Euroopan yhteisöjen

virallinen lehti

ISSN 1024-3038

L 101

44. vuosikerta

11. päivänä huhtikuuta 2001

Suomenkielinen laitos

Lainsäädäntö

Sisältö

I *Säädökset, jotka on julkaistava*

. . . . . .

II *Säädökset, joita ei tarvitse julkaista*

Neuvosto

2001/264/EY:

⋆ **Neuvoston päätös, tehty 19 päivänä maaliskuuta 2001, neuvoston turvallisuussääntöjen vahvistamisesta** 1

Hinta: 19,50 EUR

FI

Säädökset, joiden otsikot on painettu laihalla kirjasintyypillä, ovat maatalouspolitiikan alaan kuuluvia juoksevien asioiden hoitoon liittyviä säädöksiä, joiden voimassaoloaika on yleensä rajoitettu.

Kaikkien muiden säädösten otsikot on painettu lihavalla kirjasintyypillä ja merkitty tähdellä.

II

(Säädökset, joita ei tarvitse julkaista)

NEUVOSTO

NEUVOSTON PÄÄTÖS,

tehty 19 päivänä maaliskuuta 2001,

neuvoston turvallisuussääntöjen vahvistamisesta

(2001/264/EY)

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 207 artiklan 3 kohdan,

ottaa huomioon 5 päivänä kesäkuuta 2000 tehdyn neuvoston päätöksen 2000/396/EY, EHTY, Euratom neuvoston työjärjestyksen vahvistamisesta [1] ja erityisesti sen 24 artiklan,

sekä katsoo seuraavaa:

(1) Neuvoston toimintojen kehittämiseksi luottamuksellisuutta edellyttävillä aloilla on asianmukaista perustaa kattava neuvostoa, sen pääsihteeristöä ja jäsenvaltioita koskeva turvallisuusjärjestelmä.

(2) Tällaisessa järjestelmässä olisi koottava yhteen säädökseen tätä alaa koskevien kaikkien aikaisempien päätösten ja säännösten asiasisältö.

(3) Suurin osa CONFIDENTIEL UE- tai sitä luottamuksellisemman turvaluokan EU-tiedoista koskee käytännössä yhteistä turvallisuus- ja puolustuspolitiikkaa.

(4) Turvallisuusjärjestelmän tehokkuuden varmistamiseksi jäsenvaltioiden on liityttävä sen toimintaan toteuttamalla tarpeelliset kansalliset toimenpiteet tämän päätöksen säännösten noudattamiseksi, kun niiden toimivaltaiset viranomaiset ja virkamiehet käsittelevät EU:n turvaluokiteltuja tietoja.

(5) Neuvosto panee tyytyväisenä merkille komission aikovan tämän päätöksen soveltamispäivään mennessä ottaa käyttöön liitteiden mukainen kattava järjestelmä unionin päätöksentekomenettelyn kitkattoman toiminnan varmistamiseksi.

(6) Neuvosto korostaa sitä, että Euroopan parlamentti ja komissio on tarvittaessa saatava mukaan noudattamaan niitä luottamuksellisuutta koskevia sääntöjä ja vaatimuksia, jotka ovat välttämättömiä unionin ja sen jäsenvaltioiden etujen suojelemiseksi.

(7) Tämä päätös tehdään sanotun kuitenkaan rajoittamatta perustamissopimuksen 255 artiklan ja sen täytäntöönpanevien välineiden soveltamista.

(8) Tämä päätös tehdään sanotun kuitenkaan rajoittamatta jäsenvaltioiden olemassa olevien käytäntöjen soveltamista niiden ilmoittaessa kansallisille parlamenteilleen unionin toimista,

ON PÄÄTTÄNYT SEURAAVAA:

1 artikla

Hyväksytään liitteessä olevat neuvoston turvallisuussäännöt.

2 artikla

1. Korkeana edustajana toimiva pääsihteeri toteuttaa asianmukaiset toimenpiteet sen varmistamiseksi, että neuvoston pääsihteeristön virkamiehet ja muu henkilöstö, pääsihteeristön ulkopuoliset toimeksisaajat ja pääsihteeristössä avustajina toimivat henkilöt noudattavat EU:n turvaluokiteltuja tietoja käsitellessään 1 artiklassa tarkoitettuja säännöksiä, ja että niitä noudatetaan myös neuvoston tiloissa ja EU:n hajautetuissa erillisvirastoissa [2].

[1] EYVL L 149, 23.6.2000, s. 21.

[2] Ks. neuvoston päätelmät, 10. marraskuuta 2000.

2. Jäsenvaltiot toteuttavat asianmukaiset toimenpiteet kansallisten järjestelyjensä mukaisesti sen varmistamiseksi, että niiden yksiköissä ja tiloissa työskentelevät seuraavat henkilöt noudattavat 1 artiklassa tarkoitettuja säännöksiä käsitellessään EU:n turvaluokiteltuja tietoja:

a) jäsenvaltioiden pysyvien Euroopan unionissa olevien edustustojen jäsenet sekä neuvoston tai sen elinten kokouksiin tai muihin neuvoston toimiin osallistuvat kansallisten valtuuskuntien jäsenet;

b) muut jäsenvaltioiden kansallisiin hallintoihin kuuluvat henkilöt, jotka käsittelevät EU:n turvaluokiteltuja tietoja riippumatta siitä, ovatko he palveluksessa jäsenvaltioiden alueella tai ulkomailla; ja

c) EU:n turvaluokiteltuja tietoja käsittelevät jäsenvaltioiden ulkopuoliset toimeksisaajat ja lähetetyt työntekijät.

Jäsenvaltioiden on ilmoitettava toteutetuista toimenpiteistä viipymättä neuvoston pääsihteeristölle.

3. Edellä 1 ja 2 kohdassa tarkoitetut toimenpiteet on toteutettava ennen 30 päivää marraskuuta 2001.

3 artikla

Korkeana edustajana toimiva pääsihteeri voi toteuttaa liitteen II osan I jakson 1 ja 2 kohdan mukaisia toimenpiteitä noudattaen liitteen I osassa olevia turvallisuutta koskevia perusperiaatteita ja vähimmäisvaatimuksia.

4 artikla

Tällä päätöksellä korvataan sen soveltamispäivästä alkaen

a) neuvoston päätös 98/319/EY, tehty 27 päivänä huhtikuuta 1998, neuvoston hallussa olevien luokiteltujen tietojen saamiseen oikeutettuja neuvoston pääsihteeristön virkamiehiä ja muuta henkilöstöä koskevasta lupamenettelystä [1];

b) korkeana edustajana toimivan pääsihteerin päätös, tehty 27 päivänä heinäkuuta 2000, neuvoston pääsihteeristössä sovellettavista luokiteltuja tietoja koskevista suojaustoimenpiteistä [2];

c) neuvoston pääsihteerin päätös N:o 433/97, tehty 22 päivänä toukokuuta 1997, Cortesy-verkon toiminnasta vastaavien virkamiesten luotettavuusselvityksestä.

5 artikla

1. Päätöstä noudatetaan siitä päivästä, jona se julkaistaan.

2. Sitä sovelletaan 1 päivästä joulukuuta 2001.

Tehty Brysselissä 19 päivänä maaliskuuta 2001.

Neuvoston puolesta

Puheenjohtaja

A. LINDH

[1] EYVL L 140, 12.5.1998, s. 12.

[2] EYVL C 239, 23.8.2000, s. 1.

