisuutta koskevasta vastuustaan ja heidän velvollisuudestaan ilmoittaa johtajilleen tai turvallisuushenkilöstölle tietoja, jotka voivat vaikuttaa heidän turvallisuusstatukseensa.

Poikkeukselliset olosuhteet

10. Voi syntyä tilanteita, joissa joitain 6 kohdan vaatimuksista ei voida täyttää esimerkiksi kiireellisestä operaatiosta johtuen. Väliaikaisia nimityksiä sekä tilapäisesti tai kiireellisyyssyistä myönnettyä pääsyä koskevat käytännöt määritellään tarkemmin Naton turvallisuussääntöjä tukevassa henkilöstöturvallisuusdirektiivissä.

Vastuut

11. Henkilöturvallisuusselvitystodistuksen käsittely kuuluu sille Naton jäsenvaltioille, jonka kansalaista selvitys koskee. Tähän sisältyy vaatimus siitä, että jäsenvaltiot varmistavat, että niiden henkilöstöturvallisuusselvitystodistusta koskevat menettelyt täyttävät tutkinnalliset vähimmäisvaatimukset ja perusteet, joilla arvioidaan henkilön lojaaliutta, rehellisyyttä ja luotettavuutta henkilöturvallisuusselvitystodistuksen myöntämistä varten sekä henkilöturvallisuusselvitystodistuksen uusimisen vaatimukset, jotka määritellään henkilöstöturvallisuusdirektiivissä.

12. Naton siviili- ja sotilaselimet vastaavat henkilöstönsä henkilöturvallisuusselvitystodistushakemusten ja uusimispyyntöjen jättämisestä asianomaiselle kansalliselle turvallisuusviranomaiselle tai määrätylle turvallisuusviranomaiselle tai muulle toimivaltaiselle turvallisuusviranomaiselle.

13. Kansallisten turvallisuusviranomaisten tai määrättyjen turvallisuusviranomaisten tai

muiden toimivaltaisten turvallisuusviranomaisten, Naton jäsenvaltioiden ja Naton siviili- tai sotilaselinten päälliköiden yksityiskohtaiset vastuut on määritelty henkilöstöturvallisuusdirektiivissä.

TURVALLISUUSKOULUTUS JA -TIETOISUUS

14. Kaikkia henkilöitä, jotka työskentelevät tehtävissä, joissa heillä on pääsy turvallisuusluokkaan NATO RESTRICTED kuuluvaan tietoon tai joilla on henkilöturvallisuusselvitystodistus, joka antaa heille pääsyn turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, on ohjeistettava turvallisuusmenettelyistä ja heidän turvallisuusvelvoitteistaan. Kaikkien turvallisuusselvitettyjen henkilöiden on vakuutettava ymmärtävänsä täysin vastuunsa ja heihin mahdollisesti kohdistuvat seuraukset siitä, että Naton turvallisuusluokiteltua tietoa joutuu luvattomiin käsiin joko tahallisesti tai huolimattomuudesta. Tiedon tästä vakuutuksesta säilyttää se Naton jäsenvaltio tai Naton siviili- tai sotilaselin, joka on myöntänyt pääsyn Naton turvallisuusluokiteltuun tietoon.

15. Kaikille henkilöille, joille on myönnetty pääsy Naton turvallisuusluokiteltuun tietoon tai joiden edellytetään käsittelevän sitä, on aluksi tiedotettava ja säännöllisin väliajoin muistutettava niistä turvallisuusuhkista, joita voi aiheuttaa muun muassa:

    a) henkilöiden käyttäytyminen työpaikan ulkopuolella, mukaan lukien sosiaalisen median käyttö;

    b) varomattomat keskustelut sellaisten henkilöiden kanssa, joilla ei ole tiedonsaantitarvetta;

    c) työskentely työpaikan ulkopuolella ja matkustaessa;

    d) kyberuhkat;

    e) henkilöiden suhde tiedotusvälineisiin; ja

    f) Natoon ja Naton jäsenvaltioihin kohdistuvasta tiedustelutoiminnasta aiheutuva uhka.

16. Luonnollisten henkilöiden on välittömästi ilmoitettava asianomaisille turvallisuusviranomaisille epäilyttävinä tai epätavanomaisina pitämistään yhteydenotoista tai toimista.

LIITE D

TOIMITILATURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään periaatteet ja vähimmäisvaatimukset, jotka koskevat fyysisiä turvallisuustoimenpiteitä Naton turvallisuusluokitellun tiedon suojaamiseksi. Lisätietoja ja vaatimuksia löytyy Naton turvallisuussääntöjä tukevasta toimitilaturvallisuutta koskevasta direktiivistä (AC/35-D/2001).

2. Toimitilaturvallisuudella tarkoitetaan fyysisten suojatoimenpiteiden toteuttamista kohteissa, rakennuksissa, tiloissa tai laitteistoissa, joissa on turvallisuusluokiteltua tietoa, jota on suojeltava katoamiselta tai vaarantumiselta.

3. Naton jäsenvaltioiden ja Naton siviili- ja sotilaselinten on laadittava aktiivisia ja passiivisia turvallisuustoimenpiteitä sisältävät toimitilaturvallisuuden ohjelmat, joilla saavutetaan yhteinen toimitilaturvallisuuden taso, joka vastaa suojattavan tiedon uhkista, haavoittuvuuksista, turvallisuusluokituksesta ja määrästä tehtyä arviota.

TURVALLISUUSVAATIMUKSET

4. Kaikki kohteet, rakennukset, tilat, toimistot, huoneet ja muut alueet, joissa Naton turvallisuusluokiteltua tietoa säilytetään ja/tai käsitellään ja/tai joissa siitä keskustellaan, on suojattava asianmukaisin fyysisin turvallisuustoimenpitein. Tarvittavasta toimitilaturvallisuuden suojauksen tasosta päätettäessä on otettava huomioon kaikki siihen vaikuttavat tekijät, kuten:

   a) turvallisuusluokituksen taso ja tietoluokka;

   b) säilytettävän ja/tai käsiteltävän turvallisuusluokitellun tiedon määrä ja muoto (paperi- ja/tai sähköinen muoto);

   c) kulunvalvonta ja tiedonsaantitarpeen periaatteen täytäntöönpano;

   d) Natoon ja/tai Naton jäsenvaltioihin kohdistuvasta vihamielisestä tiedustelutoiminnasta aiheutuva uhka sekä paikallisesti arvioitu terrorismin, vakoilun, sabotaasin, kumouksellisen toiminnan ja (järjestäytyneen) rikollisuuden uhka; ja

   e) turvallisuusluokitellun tiedon tallennustavat (esimerkiksi paperiasiakirja tai sähköinen ja salattu).

5. Fyysisten turvallisuustoimenpiteiden tarkoituksena on

   a) estää tunkeutuminen salaa tai väkisin;

   b) ehkäistä, estää ja havaita sisäpiiriuhkan toimet;

   c) mahdollistaa Naton turvallisuusluokiteltuun tietoon pääsevän henkilöstön erottelu sen perusteella, minkä tasoinen henkilöturvallisuusselvitystodistus heillä on ja mikä heidän tiedonsaantitarpeensa on; ja

   d) havaita kaikki tietoturvapoikkeamat ja ryhtyä niiden osalta tarvittaviin toimenpiteisiin mahdollisimman nopeasti.

TOIMITILATURVALLISUUTTA KOSKEVAT YLEISET VAATIMUKSET

6. Fyysiset toimenpiteet ovat vain osa suojaavaa turvallisuutta, ja niitä tukemassa on oltava vakaat henkilöstöturvallisuuden, tietoturvallisuuden ja viestintä- ja tietojärjestelmien turvallisuustoimenpiteet. Turvallisuusriskien järkevään hallintaan kuuluu, että luodaan oikeasuhteisimmat, tehokkaimmat ja kustannusvaikuttavimmat keinot torjua uhkia ja kompensoida haavoittuvuuksia näiden alojen suojatoimenpiteitä

yhdistäen. Tehokkuus ja kustannusvaikuttavuus saavutetaan parhaiten määrittelemällä toimitilaturvallisuuden vaatimukset osana tilojen suunnittelua ja rakentamista, mikä vähentää kalliiden peruskorjausten tarvetta.

7. Toimitilaturvallisuuden ohjelmien on perustuttava syvyyssuuntaisen turvallisuuden periaatteeseen, ja niissä on käytettävä asianmukaista yhdistelmää täydentäviä fyysisiä turvallisuustoimenpiteitä, jotka tarjoavat sellaisen suojan tason, joka täyttää organisaation ja sen tietojen kriittisyyteen ja haavoittuvuuteen liittyvät vaatimukset.

8. Vaikka fyysiset turvallisuustoimenpiteet ovat kohdekohtaisia ja ne perustuvat useisiin tekijöihin, niiden tulee noudattaa seuraavia yleisiä periaatteita:

   a) ensin on tunnistettava suojattavat resurssit. Tämän jälkeen luodaan kerroksellisia turvallisuustoimenpiteitä, joilla rakennetaan syvyyssuuntainen turvallisuus ja viivyttävät tekijät;

   b) uloimmat fyysiset turvallisuustoimenpiteet rajaavat suojatun alueen ja estävät luvattoman pääsyn;

   c) seuraava toimenpiteiden taso havaitsee luvattoman pääsyn tai sen yrityksen ja varoittaa vartiointihenkilöstöä; ja

   d) sisin toimenpiteiden taso viivyttää tunkeilijoita niin kauan, että vartiointihenkilöstö voi heidät pidättää. Näin ollen vartijoiden vasteaika ja tunkeilijoiden viivyttämiseen suunnitellut fyysiset turvallisuustoimenpiteet liittyvät toisiinsa.

9. Fyysisen turvallisuuden laitteet (kuten kameravalvonta, tunkeutumisen ilmaisujärjestelmä, turvakaapit) on huollettava säännöllisesti tai erityisestä syystä sen varmistamiseksi, että ne toimivat parhaalla mahdollisella tavalla. Yksittäisten turvallisuustoimenpiteiden tehokkuutta sekä koko turvallisuusjärjestelmää on myös tarpeen arvioida määräajoin uudelleen. Tämä on erityisen tärkeää, jos kohteen käytössä tai erityisissä turvallisuusjärjestelmän osissa tapahtuu muutoksia. Tämä voidaan saavuttaa turvallisuussuunnitelmien säännöllisellä harjoittelulla.

Turva-alueet

10. Pysyvät tai tilapäiset alueet, joilla turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa säilytetään tai käsitellään tai joissa siitä keskustellaan, on järjestettävä ja jäsennettävä siten, että ne vastaavat jotakin seuraavista:

    a) **Naton luokan I turva-alue**: erityisen arkaluonteinen alue, jossa turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa säilytetään ja/tai käsitellään ja/tai siitä keskustellaan siten, että alueelle tulo merkitsee käytännössä Naton turvallisuusluokiteltuun tietoon pääsyä, jolloin luvaton tulo alueelle olisi tietoturvaloukkaus.

       Tällaisia alueita voivat olla operaatiotilat, viestintäkeskukset tai arkistotilat, ja niissä täytyy olla:

       i) selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos;

       ii) kulunvalvontajärjestelmä, joka päästää alueelle vain henkilöt, joilla on asianmukainen turvallisuusselvitys ja erityinen lupa[1] tulla alueelle;

[1] Erityisen luvan haltijoilla tarkoitetaan henkilöstöä, joilla on muodollisesti tunnustettu tiedonsaantitarve ja pääsy tietoon työtehtäviensä luonteen perusteella ja jotka ovat kulunvalvontalistalla, sekä henkilöitä, jotka kyseessä olevan organisaation päällikkö on tapauskohtaisesti muodollisesti valtuuttanut suorittamaan tiettyä tehtävää.

iii) määrittely turvallisuusluokituksen tasosta ja alueella tavanomaisesti säilytettävän tiedon luokasta eli siitä tiedosta, johon alueelle tulo antaa pääsyn; ja

iv) selkeä maininta siitä, että alueelle tulo vaatii paikallisen turvallisuusviranomaisen erityisen luvan. Tämä maininta voi sisältää tiedon turvallisuusluokituksen tasosta ja/tai alueen arkaluonteisuudesta.

b) **Naton luokan II turva-alue**: alue, jolla turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa säilytetään ja/tai käsitellään ja/tai siitä keskustellaan siten, että ulkopuolisten henkilöiden pääsy tietoon voidaan estää sisäisesti perustetuin valvontajärjestelmin. Tällaisia alueita voivat olla työskentelytilat tai neuvotteluhuoneet, joissa Naton turvallisuusluokiteltua tietoa säilytetään, ja/tai käsitellään ja/tai siitä keskustellaan. Näillä alueilla täytyy olla:

i) selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos;

ii) kulunvalvontajärjestelmä, joka päästää alueelle ilman saattajaa vain henkilöt, joilla on asianmukainen turvallisuusselvitys ja lupa tulla alueelle; ja

iii) saattaja tai vastaava valvontamekanismi, jonka avulla järjestetään sellaisten henkilöiden kulku, jotka eivät täytä edellä b) ii) alakohdassa kuvattuja perusteita, jotta voidaan estää luvaton pääsy Naton turvallisuusluokiteltuun tietoon ja hallitsematon pääsy alueille, jotka on nimenomaisesti nimetty teknisiltä hyökkäyksiltä ja salakuuntelulta suojatuiksi alueiksi.

Hallinnollinen vyöhyke

11. Naton luokan I tai II turva-alueiden ympärille tai niille johtavalle alueelle on perustettava hallinnollinen vyöhyke. Hallinnollisilla vyöhykkeillä sallitaan vain turvallisuusluokkaan NATO RESTRICTED kuuluvan tiedon säilyttäminen ja/tai käsittely ja/tai siitä keskusteleminen. Tällaisilla alueilla on oltava selkeästi määritetyt näkyvät rajat, joilla on mahdollisuus tarkastaa henkilöt ja ajoneuvot. Henkilöt eivät kuitenkaan tarvitse saattajaa.

Teknisesti suojatut turva-alueet

12. Teknisesti suojatut turva-alueet ovat joko pysyviä tai tilapäisiä alueita, jotka on nimenomaisesti tunnistettu teknisiltä hyökkäyksiltä ja salakuuntelulta suojattaviksi alueiksi. Tällaisilla alueilla on tehtävä säännöllisiä fyysisiä ja teknisiä tarkastuksia, ja niille kulkua on valvottava tarkasti. Teknisiltä hyökkäyksiltä ja salakuuntelulta on suojauduttava seuraavilla toimenpiteillä:

a) Asianmukainen fyysisten ja teknisten turvallisuustoimenpiteiden taso kulunvalvonnan toteuttamiseksi riskiin perustuen. Riskin määrittämisen vastuun jakavat asianmukaiset tekniset asiantuntijat sekä turvallisuusviranomainen, joka neuvoo riskin omistajaa päätöksentekoon tai hyväksymiseen liittyen.

b) Tällaiset alueet on lukittava ja/tai niitä on vartioitava silloin, kun niitä ei käytetä, ja kaikkia avaimia tulee käsitellä turva-avaimina. Alueella on tehtävä säännöllisiä fyysisiä ja/tai teknisiä tarkastuksia asianmukaisen turvallisuusviranomaisen vaatimusten mukaisesti. Tarkastuksia on tehtävä myös luvattoman alueelle tulon tai sen epäilyn jälkeen sekä ulkopuolisen henkilöstön (esimerkiksi huoltotöiden tai remontin vuoksi) alueelle tulon jälkeen.

c) Näille alueille ei saa tuoda mitään esineitä, kalusteita tai laitteita ennen kuin koulutettu turvallisuushenkilöstö on tutkinut ne salakuuntelulaitteiden varalta. Kaikista alueelle tuoduista tai viedyistä esineistä, kalusteista ja laitteista on

pidettävä asianmukaista luetteloa.

d) Alueilla ei saa olla tallentavia ja/tai lähettäviä elektronisia järjestelmiä tai laitteita.

e) Alueille ei yleensä saa asentaa puhelimia ja muita videoneuvottelulaitteita. Jos niiden asentaminen kuitenkin on välttämätöntä, ne tulee irrottaa verkosta, kun tilassa keskustellaan turvallisuusluokitelluista asioista. Tämä ei koske asianmukaisesti asennettuja ja hyväksyttyjä viestintävälineitä.

ERITYISET FYYSISET TURVALLISUUSTOIMENPITEET

13. Erilaiset erityiset fyysiset ja tekniset turvallisuustoimenpiteet ja -menettelyt voivat edistää organisaation tai kohteen turvallisuuskehystä. Tällaisiin toimiin ja menettelyihin kuuluvat muun muassa: rajattu-alue, tunkeutumisen ilmaisujärjestelmä, kulunvalvonta, kameravalvonta, turvavalaistus, turvakaapit ja toimistokalusteet, lukot, avainten ja numeroyhdistelmien valvonta, vierailijahallinta, sisään- ja ulostulotarkastukset. Tarkempia tietoja erityisistä fyysisistä ja teknisistä turvallisuustoimenpiteistä ja -menettelyistä on Naton turvallisuussääntöjä tukevassa toimitilaturvallisuutta koskevassa direktiivissä.

NATON TURVALLISUUSLUOKITELLUN TIEDON SÄILYTTÄMISEN VÄHIMMÄISVAATIMUKSET

14. Naton turvallisuusluokiteltua tietoa on säilytettävä alueilla, turvakaapeissa ja/tai toimistokalusteissa, jotka on suunniteltu estämään ja havaitsemaan luvattoman pääsyn tietoon.

15. **COSMIC TOP SECRET (CTS)**. Turvallisuusluokkaan COSMIC TOP SECRET kuuluva tieto on säilytettävä luokan I tai II turva-alueella noudattaen jotain seuraavista ehdoista:

    a) hyväksytyssä turvakaapissa soveltaen ainakin yhtä seuraavista lisävalvontakeinoista:

        i) jatkuva suojaus turvallisuusselvitetyn vartiointihenkilöstön tai päivystyshenkilöstön toimesta;

        ii) turvakaapin tarkastus vähintään kahden tunnin välein satunnaisin väliajoin turvallisuusselvitetyn vartiointihenkilöstön tai päivystyshenkilöstön toimesta; tai

        iii) hyväksytty tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan turvakaapin poistamiseen tai murtamiseen tai käytössä olevien fyysisten turvallisuustoimenpiteiden nujertamiseen;

    b) toimitilaturvallisuutta koskevan direktiivin vaatimusten mukaisesti rakennetulla avoimella varastoalueella, jossa on tunkeutumisen ilmaisujärjestelmä sekä hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan alueelle väkisin tunkeutumiseen; tai

    c) tunkeutumisen ilmaisujärjestelmällä varustetussa kassaholvissa, jonka lisäksi on oltava hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan kassaholviin väkisin tunkeutumiseen.