LIITE

EUROOPAN UNIONIN NEUVOSTON TURVALLISUUSSÄÄNNÖT

SISÄLLYSLUETTELO

Sivu

I OSA

Turvallisuutta koskevat perusperiaatteet ja vähimmäisvaatimukset 6

II OSA 10

I JAKSO

Euroopan unionin neuvoston turvallisuusorganisaatio 10

II JAKSO

Turvaluokat ja merkinnät 12

III JAKSO

Turvaluokittelun hallinnointi 13

IV JAKSO

Fyysinen turvallisuus 14

V JAKSO

Tarpeellisuusperiaatetta ja luotettavuusselvitystä koskevat yleissäännöt 18

VI JAKSO

Pääsihteeristön virkamiehiin ja muuhun henkilöstöön sovellettava luotettavuusselvitysmenettely 20

VII JAKSO

EU:n turvaluokitellun aineiston valmistelu, jakelu, toimittaminen, varastointi ja hävittäminen 22

VIII JAKSO

TRÈS SECRET UE / EU TOP SECRET -rekisterit 29

IX JAKSO

Turvatoimet, joita sovelletaan sellaisten neuvoston tilojen ulkopuolella pidettävien erityiskokousten aikana, joissa käsitellään arkaluonteisia asioita 31

X JAKSO

Turvallisuussääntöjen rikkominen tai EU:n turvaluokiteltujen tietojen vaarantaminen 34

XI JAKSO

Tietotekniikka- ja tietoliikennejärjestelmissä käsiteltävien tietojen suojaus 36

XII JAKSO

EU:n turvaluokiteltujen tietojen luovuttaminen kolmansille valtioille tai kansainvälisille järjestöille 48

Sivu

Lisäykset

Lisäys 1

Kansallisten turvallisuusviranomaisten luettelo 50

Lisäys 2

Kansallisten turvaluokkien vertailu 53

Lisäys 3

Luokitteluohjeet 54

Lisäys 4

Ohjeet EU:n turvaluokiteltujen tietojen luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille — Tason 1 yhteistyö 58

Lisäys 5

Ohjeet EU:n turvaluokiteltujen tietojen luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille — Tason 2 yhteistyö 61

Lisäys 6

Ohjeet EU:n turvaluokiteltujen tietojen luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille — Tason 3 yhteistyö 64

I OSA

TURVALLISUUTTA KOSKEVAT PERUSPERIAATTEET JA VÄHIMMÄISVAATIMUKSET

JOHDANTO

1. Näillä säännöksillä säädetään niistä turvallisuutta koskevista perusperiaatteista ja vähimmäisvaatimuksista, joita neuvoston, neuvoston pääsihteeristön, jäsenvaltioiden ja Euroopan unionin hajautettujen virastojen (jäljempänä 'EU:n hajautetut virastot') on noudatettava, jotta turvallisuus on taattu ja voidaan olla vakuuttuneita siitä, että yhteiset suojausvaatimukset on vahvistettu.

2. Ilmaisulla 'EU:n turvaluokitellut tiedot' tarkoitetaan mitä tahansa tietoa tai aineistoa, jonka luvaton ilmitulo vahingoittaisi eri tavoin EU:n tai jonkin sen jäsenvaltion etuja riippumatta siitä, onko tällainen tieto peräisin EU:n sisältä vai onko se saatu jäsenvaltioilta, kolmansilta valtioilta vai kansainvälisiltä järjestöiltä.

3. Näissä säännöissä tarkoitetaan:

   a) 'asiakirjalla' mitä tahansa kirjettä, ilmoitusta, pöytäkirjaa, raporttia, muistiota, signaalia/viestiä, luonnosta, valokuvaa, diakuvaa, filmiä, karttaa, taulukkoa, suunnitelmaa, lehtiötä, monistuspaperia, hiilipaperia, kirjoituskoneen tai kirjoittimen värinauhaa, nauhurin nauhaa, kasettia, tietokoneen levykettä, CD-romia tai muuta fyysistä välinettä, jolle on tallennettu tietoa;

   b) 'aineistolla' edellä a alakohdassa määriteltyä 'asiakirjaa' sekä mitä tahansa joko tuotettua tai tuotannossa olevaa laitetta tai keinoa.

4. Turvallisuuden olennaisimmat tavoitteet ovat seuraavat:

   a) EU:n turvaluokiteltujen tietojen suojaaminen vakoilulta, vaarantamiselta ja luvattomalta ilmitulolta;

   b) tieto- ja tietoliikennejärjestelmissä ja -verkoissa käsiteltävien EU:n tietojen suojaaminen tietojen eheyteen ja käyttömahdollisuuksiin liittyviltä uhilta;

   c) niiden tilojen suojaaminen sabotoinnilta ja tahalliselta vahingoittamiselta, joissa EU:n tietoja säilytetään; ja

   d) suojaamisen epäonnistuessa vahinkojen arviointi, niiden seuraamusten rajoittaminen ja tarpeellisten korjaavien toimenpiteiden toteuttaminen.

5. Taattu turvallisuus perustuu seuraaviin seikkoihin:

   a) jokaisessa jäsenvaltiossa on kansallinen turvallisuusorganisaatio, joka vastaa siitä, että

      i) vakoilua, sabotointia, terrorismia ja muuta haitallista toimintaa koskevat tiedot kerätään ja rekisteröidään; ja että

      ii) jäsenvaltion hallitukselle ja sitä kautta neuvostolle annetaan tietoa turvallisuusuhkien luonteesta ja keinoista suojautua niitä vastaan;

   b) jokaisessa jäsenvaltiossa ja neuvoston pääsihteeristössä on tietojen teknisestä turvallisuudesta vastaava tekniikkaviranomainen, jonka vastuulla on työskennellä turvallisuusviranomaisten kanssa tietojen hankkimiseksi ja neuvojen antamiseksi turvallisuutta uhkaavista teknisistä seikoista ja keinoista suojautua niitä vastaan;

   c) hallituksen yksiköt, virastot ja asiaan kuuluvien neuvoston pääsihteeristön yksiköt tekevät säännöllistä yhteistyötä, jotta päätettäisiin ja tarvittaessa suositeltaisiin,

      i) mitä tietoja, voimavaroja ja laitteita on suojeltava; ja

      ii) mitä yhteisiä suojelun vakio-ohjeita on otettava käyttöön.

6. Luottamuksellisuuden säilyttäminen edellyttää huolellisuutta ja kokemusta valittaessa suojattavaksi tarkoitettua tietoa ja aineistoa ja arvioitaessa sitä, minkä tasoista suojausta ne edellyttävät. On olennaisen tärkeää, että suojauksen taso on sitä korkeampi, mitä ratkaisevampi tehtävä suojattavalla yksittäisellä tiedolla ja aineistolla turvallisuuden kannalta on. Kitkattoman tiedonkulun varmistamiseksi on toteutettava toimenpiteitä yliluokituksen välttämiseksi. Nämä periaatteet voidaan toteuttaa luokittelujärjestelmällä: suunniteltaessa ja järjestettäessä toimia vakoilun, sabotoinnin, terrorismin ja muiden uhkien torjumiseksi olisi noudatettava samaa luokittelujärjestelmää, jotta tärkeimpiä tiloja, joissa turvaluokiteltuja tietoja säilytetään, ja näiden tilojen herkimpiä alueita suojeltaisiin tehokkaimmin.

PERUSPERIAATTEET

7. **Turvatoimet**

a) Turvatoimien on koskettava kaikkia, joilla on pääsy turvaluokiteltuihin tietoihin, turvaluokiteltuja tietoja sisältäviin tiedotusvälineisiin, kaikkiin tiloihin, joissa tällaisia tietoja säilytetään, ja tärkeisiin laitoksiin.

b) Turvatoimet on suunniteltava niin, että niiden avulla voidaan paljastaa ja vapauttaa tehtävistään tai siirtää muihin tehtäviin henkilöt, joiden aseman vuoksi turvaluokiteltujen tietojen ja tilojen, joissa niitä säilytetään, turvallisuus voisi vaarantua.

c) Turvatoimilla on estettävä luvaton pääsy turvaluokiteltuihin tietoihin ja tiloihin, joissa niitä säilytetään.

d) Turvatoimilla on varmistettava se, että luokiteltuja tietoja levitetään ainoastaan tarpeellisuusperiaatteen pohjalta: tämä on olennaista kaikkien turvallisuusnäkökohtien kannalta.

e) Turvatoimilla on varmistettava tietojen eheys (eli estettävä tietojen turmeleminen, luvaton muuttaminen tai luvaton poistaminen) ja käyttömahdollisuudet (oikeutta tutustua tietoihin ei kielletä tietoa tarvitsevilta ja tiedonsaantiin luvan saaneilta) riippumatta siitä, ovatko tiedot luokiteltuja vai eivät. Tämä koskee erityisesti sähkömagneettisesti säilytettäviä, käsiteltäviä tai lähetettäviä tietoja.

TURVALLISUUSORGANISAATIO

Yhteiset vähimmäisvaatimukset

8. Neuvoston ja jäsenvaltioiden on varmistettava se, että kaikki hallinnon ja/tai hallituksen yksiköt, muut EU:n toimielimet, virastot ja toimeksisaajat noudattavat turvallisuutta koskevia vähimmäisvaatimuksia, jotta voidaan luottaa siihen, että EU:n turvaluokiteltuja tietoja käsitellään kaikkialla yhtä huolellisesti. Vähimmäisvaatimuksiin on kuuluttava arviointiperusteet henkilöstön luotettavuuden selvittämiseksi ja menettelyt EU:n turvaluokiteltujen tietojen suojaamiseksi.

HENKILÖISTÄ RIIPPUVA TURVALLISUUS

Henkilöstön luotettavuuden selvittäminen

9. Kaikkien, jotka pyytävät saada CONFIDENTIEL UE tai sitä luottamuksellisemman turvaluokan tietoja, luotettavuus on selvitettävä asiaan kuuluvalla tavalla ennen luvan myöntämistä. Tällainen selvitys on tehtävä myös niiden henkilöiden osalta, joiden tehtäviin kuuluu turvaluokiteltuja tietoja sisältävien tieto- tai tietoliikennejärjestelmien tekninen käyttö tai kunnossapito. Selvitys on suunniteltava sellaiseksi, että tietystä henkilöstä voidaan sanoa, että

a) hän on ehdottoman luotettava;

b) hän on luonteeltaan ja harkintakyvyltään niin luja, että hänen käsiteltäväkseen voidaan epäilyksettä uskoa turvaluokiteltuja tietoja; tai että

c) hän saattaa olla altis ulkoiselle tai muista lähteistä peräisin olevalle painostukselle esimerkiksi sen vuoksi, että hän on asunut sellaisessa paikassa tai omannut sellaisia yhteyksiä, jotka saattavat muodostaa tietoturvariskin.

Erityisen perusteellisesti on tarkastettava sellaisten henkilöiden luotettavuus,

d) joille on tarkoitus sallia pääsy TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoihin;

e) jotka ovat sellaisessa asemassa, että heidän tehtäviinsä kuuluu päästä säännöllisesti huomattavaan määrään SECRET UE -turvaluokan tietoja; ja

f) joilla on tehtäviensä vuoksi oikeus päästä EU:n tehtävien kannalta oleellisiin tieto- tai tietoliikennejärjestelmiin ja joilla on näin tilaisuus päästä luvatta suureen määrään EU:n turvaluokiteltua tietoa tai aiheuttaa EU:n tehtäville teknisen sabotoinnin kautta vakavaa vahinkoa.

Edellä d, e ja f alakohdissa kuvattujen olosuhteiden ollessa kyseessä on käytettävä mahdollisimman tehokkaasti hyväksi taustatutkimustekniikkaa.

10. Jos henkilöitä, joilla ei ole tehtävien mukaista valtuutusta päästä tietoihin, on määrä ottaa palvelukseen tehtäviin, joissa he voivat päästä EU:n turvaluokiteltuihin tietoihin (kuten lähetit, turvamiehet, kunnossapitohenkilöstö ja siivoojat jne.), heidän luotettavuutensa on ensin asiaan kuuluvasti selvitettävä.

Luotettavuusselvitysrekisteri

11. Kaikkien yksiköiden, elinten tai virastojen, joissa käsitellään EU:n turvaluokiteltuja tietoja tai joissa käytetään tehtävien kannalta oleellisia tieto- ja tietoliikennejärjestelmiä, on pidettävä rekisteriä palvelukseen otetun henkilöstön luotettavuusselvityksistä. Luotettavuusselvitys on tarvittaessa tarkistettava sen varmistamiseksi, että se on kyseisen henkilön nykyisten tehtävien kannalta riittävä. Luotettavuusselvitys on tarkistettava uudelleen ensisijaisen kiireellisesti, jos saadaan uusia tietoja, joiden mukaan henkilön työskentely turvaluokiteltujen tietojen parissa ei enää ole turvallisuusetujen mukaista. Kyseisen yksikön, elimen tai viraston esimiehen on pidettävä luotettavuusselvitysrekisteriä.

Henkilöstölle annettavat turvallisuusohjeet

12. Henkilöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voisivat päästä turvaluokiteltuihin tietoihin, on annettava heti aluksi ja säännöllisin väliajoin tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyistä. Yksi hyödyllinen menettely on edellyttää, että kaikki tällaiset henkilöt todistavat kirjallisesti, että he ymmärtävät täysin tehtäviensä kannalta olennaiset turvallisuusvaatimukset.

Johdon velvollisuudet

13. Johdon velvollisuus on tietää, ketkä kyseisen johdon alaisuudessa olevasta henkilöstöstä työskentelevät turvaluokiteltujen tietojen parissa tai voivat päästä yksikön tehtävien kannalta olennaisiin tieto- ja tietoliikennejärjestelmiin, ja johdon on pidettävä kirjaa ja raportoitava kaikista tapahtumista tai ilmeisistä puutteista, jotka voivat vaikuttaa turvallisuuteen.

Henkilöstön oikeudellinen asema turvallisuusasioissa

14. On otettava käyttöön menettelyt sen varmistamiseksi, että henkilöä koskevien kielteisten seikkojen tullessa ilmi määritellään, onko hän tekemisissä turvaluokiteltujen tietojen kanssa tai sallitaanko hänen päästä yksikön toiminnan kannalta olennaisiin tieto- ja tietoliikennejärjestelmiin ja onko kyseiselle viranomaiselle ilmoitettu asiasta. Jos henkilön todetaan olevan turvallisuusriski, hänet on estettävä suorittamasta tehtäviä, joissa hän voi vaarantaa turvallisuuden, tai hänet on siirrettävä suorittamaan muita tehtäviä.

FYYSINEN TURVALLISUUS

Suojauksen tarve

15. EU:n turvaluokiteltujen tietojen suojaamiseksi sovellettavien fyysisten turvatoimien taso on suhteutettava säilytettävän tiedon ja aineiston turvaluokkaan, määrään ja uhkaan. Sen vuoksi on oltava huolellinen, jotta vältyttäisiin sekä yli- että aliluokittelulta, ja turvaluokka on tarkistettava säännöllisesti. Kaikkien EU:n turvaluokiteltuja tietoja hallussaan pitävien on noudatettava yhdenmukaista käytäntöä tietojen luokittelun osalta ja yhteisiä suojausstandardeja suojausta edellyttävän tiedon ja aineiston säilyttämisen, siirron ja levittämisen osalta.

Tarkastukset

16. Ennen kuin EU:n turvaluokiteltuja tietoja säilyttävissä tiloissa toimivat henkilöt poistuvat säilytystiloista, heidän on varmistettava, että tiedot ovat turvassa ja että kaikki turvalaitteet ovat toimintavalmiina (lukot, hälytykset jne.). Lisäksi tehdään erillisiä tarkastuksia työajan jälkeen.

Kiinteistöjen turvallisuus

17. Kiinteistöt, joissa on EU:n turvaluokiteltuja tietoja tai EU:n tehtävien kannalta olennaisia tieto- ja tietoliikennejärjestelmiä, on suojeltava, jottei niihin pääse luvatta. Suojellaanko EU:n turvaluokiteltuja tietoja esimerkiksi varustamalla niitä säilyttävien tilojen ikkunat kalterein, lukitsemalla ovet, vartioimalla sisäänkäyntiä, varustamalla tilat automaattisella sisääntulojärjestelmällä, tekemällä turvatarkastuksia ja -kierroksia, varustamalla tilat hälytys- tai murronpaljastusjärjestelmillä tai käyttämällä vartiokoiria, riippuu

a) suojattavan tiedon ja aineiston turvaluokasta, määrästä ja sijainnista;

b) ominaisuuksista, joita kyseisten tietojen ja aineiston turvalliselta säilytyspaikalta edellytetään; ja

c) itse kiinteistön fyysisistä ominaisuuksista ja sijainnista.

18. Myös tieto- ja tietoliikennejärjestelmien suojauksen luonne riippuu siitä, kuinka tärkeinä tietoja pidetään ja kuinka pahoja vahinkoja turvallisuuden vaarantamisesta koituisi sen kiinteistön fyysisistä ominaisuuksista ja sijainnista, joissa järjestelmät ovat.

Varautumissuunnitelmat

19. Turvaluokiteltujen tietojen suojauksesta paikallisen tai kansallisen hätätilan aikana on laadittava ennakkoon yksityiskohtaiset suunnitelmat.

TIETOTURVALLISUUS (INFOSEC)

20. Infosec liittyy turvatoimien määrittämiseen ja soveltamiseen käsiteltävien, tallennettavien tai välitettävien tietojen suojaamiseksi sekä tietojen ja muiden elektronisten järjestelmien suojaamiseksi tahattomilta ja tahallisilta toimilta, jotta tietojen luotettavuus, eheys ja käytettävyys säilyvät. On toteutettava asiaan kuuluvia vastatoimia, jotta käyttäjät, joilla ei ole lupa käyttää EU:n tietoja eivät voi käyttää tietoja ja jotta käyttäjiltä, joilla on lupa käyttää EU:n tietoja, ei sitä evätä ja jotta EU:n tietoja ei turmella, luvatta muuteta tai poisteta.