16. **NATO SECRET (NS)**. Turvallisuusluokkaan NATO SECRET kuuluva tieto on säilytettävä luokan I tai II turva-alueella jollakin seuraavalla tavalla:

    a) siten kuin turvallisuusluokkaan COSMIC TOP SECRET kuuluvan tiedon säilyttämisestä on määrätty;

b) hyväksytyssä turvakaapissa tai kassaholvissa ilman lisävalvontakeinoja; tai

c) avoimella varastoalueella, jolloin edellytetään ainakin yhtä seuraavista lisävalvontakeinoista:

i) avoimen varastoalueen sijoitustilaa suojaa jatkuvasti turvallisuusselvitetty vartiointihenkilöstö tai päivystyshenkilöstö;

ii) turvallisuusselvitetty vartiointihenkilöstö tai päivystyshenkilöstö tarkastaa avoimen varastoalueen vähintään kerran neljän tunnin välein; tai

iii) tunkeutumisen ilmaisujärjestelmä, jonka lisäksi on oltava hälytyksiin vastaava turvallisuushenkilöstö, joka hälytyksen saatuaan saapuu paikalle siinä ajassa, jonka arvioidaan kuluvan alueelle väkisin tunkeutumiseen.

17. **NATO CONFIDENTIAL (NC)**. Turvallisuusluokkaan NATO CONFIDENTAL kuuluva tieto on säilytettävä luokan I tai II turva-alueella hyväksytyssä turvakaapissa.

18. **NATO RESTRICTED (NR)**. Turvallisuusluokkaan NATO RESTRICTED kuuluva tieto on säilytettävä lukitussa kaapissa tai toimistokalusteessa (esimerkiksi toimistopöydän laatikossa) hallinnollisella vyöhykkeellä, luokan I turva-alueella tai luokan II turva-alueella. Turvallisuusluokkaan NATO RESTRICTED kuuluvaa tietoa voidaan säilyttää myös lukitussa kaapissa, kassaholvissa tai avoimella varastoalueella, joka on hyväksytty turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään turvallisuusluokkaan kuuluvan tiedon säilyttämiseen.

19. Lisätietoja ja -vaatimuksia Naton turvallisuusluokitellun tiedon säilyttämisestä annetaan Naton turvallisuussääntöjä tukevassa toimitilaturvallisuutta koskevassa direktiivissä.

VIESTINTÄ- JA TIETOJÄRJESTELMIEN FYYSINEN SUOJAAMINEN

20. Alueet, joilla Naton turvallisuusluokiteltua tietoa esitetään tai käsitellään tietotekniikkaa käyttäen, tai joilla on mahdollista päästä sellaiseen tietoon, on perustettava niin, että luottamuksellisuuden, eheyden ja käytettävyyden kokonaisvaatimus täyttyy.

21. Alueet, joilla viestintä- ja tietojärjestelmiä käytetään turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempiin turvallisuusluokkiin kuuluvan tiedon näyttämiseen, tallentamiseen, käsittelyyn tai siirtämiseen tai joissa on mahdollista päästä sellaiseen tietoon, on perustettava Naton luokan I tai II turva-alueena tai vastaavan kansallisen tason alueena. Alueet, joilla viestintä- ja tietojärjestelmiä käytetään turvallisuusluokkaan NATO RESTRICTED kuuluvan tiedon näyttämiseen, tallentamiseen, käsittelyyn tai siirtämiseen tai joilla on mahdollista päästä sellaiseen tietoon, voidaan perustaa hallinnollisina vyöhykkeinä.

22. Pääsyä alueille, joilla säilytetään ja hallitaan kriittisiä viestintä- ja tietojärjestelmien osia, on nimenomaisesti valvottava, ja pääsy on rajoitettava koskemaan vain sellaista turvallisuuteen ja järjestelmä-/verkko-/salaushallintaan liittyvää henkilöstöä, jolla on lupa olla alueella.

SUOJAAMINEN TEKNISILTÄ HYÖKKÄYKSILTÄ

23. Työskentelytilat tai alueet, joissa säännöllisesti keskustellaan turvallisuusluokkaan NATO SECRET tai sitä ylempiin turvallisuusluokkiin kuuluvasta tiedosta, on suojattava passiivisia ja aktiivisia salakuunteluhyökkäyksiä vastaan luotettavilla fyysisillä turvallisuustoimenpiteillä ja kulunvalvonnalla, kun riski sitä edellyttää. Vastuu riskin määrittämisestä tulee koordinoida teknisten asiantuntijoiden kanssa, ja siitä päättää asianmukainen turvallisuusviranomainen. Lisätietoja passiiviselta ja aktiiviselta salakuuntelulta suojautumisesta on Naton turvallisuussääntöjä tukevassa toimitilaturvallisuutta koskevassa direktiivissä.

HYVÄKSYTYT LAITTEET

24. Naton jäsenvaltioiden tulee käyttää vain sellaisia laitteita, jotka asianmukainen turvallisuusviranomainen on hyväksynyt Naton turvallisuusluokitellun tiedon suojaamiseen. Naton siviili- ja sotilaselinten on varmistettava, että hankitut laitteet on hyväksytty käyttöön vastaavissa olosuhteissa jossakin Naton jäsenvaltiossa. Naton siviili- ja sotilaselimet voivat myös hankkia asianmukaisen turvallisuusviranomaisen käyttöön hyväksymiä laitteita, kun hankinta perustuu tehtyyn riskinarviointiin, joka tukee tunnistetun riskin tai tunnistettujen riskien vähentämistä tai lieventämistä.

LIITE E

NATON TURVALLISUUSLUOKITELLUN TIEDON TURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään Naton turvallisuusluokitellun tiedon turvallisuutta koskevat periaatteet ja vähimmäisvaatimukset. Lisätietoja ja -vaatimuksia on Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta (AC/35-D/2002).

2. Tietoturvallisuus on yleisten suojaustoimenpiteiden ja -menettelyjen soveltamista turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, sekä katoamisen tai vaarantumisen havaitsemiseksi ja korjaamiseksi. Turvallisuusluokiteltua tietoa on suojattava koko sen elinkaaren ajan sen turvallisuusluokan mukaisella tasolla. Tietoa hallittaessa varmistetaan, että se on asianmukaisesti luokiteltu, selvästi määritetty turvallisuusluokitelluksi ja pysyy turvallisuusluokiteltuna ainoastaan niin kauan kuin tämä on tarpeen. Tietoturvallisuutta täydennetään henkilöstöturvallisuudella, toimitilaturvallisuudella sekä viestintä- ja tietojärjestelmien turvallisuudella, jotta varmistetaan tasapainoinen toimenpiteiden kokonaisuus Naton turvallisuusluokitellun tiedon suojaamiseksi.

NATON TURVALLISUUSLUOKAT, ERITYISET TUNNUKSET, MERKINNÄT JA YLEISET PERIAATTEET

3. Alkuperäinen luovuttaja vastaa turvallisuusluokitellun tiedon turvallisuusluokan määrittämisestä ja tiedon alustavasta jakelusta.

4. Turvallisuusluokkaa ei saa vaihtaa eikä alentaa eikä turvallisuusluokitusta saa poistaa ilman alkuperäisen luovuttajan suostumusta. Turvallisuusluokkaa määrittäessään alkuperäinen luovuttaja ilmoittaa mahdollisuuksien mukaan, voidaanko sitä alentaa tai voidaanko tiedon luokitus poistaa tiettynä ajankohtana tai tietyn tapahtuman jälkeen.

5. Tiedolle annettu turvallisuusluokka määrää sen, minkälaisella toimitilaturvallisuudella ja viestintä- ja tietojärjestelmien turvallisuudella tietoa suojataan sitä säilytettäessä, siirrettäessä, välitettäessä, jaettaessa ja hävitettäessä sekä minkälaista henkilöturvallisuusselvitystodistusta pääsy kyseiseen tietoon edellyttää. Siksi tosiasiallisen turvallisuuden ja tehokkuuden vuoksi on vältettävä tiedon luokittelemista sekä liian korkeaan että liian alhaiseen turvallisuusluokkaan.

6. Turvallisuusluokat merkitään turvallisuusluokiteltuun tietoon osoittamaan sitä vahinkoa, joka Naton ja/tai sen jäsenvaltioiden turvallisuudelle voi aiheutua, jos tieto altistuu luvattomalle ilmitulolle. Turvallisuusluokitellun tiedon alkuperäisellä luovuttajalla on etuoikeus määrätä turvallisuusluokka tai muuttaa sitä. Naton turvallisuusluokat ja niiden merkitykset ovat seuraavat:

   a) COSMIC TOP SECRET (CTS)

   luvaton ilmitulo aiheuttaisi Natolle poikkeuksellisen vakavaa vahinkoa;

   b) NATO SECRET (NS)

   luvaton ilmitulo aiheuttaisi Natolle vakavaa vahinkoa;

   c) NATO CONFIDENTIAL (NC)

   luvaton ilmitulo aiheuttaisi Natolle vahinkoa; ja

   d) NATO RESTRICTED (NR)

luvaton ilmitulo haittaisi Naton etuja tai sen toiminnan tehokkuutta.

7. Naton turvallisuusluokat osoittavat Naton turvallisuusluokitellun tiedon arkaluonteisuuden, ja niitä sovelletaan tarkoituksena kiinnittää vastaanottajien huomio tarpeeseen varmistaa tiedon suojaaminen sen vahingon vakavuuden mukaan, joka luvattomasta pääsystä tietoon tai sen luvattomasta ilmitulosta aiheutuisi.

8. Ryhmään NATO UNCLASSIFIED kuuluvaa tietoa ja julkista tietoa suojataan ja käsitellään Naton tiedonhallinnan periaatteiden (C-M(2007)0118) ja Naton turvallisuusluokittelemattoman tiedon hallintaa koskevan asiakirjan (C-M(2002)60) mukaisesti.

9. Naton operaatioiden, koulutuksen, harjoitusten, transformaation ja yhteistyön (OTETC) suunnittelu, valmistelu, toteuttaminen ja tukeminen voi edellyttää myös tiettyjen muiden turvallisuusnäkökulmien huomioon ottamista; Naton turvallisuussääntöjä tukeva asiakirja tiedustelutiedon ja muun tiedon jakamisesta muiden kuin Natoon kuuluvien toimijoiden kanssa (AC/35-D/1040) sisältää näissä tilanteissa sovellettavat turvallisuusmääräykset ja -ohjeet.

10. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet toteuttavat toimenpiteet, joilla varmistetaan, että Naton tuottamalle ja Natolle annettavalle turvallisuusluokitellulle tiedolle määritetään oikea turvallisuusluokka ja että tämä tieto suojataan Naton turvallisuussääntöjä tukevan Naton turvallisuusluokitellun tiedon turvallisuutta koskevan direktiivin vaatimusten mukaisesti.

11. Kukin Naton sotilas- ja siviilielin ottaa käyttöön järjestelmän, jonka avulla varmistetaan, että sen luovuttamaa turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa arvioidaan uudelleen vähintään viiden vuoden välein ja luokkaan NATO SECRET luokiteltua tietoa vähintään 10 vuoden välein tarkoituksena tarkistaa, onko turvallisuusluokkia edelleen sovellettava. Tätä arviointia ei tarvita, jos alkuperäinen luovuttaja on määrännyt ennalta, että tietyn Naton turvallisuusluokitellun tiedon turvallisuusluokkaa alennetaan ilman eri toimenpiteitä ennalta määrätyn ajan jälkeen, ja jos tämä on merkitty kyseiseen tietoon.

12. Koko asiakirjan turvallisuusluokan on oltava vähintään yhtä korkea kuin sen korkeimmalle turvallisuusluokitellun osan luokka. Kansiasiakirjoihin on merkittävä niihin liitettyyn tietoon kokonaisuutena sovellettava Naton turvallisuusluokka. Mahdollisuuksien mukaan alkuperäisen luovuttajan olisi asianmukaisesti merkittävä turvallisuusluokkaan NATO RESTRICTED ja sitä ylempiin turvallisuusluokkiin luokiteltujen asiakirjojen osat, kuten kappaleet, liitteet, lisäykset jne., helpottaakseen päätöksiä asiakirjojen jakelusta eteenpäin.

13. Kun suuri määrä Naton turvallisuusluokiteltua tietoa kootaan yhteen, sen alkuperäiset turvallisuusluokitusmerkinnät on säilytettävä ja on arvioitava, miten tämän tietokokonaisuuden katoaminen tai vaarantuminen vaikuttaisi järjestöön. Jos tämä kokonaisvaikutus arvioidaan suuremmaksi kuin kyseisten yksittäisten Naton turvallisuusluokkien mukainen vaikutus, olisi harkittava kyseisen tietokokonaisuuden käsittelemistä ja suojaamista sen turvallisuusluokan mukaisesti, joka vastaa sen katoamisen tai vaarantumisen arvioitua vaikutusta.

Lisämerkinnät

14. COSMIC ja NATO ovat Natoon viittaavia merkintöjä, jotka Naton turvallisuusluokiteltuun tietoon tehtyinä osoittavat, että tietoa on suojattava Naton turvallisuusperiaatteiden mukaisesti.

Erityisluokkien tunnukset

15. "ATOMAL" on merkintä, joka tehdään erityisluokan tietoon osoittamaan, että tieto on

suojattava Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä tehdyn sopimuksen (C-M(64)39) ja sitä tukevien hallinnollisten järjestelyjen (C-M(68)41) mukaisesti.

16. "SIOP" on merkintä, joka tehdään erityisluokan tietoon osoittamaan, että tiedon suojaamisessa on noudatettava asiakirjaa C-M(71)27(Revised), joka koskee erityismenettelyjä Yhdysvaltojen yhteistä operaatiosuunnitelmaa (US-SIOP) koskevan tiedon käsittelemiseksi Natossa.

17. "CRYPTO" on merkintä ja erityisluokan tunnus, joka merkitään kaikkeen COMSEC-avainmateriaaliin, jota käytetään suojaamaan tai todentamaan televiestintää, joka sisältää Naton salausten turvallisuuteen liittyvää tietoa ja joka osoittaa, että tieto on suojattava asianmukaisten salausturvallisuusperiaatteiden ja -ohjeiden mukaisesti.

18. "BOHEMIA" on merkintä, joka tehdään viestitiedustelusta saatuun tai siihen liittyvään erityisluokan tietoon. Kaikki merkinnällä COSMIC TOP SECRET – BOHEMIA merkitty tieto suojataan noudattaen tarkasti asiakirjaa MC 101 (Naton signaalitiedustelun periaatteet) ja siihen liittyvää liittokunnan yhteistä AJP-julkaisua, jossa käsitellään sovellettavia periaatteita, sekä Naton signaalitiedustelun neuvoa-antavan komitean SIGINT-hallinnon ja -menettelyjen oppaan määräyksiä.

Merkinnät jakelun rajoittamisesta

19. Tiedon alkuperäinen luovuttaja voi käyttää merkintää jakelun rajoittamisesta lisämerkintänä, jolla Naton turvallisuusluokitellun tiedon jakelua rajoitetaan tarkemmin.

VALVONTA JA KÄSITTELY

Tilivelvollisuuden tavoitteet

20. Tilivelvollisuuden ensisijaisena tavoitteena on saada käyttöön riittävät tiedot, joiden avulla pystytään tutkimaan tahallinen tai tahaton tilivelvollisuuden alaisen tiedon katoaminen tai vaarantuminen sekä arvioimaan katoamisesta tai vaarantumisesta aiheutunut vahinko. Tilivelvollisuuden vaatimuksen tarkoituksena on kurinalaisuus tilivelvollisuuden alaisen tiedon käsittelyssä ja siihen pääsyn valvonnassa.

21. Tilivelvollisuuden vaatimuksen toissijaisina tavoitteina on

    a) seurata pääsyä tilivelvollisuuden alaiseen tietoon: kenellä on tosiasiallisesti tai mahdollisesti ollut pääsy tällaiseen tietoon, ja kuka on yrittänyt päästä siihen;

    b) pysyä selvillä tilivelvollisuuden alaisen tiedon sijainnista;

    c) seurata tilivelvollisuuden alaisen tiedon liikkeitä Natossa ja kansallisesti; ja

    d) pitää kirjaa Naton ulkopuolisille toimijoille luovutetusta tilivelvollisuuden alaisesta tiedosta.

22. Luokkiin COSMIC TOP SECRET, NATO SECRET ja ATOMAL luokiteltu tieto on tilivelvollisuuden alaista, ja sitä on valvottava ja käsiteltävä noudattaen tämän liitteen vaatimuksia sekä Naton turvallisuusluokitellun tiedon turvallisuutta koskevaa tätä liitettä tukevaa direktiiviä. Jos kansalliset säädökset ja määräykset sitä edellyttävät, sellainen tieto, johon on merkitty muu turvallisuusluokka tai erityisluokan merkintä, voidaan katsoa tilivelvollisuuden alaiseksi tiedoksi.

Rekisterijärjestelmä

23. Rekisterijärjestelmän turvallisuusmenettelyjä ja -vaatimuksia sovelletaan yhtäläisesti sekä fyysisessä että sähköisessä ympäristössä. Sähköistä ympäristöä koskevia lisätietoja ja -vaatimuksia on tämän C-M-asiakirjan liitteessä F ja tätä asiakirjaa tukevissa ohjeissa.

24. Käytössä on oltava rekisterijärjestelmä, joka vastaa tilivelvollisuuden alaisen tiedon vastaanottamisesta, kirjaamisesta, käsittelystä, jakelusta ja hävittämisestä. Tämä vastuu voidaan täyttää joko käyttämällä yhtä rekisterijärjestelmää, jolloin turvallisuusluokkaan COSMIC TOP SECRET ja muuhun erityisluokkaan luokiteltu tieto on kaikkina aikoina pidettävä tarkasti osastoituna, tai perustamalla erilliset rekisterit ja valvontapisteet.

25. Tapauksen mukaan kukin Naton jäsenvaltio ja Naton sotilas- ja siviilielin perustaa yhden tai useamman turvallisuusluokkaan COSMIC TOP SECRET luokitellun tiedon keskusrekisterin, joka toimii sen jäsenvaltion tai elimen vastaanottavana ja lähettävänä pääviranomaisena, johon rekisteri on perustettu. Tällainen keskusrekisteri voi toimia myös tilivelvollisuuden alaisen muun tiedon rekisterinä.

26. Rekisterit ja valvontapisteet toimivat vastuuorganisaatioina turvallisuusluokkiin COSMIC TOP SECRET ja NATO SECRET luokitellun tiedon sisäisessä jakelussa sekä kaiken kyseisen rekisterin tai valvontapisteen vastuulla olevan tilivelvollisuuden alaisen tiedon kirjaamisessa; ne voidaan perustaa ministeriöiden, osastojen tai komento-osastojen tasolle. Turvallisuusluokkiin NATO CONFIDENTIAL ja NATO RESTRICTED luokiteltua tietoa ei tarvitse kirjata rekisterijärjestelmään, jolleivät kansalliset säädökset ja määräykset tätä edellytä.