SABOTOINNIN JA MUUNLAISEN TAHALLISEN VAHINGOITTAMISEN TORJUNTA

21. Fyysiset varotoimet tärkeitä turvaluokiteltuja tietoja säilyttävien laitosten suojelemiseksi on paras turvata sabotointia ja muunlaista tahallista vahingoittamista vastaan, eikä niitä voi korvata tehokkaasti henkilöstön luotettavuuden selvittämisellä. Toimivaltaisen kansallisen elimen on kerättävä tietoja vakoilusta, sabotoinnista, terrorismista ja muusta haitallisesta toiminnasta.

TURVALUOKITELTUJEN TIETOJEN LUOVUTTAMINEN KOLMANSILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE

22. Päätös neuvostossa pidettävien EU:n turvaluokiteltujen tietojen luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille tehdään neuvostossa. Jos luovutettavaksi haluttujen tietojen luovuttaja ei ole neuvosto, neuvoston on ensin saatava luovuttajan suostumus luovutukselle. Jos luovuttajaa ei tiedetä, neuvosto ottaa luovuttajan vastuun itselleen.

23. Jos neuvosto vastaanottaa turvaluokiteltuja tietoja kolmansilta valtioilta, kansainvälisiltä järjestöiltä tai muilta kolmansilta osapuolilta, tiedot on suojattava niiden turvaluokkaa ja näissä säännöissä vahvistettuja EU:n turvaluokiteltuja tietoja koskevia vaatimuksia vastaavalla tavalla, tai sellaisia tätä tiukempia vaatimuksia vastaavalla tavalla, joita tiedot luovuttava kolmas osapuoli saattaa edellyttää. Keskinäiset tarkastukset ovat mahdollisia.

24. Edellä esitetyt periaatteet on pantava täytäntöön II jaksossa esitettyjen yksityiskohtaisten säännösten mukaisesti.

II OSA

I JAKSO

EUROOPAN UNIONIN NEUVOSTON TURVALLISUUSORGANISAATIO

Korkeana edustajana toimiva pääsihteeri

1. Korkeana edustajana toimiva pääsihteeri

   a) panee täytäntöön neuvoston turvallisuuspolitiikan;

   b) käsittelee turvallisuusongelmia, jotka neuvosto tai sen toimivaltaiset elimet antavat hänen ratkaistavakseen;

   c) käsittelee tiiviissä yhteistyössä jäsenvaltioiden kansallisten turvallisuusviranomaisten (tai muiden asiaan kuuluvien viranomaisten) kanssa neuvoston turvallisuuspolitiikan muuttamiseen liittyviä kysymyksiä. Lisäyksessä 1 on luettelo näistä viranomaisista.

2. Korkeana edustajana toimivan pääsihteerin vastuulla on erityisesti

   a) koordinoida kaikkia neuvoston toimintoihin liittyviä turvallisuusasioita;

   b) pyytää jokaista jäsenmaata ja tarvittaessa EU:n hajautettuja virastoja perustamaan TRÈS SECRET UE / EU TOP SECRET -keskusrekisteri;

   c) osoittaa jäsenvaltioiden nimetyille turvallisuusviranomaisille pyyntö tehdä luotettavuusselvitys neuvoston pääsihteeristön palveluksessa olevista henkilöistä VI jakson mukaisesti;

   d) tutkia tai määrätä tutkimaan jokainen sellainen EU:n turvaluokitellun tiedon vuoto, joka on alustavan näytön perusteella tapahtunut pääsihteeristössä tai jossakin EU:n hajautetussa virastossa;

   e) pyytää asiaan kuuluvia turvallisuusviranomaisia käynnistämään tutkinta, jos EU:n turvaluokiteltuja tietoja on ilmeisesti vuotanut neuvoston pääsihteeristössä tai EU:n hajautetuissa virastoissa, ja koordinoida tutkimuksia, jos asiaa käsittelee useampi turvallisuusviranomainen;

   f) tehdä yhteisiä kyseisten kansallisten turvallisuusviranomaisten kanssa sovittuja määräaikaistarkastuksia EU:n turvaluokiteltujen tietojen turvajärjestelyistä jäsenvaltioissa;

   g) olla tiiviissä yhteydessä kaikkien asiaan kuuluvien turvallisuusviranomaisten kanssa turvallisuuden kokonaiskoordinoinnin varmistamiseksi; ja

   h) valvoa jatkuvasti neuvoston turvallisuuspolitiikkaa ja -menettelyjä ja laatia pyynnöstä aiheellisia suosituksia. Tätä silmällä pitäen korkeana edustajana toimiva pääsihteeri esittää neuvostolle vuosittaisen tarkastussuunnitelman, jonka on laatinut neuvoston pääsihteeristön turvallisuusyksikkö.

Neuvoston turvakomitea

3. On perustettava turvakomitea. Se koostuu kunkin jäsenvaltion turvallisuusviranomaisten edustajista. Turvakomitean puheenjohtajana toimii korkeana edustajana toimiva pääsihteeri tai hänen sijaisensa. Myös EU:n hajautettujen virastojen edustajia voidaan kutsua komitean kokouksiin, jos niissä käsitellään niitä koskevia kysymyksiä.

4. Turvakomitea kokoontuu neuvoston toimeksiannosta tai korkeana edustajana toimivan pääsihteerin taikka kansallisen turvallisuusviranomaisen pyynnöstä. Komitealla on valtuudet tutkia ja arvioida kaikkia neuvoston menettelyihin liittyviä turvallisuusasioita ja esittää tarvittaessa suosituksia neuvostolle. Neuvoston pääsihteeristön toimien osalta komitealla on valtuudet tehdä suosituksia turvallisuuskysymyksistä korkeana edustajana toimivalle pääsihteerille.

Neuvoston pääsihteeristön turvallisuusyksikkö

5. Täyttääkseen edellä 1 ja 2 kohdassa mainitut velvoitteensa korkeana edustajana toimivalla pääsihteerillä on oltava käytössään neuvoston pääsihteeristön turvallisuusyksikkö turvatoimien koordinoimiseksi, johtamiseksi ja täytäntöönpanemiseksi.

6. Neuvoston pääsihteeristön turvallisuusyksikön päällikkö on korkeana edustajana toimivan pääsihteerin tärkein neuvonantaja turvallisuusasioissa, ja hän toimii turvakomitean sihteerinä. Hän johtaa turvallisuussääntöjen ajan tasalle saattamista ja koordinoi turvatoimia jäsenvaltioiden toimivaltaisten viranomaisten kanssa ja tarvittaessa turvallisuussopimusten kautta neuvoston kanssa yhteydessä olevien kansainvälisten järjestöjen kanssa. Tältä osin hän toimii yhteyshenkilönä.

7. Neuvoston pääsihteeristön turvallisuusyksikön päällikkö vastaa neuvoston pääsihteeristöön hankittavien tietojärjestelmien ja -verkkojen hyväksymisestä. Hän päättää tarvittaessa yhdessä asiaan kuuluvien kansallisten turvallisuusviranomaisten kanssa sellaisten tietojärjestelmien ja -verkkojen hyväksymisestä, joissa neuvoston pääsihteeristö, jäsenvaltiot, EU:n hajautetut virastot ja/tai kolmannet osapuolet (valtiot tai kansainväliset järjestöt) ovat osallisina.

EU:n hajautetut virastot

8. EU:n hajautettujen virastojen johtajat vastaavat turvallisuuden täytäntöönpanosta laitoksessaan. Yleensä he nimittävät jonkin alaisensa vastuuhenkilökseen turvallisuusasioissa. Tämä nimitetään turvavirkailijaksi.

Jäsenvaltiot

9. Jäsenvaltion on nimettävä kansallinen turvallisuusviranomainen, joka vastaa EU:n turvaluokiteltujen tietojen turvallisuudesta [1].

10. Kukin jäsenvaltioiden hallinnon osalta vastaava kansallinen turvallisuusviranomainen vastaa

    a) julkisten tai yksityisten kotimaassa tai ulkomailla toimivien kansallisten yksiköiden, elinten tai virastojen hallussa olevien EU:n turvaluokiteltujen tietojen turvallisuuden ylläpidosta;

    b) TRÈS SECRET UE / EU TOP SECRET -rekisterien pitämistä koskevan luvan antamisesta (lupa voidaan antaa keskusrekisterissä toimivan TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoja valvovan viranomaisen tehtäväksi);

    c) EU:n turvaluokiteltujen tietojen suojaamiseksi tehtyjen turvajärjestelyjen määräaikaistarkastuksista;

    d) sen varmistamisesta, että kansallisissa yksiköissä, elimissä tai virastoissa toimiville sekä koti- että ulkomaisille henkilöille, joilla on pääsy TRÈS SECRET UE / EU TOP SECRET-, SECRET UE- tai CONFIDENTIEL UE -turvaluokkien tietoihin, on tehty luotettavuusselvitys; ja

    e) tarpeellisina pitämiensä turvallisuussuunnitelmien laatimisesta sen estämiseksi, ettei EU:n turvaluokiteltuja tietoja joudu vääriin käsiin.