27. Rekisterien ja valvontapisteiden on kaikkina aikoina pystyttävä paikantamaan Naton tilivelvollisuuden alaisen tiedon sijainti. Harvoin sallittava ja tilapäinen pääsy tällaiseen tietoon ei välttämättä edellytä rekisterin tai valvontapisteen perustamista, jos käytössä on menettelyt, joilla varmistetaan, että tieto pysyy rekisterijärjestelmän valvonnassa.

28. Turvallisuusluokkaan COSMIC TOP SECRET luokitellun tiedon jakelun on tapahduttava COSMIC-rekisterin välityksellä. Kunkin rekisterin on vähintään kerran vuodessa luetteloitava kaikki turvallisuusluokkaan COSMIC TOP SECRET luokiteltu tieto, josta rekisteri on tilivelvollinen, noudattaen Naton turvallisuusluokitellun tiedon turvallisuutta koskevan Naton turvallisuussääntöjä tukevan direktiivin vaatimuksia. Rekisteriorganisaation tyypistä riippumatta niiden organisaatioiden, jotka käsittelevät turvallisuusluokkaan COSMIC TOP SECRET luokiteltua tietoa, on nimettävä COSMIC-tiedon valvoja (CCO).

29. Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta käsitellään muun muassa COSMIC-tiedon valvojan tehtäviä, turvallisuusluokkiin COSMIC TOP SECRET ja NATO SECRET luokitellun tiedon yksityiskohtaisia käsittelyprosesseja rekisterijärjestelmässä, Naton turvallisuusluokitellun tiedon jäljennöksiä, käännöksiä ja otteita koskevia menettelyjä, sen jakelua ja lähettämistä koskevia vaatimuksia sekä sen hallussapitoa ja hävittämistä koskevia vaatimuksia.

30. Sotilaskomitea on perustanut erillisen järjestelmän salausaineistoa koskevan tilivelvollisuuden täyttämistä sekä salausaineiston valvontaa ja jakelua varten. Tämän järjestelmän kautta välitettävä aineisto ei edellytä tilivelvollisuuden täyttämistä rekisterijärjestelmässä.

VALMIUSSUUNNITTELU

31. Naton jäsenvaltiot ja Naton sotilas- ja siviilielimet laativat valmiussuunnitelmat Naton turvallisuusluokitellun tiedon suojaamiseksi ja hävittämiseksi poikkeusolojen aikana estääkseen luvattoman pääsyn tähän tietoon sekä sen luvattoman ilmitulon ja sen käytettävyyden estymisen. Nämä suunnitelmat perustuvat määräajoin tarkistettaviin uhka-arvioihin, ja niissä asetetaan etusijalle arkaluonteisin sekä tehtävän tai ajan kannalta ratkaisevin tieto.

TIETOTURVAPOIKKEAMAT

32. Tietoturvapoikkeama on tapahtuma tai muu tilanne, joka voi vaikuttaa haitallisesti Naton turvallisuusluokitellun tiedon turvallisuuteen ja joka edellyttää tarkempia tutkintatoimia, jotta voidaan todeta tarkasti, onko kyseessä tietoturvaloukkaus vai vähäinen tietoturvapoikkeama.

Tietoturvaloukkaus

33. Tietoturvaloukkaus on tahallinen tai tahaton teko tai laiminlyönti, joka on näiden turvallisuussääntöjen vastainen ja voi johtaa Naton turvallisuusluokitellun tiedon tai sitä tukevien palvelujen ja resurssien tosiasialliseen tai mahdolliseen vaarantumiseen.

Vaarantuminen

34. Vaarantuminen tarkoittaa tilannetta, jossa tietoturvaloukkauksen tai haitallisen toiminnan vuoksi Naton turvallisuusluokiteltu tieto on menettänyt luottamuksellisuutensa, eheytensä tai käytettävyytensä tai tätä tietoa tukevat palvelut ja resurssit ovat menettäneet eheytensä tai käytettävyytensä. Vaarantumiseen sisältyvät katoaminen, ilmitulo asiattomille, luvaton muuttaminen, hävittäminen luvattomalla tavalla ja palvelun estyminen.

Vähäinen tietoturvapoikkeama

35. Vähäinen tietoturvapoikkeama on tahallinen tai tahaton teko tai laiminlyönti, joka on näiden turvallisuussääntöjen vastainen, mutta ei johda Naton turvallisuusluokitellun tiedon tosiasialliseen tai mahdolliseen vaarantumiseen.

36. Kaikista tosiasiallisista ja mahdollisista tietoturvaloukkauksista on ilmoitettava viipymättä toimivaltaiselle turvallisuusviranomaiselle. Kaikki ilmoitetut tietoturvaloukkaukset on tutkittava sellaisten henkilöiden toimesta, joilla on asiantuntemusta turvallisuuden, tutkinnan ja tarvittaessa vastatiedustelun alalla ja jotka ovat riippumattomia niistä henkilöistä, joita tietoturvaloukkaus välittömästi koskee. Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta selostetaan yksityiskohtaisesti toimia, jotka on toteutettava todettaessa tietoturvaloukkaus tai vähäinen tietoturvapoikkeama.

ILMOITTAMINEN

37. Naton turvallisuusluokiteltuun tietoon kohdistuneiden tietoturvaloukkausten ja vaarantumisten ilmoittamisella pyritään ensisijaisesti antamaan tiedon luovuttaneelle Naton organisaatiolle mahdollisuus arvioida Natolle aiheutunut vahinko ja ryhtyä tarpeellisiksi katsottaviin tai mahdollisiin toimenpiteisiin vahingon minimoimiseksi. Kansallinen turvallisuusviranomainen / määrätty turvallisuusviranomainen tai kyseisen Naton sotilas- tai siviilielimen johtaja välittää tiedot vahingon arvioinnista ja vahingon mimimoimiseksi tehdyistä toimenpiteistä Naton turvallisuustoimistolle.

38. Ilmoittavan viranomaisen olisi mahdollisuuksien mukaan ilmoitettava asiasta tiedon luovuttaneelle Naton organisaatiolle samaan aikaan kuin Naton turvallisuustoimistolle, mutta Naton turvallisuustoimistoa voidaan pyytää tekemään ilmoitus, jos alkuperäistä luovuttajaa on vaikea selvittää. Naton turvallisuustoimistolle tehtävien ilmoitusten ajoitus riippuu tiedon arkaluonteisuudesta ja olosuhteista.

39. Naton turvallisuustoimisto voi Naton pääsihteerin puolesta pyytää toimivaltaisia viranomaisia tutkimaan asiaa tarkemmin ja ilmoittamaan havainnoistaan Naton turvallisuustoimistolle. Olosuhteista ja vaarantumisen vakavuudesta riippuen Naton turvallisuustoimisto voi ilmoittaa asiasta turvallisuuskomitealle.

40. Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta käsitellään tietoturvaloukkauksiin ja turvallisuuden vaarantumisiin liittyviä yksityiskohtaisia toimia, kirjauksia ja ilmoittamista koskevia vaatimuksia

41. Sotilaskomitea on antanut Naton jäsenvaltioiden viestintäturvallisuusviranomaisille ja

Naton sotilas- ja siviilielimille erilliset määräykset salausaineiston vaarantumisesta.

LIITE F

VIESTINTÄ- JA TIETOJÄRJESTELMIEN TURVALLISUUS

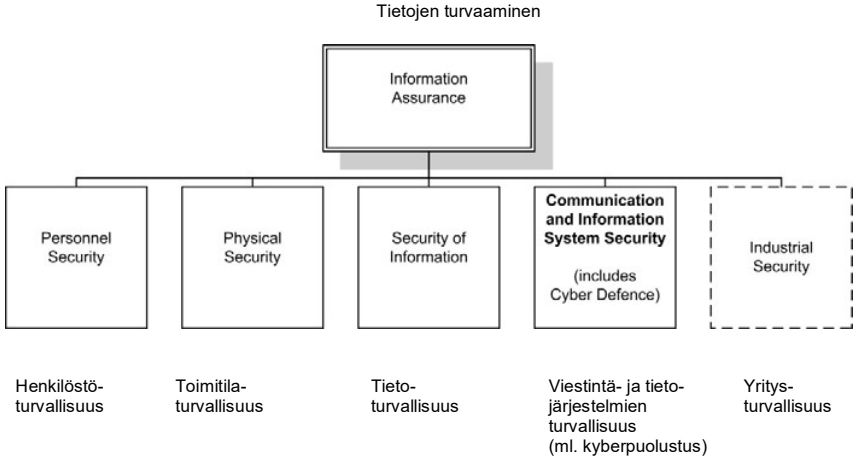
1. JOHDANTO

1.1. Tässä liitteessä esitetään periaatteet ja vähimmäisvaatimukset, jotka koskevat Naton turvallisuusluokitellun tiedon sekä sitä tukevien järjestelmäpalvelujen ja resurssien[1] suojaamista viestinnässä, tallennettaessa tätä tietoa tietojärjestelmiin ja muihin sähköisiin järjestelmiin sekä käsiteltäessä ja siirrettäessä sitä näissä järjestelmissä.

1.2. Tämä liite tukee Naton tiedonhallinnan periaatteita ja täydentää Naton turvallisuusluokittelemattoman tiedon hallinnan periaatteita, joissa käsitellään niitä perusperiaatteita ja vaatimuksia, joita Naton sotilas- ja siviilielimissä sekä Naton jäsenvaltioissa sovelletaan Naton turvallisuusluokittelemattoman tiedon suojaamiseksi.

1.3. Viestintä- ja tietojärjestelmien turvallisuus (CIS Security) on yksi tietojen turvaamisen (kuva 1) osatekijöistä, ja sillä tarkoitetaan turvatoimien soveltamista tarkoituksena suojata viestinnän, tietojärjestelmien ja muiden sähköisten järjestelmien[2] sekä näihin järjestelmiin tallennettavan ja niissä käsiteltävän ja siirrettävän[3] tiedon luottamuksellisuutta, eheyttä, käytettävyyttä, aitoutta ja kiistämättömyyttä.

1.4. Jotta saavutetaan näissä viestintä- ja tietojärjestelmissä käsiteltävän turvallisuusluokitellun tiedon luottamuksellisuuden, eheyden, käytettävyyden, aitouden ja kiistämättömyyden turvallisuustavoitteet[4], toteutetaan tasapainoinen toimitila-, henkilöstö- ja tietoturvallisuutta sekä viestintä- ja tietojärjestelmien turvallisuutta koskevien toimenpiteiden kokonaisuus turvallisen käyttöympäristön aikaansaamiseksi näille järjestelmille. Kun yritykset käsittelevät turvallisuusluokiteltua tietoa sopimusten perusteella, sovelletaan lisäksi erityisiä yritysturvallisuustoimia tämän C-M-asiakirjan liitteen G ja sitä tukevan yritysturvallisuusdirektiivin mukaisesti.



Kuva 1 – Suhde tietojen turvaamisen ja viestintä- ja tietojärjestelmien turvallisuuden välillä

[1] Tietoa tukevilla järjestelmäpalveluilla ja resursseilla tarkoitetaan niitä palveluja ja resursseja, jotka tarvitaan varmistamaan, että viestintä- ja tietojärjestelmien turvallisuustavoitteet saavutetaan; näitä palveluja ja resursseja ovat esimerkiksi salaustuotteet ja -menetelmät, COMSEC-aineisto, luettelopalvelut sekä käyttöympäristön järjestelyt ja valvonta.

[2] Jäljempänä tässä liitteessä "CIS".

[3] Jäljempänä tässä liitteessä "käsiteltävä".

[4] Jäljempänä tässä liitteessä "turvallisuustavoitteet".

1.5. Viestintä- ja tietojärjestelmien turvallisuuden päädirektiivissä, jonka turvallisuuskomitea (SC) ja tiedonvälityksen, johtamisen ja valvonnan ohjausryhmä (C3B) ovat julkaisseet näiden turvallisuussääntöjen tueksi, käsitellään näitä järjestelmiä koskevia turvallisuustoimia niiden elinkaaren aikana sekä komiteoiden ja Naton sotilas- ja siviilielinten vastuuta näiden järjestelmien turvallisuudesta. Viestintä- ja tietojärjestelmien turvallisuuden päädirektiiviä tukevat direktiivit, joissa käsitellään viestintä- ja tietojärjestelmien turvallisuuden hallintaa (kuten turvallisuusriskien hallintaa, turvallisuuden akkreditointia, turvallisuuteen liittyvää dokumentointia ja turvallisuuden uudelleenarviointia/tarkastamista) sekä viestintä- ja tietojärjestelmien turvallisuuden teknisiä ja toteuttamiseen liittyviä näkökohtia (kuten tietokoneiden ja lähiverkkojen turvallisuutta, yhteen liitettyjen verkkojen turvallisuutta, salaukseen perustuvaa turvallisuutta, tiedonsiirron turvallisuutta ja hajasäteilyn turvallisuutta).

2. TURVALLISUUSTAVOITTEET

2.1. Viestintä- ja tietojärjestelmissä käsiteltävän Naton turvallisuusluokitellun tiedon suojaamiseksi asianmukaisesti määritetään ja toteutetaan tasapainoinen toimitila- ja henkilöstöturvallisuuden, tietoturvallisuuden sekä viestintä- ja tietojärjestelmien turvallisuuden toimenpiteiden kokonaisuus turvallisen ympäristön luomiseksi näiden järjestelmien toiminnalle ja seuraavien turvallisuustavoitteiden saavuttamiseksi:

a) varmistetaan Naton turvallisuusluokitellun tiedon luottamuksellisuus valvomalla tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien paljastamista ja pääsyä niihin;

b) varmistetaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien eheys;

c) varmistetaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien käytettävyys;

d) varmistetaan niiden henkilöiden, laitteiden ja palvelujen luotettava määrittäminen ja tunnistaminen, jotka pääsevät Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin; ja

e) varmistetaan tietoa käsitelleiden henkilöiden ja toimijoiden asianmukainen kiistämättömyys.

2.2. Naton turvallisuusluokiteltu tieto sekä sitä tukevat järjestelmäpalvelut ja resurssit suojataan vähintään toimenpidekokonaisuudella, jonka tarkoituksena on varmistaa yleinen suojaus yleisesti esiintyviltä (tahattomilta tai tahallisilta) ongelmilta, joiden tiedetään vaikuttavan kaikkiin järjestelmiin ja tietoa tukeviin järjestelmäpalveluihin ja resursseihin. Olosuhteiden mukaan ryhdytään muihin toimenpiteisiin, jos turvallisuusriskien arvioinnissa on todettu, että Naton turvallisuusluokiteltuun tietoon ja/tai sitä tukeviin järjestelmäpalveluihin ja resursseihin kohdistuu tiettyjen uhkien ja haavoittuvuuksien vuoksi aiempaa suurempia riskejä.

2.3. Käsiteltävän Naton tiedon turvallisuusluokasta riippumatta Naton turvallisuusviranomaiset arvioivat riskit ja sen vahingon tason, joka Natolle aiheutuu, jos toimenpiteet muiden turvallisuustavoitteiden kuin luottamuksellisuuden saavuttamiseksi laiminlyödään. Muun kuin luottamuksellisuuden varmistavia palveluja koskevien toimenpiteiden vähimmäiskokonaisuus määritetään näitä turvallisuussääntöjä tukevien direktiivien mukaisesti.

3. TURVALLISUUDEN AKKREDITOINTI

3.1. Se, missä määrin turvallisuustavoitteet on saavutettava ja missä määrin viestintä- ja tietojärjestelmiin kohdistuvia turvallisuustoimenpiteitä tarvitaan Naton

turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien suojaamiseksi, määritellään kyseistä turvallisuusvaatimusta laadittaessa. Turvallisuuden akkreditoinnilla todetaan, että riittävä suojauksen taso on saavutettu ja sitä ylläpidetään.

3.2. Kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien kansallisten viestintä- ja tietojärjestelmien osalta suoritetaan turvallisuuden akkreditointi, jossa käsitellään turvallisuustavoitteita.

4. HENKILÖSTÖTURVALLISUUS

4.1. Henkilöt, joille sallitaan pääsy Naton turvallisuusluokiteltuun tietoon sen jossakin muodossa, on turvallisuusselvitettävä, ottaen tarvittaessa huomioon heidän kokonaisvastuunsa tietoa ja sitä tukevia järjestelmäpalveluja ja resursseja koskevien turvallisuustavoitteiden saavuttamisesta. Näitä henkilöitä ovat myös ne, joille sallitaan pääsy tietoa tukeviin järjestelmäpalveluihin ja resursseihin tai jotka vastaavat niiden suojauksesta, vaikkei heille sallittaisikaan pääsyä järjestelmässä käsiteltävään tietoon.

5. TOIMITILATURVALLISUUS

5.1. Alueet, joilla Naton turvallisuusluokiteltua tietoa esitetään tai käsitellään tietotekniikkaa käyttäen tai joilla on mahdollista päästä sellaiseen tietoon, on perustettava siten, että turvallisuustavoitteiden saavuttamisen kokonaisvaatimus täyttyy.

6. TIETOTURVALLISUUS

6.1. Kaikki turvallisuusluokitellut tietokoneiden tallennusvälineet on merkittävä, säilytettävä ja suojattava asianmukaisesti, tallennettavan tiedon korkeimman turvallisuusluokan mukaan.

6.2. Uudelleen käytettävälle tietokoneen tallennusvälineelle tallennetun Naton turvallisuusluokitellun tiedon saa poistaa tallennusvälineeltä ainoastaan toimivaltaisen turvallisuusviranomaisen hyväksymiä menettelyjä noudattaen.

6.3. Tietokoneen tallennusvälineelle tallennetun Naton turvallisuusluokitellun tiedon suojaamiseen voidaan soveltaa näitä turvallisuussääntöjä tukevien direktiivien mukaisesti toteutettavia hyväksyttyjä (luottamuksellisuutta ja muuta kuin luottamuksellisuutta koskevia) turvatoimia siten, että toimitilaturvallisuuden vaatimuksia lievennetään alempaa turvallisuusluokkaa vastaaviksi.

7. YRITYSTURVALLISUUS

7.1 Sopimusten toteuttamiseen käytettävä hankeosapuolen toimitila, jossa käsitellään Naton turvallisuusluokiteltua tietoa viestintä- ja tietojärjestelmissä, on perustettava siten, että se täyttää turvallisuustavoitteiden saavuttamisen kokonaisvaatimuksen.

7.2. Tapauksen mukaan sopimuksissa, turvallisuusnäkökohtia koskevissa kirjeissä (SAL) ja/tai ohjelman/hankkeen turvallisuusohjeissa (PSI) ja/tai palvelutasosopimuksissa (SLA) on selostettava johdonmukainen viestintä- ja tietojärjestelmiin kohdistuvien turvatoimien kokonaisuus, joka hankeosapuolten on toteutettava saavuttaakseen Naton viestintä- ja tietojärjestelmien turvallisuustavoitteet ja suojatakseen Naton turvallisuusluokitellun tiedon ja sitä tukevat palvelut.