Keskinäiset turvatarkastukset

11. Neuvoston pääsihteeristön turvallisuusyksikön ja kyseisten kansallisten turvallisuusviranomaisten on yhdessä ja yhteisestä sopimuksesta [2] tehtävä määräaikaistarkastuksia, jotka koskevat EU:n turvaluokiteltujen tietojen suojaamiseksi tehtäviä turvajärjestelyjä neuvoston pääsihteeristössä, Euroopan unionin jäsenvaltioiden pysyvissä edustustoissa sekä neuvoston rakennuksissa sijaitsevissa jäsenvaltioiden tiloissa.

12. Neuvoston pääsihteeristön turvallisuusyksikön tai pääsihteerin pyynnöstä EU:n turvaluokiteltuja tietoja säilyttävän jäsenvaltion kansallisten viranomaisten on tehtävä määräaikaistarkastuksia, jotka koskevat tietojen suojaamista EU:n hajautetuissa virastoissa.

---

[1] Lisäyksessä 1 on luettelo EU:n turvaluokitelluista tiedoista vastaavista kansallisista turvallisuusviranomaisista.

[2] Sanotun kuitenkaan rajoittamatta vuonna 1961 tehdyn diplomaattisia suhteita koskevan Wienin yleissopimuksen soveltamista.

II JAKSO

TURVALUOKAT JA MERKINNÄT

TURVALUOKAT ([1])

Tiedot jaetaan seuraaviin turvaluokkiin:

1. TRÈS SECRET UE / EU TOP SECRET: Tätä turvaluokkaa sovelletaan vain sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi vahingoittaa poikkeuksellisen vakavasti Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja.

2. SECRET UE: Tätä turvaluokkaa sovelletaan vain sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi vahingoittaa vakavasti Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja.

3. CONFIDENTIEL UE: Tätä turvaluokkaa sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi haitata Euroopan unionin tai sen yhden tai useamman jäsenvaltion etuja.

4. RESTREINT UE: Tätä turvaluokkaa sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi olla epäedullista Euroopan unionin tai sen yhden tai useamman jäsenvaltion etujen kannalta.

MERKINNÄT

5. Asiakirjan, joka annetaan tiedoksi tarpeellisuusperiaatteella, tiettyyn kohtaan ja erityisjakelun yhteyteen voidaan tehdä *varoitus*merkintä.

6. ESDP/PESD -merkintää käytetään sellaisissa asiakirjoissa tai asiakirjojen käännöksissä, jotka koskevat unionin tai sen yhden tai useamman jäsenvaltion turvallisuutta ja puolustusta tai sotilaallista taikka ei-sotilaallista kriisinhallintaa.

7. Erityisesti tietotekniikkajärjestelmiin liittyvissä asiakirjoissa voidaan käyttää lisämerkintää, jolla osoitetaan asianmukaisissa säännöissä määriteltyjen lisäturvatoimien tarve.

TURVALUOKAN JA MERKINTÖJEN ILMOITTAMINEN ASIAKIRJOISSA

8. Turvaluokka ja merkinnät tehdään seuraavasti:

   a) RESTREINT UE -turvaluokkien asiakirjoihin mekaanisesti tai sähköisesti;

   b) CONFIDENTIEL UE -turvaluokkien asiakirjoihin mekaanisesti ja käsin tai painamalla leimoin varustettuun, kirjattuun asiakirjaan; ja

   c) SECRET UE- ja TRÈS SECRET UE / EU TOP SECRET -turvaluokkien asiakirjoihin mekaanisesti ja käsin.

([1]) Lisäyksessä 2 on EU:n, NATOn, WEU:n ja jäsenvaltioiden turvaluokittelua koskeva vertailutaulukko.

III JAKSO

TURVALUOKITTELUN HALLINNOINTI

1. Tiedot turvaluokitellaan vain, jos se on tarpeen. Turvaluokka on ilmoitettava selvästi ja oikein, ja se on säilytettävä vain niin kauan, kuin tiedot on suojattava.

2. Vain tietojen luovuttaja vastaa tietojen luokittelusta ja mahdollisesta myöhemmästä turvaluokan alentamisesta tai poistamisesta ([1]).

   Neuvoston pääsihteeristön virkamiehet ja muuhun henkilöstöön kuuluvat luokittelevat tiedot ja alentavat tai poistavat turvaluokan pääjohtajansa ohjeiden mukaan tai hänen suostumuksellaan.

3. Turvaluokiteltujen asiakirjojen käsittelyä koskevat menettelyt on vahvistettu varmistaen, että ne suojataan niiden sisältämien tietojen edellyttämällä tavalla.

4. Niiden henkilöiden, joilla on lupa luovuttaa TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjoja, lukumäärä on pidettävä mahdollisimman pienenä ja heidän nimensä on pidettävä neuvoston pääsihteeristön, kunkin jäsenvaltion ja tarvittaessa kunkin EU:n hajautetun viraston laatimassa luettelossa.

TURVALUOKITUKSEN SOVELTAMINEN

5. Asiakirjan turvaluokka on määriteltävä sen sisällön arkaluonteisuuden mukaan II jakson 1—4 kohdan määritelmän mukaisesti. On tärkeää, että luokittelua käytetään oikein ja rajoitetusti. Tämä koskee erityisesti TRÈS SECRET UE / EU TOP SECRET -luokkaa.

6. Luokiteltavaksi tarkoitetun asiakirjan luovuttajan on pidettävä mielessä edellä mainitut säännöt ja hillittävä taipumusta yli- ja aliluokitteluun.

   Vaikka korkea turvaluokka saattaakin ensi näkemältä taata paremman suojauksen asiakirjalle, jatkuva yliluokittelu voi johtaa siihen, ettei luokittelujärjestelmän kelpoisuuteen enää luoteta.

   Toisaalta asiakirjoja ei pidä myöskään aliluokitella suojaukseen liittyvien rajoitusten välttämiseksi.

   Luokitteluohjeet ovat lisäyksessä 3.

7. Tietyn asiakirjan yksittäiset sivut, kohdat, jaksot, liitteet, lisäykset, saatteet ja oheistukset saattavat edellyttää eri turvaluokkaa, joten ne on merkittävä sen mukaisesti. Koko asiakirja on luokiteltava korkeimman luokitteluasteen saaneen osansa mukaan.

8. Liitteitä sisältävän kirjeen tai ilmoituksen turvaluokan on oltava yhtä korkea kuin sen liitteiden korkein turvaluokka. Asiakirjan luovuttajan olisi ilmoitettava selvästi, mille tasolle asiakirja on luokiteltava, jos se irrotetaan liitteistään.

TURVALUOKAN ALENTAMINEN JA POISTAMINEN

9. EU:n turvaluokitellun asiakirjan turvaluokan alentaminen tai poistaminen on mahdollista vain asiakirjan luovuttajan luvalla ja jos se on tarpeen, vasta kun muita asianomaisia osapuolia on kuultu asiasta. Turvaluokan alentaminen tai poistaminen on vahvistettava kirjallisesti. Asiakirjan luovuttavan toimielimen, jäsenvaltion, viraston, seuraajaorganisaation tai korkeamman viranomaisen on ilmoitettava vastaanottajille muutoksesta, ja näiden on puolestaan ilmoitettava muutoksesta kaikille myöhemmille vastaanottajille, joille he ovat lähettäneet asiakirjan tai sen käännöksen.

10. Asiakirjan luovuttajat ilmoittavat mahdollisuuksien mukaan turvaluokitellun asiakirjan osalta sen, minä päivänä tai minkä ajan jälkeen asiakirjan sisällön turvaluokka voidaan alentaa tai poistaa. Muussa tapauksessa he tarkistavat asiakirjan vähintään joka viides vuosi varmistaakseen, onko alkuperäinen luokitus tarpeellinen.

([1]) Turvaluokan alentamisella (downgrading) tarkoitetaan salassapitotason alentamisesta johtuvaa luokan muuttamista. Turvaluokan poistamisella (declassification) tarkoitetaan minkä tahansa luokan poistamista.