8. TURVATOIMET

8.1. Kaikkiin Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin on

sovellettava johdonmukaista turvallisuustoimenpiteiden kokonaisuutta, jotta saavutetaan tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien suojaamisen turvallisuustavoitteet. Näitä turvallisuustoimenpiteitä ovat tapauksen mukaan seuraavat:

a) keinot, joiden avulla saadaan riittävät tiedot, jotta pystytään tutkimaan mahdollisesti aiheutuvan vahingon edellyttämällä tavalla tahallinen tai tahaton turvallisuusluokiteltua tietoa ja sitä tukevia järjestelmäpalveluja ja resursseja koskevien turvallisuustavoitteiden vaarantuminen tai vaarantamisen yritys;

b) keinot, joiden avulla määritetään ja tunnistetaan luotettavasti henkilöt, laitteet ja palvelut, joille sallitaan pääsy tietoon, järjestelmäpalveluihin ja resursseihin. Tietoa ja aineistoa, jonka avulla säädellään pääsyä viestintä- tai tietojärjestelmään, on valvottava ja se on suojattava sitä tietoa vastaavien järjestelyjen mukaisesti, johon tieto tai aineisto voi mahdollistaa pääsyn. Naton viestintä- ja tietojärjestelmissä on sovellettava henkilöiden vahvan tunnistamisen menetelmää;

c) keinot, joiden avulla valvotaan tiedonsaantitarpeen periaatteen perusteella Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien paljastamista ja pääsyä niihin;

d) keinot, joiden avulla todennetaan Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien eheys ja alkuperä;

e) keinot, joiden avulla ylläpidetään Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien eheyttä;

f) keinot, joiden avulla ylläpidetään Naton turvallisuusluokitellun tiedon ja sitä tukevien järjestelmäpalvelujen ja resurssien käytettävyyttä;

g) keinot, joiden avulla valvotaan Naton turvallisuusluokiteltua tietoa käsittelevien viestintä- ja tietojärjestelmien yhteyttä;

h) viestintä- ja tietojärjestelmien suojausmenetelmien luotettavuuden toteaminen;

i) keinot, joiden avulla arvioidaan ja todennetaan viestintä- ja tietojärjestelmien turvallisuuden suojausmenetelmien asianmukainen toimivuus näiden järjestelmien elinkaaren ajan;

j) keinot, joiden avulla tutkia käyttäjien ja viestintä- ja tietojärjestelmien toimintaa;

k) keinot, joiden avulla annetaan takeet kiistämättömyydestä siten, että tiedon lähettäjälle todistetaan, että tieto on lähetetty, ja tiedon vastaanottajalle todistetaan lähettäjän identiteetti; ja

l) keinot, joiden avulla suojataan säilytettävä Naton turvallisuusluokiteltu tieto, jos fyysiset turvallisuustoimenpiteet eivät täytä vähimmäisvaatimuksia.

8.2. Käytössä on oltava turvallisuuden hallintajärjestelmät ja -menettelyt, joiden avulla estetään, torjutaan, havaitaan ja kestetään Naton turvallisuusluokiteltua tietoa ja sitä tukevia järjestelmäpalveluja ja resursseja koskeviin turvallisuustavoitteisiin vaikuttavien tapahtumien vaikutukset ja korjataan ne, mukaan lukien tietoturvapoikkeamista ilmoittaminen.

8.3. Turvallisuustoimenpiteitä hallitaan ja ne toteutetaan näitä turvallisuusääntöjä tukevien direktiivien mukaisesti.

9. TURVALLISUUSRISKIEN HALLINTA

9.1. Naton sotilas- ja siviilielimissä käytettäviin Naton turvallisuusluokiteltua tietoa käsitteleviin viestintä- ja tietojärjestelmiin sovelletaan turvallisuusriskien hallintaa,

mukaan lukien turvallisuusriskien arviointi, näitä turvallisuussääntöjä tukevien direktiivien vaatimusten mukaisesti.

9.2. Naton viestintä- ja tietojärjestelmien turvallisuusriskien hallinnalla varmistetaan järjestelmän haavoittuvuuksien ja turvallisuusvaatimustenmukaisuuden jatkuva arviointi, ja siinä on pyrittävä dynaamiseen riskienhallintaan, jotta voidaan reagoida tehokkaasti nykyisten monimutkaisten toimintaskenaarioiden ja monitahoisten uhkaympäristöjen asettamiin haasteisiin.

10. NATON TURVALLISUUSLUOKITELLUN TIEDON SÄHKÖMAGNEETTINEN SIIRTÄMINEN[5]

10.1. Kun Naton turvallisuusluokiteltua tietoa siirretään sähkömagneettisesti, on toteutettava erityiset toimenpiteet turvallisuustavoitteiden saavuttamiseksi näissä siirroissa. Naton viranomaiset määräävät vaatimukset, joita sovelletaan siirrettävän tiedon suojaamiseksi ilmitulolta, sieppaamiselta tai hyväksikäytöltä.

11. SALAUKSEEN PERUSTUVA TURVALLISUUS

11.1. Kun luottamuksellisuuden ja muun kuin luottamuksellisuuden suojaamiseksi tarvitaan salaustuotteita tai -menetelmiä tiedon siirtämisen, käsittelyn tai säilyttämisen (data at rest) aikana, nämä tuotteet tai menetelmät on erikseen hyväksytettävä tätä tarkoitusta varten ja fyysisten, menettelyllisten ja teknisten toimenpiteiden on täytettävä erityiset salausta koskevat vaatimukset, jotta vaadittavat turvallisuustavoitteet saavutetaan.

11.2. Säilytettävä tieto on suojattava vaadittavien turvallisuustavoitteiden edellyttämää tasoa vastaavasti, ja käytettäessä salaustuotteita tai -menetelmiä on salausta koskevien turvallisuusvaatimusten oltava sovellettavien Naton teknisten ja täytäntöönpanoa koskevien direktiivien mukaiset.

11.3. Turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava Naton sotilaskomitean (NAVMILCOM) hyväksymillä salaustuotteilla tai -menetelmillä.

11.4. Turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokitellun tiedon luottamuksellisuus on tietoa siirrettäessä suojattava joko Naton sotilaskomitean tai Naton jäsenvaltion hyväksymillä salaustuotteilla tai -menetelmillä.

11.5. Tietoa siirrettäessä on muuta kuin luottamuksellisuutta koskevien vaatimusten täyttäminen varmistettava viestintäjärjestelmää koskevan käyttövaatimuksen mukaisesti. Salaustekniikkaan perustuvien muuta kuin luottamuksellisuutta koskevien menetelmien arviointia koskevat vaatimukset ja näiden menetelmien hyväksyntäviranomainen on yksilöitävä ja hyväksyttävä teknisissä direktiiveissä hyväksytyllä tavalla käyttövaatimukseen sisältyvien näitä menetelmiä koskevien vaatimusten yhteydessä.

11.6. Poikkeuksellisissa toimintaolosuhteissa turvallisuusluokkiin NATO CONFIDENTIAL ja NATO SECRET luokiteltu tieto voidaan siirtää selväkielisenä, jos kukin tällainen siirto raportoidaan asianmukaisesti ylemmille viranomaisille. Poikkeuksellisia olosuhteita ovat seuraavat:

a) kriisin uhka tai toteutuminen, selkkaus tai sotatila; ja

b) tilanteet, joissa lähetyksen nopeus on ensiarvoisen tärkeää, salauskeinoja ei ole käytettävissä ja arvioidaan, ettei siirrettävää tietoa ehditä käyttää ajoissa toiminnan haittaamiseen.

[5] "Sähkömagneettinen siirtäminen" tarkoittaa siirtämistä, joka on luonteeltaan tai ominaisuuksiltaan sekä sähköistä että magneettista, ja se sisältää muun muassa näkyvän valon, radioaallot, mikroaallot ja infrapunasäteilyn.

11.7. Poikkeuksellisissa toimintaolosuhteissa, joissa nopeus on ensiarvoisen tärkeää, salauskeinoja ei ole käytettävissä ja arvioidaan, ettei siirrettävää tietoa ehditä käyttää ajoissa toiminnan haittaamiseen, turvallisuusluokkaan NATO RESTRICTED luokiteltu tieto voidaan siirtää selväkielisenä.

11.8. Kun turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokiteltua tietoa siirretään Naton ja Naton ulkopuolisen valtion tai kansainvälisen järjestön (NNN/IO) viestintä- ja tietojärjestelmien välillä, tiedon luottamuksellisuus on siirron aikana suojattava Naton sotilaskomitean hyväksymillä salaustuotteilla tai -menetelmillä.

11.9. Kun turvallisuusluokkaan NATO SECRET ja sitä ylempiin luokkiin luokiteltua tietoa siirretään Naton ulkopuolisen valtion tai kansainvälisen järjestön viestintä- ja tietojärjestelmissä, tiedon luottamuksellisuus on siirron aikana suojattava Naton sotilaskomitean (NAVMILCOM) hyväksymillä salaustuotteilla tai -menetelmillä.

11.10. Jos 11.8 ja 11.9 kohdan vaatimuksia ei voida täyttää, Nato ja kansainvälinen järjestö voivat sopia, että ne hyväksyvät vastavuoroisesti toistensa arviointi- valinta- ja hyväksymismenettelyt, joita sovelletaan niihin salaustuotteisiin tai -menetelmiin, joiden käyttö sallitaan turvallisuusluokkaan NATO SECRET tai kansainvälisen järjestön vastaavaan turvallisuusluokkaan luokitellun tiedon suojaamiseksi sitä siirrettäessä. Tämän hyväksynnän ehdot on esitetty jäljempänä kohdassa 11.12.

11.11. Poikkeuksellisissa olosuhteissa, jos 11.8 ja 11.9 kohdan vaatimuksia ei voida täyttää, Nato voi tiettyjen käyttövaatimusten täyttämistä tukeakseen hyväksyä Naton ulkopuolisen valtion arviointi- valinta- ja hyväksymismenettelyt, joita sovelletaan niihin salaustuotteisiin tai -menetelmiin, joiden käyttö sallitaan turvallisuusluokkaan NATO SECRET tai Naton ulkopuolisen valtion vastaavaan turvallisuusluokkaan luokitellun tiedon suojaamiseksi sitä siirrettäessä. Tämän hyväksynnän ehdot on esitetty jäljempänä kohdassa 11.12.

11.12. Edellä 11.10 ja 11.11 kohdassa esitettyihin tilanteisiin sovelletaan seuraavia ehtoja:

a) Naton ulkopuolisella valtiolla tai kansainvälisellä järjestöllä on oltava voimassa Naton kanssa tehty turvallisuussopimus ja Naton turvallisuustoimiston todistus siitä, että ne pystyvät asianmukaisesti suojaamaan luovutettavaa Naton turvallisuusluokiteltua tietoa;

b) kutakin Naton ulkopuolista valtiota tai kansainvälistä järjestöä kohdellaan tapauskohtaisesti, ja kunkin hyväksynnän perusta määrätään Naton ja Naton ulkopuolisen valtion tai kansainvälisen järjestön välistä turvallisuussopimusta tukevissa turvallisuusjärjestelyissä;

c) hyväksynnän ehdot on hyväksytettävä Naton sotilaskomitealla Naton turvallisuustoimiston tekemän puolueettoman arvion pohjalta; tämä arvio koskee Naton ulkopuolisen valtion tai kansainvälisen järjestön valmiutta tehdä salausta koskevia arvioita, jotka täyttävät vastaavat vaatimukset kuin Naton vaatimukset turvallisuusluokkaan NATO SECRET luokitellun tiedon suojaamiselle salauksen avulla; arvion tekee Naton turvallisuustoimisto yhdessä sotilaskomitean viestintä- ja tietojärjestelmien turvallisuus- ja arviointiviraston (SECAN), tiedonvälityksen, johtamisen ja valvonnan ohjausryhmän tietojen turvaamista ja kyberpuolustusvalmiutta käsittelevän paneelin sekä Naton päämajan tiedonvälityksen, johtamisen ja valvonnan esikunnan kanssa; ja

d) Naton turvallisuustoimiston, SECANin ja Naton päämajan tiedonvälityksen, johtamisen ja valvonnan esikunnan on yhdessä vakuututtava todentamisen ja määräajoin tapahtuvan uudelleen todentamisen avulla siitä, että Naton ulkopuolisella valtiolla tai kansainvälisellä järjestöllä on käytössään asianmukaiset rakenteet, säännöt ja menettelyt salaustuotteiden ja -menetelmien arviointia, valintaa, hyväksyntää ja valvontaa varten ja että näitä

rakenteita, sääntöjä ja menettelyjä sovelletaan käytännössä tehokkaasti ja turvallisesti.

11.13. Kun hyväksyntä tapahtuu 11.12 kohdan ehtojen mukaisesti, turvallisuusluokkaan NATO SECRET luokitellun tiedon luottamuksellisuus voidaan suojata joko Naton sotilaskomitean hyväksymillä salaustuotteilla tai -menetelmillä tai sellaisilla salaustuotteilla tai -menetelmillä, jotka Naton ulkopuolisen valtion tai kansainvälisen järjestön kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen (tai vastaava viranomainen) on hyväksynyt vastaavan turvallisuusluokan tiedon suojaamiseen.

11.14. Kun turvallisuusluokkaan NATO CONFIDENTIAL tai NATO RESTRICTED luokiteltua tietoa siirretään Naton ja Naton ulkopuolisen valtion tai kansainvälisen järjestön viestintä- ja tietojärjestelmien välillä ja Naton ulkopuolisen valtion tai kansainvälisen järjestön viestintä- ja tietojärjestelmissä, tiedon luottamuksellisuus on siirron aikana suojattava toimivaltaisen viranomaisen hyväksymillä salaustuotteilla tai -menetelmillä. Toimivaltainen viranomainen voi olla Naton sotilaskomitea, Naton jäsenvaltion kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen tai Naton ulkopuolisen valtion tai kansainvälisen järjestön vastaava viranomainen, jos tällä valtiolla tai järjestöllä on käytössään asianmukaiset rakenteet, säännöt ja menettelyt kyseisten tuotteiden ja menetelmien arviointia, valintaa, hyväksyntää ja valvontaa varten ja jos näitä rakenteita, sääntöjä ja menettelyjä sovelletaan käytännössä tehokkaasti ja turvallisesti. Näistä rakenteista, säännöistä ja menettelyistä sovitaan Naton sotilaskomitean ja kyseisen Naton ulkopuolisen valtion tai kansainvälisen järjestön välillä.

11.15. Naton turvallisuusluokitellun tiedon suojaamiseen käytettävän salausaineiston arkaluonteisuus edellyttää erityisten turvatoimien soveltamista niiden toimien lisäksi, jotka vaaditaan Naton muun turvallisuusluokitellun tiedon suojaamiseksi.

11.16. Salausaineiston suojauksen on vastattava sitä vahinkoa, joka voi aiheutua, jos suojaus laiminlyödään. Käytössä on oltava positiiviset keinot, joilla arvioidaan ja todennetaan salaustuotteiden ja -menetelmien suojaaminen ja asianmukainen toiminta sekä salaustiedon (esim. toteuttamisen yksityiskohtien ja niihin liittyvän dokumentoinnin) suojaaminen ja hallinta.

11.17. Salaustiedon erityisen arkaluonteisuuden vuoksi Natossa ja kaikissa jäsenvaltioissa on oltava käytössä erityismääräykset ja -elimet, jotka säätelevät Naton salaustiedon vastaanottamista ja hallintaa sekä sen jakelua erikseen hyväksytyille henkilöille.

11.18. On myös noudatettava erityisiä menettelyjä, joilla säädellään teknisen tiedon jakamista sekä salaustuotteiden ja -menetelmien valintaa, tuottamista ja hankintaa.

12. HAJASÄTEILYTURVALLISUUS

12.1. On toteutettava turvatoimet, joilla suojataan turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltu tieto vaarantumiselta, joka johtuu tahattomasta sähkömagneettisesta hajasäteilystä. Toimenpiteiden on oltava hyväksikäytön riskin ja tiedon arkaluonteisuuden mukaiset.

13. VIESTINTÄ- JA TIETOJÄRJESTELMIÄ KOSKEVAT ERITYISET VASTUUT

13.1. Naton sotilaskomitea (NAVMILCOM)

13.1.1. Naton sotilaskomitean vastuulla viestintä- ja tietojärjestelmien turvallisuuden osalta on salauslaitteiden turvallisuuden hyväksyminen ja niiden luovuttaminen sekä osallistuminen salaustuotteiden ja -menetelmien arviointiin ja valintaan Naton tavanomaista käyttöä varten. Sotilaskomitean neljä virastoa (SECAN, DACAN, EUSEC

ja EUDAC), joissa on kansallinen henkilöstö, neuvovat ja tukevat viestintä- ja tietojärjestelmien turvallisuusasioissa sotilaskomiteaa, turvallisuuskomiteaa, tiedonvälityksen, johtamisen ja valvonnan ohjausryhmää sekä tarvittaessa näiden alaisia yksiköitä, jäsenvaltioita ja muita Naton organisaatioita.

13.2. **C3-ohjausryhmä (C3B)**

13.2.1. Liittokunnan ylimpänä alansa komiteana tiedonvälityksen, johtamisen ja valvonnan (C3) ohjausryhmä tukee Naton sotilaskomiteaa ja Naton poliittisia viranomaisia niiden C3-toiminnan valmiuksien ja hankkeiden arviointiprosessissa arvioimalla C3-toimintaa koskevia operatiivisia vaatimuksia. Ohjausryhmä vastaa turvallisten ja yhteentoimivien Naton laajuisten C3-järjestelmien saattamisesta käyttöön. Naton päämajan C3-esikunta antaa henkilöstöä C3-ohjausryhmän tueksi.

13.3. **Naton kyberpuolustuksen ohjausryhmä (CDMB)**

13.3.1. Kyberpuolustuksen ohjausryhmä on kyberpuolustusta koordinoiva elin, joka vastaa kyberpuolustuksen periaatteiden toteuttamisen strategisesta suunnittelusta ja ohjauksesta sekä Naton jäsenvaltioiden kanssa tehtävän yhteistyön edistämisestä. Kyberpuolustuksen ohjausryhmä raportoi Pohjois-Atlantin neuvostolle ja saa siltä poliittista ohjausta puolustuspolitiikan ja -suunnittelun komitean vahvistetun kokoonpanon (DPPC(R)) välityksellä. Jäsenvaltiot valvovat kyberpuolustuksen ohjausryhmää kyberpuolustuksen periaatteita ja C3-periaatteiden toteuttamista koskevissa asioissa C3-ohjausryhmän välityksellä. Kyberpuolustuksen ohjausryhmä neuvottelee yksittäisistä asioista toimivaltaisten Naton komiteoiden välityksellä.

13.4. **Kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen (NCSA)**

13.4.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio määrää kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen, joka voidaan perustaa virastoksi kansalliseen turvallisuusinfrastruktuuriin. Kansallisen viestintä- ja tietojärjestelmien turvallisuusviranomaisen vastuulla on

a) valvoa teknistä salaustietoa, joka liittyy Naton tiedon suojaamiseen kyseisessä valtiossa;

b) varmistaa, että Naton tiedon suojaamiseen käytettävät salausjärjestelmät, -tuotteet ja -menetelmät valitaan asianmukaisesti ja niitä käytetään ja ylläpidetään asianmukaisesti;

c) varmistaa, että Naton tiedon suojaamiseen käytettävät viestintä- ja tietojärjestelmien turvallisuustuotteet valitaan asianmukaisesti ja niitä käytetään ja ylläpidetään asianmukaisesti kyseisessä valtiossa;

d) olla yhteydessä toimivaltaisiin Naton elimiin ja kansallisiin elimiin viestintä- ja tietojärjestelmien turvallisuuteen liittyvissä Naton viestintäturvallisuutta ja tekniikkaa koskevissa asioissa sekä sotilas- että siviilialalla; ja

e) kansallisen TEMPEST-viranomaisen yksilöiminen tarvittaessa.

13.4.2. Kansallisten viestintä- ja tietojärjestelmien turvallisuusviranomaisten toiminta koordinoidaan kansallisten turvallisuusviranomaisten toiminnan kanssa.

13.5. **Kansallinen jakeluviranomainen (NDA)**

13.5.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio yksilöi kansallisen jakeluviranomaisen, joka voidaan perustaa virastoksi kansalliseen turvallisuusinfrastruktuuriin ja joka vastaa Naton salausaineiston hallinnasta kyseisessä valtiossa ja varmistaa, että kaiken salausaineiston kattavaa kirjaamista, turvallista käsittelyä, säilyttämistä, jakelua ja hävittämistä varten toteutetaan asianmukaiset menettelyt ja perustetaan tarvittavat kanavat.

13.5.2. Kansallisten jakeluviranomaisten toiminta koordinoidaan kansallisten turvallisuusviranomaisten toiminnan kanssa.

13.6. **Turvallisuuden akkreditointiviranomainen/viranomaiset**

13.6.1. Kukin Naton jäsenvaltio ja tapauksen mukaan Naton ulkopuolinen valtio määrää yhden tai useamman turvallisuuden akkreditointiviranomaisen, joka vastaa seuraavien turvallisuuden akkreditoinnista:

a) Naton turvallisuusluokiteltua tietoa käsittelevät kansalliset viestintä- ja tietojärjestelmät; ja

b)kansallisissa elimissä/organisaatioissa käytettävät Naton viestintä- ja tietojärjestelmät, tapauksen mukaan Naton ulkopuolisissa valtioissa.

13.6.2. Jos Naton jäsenvaltioon perustetaan Naton sotilas- tai siviilielin, Naton viestintä- ja tietojärjestelmien turvallisuuden akkreditoi Naton turvallisuuden akkreditointiviranomainen (SAA). Tällöin turvallisuuden akkreditointi voidaan koordinoida toimivaltaisen kansallisen turvallisuuden akkreditointiviranomaisen kanssa.

13.7. **Naton turvallisuuden akkreditointiviranomainen (SAA)**

13.7.1. Naton turvallisuusluokiteltua tietoa käsittelevien Naton viestintä- ja tietojärjestelmien turvallisuuden akkreditoinnista vastaa kolme Naton turvallisuuden akkreditointiviranomaista. Turvallisuuden akkreditointiviranomaiset ovat Naton turvallisuustoimiston johtaja ja strategiset komentajat tai heidän valtuutetut/nimetyt edustajansa, akkreditoitavan viestintä- tai tietojärjestelmän mukaan.

13.7.2. Naton viestintä- ja tietojärjestelmien turvallisuusjärjestelyjen hyväksyntälautakunta, joka koostuu edellisessä kohdassa tarkoitetuista Naton turvallisuuden akkreditointiviranomaisista, valvoo turvallisuuden akkreditointia kaikkien Naton turvallisuusluokiteltua tietoa käsittelevien Naton viestintä- ja tietojärjestelmien osalta varmistaakseen yhteisen ja johdonmukaisen lähestymistavan näiden järjestelmien turvallisuuteen. Hyväksyntälautakunnan työjärjestys hyväksytetään turvallisuuskomitealla.

13.8. **Naton ulkopuolisen valtion turvallisuusviranomainen**

13.8.1. Naton ulkopuolinen valtio nimeää turvallisuusviranomaisen vastaamaan tämän liitteen turvallisuusmääräysten noudattamisesta sekä valvonnasta, joka kohdistuu sellaisiin Naton ulkopuolisen valtion viranomaisiin, joilla on erityisiä turvallisuusvastuita Naton turvallisuusluokiteltua tietoa käsittelevistä kansallisista viestintä- ja tietojärjestelmistä (mukaan lukien kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen, kansallinen jakeluviranomainen ja turvallisuuden akkreditointiviranomaiset).

LIITE G

TURVALLISUUSLUOKITELTUJEN HANKKEIDEN TURVALLISUUS JA YRITYSTURVALLISUUS

JOHDANTO

1. Tässä liitteessä esitetään Naton turvallisuusluokitellun tiedon turvallisuutta yrityksissä koskevat periaatteet ja vähimmäisvaatimukset. Lisätietoja ja -vaatimuksia on Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

2. Yritysturvallisuus on suojaustoimien ja -menettelyjen soveltamista sellaisen turvallisuusluokitellun tiedon katoamisen tai vaarantumisen estämiseksi, havaitsemiseksi ja korjaamiseksi, jota yritykset käsittelevät hankesopimusten perusteella. Yrityksille annettava ja yritysten kanssa tehtävien hankesopimusten perusteella tuotettava Naton turvallisuusluokiteltu tieto sekä yritysten kanssa tehtävät turvallisuusluokitellut hankesopimukset on suojattava Naton turvallisuussääntöjen ja niitä tukevien direktiivien mukaisesti.

3. Kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten on varmistettava, että niillä on keinot määrätä yritysturvallisuutta koskevat vaatimuksensa yrityksiä sitoviksi sekä oikeus tarkastaa ja hyväksyä yritysten toimet turvallisuusluokitellun tiedon suojaamiseksi.

YRITYSTURVALLISUUTTA KOSKEVAT VAATIMUKSET

4. Kaikilla hankeosapuolilla / alihankkijoilla, jotka tekevät sellaisia hankesopimuksia, joihin liittyy Naton turvallisuusluokiteltua tietoa ja jotka edellyttävät pääsyä turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään luokkaan luokiteltuun tietoon tai tällaisen tiedon tuottamista, on oltava asianmukaisen tason yritysturvallisuusselvityksestä annettu todistus (FSC), jonka on antanut sen valtion toimivaltainen kansallinen turvallisuusviranomainen / määrätty turvallisuusviranomainen, jonka toimivaltaan hankeosapuolen / alihankkijan yksikkö kuuluu.

5. Turvallisuusluokkaan NATO RESTRICTED luokiteltuun tietoon pääsemiseksi tai tällaisen tiedon tuottamiseksi ei vaadita todistusta yritysturvallisuusselvityksestä.

TARJOUSKILPAILUT, NEUVOTTELUT JA PÄÄTÖKSET SOPIMUKSISTA, JOIHIN LIITTYY NATON TURVALLISUUSLUOKITELTUA TIETOA

6. Naton ohjelman/hankkeen pääsopimuksen neuvottelee ja tekee Naton ohjelman/hankkeen johtokunta/toimisto. Todistus yritysturvallisuusselvityksestä vaaditaan kaikilta sellaisilta hankeosapuolilta, joilta hankesopimukset edellyttävät, että yksikkö hallitsee tai tuottaa turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa tai pääsee tähän tietoon. Turvallisuusluokkaan NATO RESTRICTED luokiteltujen hankesopimusten osalta ei vaadita todistusta yritysturvallisuusselvityksestä.

7. Naton ohjelman/hankkeen johtokunta/toimisto tai muu sopimusviranomainen, joka panee sopimuksenteon vireille, varmistaa, että hankeosapuolen yksiköillä on asianmukaiset todistukset yritysturvallisuusselvityksestä kyseistä sopimuksenteon vaihetta varten. Sopimusviranomainen tarkistaa, että hankeosapuolen henkilöstöllä, joka pääsee turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään luokkaan luokiteltuun tietoon sopimusviranomaisen toimitiloissa, on asianmukainen todistus

henkilöturvallisuusselvityksestä.

8. Kun pääsopimus on tehty, ensisijainen hankeosapuoli voi neuvotella alihankintasopimuksia muiden hankeosapuolten eli alihankkijoiden kanssa. Nämä alihankkijat voivat myös neuvotella alihankintasopimuksia muiden alihankkijoiden kanssa. Jos nämä alihankintasopimukset edellyttävät pääsyä turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon, sovelletaan niitä yritys- ja henkilöstöturvallisuutta koskevia vaatimuksia, jotka on asetettu tämän liitteen osassa "Naton hankesopimuksiin liittyvät yritysturvallisuusselvitykset" sekä direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta. Jos mahdollinen alihankkija kuuluu Naton ulkopuolisen valtion toimivaltaan[1], Naton ohjelman/hankkeen johtokunnalta/toimistolta tai muulta sopimusviranomaiselta on saatava etukäteen lupa neuvotella alihankintasopimus. Jos Naton ohjelman/hankkeen johtokunta/toimisto on rajoittanut sopimusten tekemistä sellaisten Naton jäsenvaltioiden toimivaltaan kuuluvien hankeosapuolten kanssa, jotka eivät osallistu ohjelmaan/hankkeeseen, johtokuntaa/toimistoa pyydetään harkitsemaan luvan antamista ja antamaan luvan ennen sopimusneuvotteluja kyseisten valtioiden hankeosapuolten kanssa.

9. Tehtyään hankesopimuksen Naton ohjelman/hankkeen johtokunta/toimisto tai muu sopimusviranomainen ilmoittaa asiasta hankeosapuolen valtion kansalliselle turvallisuusviranomaiselle / määrätylle turvallisuusviranomaiselle ja varmistaa, että ensisijaiselle hankeosapuolelle annetaan hankesopimuksen mukana tapauksen mukaan turvallisuusnäkökohtia koskeva kirje (SAL) ja/tai ohjelman/hankkeen turvallisuusohjeet (PSI).

TURVALLISUUSVAATIMUKSET HANKESOPIMUKSILLE, JOIHIN LIITTYY NATON TURVALLISUUSLUOKITELTUA TIETOA

10. Ensisijaisen hankeosapuolen ja alihankkijoiden on sopimuksella edellytettävä toteuttavan niiden sopimuksen irtisanomisen uhalla kaikki kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten määräämät toimet hankeosapuolen tuottaman tai sille annetun tai hankeosapuolen valmistamiin esineisiin sisältyvän Naton turvallisuusluokitellun tiedon suojaamiseksi.

    a) Merkittäviä ohjelmia/hankkeita koskeviin hankesopimuksiin, joihin liittyy Naton turvallisuusluokiteltua tietoa, on liitettävä ohjelman/hankkeen turvallisuusohjeet; turvallisuusohjeiden osana on oltava ohjelman/hankkeen turvallisuusluokitusopas. Kaikkiin muihin hankesopimuksiin, joihin liittyy Naton turvallisuusluokiteltua tietoa, on sisällytettävä vähintään turvallisuusnäkökohtia koskeva kirje, jona voivat toimia soveltamisalaltaan rajoitetut ohjelman/hankkeen turvallisuusohjeet. Viimeksi mainitussa tapauksessa ohjelman/hankkeen turvallisuusluokitusoppaaseen voidaan viitata "turvallisuusluokituksen tarkistuslistana". Ohjelman/hankkeen turvallisuusohjeet täydentävät Naton turvallisuussääntöjä ja -vaatimuksia, ja näissä ohjeissa määrätään kyseiseen Naton ohjelmaan/hankkeeseen liittyvät erityiset turvallisuusmenettelyt sekä vastuut turvallisuusluokiteltua tietoa koskevien turvatoimien toteuttamisesta.

    b) Hankesopimuksista, joihin liittyy ainoastaan turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa, on erityiset määräykset direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta, etenkin sen liitteessä 4 sellaisten tarjousten ja hankesopimusten turvallisuuslausekkeesta, joihin liittyy turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa.

11. Ohjelman/hankkeen mahdollisiin alihankintasopimuksiin liittyvän tiedon turvallisuusluokituksen on perustuttava ohjelman/hankkeen

[1] Oikeus käyttää valtaa tietyssä asiassa tai tietyllä maantieteellisellä alueella.

turvallisuusluokitusoppaaseen.

NATON ULKOPUOLISTEN VALTIOIDEN HANKEOSAPUOLTEN KANSSA TEHTÄVÄT HANKESOPIMUKSET, JOIHIN LIITTYY NATON TURVALLISUUSLUOKITELTUA TIETOA

12. Kun Naton ulkopuolisten valtioiden hankeosapuolten kanssa tehdään hankesopimuksia, joihin liittyy Naton turvallisuusluokiteltua tietoa, tämä on tiedon luovuttamista, ja siinä on noudatettava tämän C-M-asiakirjan liitettä E, direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta. Tiedon luovuttamiseen on aina oltava sen alkuperäisen yhden tai useamman luovuttajan suostumus.

13. Naton ulkopuolisten valtioiden hankeosapuolten kanssa tehtävät hankesopimukset, joihin liittyy Naton turvallisuusluokiteltua tietoa, edellyttävät kahdenvälisen turvallisuussopimuksen / järjestelyn olemassaoloa Naton tai sopimuksen tekevän / takaajana toimivan Naton jäsenvaltion ja kyseisen Naton ulkopuolisen valtion välillä. Jos hankesopimukseen sovelletaan kahdenvälistä turvallisuussopimusta / järjestelyä sopimuksen tekevän / takaajana toimivan Naton jäsenvaltion ja Naton ulkopuolisen valtion välillä, Naton jäsenvaltion on annettava Natolle kirjallinen turvallisuusvakuutus, jossa vahvistetaan, että luovutettavaan Naton turvallisuusluokiteltuun tietoon sovelletaan kyseistä turvallisuussopimusta / järjestelyä. Jäljennös vakuutuksesta on annettava Naton turvallisuustoimistolle ja kyseiselle Naton ohjelman/hankkeen toimistolle/johtokunnalle.

14. Tehtäessä hankesopimusta Naton ulkopuolisen valtion hankeosapuolen kanssa on noudatettava menettelyjä, jotka kuvataan direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

15. Naton ulkopuolisiin valtioihin on nimettävä yksi tai useampi toimivaltainen turvallisuusviranomainen, joka hoitaa Naton jäsenvaltion kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen tehtäviä vastaavia tehtäviä.

NATON HANKESOPIMUKSIIN LIITTYVÄT YRITYSTURVALLISUUSSELVITYKSET

Yleistä

16. Hankesopimuksiin ja alihankintasopimuksiin sovelletaan yksiköitä ja henkilöitä koskevia periaatteita, jotka esitetään seuraavissa kohdissa.

Yritysturvallisuusselvitystodistukset (FSC)

17. Kunkin Naton jäsenvaltion kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen vastuulla on varmistaa, että sen toimivaltaan kuuluvat yksiköt, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon, ovat toteuttaneet tarvittavat suojaustoimet saadakseen todistuksen yritysturvallisuusselvityksestä. Antaessaan todistuksen yritysturvallisuusselvityksestä kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen on varmistettava, että sillä on keinot saada tieto seikoista, jotka voivat vaikuttaa todistuksen antamiseen.

18. Arvioinnissa, joka tehdään ennen yritysturvallisuusselvitystä koskevan todistuksen antamista, on noudatettava sovellettavia kansallisia säädöksiä ja määräyksiä sekä niitä vaatimuksia ja perusteita, jotka on kuvattu direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta. Arvioinnin tulee kohdistua ainakin hankeosapuolen/alihankkijan rehellisyyteen ja nuhteettomuuteen, sen henkilöstön ja muiden sellaisten henkilöiden turvallisuusprofiiliin, jotka saattavat yhteyksiensä vuoksi tarvita pääsyä Naton turvallisuusluokiteltuun tietoon, sekä ulkomaiseen omistukseen, määräysvaltaan ja vaikutusvaltaan.

19. Tarjoajaa, jolla ei ole mahdollisen hankesopimuksen/alihankintasopimuksen edellyttämää asianmukaista todistusta yritysturvallisuusselvityksestä, ei saa automaattisesti sulkea pois kilpailusta. Sopimusviranomaisen olisi pyrittävä kaikin keinoin rajoittamaan tarjoajille annettava tieto mahdollisimman alhaisen turvallisuusluokan tietoon, joka kuitenkin edelleen mahdollistaa tietoon perustuvan ja kilpailukelpoisen vastauksen tarjouspyyntöön. Tarjouspyyntöasiakirjassa on kuitenkin ilmoitettava, että ennen hankesopimuksen/alihankintasopimuksen tekemistä vaaditaan asianmukainen todistus yritysturvallisuusselvityksestä.

20. Yritysturvallisuusselvityksiä koskevien vaatimusten soveltamistilanteita esitetään Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

21. Todistusta yritys- tai henkilöturvallisuusselvityksestä ei vaadita sellaisia hankesopimuksia varten, joihin liittyy turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa, eikä tällaiseen tietoon pääsyä varten. Valtio, jonka kansalliset turvallisuussäädökset ja -määräykset edellyttävät todistusta yritysturvallisuusselvityksestä turvallisuusluokkaan NATO RESTRICTED luokitellun hankesopimuksen tai alihankintasopimuksen tekemiseksi, eivät saa syrjiä tällaista todistusta vaatimattoman valtion hankeosapuolta, vaan niiden on varmistettava, että hankeosapuolelle on tiedotettu sen velvollisuuksista tiedon suojaamisen suhteen ja että sille annetaan vahvistus näistä velvollisuuksista.

Yksiköiden työntekijöiden henkilöturvallisuusselvitykset

22. Yksikön työntekijöillä, jotka tarvitsevat pääsyn turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin luokiteltuun Naton turvallisuusluokiteltuun tietoon, on oltava asianmukainen todistus henkilöturvallisuusselvityksestä. Todistukset henkilöturvallisuusselvityksestä on annettava noudattaen tämän C-M-asiakirjan liitettä C, direktiiviä henkilöstöturvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

23. Hankeosapuolen työntekijöiden turvallisuusselvityksiä haetaan siltä kansalliselta turvallisuusviranomaiselta / määrätyltä turvallisuusviranomaiselta, jonka vastuulle kyseinen yksikkö kuuluu.