IV JAKSO

FYYSINEN TURVALLISUUS

YLEISTÄ

1. Fyysisten turvatoimien pääasiallisena tavoitteena on estää sivullisten henkilöiden pääsy EU:n turvaluokiteltuun tietoon ja/tai aineistoon.

TURVALLISUUTTA KOSKEVAT VAATIMUKSET

2. Kaikki tilat, alueet, kiinteistöt, toimistot, huoneet, tietoliikenne- ja tietojärjestelmät jne., joissa EU:n turvaluokiteltua tietoa ja aineistoa varastoidaan ja/tai käsitellään, on suojattava asianmukaisin fyysisin turvatoimin.

3. Päätettäessä minkä asteinen fyysisen turvallisuuden suojaus on tarpeellista, on otettava huomioon kaikki asiaankuuluvat tekijät, kuten esimerkiksi:

   a) tiedon ja/tai aineiston luokittelu;

   b) hallussa olevan tiedon määrä ja muoto (esim. paperituloste, atk-tallennusväline);

   c) paikallisesti arvioitu lähinnä sabotaasin, terrorismin ja muun haitallisen ja/tai rikollisen toiminnan uhka niiden tiedustelupalvelujen taholta, jotka kohdistavat toimiaan EU:iin, jäsenvaltioihin ja/tai muihin laitoksiin tai kolmansiin osapuoliin, joilla on hallussaan EU:n turvaluokiteltua tietoa.

4. Sovellettavilla fyysisillä turvatoimilla on pyrittävä:

   a) epäämään tunkeutuminen salaa tai väkisin;

   b) ehkäisemään, estämään ja havaitsemaan epärehellisten henkilöiden toimet (sisäinen vakooja);

   c) estämään niiden neuvoston pääsihteeristön, jäsenvaltioiden julkishallinnon yksiköiden ja/tai muiden laitosten tai kolmansien osapuolten virkamiesten ja muun henkilöstön, joilla ei ole yleisvaltuutusta, pääsy EU:n turvaluokiteltuun tietoon.

FYYSISET TURVATOIMET

Turva-alueet

5. Alueiden, joissa CONFIDENTIEL UE- tai sitä korkeamman turvaluokan tietoa käsitellään ja varastoidaan, on oltava järjestelyiltään ja rakenteeltaan sellaisia, että ne vastaavat jotakin seuraavista:

   a) Turvaluokan I turva-alue: alue, jossa CONFIDENTIEL UE- tai sitä korkeamman turvaluokan tietoa käsitellään tai varastoidaan siten, että alueelle tulo vastaa, kaikkia käytännön käyttötarkoituksia varten, pääsyä turvaluokiteltuun tietoon. Tällaiselta alueelta edellytetään:

      i) selkeästi määriteltyä ja suojattua rajattua aluetta, jossa kulku sekä sisään ja ulos on valvottua;

      ii) kulunvalvontajärjestelmää, joka sallii alueelle vain asianmukaisen selvityksen läpikäyneet ja erityisen valtuutuksen saaneet henkilöt;

      iii) alueella tavanomaisesti säilytetyn tiedon, so. tiedon, johon sisääntulo antaa pääsyn, turvaluokan määrittelyä.

   b) Turvaluokan II turva-alue: alue, jossa CONFIDENTIEL UE- tai sitä korkeamman turvaluokan tietoa käsitellään tai varastoidaan siten, että tieto voidaan suojata sivullisilta sisäisesti asennetuin tarkastuksin, esim. tilat, joissa on toimistoja joissa CONFIDENTIEL UE -turvaluokan tietoa käsitellään tai varastoidaan säännöllisesti. Tällaiselta alueelta edellytetään:

      i) selkeästi määriteltyä ja suojattua rajattua aluetta, jossa kulku sekä sisään ja ulos on valvottua;

      ii) kulunvalvontajärjestelmää, joka sallii alueelle saattajalta tulon vain asianmukaisen selvityksen läpikäyneille ja erityisen valtuutuksen saaneille henkilöille. Kaikkien muiden henkilöiden osalta on varauduttava saattajien käyttöön tai tekemään vastaavat tarkastukset, jotta sivullisten pääsy EU:n turvaluokiteltuun tietoon ja valvomaton pääsy teknisesti suojatuille alueille voidaan estää.

Alueet, joilla ei ole henkilöstöä palveluksessa vuorokauden ympäri, tarkastetaan välittömästi normaalin työajan jälkeen sen varmistamiseksi, että EU:n turvaluokiteltu tieto on asianmukaisesti turvattu.

Hallinnollinen alue

6. Turvaluokkien I ja II turva-alueiden ympärille tai niihin johtaviin tiloihin voidaan perustaa kevyemmin suojattu hallinnollinen alue. Tällaisella alueella edellytetään olevan silmin nähden rajattu alue, jossa henkilöstö ja ajoneuvot voidaan tarkastaa. Vain RESTREINT UE -turvaluokan tietoa voidaan käsitellä ja varastoida hallinnollisilla alueilla.

Tulo- ja lähtötarkastukset

7. Pääsyä turvaluokkien I ja II turvallisuusalueille valvotaan kulkuluvin tai pysyvän henkilöstön osalta henkilökohtaisesti tunnistamalla. On myös luotava järjestelmä vierailijoiden tarkastamiseksi, jonka tarkoituksena on estää sivullisten pääsy EU:n turvaluokiteltuun tietoon. Kulkulupajärjestelmää voidaan myös tukea automatisoidulla tunnistamisella, jonka voidaan katsoa täydentävän, mutta ei kokonaan korvaavan, vartijoita. Muutos uhkien arvioinnissa voi edellyttää kulunvalvontatoimien tehostamista, esimerkiksi huomattavien henkilöiden vierailuiden aikana.

Vartiointikierrokset

8. Turvaluokkien I ja II turva-alueita on vartioitava normaalien työaikojen ulkopuolella EU:n omaisuuden suojaamiseksi vaaralta, vahingoilta ja katoamiselta. Vartiointikierrosten tiheys määräytyy paikallisten olosuhteiden mukaan, mutta ohjeena voidaan pitää kierroksen suorittamista kerran kahdessa tunnissa.

Turvalliset säilytyspaikat ja kassaholvit

9. EU:n turvaluokiteltu tieto varastoidaan säilytyspaikassa, jonka on vastattava jotakin seuraavista kolmesta luokasta:

   — Luokka A: kansallisesti TRÈS SECRET UE / EU TOP SECRET -turvaluokan tiedon varastoimiseen hyväksyttyjä säilytyspaikkoja turvaluokkien I ja II turva-alueilla,

   — Luokka B: kansallisesti SECRET UE- ja CONFIDENTIEL UE -turvaluokan tiedon varastoimiseen hyväksyttyjä säilytyspaikkoja turvaluokkien I ja II turva-alueilla,

   — Luokka C: ainoastaan RESTREINT UE -turvaluokan tiedon varastoimiseen soveltuvaa toimistokalustoa.

10. Turvaluokkien I ja II turva-alueille rakennetuissa kassaholveissa ja turvaluokan I turva-alueilla, joissa CONFIDENTIEL UE- tai sitä korkeamman turvaluokan tietoa varastoidaan avoimille hyllyille tai pannaan näytteille taulukkoihin, karttoihin jne., seinien, lattioiden ja kattojen, lukittavan oven tai lukittavien ovien osalta on oltava kansallisen turvallisuusviranomaisen varmennus siitä, että niiden suojaus on yhtäläinen saman turvaluokan tiedon varastoimiseen hyväksytyn turvallisen säilytyspaikan kanssa.

Lukot

11. Turvallisissa säilytyspaikoissa ja kassaholveissa, joissa EU:n turvaluokiteltavaa tietoa varastoidaan, käytettävien lukkojen on oltava seuraavien normien mukaisia:

   — Ryhmä A: kansallisesti hyväksytty luokan A säilytyspaikkoihin,

   — Ryhmä B: kansallisesti hyväksytty luokan B säilytyspaikkoihin,

   — Ryhmä C: soveltuu ainoastaan luokan C toimistokalustolle.

Avainten ja yhdistelmien valvonta

12. Turvallisten säilytyspaikkojen avaimia ei saa viedä pois toimistorakennuksesta. Valtuutuksen saaneet henkilöt opettelevat ulkoa turvallisten säilytyspaikkojen numeroyhdistelmät. Hätätapauksia varten asianomaisen laitoksen turvavirkailija on vastuussa vara-avaimista ja pitää kirjaa jokaisesta numeroyhdistelmästä; jälkimmäiset säilytetään erillisissä sinetöidyissä läpinäkymättömissä kuorissa. Työavaimet, turva-avaimien varakappaleet ja numeroyhdistelmät säilytetään erillisissä turvallisissa säilytyspaikoissa. Nämä avaimet ja numeroyhdistelmät on suojattava vähintään yhtä huolellisesti kuin aineisto, johon ne antavat pääsyn.