24. Jos yksikkö tahtoo palkata Naton ulkopuolisen valtion kansalaisen tehtävään, joka edellyttää pääsyä Naton turvallisuusluokiteltuun tietoon, palkkaajayksikön suhteen toimivaltaisen valtion kansallisen turvallisuusviranomaisen / määrätyn turvallisuusviranomaisen on tehtävä tässä määrätty turvallisuusselvitys ja päätettävä, voidaanko henkilölle sallia pääsy tietoon noudattaen tämän C-M-asiakirjan liitteen C vaatimuksia, direktiiviä henkilöstöturvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

NATON TURVALLISUUSLUOKITELLUN TIEDON LUOVUTTAMINEN HANKESOPIMUKSIA TEHTÄESSÄ

25. Hankesopimuksia tehtäessä Naton turvallisuusluokiteltua tietoa voidaan luovuttaa joko Naton ulkopuolisille valtioille ja kansainvälisille järjestöille tai Naton valtioiden toimijoille, jotka eivät osallistu ohjelmiin/hankkeisiin. Luovuttamiseen on saatava tapauksen mukaan kyseisen ohjelman/hankkeen johtokunnan/toimiston ja/tai tiedon alkuperäisen luovuttajan suostumus, ja siinä on noudatettava muita sovellettavia Naton turvallisuussääntöjen liitteitä, direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta sekä direktiiviä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY VIESTINTÄ- JA

TIETOJÄRJESTELMISSÄ

26. Naton turvallisuusluokitellun tiedon säilyttämiseen, käsittelyyn ja siirtämiseen (jäljempänä "käsittely") saa käyttää ainoastaan asianmukaisesti akkreditoituja viestintä- ja tietojärjestelmiä. Tämän C-M-asiakirjan liitteessä F, päädirektiivissä viestintä- ja tietojärjestelmien turvallisuudesta (AC/35-D/2004), viestintä- ja tietojärjestelmien turvallisuuden hallintaa koskevassa direktiivissä (AC/35-D/2005) sekä kaikissa sovellettavissa viestintä- ja tietojärjestelmien turvallisuuden teknisissä ja toimeenpanodirektiiveissä (AC/322-asiakirjat) esitetään lisää periaatteita ja ohjeita Naton turvallisuusluokiteltua tietoa käsittelevien viestintä- ja tietojärjestelmien vaatimustenmukaisesta toteuttamisesta.

27. Turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa käsittelevien viestintä- ja tietojärjestelmien akkreditointi voidaan kansallisten turvallisuussäädösten ja -määräysten perusteella siirtää hankeosapuolten tehtäväksi. Jos tehtävä siirretään hankeosapuolille, toimivaltaisten kansallisten turvallisuusviranomaisten / määrättyjen turvallisuusviranomaisten / akkreditointiviranomaisten on vastattava hankeosapuolen käsittelemän turvallisuusluokkaan NATO RESTRICTED luokitellun tiedon suojaamisesta, ja niillä on oikeus tarkastaa hankeosapuolten toteuttamat turvatoimet.

KANSAINVÄLISIIN VIERAILUIHIN LIITTYVÄT VALVONTAMENETTELYT

28. Naton jäsenvaltioiden, Naton sotilas- ja siviilielinten, hankeosapuolten ja alihankkijoiden edustajien kansainvälisiin vierailuihin, joihin liittyy Naton turvallisuusluokiteltua tietoa, sovelletaan kansainvälisiin vierailuihin liittyviä valvontamenettelyjä. Niitä sovelletaan myös Naton ulkopuolisen valtion edustajiin, sen hankeosapuolet/alihankkijat mukaan lukien, jos tämä valtio on ottanut kansainvälisiin vierailuihin liittyvät valvontamenettelyt käyttöön.

29. Vierailut, joihin liittyy pääsy turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltuun tietoon tai pääsy turvallisuusalueille ilman saattajaa, on hyväksytettävä kansallisella turvallisuusviranomaisella / määrätyllä turvallisuusviranomaisella. Vierailut, joihin liittyy pääsy ryhmään NATO UNCLASSIFIED[2] kuuluvaan tai turvallisuusluokkaan NATO RESTRICTED luokiteltuun tietoon, voidaan järjestää suoraan lähettävän ja vastaanottavan yksikön välillä ilman muodollisia vaatimuksia.

30. Yksityiskohtaisia järjestelyitä kansainvälisten vierailujen toteuttamiseksi on kuvattu direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

NATON HANKKEESEEN/OHJELMAAN LAINATTAVA HENKILÖSTÖ

31. Jos henkilö, josta on tehty turvallisuusselvitys Naton turvallisuusluokiteltuun tietoon pääsyä varten, on määrä lainata yksiköstä toiseen samassa Naton ohjemassa/hankkeessa, mutta toisessa Naton jäsenvaltiossa, henkilön oman yksikön on pyydettävä valtionsa kansallista turvallisuusviranomaista / määrättyä turvallisuusviranomaista antamaan vahvistus tämän henkilön henkilöturvallisuusselvityksestä sen yksikön valtion kansalliselle turvallisuusviranomaiselle / määrätylle turvallisuusviranomaiselle, johon hänet on määrä lainata.

NATON TURVALLISUUSLUOKITELLUN AINEISTON SIIRTÄMINEN JA

[2] NATO UNCLASSIFIED ei ole Naton turvallisuusluokka.

KULJETTAMINEN KANSAINVÄLISESTI

Kaikkiin kuljetusmuotoihin sovellettavat turvallisuusperiaatteet

32. Tarkasteltaessa turvallisuusjärjestelyjä, joita aiotaan noudattaa turvallisuusluokiteltua aineistoa sisältävien lähetysten kansainvälisissä kuljetuksissa, on noudatettava seuraavia periaatteita:

    a) turvallisuus on varmistettava kaikissa kuljetuksen vaiheissa ja olosuhteissa alkuperäisestä lähtöpaikasta lopulliseen kohteeseen;

    b) lähetyksen suojauksen taso on määritettävä sen sisältämän aineiston ylimmän turvallisuusluokan mukaan;

    c) kuljetuksen hoitaville yrityksille on tarvittaessa hankittava todistus yritysturvallisuusselvityksestä. Näissä tapauksissa lähetystä käsittelevälle henkilöstölle on annettava todistus henkilöturvallisuusselvityksestä tämän liitteen määräysten mukaisesti;

    d) kuljetusten on mahdollisuuksien mukaan tapahduttava suoraan pisteestä pisteeseen, ja ne on tehtävä niin pian kuin olosuhteet sallivat; ja

    e) kuljetusreitit on huolellisesti järjestettävä kulkemaan ainoastaan Naton jäsenvaltioiden kautta. Naton ulkopuolisten valtioiden kautta kulkevia reittejä olisi käytettävä vain, jos lähettäjän suhteen toimivaltainen kansallinen turvallisuusviranomainen / määrätty turvallisuusviranomainen sallii tämän, ja tällöin on noudatettava Naton turvallisuussääntöjä tukevaa direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta.

33. Järjestelyistä turvallisuusluokitellun aineiston lähettämiseksi määrätään erikseen kunkin ohjelman/hankkeen yhteydessä. Näitä järjestelyjä on kuitenkin noudatettava, jotta minimoidaan todennäköisyys luvattomaan pääsyyn tähän aineistoon.

34. Naton turvallisuusluokitellun tiedon kansainvälistä välittämistä koskevat turvallisuusvaatimukset esitetään Naton turvallisuussääntöjä tukevassa direktiivissä Naton turvallisuusluokitellun tiedon turvallisuudesta. Yksityiskohtaiset vaatimukset Naton turvallisuusluokitellun aineiston kuljettamiselle mukana ja kaupallisten kuriiriyritysten, turvallisuusvartijoiden ja saattajien välityksellä sekä räjähteiden, ajoaineiden ja muiden vaarallisten aineiden kuljettamiselle esitetään kuitenkin Naton turvallisuussääntökä tukevassa direktiivissä turvallisuusluokiteltujen hankkeiden turvallisuudesta ja yritysturvallisuudesta.

LIITE H

TURVALLISUUS SUHTEISSA NATON ULKOPUOLISIIN TOIMIJOIHIN

JOHDANTO

1. Tässä liitteessä esitetään ne periaatteet ja vähimmäisvaatimukset, joita noudatetaan suojattaessa Naton ulkopuolisille valtioille ja muille Naton ulkopuolisille elimille (esim. kansainvälisille järjestöille) (jäljempänä "Naton ulkopuoliset toimijat" (NNE)) luovutettavaa tai näiden pääsyoikeuden piiriin kuuluvaa Naton turvallisuusluokiteltua tietoa, mukaan lukien näitä valtioita tai elimiä edustavat henkilöt.

2. Naton turvallisuusluokitellun tiedon jakamisen Naton ulkopuolisten toimijoiden kanssa tulee tapahtua Pohjois-Atlantin neuvoston (NAC) hyväksymän Naton yhteistyötoiminnan yhteydessä. Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen käsittelee ja hyväksyy tapauskohtaisesti pyynnöt Naton turvallisuusluokitellun tiedon jakamisesta Naton ulkopuolisten toimijoiden kanssa tällaisen yhteistyötoiminnan ulkopuolella. Lisätietoja ja -vaatimuksia Naton ulkopuolisille toimijoille luovutettavan tai näiden pääsyoikeuden piiriin kuuluvan Naton turvallisuusluokitellun tiedon suojaamiseksi on Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin.

3. "7 Naton ulkopuolista valtiota", "(7NNN)", tarkoittaa yksinomaan seuraavia valtioita ja niiden kansalaisia: Australia, Irlanti, Itävalta, Ruotsi, Suomi, Sveitsi ja Uusi-Seelanti.[1]

4. Kukin Naton ulkopuolinen toimija perustaa asianmukaisen turvallisuusviranomaisen, joka vastaa Naton turvallisuusluokitellun tiedon turvallisuudesta. Naton turvallisuussääntöjä tukevassa asiakirjassa turvallisuudesta Naton ulkopuolisten toimijoiden suhteissa Natoon annetaan näille toimijoille yleiskuva niistä turvallisuuden perusperiaatteista ja vähimmäisvaatimuksista, joita on sovellettava suojattaessa ja käsiteltäessä Naton turvallisuusluokiteltua tietoa ja vastaavaa kansallista tietoa, kun sitä vaihdetaan Pohjois-Atlantin neuvoston hyväksymän Naton yhteistyötoiminnan yhteydessä.

YLEISET VAATIMUKSET

5. Naton turvallisuusluokiteltua tietoa voidaan vaihtaa Naton ulkopuolisten toimijoiden kanssa seuraavissa yhteyksissä:

   a) Pohjois-Atlantin neuvoston hyväksymä yhteistyötoiminta, johon Pohjois-Atlantin neuvosto on hyväksynyt Naton ulkopuolisen toimijan osallistumaan;

   b) Naton toiminta (esim. ohjelma, hanke, operaatio, tehtävä), jossa Naton ulkopuolisen toimijan osallistumisen ja sen mukanaolon toiminnassa joltakin osin katsotaan hyödyttävän Natoa; tai

   c) Naton jäsenvaltion ja Naton ulkopuolisen toimijan väliset kahdenväliset sitoumukset, joiden osalta Naton turvallisuusluokitellun tiedon jakamisen Naton ulkopuolisen toimijan kanssa katsotaan hyödyttävän Natoa.

6. Ennen Naton turvallisuusluokitellun tiedon jakamista Naton ulkopuolisen toimijan kanssa kyseisen toimijan ja Naton on tullut tehdä turvallisuussopimus, jonka toteuttaminen Naton turvallisuustoimiston (NOS) on vahvistettava. Jos

[1] Kansalliset turvallisuusviranomaiset / määrätyt turvallisuusviranomaiset voivat ehdottaa muutoksia valtioiden luetteloon turvallisuuskomitean hyväksyttäväksi.

turvallisuussopimusta ei ole tehty, on tullut antaa turvallisuusvakuutus, jos on poliittisesti tai operatiivisesti välttämätöntä jakaa Naton turvallisuusluokiteltua tietoa oikea-aikaisesti Pohjois-Atlantin neuvoston hyväksymän yhteistyötoiminnan tukemiseksi tai poikkeustapauksissa tällaisen toiminnan ulkopuolella. Turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin kuvataan yksityiskohtaiset määräykset, joita sovelletaan Naton turvallisuusluokitellun tiedon jakamiseen Naton ulkopuolisten toimijoiden kanssa 5. kohdassa mainituissa yhteyksissä.

TURVALLISUUSSOPIMUKSET JA HALLINNOLLISET JÄRJESTELYT

7. Turvallisuussopimus on järjestelmä, jonka avulla mahdollistetaan turvallisuusluokitellun tiedon vaihtaminen tietyn Naton ulkopuolisen toimijan kanssa. Turvallisuussopimuksessa määrätään Naton ja Naton ulkopuolisen toimijan välillä sovitut korkean tason strategiset periaatteet, jotka toimivat perustana asianmukaisten turvatoimien toteuttamiselle tarkoituksena suojata tarvittaessa sekä Naton että Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa. Ennen Naton turvallisuusluokitellun tiedon luovuttamista Naton ulkopuoliselle toimijalle Naton turvallisuustoimiston on vahvistettava, että tämä toimija noudattaa turvallisuussopimusta.

8. Turvallisuussopimuksen turvallisuusperiaatteita tuetaan asianmukaisella hallinnollisten järjestelyjen kokonaisuudella. Hallinnolliset järjestelyt tukevat turvallisuussopimuksen toteuttamista ja koostuvat määräyksistä, joissa asetetaan turvallisuuden perusvaatimukset vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi asianmukaisella ja keskinäisesti hyväksyttävällä tavalla. Kun hallinnollisista järjestelyistä on sovittu, Naton turvallisuustoimisto vahvistaa niiden soveltamisen turvallisuustarkastuksen avulla.

9. Naton turvallisuustoimisto tekee Naton ulkopuolisten toimijoiden asianomaisille elimille määräajoin, vähintään kahden vuoden välein, riskinhallinnan lähestymistapaan perustuvia turvallisuustarkastuksia varmistaakseen turvallisuussopimuksen ja hallinnollisten järjestelyjen jatkuvan noudattamisen.

TURVALLISUUSVAKUUTUKSET

10. Turvallisuusvakuutusta käytetään, jos Naton ja Naton ulkopuolisen toimijan välillä ei ole voimassa vahvistettua turvallisuussopimusta ja jos on poliittisesti tai operatiivisesti välttämätöntä jakaa Naton turvallisuusluokiteltua tietoa oikea-aikaisesti Pohjois-Atlantin neuvoston hyväksymän yhteistyötoiminnan tukemiseksi tai poikkeustapauksissa tällaisen toiminnan ulkopuolella. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään yksityiskohtaisista edellytyksistä, jotka on täytettävä käytettäessä turvallisuusvakuutusta.

11. Turvallisuusvakuutus virallistaa Naton ulkopuolisen toimijan sitoumuksen suojata vastaanottamansa Naton turvallisuusluokiteltu tieto asianmukaista tasoa noudattaen. Turvallisuusvakuutus rajoitetaan koskemaan tiettyä toimintaa tietyn ajan.

12. Naton ulkopuolisen toimijan antama turvallisuusvakuutus, jonka tämän toimijan asianmukaisesti valtuuttama edustaja on allekirjoittanut, annetaan Naton turvallisuustoimistolle, kun turvallisuusvakuutusta käytetään tarkoituksena mahdollistaa Naton turvallisuusluokitellun tiedon jakaminen seuraavien tukemiseksi:

    a) Pohjois-Atlantin neuvoston hyväksymä yhteistyötoiminta tai

    b) tapauskohtaisesti Naton toiminta, johon Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen on hyväksynyt Naton ulkopuolisen toimijan osallistumaan.

Naton jäsenvaltion toimiminen takaajana

13. Naton turvallisuusluokitellun tiedon jakaminen muun kuin 12.a tai 12.b kohdassa määritellyn toiminnan yhteydessä Naton jäsenvaltion erityisestä pyynnöstä edellyttää takaajaa. Takaajana toimiminen tarkoittaa tietynlaista Naton jäsenvaltion tukea Naton ulkopuoliselle toimijalle tarkoituksena mahdollistaa Naton turvallisuusluokitellun tiedon jakaminen tämän toimijan kanssa, jos Naton ja tämän toimijan välillä ei ole voimassa vahvistettua turvallisuussopimusta.

14. Jotta Naton jäsenvaltio voi toimia takaajana, takaajan ja Naton ulkopuolisen toimijan välillä on oltava olemassa asianmukainen turvallisuusjärjestely (esim. turvallisuussopimus tai muu sovellettava järjestely). Takaajan on toimitettava Naton turvallisuustoimistolle kirjallinen turvallisuusvakuutus, jonka on allekirjoittanut Naton ulkopuolisen toimijan asianmukaisesti valtuuttama edustaja. Turvallisuusvakuutuksessa asetetaan ne vähimmäisvaatimukset, joita Naton ulkopuolisen toimijan on sovellettava Naton turvallisuusluokitellun tiedon suojaamiseksi.

15. Takaajana toimiminen rajoitetaan koskemaan tiettyä toimintaa tietyn ajan.

ERITYISET TURVALLISUUSMÄÄRÄYKSET

16. Jaettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisten toimijoiden kanssa voidaan pääsy Naton turvallisuusluokiteltuun tietoon tai toimitilaan sallia näille toimijoille kolmella tavalla: pääsy Naton toimitiloihin, pääsy Naton turvallisuusluokiteltuun tietoon ja Naton turvallisuusluokitellun tiedon luovuttaminen. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään kussakin tilanteessa sovellettavista yksityiskohtaisista edellytyksistä sekä erityistoimista ja -menettelyistä.

Henkilöstöturvallisuus

17. Ennen kuin Naton ulkopuolista toimijaa edustavalle henkilölle annetaan pääsy turvallisuusluokkaan NATO CONFIDENTIAL tai sitä ylempään luokkaan luokiteltuun tietoon, hänen on tullut läpäistä vähintään samantasoinen PSC-menettely kuin se, joka Naton turvallisuusperiaatteiden ja niitä tukevien ohjeiden mukaan vaaditaan Naton jäsenvaltion kansalaiselta.

18. Turvallisuusluokkaan NATO RESTRICTED luokiteltuun tietoon pääsemiseksi ei vaadita todistusta henkilöturvallisuusselvityksestä. Kyseisellä Naton ulkopuolista toimijaa edustavalla henkilöllä on kuitenkin oltava tiedonsaantitarve, hänelle on selostettava hänen turvallisuusvelvoitteensa Naton turvallisuusluokitellun tiedon suojaamisen suhteen, ja hänen on tullut kirjallisesti tai vastaavalla kiistämättömyyden varmistavalla menetelmällä ilmoittaa ymmärtäneensä turvallisuusvelvoitteensa.

19. Todistusta henkilöturvallisuusselvityksestä voidaan vaatia edellytyksenä pääsylle Naton toimitiloihin sellaisten erityisten edellytysten perusteella, joista määrätään Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin ja sovellettavissa paikallisissa turvallisuusmääräyksissä.

Toimitilaturvallisuus

20. Naton ulkopuolisia toimijoita edustaville henkilöille, joiden on toimeksiantonsa ja virallisten tehtäviensä vuoksi tavattava säännöllisesti Naton henkilöstöä, voidaan sallia pääsy tietyille alueille, joilla säilytetään tai käsitellään turvallisuusluokkaan NATO RESTRICTED ja sitä ylempiin luokkiin luokiteltua tietoa ja/tai siitä keskustellaan. Näille henkilöille voidaan myös antaa työskentelytilaa tietyiltä alueilta. Pääsyn salliminen ilman saattajaa ja/tai työskentelytilan antaminen käsitellään tapauskohtaisesti.

21. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin on yksityiskohtaista tietoa edellytyksistä, joilla Naton ulkopuolisia toimijoita edustaville henkilöille voidaan sallia pääsy Naton luokan I tai II turva-alueelle tai hallinnolliselle vyöhykkeelle, sekä tällöin noudatettavasta menettelystä ja toimivaltaisista hyväksyntäviranomaisista.

Tietoaineistoturvallisuus

22. Naton ulkopuolisten toimijoiden kanssa tehtävässä yhteistyössä voidaan pääsy Naton turvallisuusluokiteltuun tietoon sallia näille toimijoille kolmella tavalla:

    a) **pääsy Naton toimitiloihin.** Naton ulkopuolista toimijaa edustavalle henkilölle sallitaan fyysinen pääsy tiettyyn Naton tilaan tai yksikköön tai tietylle alueelle yksikön sisällä. Fyysinen pääsy ei automaattisesti sisällä pääsyä Naton turvallisuusluokiteltuun tietoon;

    b) **pääsy Naton turvallisuusluokiteltuun tietoon.** Naton ulkopuolista toimijaa edustavalle henkilölle sallitaan pääsy Naton turvallisuusluokiteltuun tietoon, jotta hän voi hoitaa toimeksiantonsa ja viralliset tehtävänsä, kun pääsy hyödyttää Natoa. Pääsy sallitaan vain kyseiselle henkilölle, eikä hän saa jakaa Naton turvallisuusluokiteltua tietoa eteenpäin edustamalleen Naton ulkopuoliselle toimijalle, ellei kyseistä tietoa ole luovutettu vakiintuneiden menettelyjen mukaisesti;

    c) **Naton turvallisuusluokitellun tiedon luovuttaminen.** Naton turvallisuusluokiteltua tietoa sallitaan luovutettavan Naton ulkopuoliselle toimijalle.

23. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään yksityiskohtaisista edellytyksistä, jotka on täytettävä tietyissä tilanteissa, kun Naton sotilas- tai siviilielinten tai Naton jäsenvaltioiden on määrä sallia pääsy Naton turvallisuusluokiteltuun tietoon tai luovuttaa sitä.

24. Naton turvallisuusluokitellun tiedon luovuttaminen Naton ulkopuoliselle toimijalle edellyttää aina alkuperäisen yhden tai useamman luovuttajan kirjallista ennakkosuostumusta.

25. Naton turvallisuusluokiteltua tietoa voidaan luovuttaa Pohjois-Atlantin neuvoston hyväksymän yhteistyötoiminnan yhteydessä tai Naton toiminnan yhteydessä, jos Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen on hyväksynyt tähän toimintaan osallistuvat Naton ulkopuoliset toimijat. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määrätään lisäedellytyksistä, joita on sovellettava ennen tiedon luovuttamista.

26. Direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin määritetään myös lisäedellytykset, joita on sovellettava ennen Naton turvallisuusluokitellun tiedon luovuttamista, kun sitä luovutetaan Naton jäsenvaltion (takaajan) erityisestä pyynnöstä Naton ulkopuoliselle toimijalle, joka ei osallistu Pohjois-Atlantin neuvoston hyväksymään yhteistyötoimintaan tai Naton toimintaan, ja kun Pohjois-Atlantin neuvosto tai asianomainen valtuutettu viranomainen on hyväksynyt kyseiseen toimintaan osallistuvat Naton ulkopuoliset toimijat.

27. Jos kansainvälisen järjestön kanssa on voimassa turvallisuussopimus tai turvallisuusvakuutus, on luovutettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisille järjestön jäsenille noudatettava sovellettavia turvallisuussopimuksen määräyksiä sekä muita vakiintuneita sääntöjä niiden osallistumisesta Naton toimintaan. Jollei turvallisuussopimusta ole voimassa, ja jos kansainvälisen järjestön kanssa on voimassa turvallisuusvakuutus, on luovutettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisille järjestön jäsenille noudatettava Naton turvallisuussääntöjä tukevan direktiivin sovellettavia määräyksiä ja turvallisuusvakuutusta.

28. Mihinkään turvallisuusluokkaan luokiteltuun ATOMAL-tietoon ei saa sallia pääsyä eikä sitä saa luovuttaa Naton ulkopuoliselle toimijalle, joka ei ole osapuolena voimassa olevassa sopimuksessa Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä (C-M(64)39).

Luovuttajaviranomainen

29. Pohjois-Atlantin neuvostolla on ylin toimivalta luovutettaessa Naton turvallisuusluokiteltua tietoa Naton ulkopuolisille toimijoille. Tätä toimivaltaa käytettäessä noudatetaan alkuperäisen luovuttajan suostumuksen periaatetta, ja toimivaltaa siirretään

    a) asianomaiselle aihekohtaiselle komitealle sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka on peräisin kyseiseltä komitealta ja/tai sen alaisilta elimiltä. Turvallisuusluokkaan NATO RESTRICTED luokitellun tiedon osalta asianomainen aihekohtainen komitea voi siirtää toimivaltaa edelleen käytettäväksi selvästi määritellyssä henkilöstön tukitoiminnossa tai kyseisen komitean tukihenkilöstön tietyssä yhdessä tai useammassa tehtävässä;

    b) sotilaskomitealle sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka on peräisin sotilaskomitealta ja/tai sen alaisilta elimiltä. Turvallisuusluokkaan NATO RESTRICTED luokitellun tiedon osalta sotilaskomitea voi siirtää toimivaltaa edelleen käytettäväksi selvästi määritellyssä henkilöstön tukitoiminnossa tai sotilaskomitean tukihenkilöstön tietyssä yhdessä tai useammassa tehtävässä;

    c) Naton Euroopan joukkojen komentajalle tai varakomentajalle sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka katsotaan voitavan luovuttaa kulloisellekin operaatiolle (XFOR) tai joka on luokiteltu turvallisuusluokkaan NATO/XFOR SECRET (mission SECRET), tietyin edellytyksin, joista määrätään yksityiskohtaisesti Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin.

    d) Naton transformaatioesikunnan komentajalle tai varakomentajalle turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta tietyin edellytyksin, joista määrätään yksityiskohtaisesti Naton turvallisuussääntöjä tukevassa ohjeessa turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin;

    e) operaation komentajalle Pohjois-Atlantin neuvoston hyväksymässä operaatiossa, johon osallistuu joukkoja luovuttavia Naton ulkopuolisia valtioita (NNTCN), sellaisen turvallisuusluokkaan NATO SECRET ja sitä alempiin luokkiin luokitellun tiedon osalta, joka on jo katsottu voitavan luovuttaa operaatiolle (XFOR), tietyin edellytyksin, joista määrätään yksityiskohtaisesti Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin;

    f) Naton tuotanto- ja logistiikkaorganisaatiolle (NPLO), organisaatioon osallistuvien valtioiden kanssa koordinoiden, sellaisen Naton turvallisuusluokitellun tiedon osalta, joka on peräisin yhdeltä tai useammalta organisaatioon osallistuvalta valtiolta ja kuuluu tälle.

30. Lukuun ottamatta 29.a ja 29.b kohdassa mainittuja poikkeuksia, jotka koskevat turvallisuusluokkaan NATO RESTRICTED luokiteltua tietoa, valtuutetut luovuttajaviranomaiset eivät saa siirtää valtuuksiaan eteenpäin.

31. Toimivaltaa luovuttamiseen saa siirtää asianomaiselle aihekohtaiselle komitealle vain, jos tiedon alkuperäinen yksi tai useampi luovuttaja on edustettuna komiteassa. Jos alkuperäistä yhtä tai useampaa luovuttajaa ei voida selvittää, asianomainen

aihekohtainen komitea ottaa alkuperäisen luovuttajan vastuun.

32. Täytäntöönpano-ohjeissa tiedustelutiedon jakamiseksi Naton ja Naton ulkopuolisten toimijoiden välillä (DSG(2015)0307-REV1) sekä Naton turvallisuussääntöjä tukevassa asiakirjassa tiedon ja tiedustelutiedon jakamisesta Naton ulkopuolisten toimijoiden kanssa (AC/35-D/1040) määritellään luovuttajaviranomainen operaatioiden, koulutuksen, harjoitusten, transformaation ja yhteistyön yhteydessä.

Luovutettua tietoa koskeva kirjanpito

33. Naton sotilas- ja siviilielinten on pidettävä kirjaa kaikista päätöksistä, jotka koskevat niiden Naton ulkopuoliselle toimijalle luovuttamaa turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin luokkiin luokiteltua tietoa, sekä ilmoitettava yksityiskohtaisesti päätösten viitenumerot, otsikot ja antamispäivät vähintään kuuden kuukauden välein Naton keskusrekisterille Brysseliin, jollei toimivaltainen turvallisuusviranomainen toisin määrää.

Viestintä- ja tietojärjestelmien turvallisuus

34. Naton turvallisuussääntöjä tukevassa direktiivissä turvallisuudesta Naton suhteissa Naton ulkopuolisiin toimijoihin asetetaan erityiset vaatimukset, jotka on täytettävä, jotta Naton ulkopuolista toimijaa edustavalle henkilölle voidaan sallia pääsy Naton viestintä- ja tietojärjestelmiin.

35. Naton viestintä- ja tietojärjestelmien yhteenkytkentä Naton ulkopuolisen toimijan viestintä- ja tietojärjestelmien kanssa on akkreditoitava Naton turvallisuussääntöjen ja niitä tukevien direktiivien mukaisesti.

TIETOTURVAPOIKKEAMAT

36. Sellaisten tietoturvapoikkeamien käsittelyssä, joihin liittyy Naton hallussa olevaa Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa, on noudatettava direktiiviä Naton turvallisuusluokitellun tiedon turvallisuudesta (AC/35-D/2002) ja mahdollisia muita määräyksiä, jotka on annettu turvallisuussopimuksessa ja täytäntöönpanoa koskevissa hallinnollisissa järjestelyissä tai Naton ulkopuolisen toimijan kanssa sovellettavassa turvallisuusvakuutuksessa.

37. Tietoturvapoikkeamista, joihin liittyy Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa, on viipymättä ilmoitettava Naton turvallisuustoimistolle. Naton turvallisuustoimiston vastuulla on ilmoittaa viipymättä asianomaisen Naton ulkopuolisen toimijan turvallisuusviranomaiselle tietoturvapoikkeamista, joihin liittyy Naton ulkopuolisen toimijan turvallisuusluokiteltua tietoa, noudattaen turvallisuussopimusta ja täytäntöönpanoa koskevia hallinnollisia järjestelyjä tai turvallisuusvakuutusta.

SANASTO

Pääsy tietoon	Luvan antaminen yhdelle tai useammalle henkilölle mahdollisuuteen saada tiettyä tietoa vaadittavien turvallisuusrajoitusten mukaisesti, jotta henkilö voi suorittaa selvästi määritellyt tehtävänsä, joihin hänellä on asianmukaiset valtuudet. Pääsy tietoon tällaisissa olosuhteissa on kyseisen henkilön erioikeus, johon ei sisälly oikeuksia tiedon levittämiseen laajemmalti.
Pääsy toimitiloihin	Luvan antaminen fyysiseen pääsyyn tiettyyn paikkaan, jossa nimetty yksi tai useampi henkilö saa oleskella joko nimetyn saattajan kanssa tai ilman tätä, sen mukaan, mitä kulloisetkin turvallisuusvaatimukset edellyttävät ja kulloisetkin turvallisuusselvitykset mahdollistavat.
Tilivelvollisuuden alainen tieto	Kaikki tieto, joka on luokiteltu turvallisuusluokkiin COSMIC TOP SECRET (CTS) ja NATO SECRET (NS) sekä kaikki erityisluokan (kuten ATOMAL) tieto.
Hallinnollinen vyöhyke	Selvästi määritelty suojattu alue, jolla henkilöillä ei tarvitse olla saattajaa ja jolle pääsy on luvanvarainen.
Kasautumisperiaate	Kun suuri määrä Naton turvallisuusluokiteltua tietoa kootaan yhteen, sen alkuperäiset turvallisuusluokitusmerkinnät on säilytettävä, ja on arvioitava, miten tämän tietokokonaisuuden katoaminen tai vaarantuminen vaikuttaisi järjestöön. Jos tämä kokonaisvaikutus arvioidaan suuremmaksi kuin kyseisten yksittäisten Naton turvallisuusluokkien mukainen vaikutus, olisi harkittava kyseisen tietokokonaisuuden käsittelemistä ja suojaamista sen turvallisuusluokan mukaisesti, joka vastaa tietokokonaisuuden katoamisen tai vaarantumisen arvioitua vaikutusta.
Tunnistaminen	Tunnistaminen on toimi, jolla varmistetaan tietyn toimijan väitetty identiteetti.
Käytettävyys	Tiedon ja aineiston saavutettavuus ja käyttökelpoisuus valtuutetun henkilön tai yksikön pyytäessä sitä.
Turvallisuusluokiteltu tieto	Sellainen tieto (jota voidaan välittää missä tahansa muodossa) tai aineisto, jonka katsotaan edellyttävän suojaamista luvattomalta ilmitulolta ja joka on turvallisuusluokituksella osoitettu sellaiseksi.
Viestintä- ja tietojärjestelmien turvallisuus (CIS Security)	Turvallisuustoimenpiteiden soveltaminen viestintä- ja tietojärjestelmien ja muiden sähköisten järjestelmien sekä näihin järjestelmiin tallennettavien ja niissä käsiteltävien tai siirrettävien tietojen luottamuksellisuuden, eheyden, käytettävyyden, aitouden ja kiistämättömyyden suojaamiseksi.

Toimivaltainen turvallisuusviranomainen (CSA)	Kansallisen turvallisuusviranomaisen nimeämä viranomainen, jolla on toimivalta hoitaa tiettyjä turvallisuustehtäviä, jotka liittyvät muun muassa henkilöturvallisuusselvityksiin, jotta kyseisen valtion kansalaisille voidaan sallia pääsy Naton turvallisuusluokiteltuun tietoon.

Vaarantuminen	Vaarantuminen tarkoittaa tilannetta, jossa tietoturvaloukkauksen tai haitallisen toiminnan (kuten vakoilun, terroriteon, sabotaasin tai varkauden) vuoksi Naton turvallisuusluokiteltu tieto on menettänyt luottamuksellisuutensa, eheytensä tai käytettävyytensä tai tätä tietoa tukevat palvelut ja resurssit ovat menettäneet eheytensä tai käytettävyytensä. Vaarantumiseen sisältyvät katoaminen, paljastuminen asiattomille (esim. joukkoviestimille tai vakoilun vuoksi), luvaton muuttaminen, hävittäminen luvattomalla tavalla tai palvelun estyminen.
Viestintäkeskus	Organisaatio, joka vastaa viestintäliikenteen käsittelystä ja valvonnasta ja johon tavallisesti kuuluu sanomakeskus ja salauskeskus sekä lähetys- ja vastaanottokeskukset.
Luottamuksellisuus	Se, ettei tietoa saateta asiattomien henkilöiden tai muiden toimijoiden saataville eikä paljasteta näille.
Vastaanottaja	Hankeosapuoli, yksikkö tai muu organisaatio, joka vastaanottaa aineistoa lähettäjältä.
Lähettäjä	Hankeosapuoli, yksikkö tai muu organisaatio, joka vastaa aineiston järjestämisestä ja lähettämisestä.
Hankesopimus	Oikeudellisesti täytäntöönpanokelpoinen sopimus tavaroiden tai palvelujen toimittamisesta.
Hankeosapuoli	Teollinen, kaupallinen tai muu toimija, joka tekee sopimuksen tavaroiden tai palvelujen toimittamisesta.
Kuriiri	Henkilö, joka on virallisesti määrätty kuljettamaan aineistoa mukanaan.
Kuriiripalvelu	Palvelu, joka välittää henkilöitä, jotka on virallisesti määrätty kuljettamaan aineistoa mukanaan.
Salausaineisto	Salausalgoritmit, salauslaitteistot ja -ohjelmistomoduulit sekä tuotteet, joihin sisältyy täytäntöönpanoa koskevia yksityiskohtia sekä niihin liittyviä asiakirjoja ja avainnusaineistoa (sekä symmetrisiä että epäsymmetrisiä salausmenetelmiä varten).
Määrätty turvallisuusviranomainen (DSA)	Viranomainen, jonka vastuulla on tiedottaa yrityksille ja muille yhteisöille kansallisista periaatteista kaikissa Naton yhteisöturvallisuuden periaatteita koskevissa asioissa sekä antaa ohjausta ja apua niiden soveltamisessa. Joissakin maissa määrätyn turvallisuusviranomaisen tehtävää voi hoitaa kansallinen turvallisuusviranomainen.

Asiakirja	Mikä tahansa tallennettu tieto riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien rajoituksetta kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja -paperit, hiilipaperikopiot ja värinauhat; millä tahansa menetelmällä tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat tietotekniset laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet.

Dynaaminen riskienhallinta	Kyky harjoittaa riskienhallintaa siten, että viestintä- ja tietojärjestelmien käytön riskiä arvioidaan jatkuvasti, että kaikki viestintä- ja tietojärjestelmien toiminnan yhteyteen liittyvät muutokset kuvastuvat dynaamisesti riskien tunnisteissa ja että kussakin tilanteessa sovelletaan oikea-aikaisesti tarkoituksenmukaisimpia vastatoimia turvallisuuden ylläpitämiseksi.
Saattajat	Aseistetut tai aseistamattomat kansalliset poliisit tai sotilashenkilöt tai muu valtion henkilöstö. Saattajien tehtävänä on helpottaa aineiston siirtämistä turvallisesti, mutta he eivät ole välittömästi vastuussa aineiston varsinaiseen suojaamiseen liittyvistä asioista.
Yksikkö	Laitos, tehdas, laboratorio, toimisto, yliopisto tai muu oppilaitos tai kaupallinen yritys, mukaan lukien näihin liittyvät varastot, säilytysalueet, aputilat ja osat, jotka tehtävänsä ja sijaintinsa suhteen muodostavat toimivan kokonaisuuden.
Yritysturvallisuusselvitystodistus (FSC)	Kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen hallinnollinen päätös siitä, että turvallisuuden näkökulmasta yksikkö pystyy suojaamaan asianmukaisesti tiettyyn tai sitä alempaan turvallisuusluokkaan kuuluvan Naton turvallisuusluokitellun tiedon ja että yksikön henkilöstöstä, joka tarvitsee pääsyn Naton turvallisuusluokiteltuun tietoon, on tehty asianmukaisesti turvallisuusselvitys ja sille on selostettu ne Naton turvallisuusvaatimukset, joita on noudatettava Naton turvallisuusluokiteltuja sopimuksia toteutettaessa.
Vartijat	Sotilashenkilöstö tai (valtion tai osallistuvan hankeosapuolen työntekijöistä koostuva) siviilihenkilöstö, joka voi olla aseistettu tai aseistamaton. Vartijat voidaan määrätä joko pelkästään turvallisuusvartiointiin tai sekä turvallisuusvartiointiin että muihin tehtäviin.
Henkilökohtainen kuljettaminen	Tiedon siirtäminen siten, että henkilö kuljettaa sen mukanaan.
Isäntävaltio	<u>Yleisesti:</u> Valtio, johon Naton sotilas- tai siviilielin on sijoitettu. <u>Yritysturvallisuuden yhteydessä:</u> Valtio, jonka Naton virallinen elin on nimennyt siksi valtion virastoksi, joka tekee sopimuksen Naton pääsopimuksen toteuttamiseksi. Valtioita, joissa toteutetaan alihankintasopimuksia, ei sanota isäntävaltioiksi.
Tieto	Missä tahansa muodossa välitettävä tieto.