13. Tieto turvallisten säilytyspaikkojen numeroyhdistelmistä annetaan mahdollisimman harvalle henkilölle. Yhdistelmät muutetaan:

a) uuden turvallisen säilytyspaikan vastaanoton yhteydessä;

b) aina henkilöstön vaihtuessa;

c) aina vaaratilanteen tai vaaratilanteen epäilyksen ilmetessä;

d) mieluummin kuuden ja vähintään kahdentoista kuukauden välein.

Tunkeutumisen havaitsemislaitteet

14. Käytettäessä hälytysjärjestelmiä, suljettuja televisiopiirejä ja muita sähköisiä laitteita EU:n turvaluokiteltavan tiedon suojaamiseksi, on varavirtalähteen oltava käytettävissä järjestelmän jatkuvan toiminnan varmistamiseksi siltä varalta, että päävirranlähteen toiminta keskeytyy. Toinen perusvaatimus on, että tällaisten järjestelmien toimintahäiriö tai häirintä aiheuttaa hälytyksen tai muulla luotettavalla tavalla varoittaa valvontahenkilöstöä.

Hyväksytty laitteisto

15. Kansalliset turvallisuusviranomaiset ylläpitävät, omin tai kahdenvälisin voimavaroin, ajan tasalla olevia luetteloita niiden suojauslaitteiden tyypeistä ja malleista, jotka ne ovat hyväksyneet turvaluokitellun tiedon suoraan tai epäsuoraan suojaamiseen vaihtelevissa erityisissä olosuhteissa ja erityisten edellytysten mukaisesti. Neuvoston pääsihteeristön turvallisuusyksikkö ylläpitää vastaavanlaista luetteloa, joka perustuu muun muassa kansallisilta turvallisuusviranomaisilta saatuun tietoon. EU:n hajautetut erillisvirastot neuvottelevat neuvoston pääsihteeristön turvallisuusyksikön ja soveltuvin osin isäntävaltionsa kansallisten turvallisuusviranomaisten kanssa ennen tällaisen laitteiston hankkimista.

Kopio- ja telefaksilaitteiden fyysinen suojaus

16. Kopio- ja telefaksilaitteet suojataan fyysisesti tarpeellisissa määrin sen varmistamiseksi, että vain valtuutetut henkilöt voivat käyttää niitä ja että kaikki turvaluokiteltavat tuotteet ovat asianmukaisesti valvottuja.

SUOJAUTUMINEN SALAKATSELULTA JA SALAKUUNTELULTA

Salakatselu

17. Kaikki asianmukaiset toimet on toteutettava sekä päivällä että yöllä sen varmistamiseksi, että edes vahingossa yksikään sivullinen ei näe EU:n turvaluokiteltua tietoa.

Salakuuntelu

18. Toimistot ja alueet, joilla SECRET UE- tai sitä korkeamman turvaluokan tiedosta keskustellaan säännöllisesti, suojataan tahatonta ja tahallista salakuunteluyritystä vastaan riskin edellyttämissä paikoissa. Tällaisten yritysten riskien arviointi on toimivaltaisen turvallisuusviranomaisen vastuulla sen kuultua tarvittaessa kansallista turvallisuusviranomaista.

19. Toteutettavien suojaustoimenpiteiden määrittämiseksi tahattomalle salakuuntelulle (esim. seinien, ovien, lattioiden ja kattojen eristäminen, paljastavien vuotojen mittaus) tai tahalliselle salakuuntelulle (esim. mikrofonien etsintä) alttiissa tiloissa, neuvoston pääsihteeristön turvallisuusyksikkö voi pyytää apua kansallisten turvallisuusviranomaisten asiantuntijoilta. EU:n hajautettujen erillisvirastojen turvavirkailijat voivat pyytää neuvoston pääsihteeristön turvallisuusyksikköä toteuttamaan teknisiä tarkastuksia ja/tai kansallisten turvallisuusviranomaisten asiantuntijoiden apua.

20. Samoin, olosuhteiden niin vaatiessa, kansallisten turvallisuusviranomaisten tekniset turvallisuusasiantuntijat voivat toimivaltaisen turvavirkailijan pyynnöstä tarkastaa telelaitteet ja kaikki sähköiset tai elektroniset toimistolaitteet, joita käytetään SECRET UE- tai sitä korkeamman turvaluokan kokouksissa.

TEKNISESTI SUOJATUT ALUEET

21. Tietyt alueet voidaan osoittaa teknisesti suojatuiksi alueiksi. Näillä alueilla suoritetaan erityinen sisääntulotarkastus. Tällaiset alueet pidetään lukittuina hyväksytyin menetelmin silloin kun ne eivät ole käytössä ja kaikkia avaimia käsitellään turva-avaimina. Tällaisilla alueilla suoritetaan säännöllisesti fyysisiä tarkastuksia sekä myös jokaisen luvattoman sisäänpääsyn tai sen epäilyksen jälkeen.

22. Laitteistosta ja kalustosta pidetään yksityiskohtaista inventaariota niiden sijoituspaikkamuutosten seuraamiseksi. Yhtäkään laitteistoon tai kalustoon kuuluvaa esinettä ei tuoda alueelle kunnes erikoiskoulutettu turvavirkailija on suorittanut perusteellisen tarkastuksen kuuntelulaitteiden havaitsemiseksi. Yleisenä sääntönä on, että teknisesti suojatuille alueille olisi vältettävä asentamasta tietoliikenneyhteyksiä.

V JAKSO

VALTUUTUSPERIAATETTA JA LUOTETTAVUUSSELVITYSTÄ KOSKEVAT YLEISET SÄÄNNÖT

1. Pääsy EU:n turvaluokiteltavaan tietoon myönnetään vain henkilöille, joiden on tarpeen saada siihen valtuutus voidakseen suorittaa velvollisuutensa tai tehtävänsä. Pääsy TRÈS SECRET UE / EU TOP SECRET-, SECRET UE- ja CONFIDENTIEL UE -turvaluokan tietoon myönnetään vain henkilöille, joille on tehty asianmukainen luotettavuusselvitys.

2. Vastuu valtuutuksen tarpeellisuuden määrittämisestä on neuvoston pääsihteeristöllä, EU:n hajautetuilla erillisvirastoilla ja niillä jäsenvaltioiden yksiköillä tai osastoilla, joissa asianosaiset henkilöt työskentelevät, tehtävien asettamien vaatimusten mukaisesti.

3. Henkilöstölle tehtävät luotettavuusselvitykset ovat virkamiehen työnantajan vastuulla ja perustuvat asianmukaisesti sovellettaviin menettelyihin. Neuvoston pääsihteeristön virkamiesten ja muun henkilöstön osalta luotettavuusselvitysmenettelystä säädetään jaksossa VI.

   Tämän seurauksena myönnetään ”luotettavuustodistus”, josta ilmenee turvaluokitellun tiedon turvaluokka, johon luotettavuusselvityksen läpikäynyt henkilö valtuutetaan pääsemään, sekä valtuutuksen erääntymisaika.

   Tietyn turvaluokan luotettavuustodistus voi antaa kantajalle valtuutuksen päästä alemman turvaluokan tietoon.

4. Muilla henkilöillä kuin neuvoston pääsihteeristön tai jäsenvaltioiden virkamiehillä ja muulla henkilöstöllä, esim. EU:n toimielinten jäsenillä, virkamiehillä tai henkilöstöllä, joiden kanssa voi olla tarpeen keskustella EU:n turvaluokitellusta tiedosta tai joille on esitettävä EU:n turvaluokiteltua tietoa, on oltava EU:n turvaluokiteltua tietoa koskeva luotettavuustodistus ja heille on selvitettävä turvallisuusvastuunsa. Sama sääntö soveltuu samankaltaisissa olosuhteissa ulkopuolisiin yrittäjiin, asiantuntijoihin tai neuvonantajiin.

TRÈS SECRET UE / EU TOP SECRET -TURVALUOKAN TIETOON PÄÄSYÄ KOSKEVAT ERITYISSÄÄNNÖT

5. Kaikki henkilöt, joiden on päästävä TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoon, on ensin seulottava päästäkseen tällaiseen tietoon.

6. Osastojen päälliköt nimittävät kaikki henkilöt, joiden on päästävä TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoon, ja heidän nimensä merkitään asianmukaiseen TRÈS SECRET UE / EU TOP SECRET -rekisteriin.