Tietojen turvaaminen	Tieto on suojattava soveltamalla tietojen turvaamisen periaatetta, jolla tarkoitetaan niiden toimenpiteiden kokonaisuutta, joilla pyritään saavuttamaan tietty luottamuksen taso viestintä- ja tietojärjestelmien, muiden sähköisten järjestelmien ja muiden kuin sähköisten järjestelmien sekä näihin järjestelmiin tallennettavien ja niissä käsiteltävien tai siirrettävien tietojen luottamuksellisuuden, eheyden, käytettävyyden, kiistämättömyyden ja aitouden suojaamisessa.

Vähäinen tietoturvapoikkeama	Vähäinen tietoturvapoikkeama on tahallinen tai tahaton teko tai laiminlyönti, joka on Naton turvallisuussääntöjen ja niitä tukevien direktiivien vastainen mutta ei johda Naton turvallisuusluokitellun tiedon tosiasialliseen tai mahdolliseen vaarantumiseen (esimerkkejä: Naton turvallisuusluokiteltua tietoa jätetään suojaamattomana suojattuihin toimitiloihin, joissa toimivista henkilöistä on kaikista tehty asianmukaisesti turvallisuusselvitys; Naton turvallisuusluokiteltu tieto jätetään sulkematta kaksinkertaiseen suojakuoreen).
Eheys	Se, ettei tietoa (myöskään dataa, kuten salatekstiä) ole muutettu eikä hävitetty luvattomalla tavalla.
Kansainväliset vierailut	Vierailut, joita kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen toimivaltaan tai Naton elimeen kuuluva henkilöstö tekee toisen kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen tai Naton toimivaltaan kuuluviin yksiköihin tai elimiin ja jotka edellyttävät pääsyä Naton turvallisuusluokiteltuun tietoon tai joihin voi liittyä pääsy siihen tai jotka kyseisen tiedon turvallisuusluokasta riippumatta edellyttävät toimivaltaisen kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen hyväksyntää sen kansallisen lainsäädännön mukaan, joka koskee tällaisen Naton hyväksymää toimintaa tukevan vierailun kohteena olevaa yksikköä tai elintä. Kaikki Naton sotilas- ja siviilielimet kuuluvat turvallisuusasioissa Naton toimivaltaan.
Elinkaari	Tiedon elinkaari käsittää tiedon suunnittelun, keräämisen, luomisen tai tuottamisen; sen järjestämisen, haun, käytön, saavutettavuuden ja siirtämisen; sen säilyttämisen ja suojaamisen; sekä lopulta sen käytöstä poistamisen arkistoimalla tai hävittämällä.
Koneellisesti luettava tietoväline	Tietoväline, joka voi välittää tietoja tiettyyn lukulaitteeseen.
Merkittävä ohjelma/hanke	Suurimerkityksinen ohjelma tai hanke, johon tavallisesti liittyy enemmän kuin kaksi valtiota sekä sellaisia turvatoimia, jotka ylittävät tavanomaiset Naton turvallisuusperiaatteissa määritellyt perusvaatimukset.
Aineisto	Aineisto sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet/komponentit, aseet ja työvälineet.
Sotilaskomitea (MC)	Naton korkein sotilasviranomainen; sotilaskomitea vastaa sotilasasioiden hoitamisesta yleisesti. Sotilaskomitea vastaa operatiivisesti niiden käyttäjien vaatimusten hyväksymisestä, joita strategiset komentajat välittävät, sekä näiden vaatimusten asettamisesta etusijajärjestykseen.

Kansalaiset	Kansalaisia ovat eri valtioiden kansalaiset ja Kanadan pysyvät asukkaat. Kanadan pysyvät asukkaat ovat henkilöitä, jotka ovat läpäisseet asuinpaikkaa ja rikosrekisteriä koskevat tarkastukset sekä turvallisuustarkastukset sisältävän kansallisen arviointimenettelyn ja saavat laillisen luvan pysyvään oleskeluun Kanadassa.

Kansallinen turvallisuusviranomainen (NSA)	Viranomainen, joka vastaa Naton turvallisuusluokiteltujen tietojen turvallisuudesta kansallisissa virastoissa ja yksiköissä, sekä sotilas- että siviilialalla, kotimaassa ja ulkomailla.
Nato	”Nato” tarkoittaa Pohjois-Atlantin liittoa ja niitä elimiä, joihin sovelletaan joko Ottawassa 20. syyskuuta 1951 allekirjoitettua sopimusta Pohjois-Atlantin liiton, kansallisten edustajien ja kansainvälisen henkilöstön asemasta tai Pariisissa 28. elokuuta 1952 allekirjoitettua pöytäkirjaa Pohjois-Atlantin sopimuksen mukaisesti perustettujen kansainvälisten sotilasesikuntien asemasta.
Naton turvallisuusluokiteltu sopimus	Naton sotilas- tai siviilielimen tai Naton jäsenvaltion tekemä sopimus, jolla tuetaan Naton rahoittamaa tai hallinnoimaa ohjelmaa tai hanketta, joka edellyttää pääsyä Naton turvallisuusluokiteltuun tietoon tai tällaisen tiedon tuottamista.
Naton turvallisuusluokiteltu tieto	a) Tieto tarkoittaa missä tahansa muodossa välitettävää tietoa; b) turvallisuusluokiteltu tieto tarkoittaa tietoa tai aineistoa, jonka katsotaan edellyttävän suojaamista luvattomalta ilmitulolta ja joka on turvallisuusluokituksella osoitettu sellaiseksi; c) "aineisto" sisältää asiakirjat ja myös valmistetut ja valmisteilla olevat koneet, laitteet ja aseet; d) "asiakirja" tarkoittaa mitä tahansa muodossa tallennettua tietoa riippumatta sen fyysisestä muodosta tai ominaisuuksista, mukaan lukien rajoituksetta kirjalliset ja painotuotteet; tietojenkäsittelyssä käytettävät kortit ja nauhat; kartat, kaaviot, valokuvat, maalaukset, piirustukset, kaiverrukset, luonnokset, työmuistiinpanot ja -paperit, hiilipaperikopiot ja värinauhat; millä tahansa menetelmällä tai menettelyllä tehdyt jäljennökset; kaikenlaiset ääni-, puhe- ja magneettitallenteet sekä elektroniset, optiset ja videotallenteet; kannettavat tietotekniset laitteet, joissa on kiinteät tallennusvälineet, ja irrotettavat tietokoneen tallennusvälineet.
Naton tieto	Naton tietoa on kaikki turvallisuusluokiteltu ja turvallisuusluokittelematon tieto, jota jaetaan Natossa, riippumatta siitä, onko tieto peräisin Naton sotilas- tai siviilielimiltä vai onko se saatu Naton jäsenvaltioilta tai muista lähteistä kuin Natosta.

Naton tuotanto- ja logistiikkaorganisaatio (NPLO)	Apuelin, joka on perustettu Natoon suorittamaan Pohjois-Atlantin sopimuksesta johtuvia tehtäviä ja jolle Pohjois-Atlantin neuvosto antaa selvästi määritellyn organisatorisen, hallinnollisen ja taloudellisen riippumattomuuden. NPLO:ssa on johtokunta ja toimeenpaneva elin, joka koostuu pääjohtajasta ja henkilöstöstä.
Naton ohjelma	Neuvoston hyväksymä ohjelma, jota hallinnoi Naton määräämä johtokunta/toimisto Naton sääntöjen mukaisesti.
Naton hanke	Neuvoston hyväksymä hanke, jota hallinnoi Naton määräämä johtokunta/toimisto Naton sääntöjen mukaisesti.

Naton tuotanto- ja logistiikkaorganisaation johtokunta	NPLO:n toimeenpaneva elin.
Tiedonsaantitarve	Periaate, jonka mukaan tiedon mahdollisella vastaanottajalla katsotaan olevan tarve päästä tietoon, saada tieto siitä tai saada se haltuunsa pystyäkseen suorittamaan virallisia tehtäviä tai palveluja.
Neuvottelut	Ilmaus käsittää kaikki hankinta- tai alihankintasopimuksen tekemisen näkökohdat alkuvaiheen tarjouspyyntöjä koskevasta aieilmoituksesta lopulliseen päätökseen tehdä hankinta- tai alihankintasopimus.
Muun kuin luottamuksellisuuden varmistavat palvelut	Viestintä- ja tietojärjestelmien turvallisuuden varmistavat palvelut, joilla varmistetaan muiden turvallisuustavoitteiden kuin luottamuksellisuuden saavuttaminen, eli käytettävyys, eheys, todentaminen ja kiistämättömyys.
Kiistämättömyys	Toimenpide, jolla varmistetaan vastaanottajalle, että tiedon on lähettänyt tietty henkilö tai organisaatio, ja lähettäjälle, että aiotut vastaanottajat ovat vastaanottaneet tiedon.
Avoin säilytysalue	Alue, joka on rakennettu turvallisuusluokitellun tiedon avointa säilyttämistä varten turvallisuusvaatimusten mukaisesti ja jonka sotilas- tai siviilielimen johtaja on hyväksynyt tähän tarkoitukseen.
Alkuperäinen luovuttaja	Valtio tai kansainvälinen järjestö, jonka alaisuudessa tieto on tuotettu tai tuotu Natoon.
Alkuperäisen luovuttajan määräysvalta	Periaate, jonka mukaan valtio, Nato tai muu organisaatio, jonka alaisuudessa tieto on luotu, tuotettu tai tuotu Natoon, määrää tämän tiedon käyttöön sovellettavat säännöt ja vaatimukset ja on toimivaltainen tiedon koko elinkaaren aikaisten muutosten suhteen.
Kansalaisuusvaltio	Se maa, jonka kansalainen henkilö on.

Henkilöturvallisuusselvitystodistus (PSC)	Henkilöturvallisuusselvitystodistus (PSC) on kansallisen turvallisuusviranomaisen tai määrätyn turvallisuusviranomaisen myönteinen arvio, jolla virallisesti tunnustetaan luonnollisen henkilön kelpoisuus päästä turvallisuusluokkaan NATO CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin kuuluvaan tietoon, ottaen huomion henkilön lojaliteetti ja luotettavuus.
Ohjelman/hankkeen pääsopimus	Alkuperäinen hankesopimus, jonka toteuttamista johtaa ohjelmaa/hanketta varten määrätty Naton hankkeen johtokunta/toimisto.
Ensisijainen hankeosapuoli	Jäsenvaltion teollinen, kaupallinen tai muu toimija, joka on tehnyt Naton hankkeen johtokunnan/toimiston kanssa sopimuksen palvelun suorittamisesta tai tuotteen valmistamisesta Naton hankkeen yhteydessä ja joka voi puolestaan tehdä alihankintasopimuksia mahdollisten alihankkijoiden kanssa, jos tämä hyväksytään.

Ohjelman tai hankkeen turvallisuusluokituso pas	Ohjelman (hankkeen) turvallisuusohjeiden osa, jossa määritellään ohjelman turvallisuusluokitellut osat ja ilmoitetaan kyseiset turvallisuusluokat. Turvallisuusluokitusopasta voidaan laajentaa ohjelman koko elinkaaren ajan, ja tietoa sisältäviä osia voidaan turvallisuusluokitella uudelleen tai niiden luokitusta voidaan alentaa.
Ohjelman/hankkeen turvallisuusohjeet (PSI)	Turvallisuusmääräysten/-menettelyjen kokoelma, joka perustuu niihin Naton turvallisuussääntöihin ja näitä tukeviin direktiiveihin, joita sovelletaan tiettyyn hankkeeseen/ohjelmaan turvallisuusmenettelyjen vakioimiseksi. Turvallisuusohjeet ovat myös yksi pääsopimuksen liitteistä ja niitä voidaan tarkistaa ohjelman koko elinkaaren ajan. Ohjelmassa tehtävien alihankintasopimusten turvallisuutta koskeva lisälauseke perustuu turvallisuusohjeisiin.
Kirjattu postilähetys	Postin palvelu, jonka avulla lähetyksen kulkua lähettäjältä vastaanottajalle voidaan seurata ja lähettäjälle todistetaan, että lähetys on toimitettu.
Tiedon luovuttaminen	Tiedon vastaanottamisen salliminen vastaanottajana olevalle toimijalle siten, että tiedon katsotaan olevan koko toimijan käytettävissä. Luovuttamista voidaan edistää kyseistä toimijaa edustavan henkilön välityksellä.
Riski	Todennäköisyys siihen, että uhka toteutuu haavoittuvuuden vuoksi, jolloin luottamuksellisuus, eheys ja/tai käytettävyys vaarantuvat ja syntyy vahinkoa.
Riskienhallinta	Uhkien ja haavoittuvuuksien arviointiin perustuva järjestelmällinen lähestymistapa sen määrittämiseksi, mitä vastatoimia tarvitaan tietojen sekä niitä tukevien palvelujen ja resurssien turvallisuuden suojaamiseksi. Riskienhallintaan sisältyy niiden resurssien suunnittelu, järjestäminen, ohjaaminen ja valvonta, joiden avulla varmistetaan, että riski pysyy hyväksyttävyyden rajoissa.

Riskin omistaja	Henkilö tai elin, jonka vastuulla on arvioida tiettyyn riskiin liittyvät uhat, haavoittuvuudet ja vaikutukset tarkoituksena määrittää asianmukainen riskinottohalu riskiä vähentävien tekijöiden toteutumisen perusteella.
Turvallisuusnäkökoht ia koskeva kirje (SAL)	Asiakirja, jonka toimivaltainen viranomainen antaa osana muuta Naton turvallisuusluokiteltua sopimusta tai alihankintasopimusta kuin merkittäviä ohjelmia/hankkeita koskevia sopimuksia ja jossa yksilöidään sovellettavat turvallisuusvaatimukset tai tietoturvallisuuden suojaamista edellyttävät sopimuksen osat.
Turvallisuusvakuutus	Takeet, jotka annetaan Natolle joko suoraan tai Naton jäsenvaltion tai tietoa luovutettaessa takaajana toimivan Naton sotilas- tai siviilielimen välityksellä ja joiden mukaan muu kuin Natoon kuuluva Naton turvallisuusluokitellun tiedon vastaanottaja antaa tiedolle samantasoisen suojan kuin se suoja, jota Naton turvallisuusperiaatteet edellyttävät.

Tietoturvaloukkaus	Tahallinen tai tahaton teko tai laiminlyönti, joka on Naton turvallisuussääntöjen ja niitä tukevien direktiivien vastainen ja johtaa Naton turvallisuusluokitellun tiedon tai sitä tukevien palvelujen ja resurssien tosiasialliseen tai mahdolliseen vaarantumiseen (esimerkkejä: turvallisuusluokiteltu tieto katoaa kuljetuksen aikana; turvallisuusluokiteltua tietoa jätetään suojaamattomalle alueelle, jolle turvallisuusselvittämättömillä henkilöillä on pääsy ilman saattajaa; tilivelvollisuuden alaista asiakirjaa ei löydetä; turvallisuusluokiteltua tietoa on muutettu ilman lupaa tai hävitetty luvattomalla tavalla; tai viestintä- tai tietojärjestelmien palvelu estyy).
Turvallisuusluokituksen tarkistuslista	Turvallisuusnäkökohtia koskevan kirjeen (SAL) osa, jossa määritellään sopimuksen turvallisuusluokitellut osat ja ilmoitetaan kyseiset turvallisuusluokat. Ohjelmassa/hankkeessa tehtyjen sopimusten osien turvallisuusluokittelu perustuu kyseisen ohjelman/hankkeen turvallisuusohjeisiin.
Turva-avaimet	Turva-avaimet ovat avaimia, joita käytetään seuraavien lukoissa: turvallisuusluokitellun aineiston säilyttämiseen tarkoitetut turvakaapit; turvahuoneiden tai -vyöhykkeiden ovet; teknisesti turvallisuustarkastettujen turvahuoneiden tai -vyöhykkeiden ovet; ja turvallisuusluokiteltujen asiakirjojen jakeluun tarkoitetut turvakaapit.
Tietoturvapoikkeama	Tapahtuma tai muu tilanne, joka voi vaikuttaa haitallisesti Naton turvallisuusluokitellun tiedon turvallisuuteen ja edellyttää tutkintatoimia, jotta voidaan todeta tarkasti, onko kyseessä tietoturvaloukkaus vai vähäinen tietoturvapoikkeama.
Erityisluokan tieto	Tieto, johon sovelletaan ylimääräisiä käsittely-/suojaamismenettelyjä, kuten ATOMAL, yhteinen operaatiosuunnitelma (SIOP), BOHEMIA tai CRYPTO.
Takaaja	Naton jäsenvaltio tai Naton sotilas- tai siviilielin, joka toimii takeiden antajana vakuuttamalla tarvittavalla tavalla, että Naton turvallisuusluokiteltua tietoa vastaanottava Naton ulkopuolinen toimija antaa tälle tiedolle tarvittavan suojan Naton turvallisuusperiaatteissa ja niitä tukevissa ohjeissa määriteltyjen perusperiaatteiden ja vaatimusten mukaisesti.
Alihankintasopimus	Sopimus, jonka ensisijainen hankeosapuoli tekee toisen hankeosapuolen (alihankkijan) kanssa tavaroiden tai palvelujen toimittamisesta.
Alihankkija	Hankeosapuoli, jonka kanssa ensisijainen hankeosapuoli tekee alihankintasopimuksen.
Uhka	Naton turvallisuusluokitellun tiedon tai sitä tukevien palvelujen ja resurssien vaarantumisen, katoamisen tai varastamisen mahdollisuus. Uhka voidaan määritellä sen lähteen, motiivin tai tuloksen mukaan ja se voi olla tahallinen tai tahaton, väkivaltainen tai huomaamaton, ulkoinen tai sisäinen.

Haavoittuvuus	Heikkous, ominaisuus tai valvonnan puute, joka mahdollistaisi Naton turvallisuusluokiteltuun tietoon tai sitä tukeviin palveluihin ja resursseihin kohdistuvan uhan toteutumisen tai helpottaisi sitä.