7. Ennen kuin he saavat pääsyn TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoon, kaikkien henkilöiden on allekirjoitettava todistus siitä, että heille on selvitetty neuvoston turvallisuustoimet ja että he täysin ymmärtävät erityisen velvollisuutensa suojata TRÈS SECRET UE / EU TOP SECRET -turvaluokan tiedot sekä EU:n säännöissä ja kansallisessa lainsäädännössä tai hallinnollisissa säännöissä määrätyt seuraamukset turvaluokitellun tiedon joutumisesta sivullisille, joko tarkoituksellisesti tai laiminlyönnin seurauksena.

8. TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoon pääsyn omaavien henkilöiden osallistuessa kokouksiin jne., asianomaisen henkilön palkanneen yksikön tai elimen toimivaltainen valvontaviranomainen tiedottaa kokouksen järjestävälle elimelle, onko kyseisille henkilöille myönnetty tällainen valtuutus.

9. Kaikkien niiden henkilöiden, jotka eivät enää työskentele TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoon pääsyä edellyttävissä tehtävissä, nimet poistetaan TRÈS SECRET UE / EU TOP SECRET -luettelosta. Lisäksi kaikkia tällaisia henkilöitä muistutetaan uudelleen erityisestä velvollisuudestaan suojata TRÈS SECRET UE / EU TOP SECRET -turvaluokan tiedot. He allekirjoittavat myös vakuutuksen siitä, että he eivät käytä tai edelleen välitä hallussaan olevaa TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoa.

SECRET UE- JA CONFIDENTIEL UE -TURVALUOKAN TIETOON PÄÄSYÄ KOSKEVAT ERITYISSÄÄNNÖT

10. Kaikki henkilöt, joiden on päästävä SECRET UE- ja CONFIDENTIEL UE -turvaluokan tietoon, on ensin seulottava asianmukaisen turvaluokan mukaisesti.

11. Kaikille henkilöille, joiden on päästävä SECRET UE- ja CONFIDENTIEL UE -turvaluokan tietoon, selvitetään asianmukaisesti turvallisuussäännöt ja heidän on oltava tietoisia laiminlyönnin seuraamuksista.

12. SECRET UE- ja CONFIDENTIEL UE -turvaluokan tietoon pääsyn omaavien henkilöiden osallistuessa kokouksiin jne., kyseisen henkilön palkanneen elimen turvavirkailija tiedottaa kokouksen järjestävää elintä siitä, että kyseisillä henkilöillä on tällainen valtuutus.

RESTREINT UE -TURVALUOKAN TIETOON PÄÄSYÄ KOSKEVAT ERITYISSÄÄNNÖT

13. Henkilöitä, joilla on pääsy RESTREINT UE -turvaluokan tietoon, tiedotetaan näistä turvallisuussäännöistä ja laiminlyönnin seuraamuksista.

HENKILÖSIIRROT

14. Kun henkilöstön jäsen siirretään pois toimesta, joka edellyttää EU:n turvaluokitellun aineiston käsittelyä, rekisterinpitäjä valvoo, että kyseinen aineisto siirretään asianmukaisesti lähtevältä viranomaiselta saapuvalle viranomaiselle.

ERITYISOHJEET

15. Henkilöille, joiden edellytetään käsittelevän EU:n turvaluokiteltua tietoa, on ensimmäistä kertaa palvelukseen tullessaan ja sen jälkeen säännöllisesti selvitettävä:

    a) harkitsemattoman keskustelun aiheuttamat turvallisuusriskit;

    b) käytettävät varotoimet suhteessa tiedotusvälineisiin;

    c) tiedustelupalvelujen EU:iin ja jäsenvaltioihin kohdistuvan toiminnan muodostama uhka EU:n turvaluokitellun tiedon ja toiminnan osalta;

    d) velvollisuus ilmoittaa välittömästi asianmukaisille turvallisuusviranomaisille sellaisista lähestymisistä tai liikkeistä sekä epätavallisista turvallisuuteen liittyvistä olosuhteista, jotka antavat aihetta epäillä vakoilutoimintaa.

16. Henkilöitä, jotka tavallisesti ovat usein yhteydessä sellaisten valtioiden edustajiin, joiden tiedustelupalvelut kohdistavat toimintaansa EU:iin ja jäsenvaltioihin EU:n turvaluokitellun tiedon ja toiminnan osalta, on välitettävä tiedot niistä tekniikoista, joita eri tiedustelupalvelujen tiedetään käyttävän.

17. Neuvostolla ei ole turvallisuussäännöksiä EU:n turvaluokiteltuun tietoon pääsyn omaavien henkilöiden yksityisen matkustamisen osalta mihinkään kohteeseen. Toimivaltaiset turvallisuusviranomaiset selvittävät kuitenkin vastuualueeseensa kuuluville virkamiehille ja muulle henkilöstölle matkustussäännöistä, joita heihin saatetaan soveltaa. Turvallisuusviranomaisten velvollisuutena on järjestää näiden erityisohjeiden kertaustilaisuuksia.

VI JAKSO

NEUVOSTON PÄÄSIHTEERISTÖN VIRKAMIESTEN JA MUUN HENKILÖSTÖN LUOTETTAVUUSSELVITYSMENETTELY

1. Neuvoston hallussa olevia turvaluokiteltuja tietoja saavat ainoastaan ne neuvoston pääsihteeristön virkamiehet ja muuhun henkilöstöön kuuluvat tai muut pääsihteeristössä työskentelevät henkilöt, joiden on tehtäviensä ja yksikön tarpeiden vuoksi saatava tutustua niihin tai voitava käsitellä niitä.

2. Saadakseen TRÈS SECRET UE / EU TOP SECRET-, SECRET UE- ja CONFIDENTIEL UE -turvaluokan tietoja 1 kohdassa tarkoitetuilla henkilöillä on oltava 4 ja 5 kohdassa tarkoitetun menettelyn mukaisesti annettu valtuutus.

3. Valtuutus annetaan ainoastaan henkilöille, joista jäsenvaltioiden toimivaltaiset kansalliset viranomaiset (kansalliset turvallisuusviranomaiset) ovat tehneet luotettavuusselvityksen 6—10 kohdassa tarkoitetun menettelyn mukaisesti.

4. Nimittävän viranomaisen, sellaisena kuin se määritellään henkilöstösääntöjen 2 artiklan ensimmäisessä alakohdassa, tehtävänä on päättää 1, 2 ja 3 kohdassa tarkoitetusta valtuutuksesta.

   Nimittävä viranomainen myöntää valtuutuksen saatuaan 6—10 kohdan mukaisesti suoritettuun luotettavuusselvitykseen perustuvan jäsenvaltioiden kansallisten toimivaltaisten viranomaisten lausunnon.

5. Valtuutus on voimassa viisi vuotta, ei kuitenkaan kauemmin kuin henkilö on luvan saannin perusteena olevissa tehtävissä. Nimittävä viranomainen voi jatkaa valtuutuksen voimassaoloa 4 kohdassa säädettyä menettelyä noudattaen.

   Nimittävä viranomainen voi peruuttaa valtuutuksen, jos hän katsoo siihen olevan perusteita. Päätös peruuttamisesta ilmoitetaan asianomaiselle henkilölle, joka voi pyytää, että nimittävä viranomainen kuulee häntä, sekä toimivaltaiselle kansalliselle viranomaiselle.

6. Luotettavuusselvityksen tarkoituksena on varmistaa, ettei ole estettä sille, että kyseinen henkilö saa käyttää neuvoston hallussa olevia turvaluokiteltuja tietoja.

7. Luotettavuusselvityksen tekevät nimittävän viranomaisen pyynnöstä yhteistyössä asianomaisen henkilön kanssa sen jäsenvaltion toimivaltaiset kansalliset viranomaiset, jonka kansalainen asianomainen henkilö on. Jos asianomainen henkilö asuu toisen jäsenvaltion alueella, kyseiset kansalliset viranomaiset voivat huolehtia yhteistyöstä asuinvaltion viranomaisten kanssa.

8. Luotettavuusselvitystä varten asianomaisen henkilön on täytettävä henkilötietoilmoitus.

9. Nimittävä viranomainen yksilöi pyynnössään niiden tietojen laadun ja turvaluokan, jotka asianomainen henkilö työssään saisi tietoonsa, jotta toimivaltaiset kansalliset viranomaiset voivat tehdä selvityksen, ja antaa lausunnon kyseiselle henkilölle annettavan valtuutuksen asianmukaista tasoa varten.

10. Luotettavuutta koskevan selvitysmenettelyn kaikkiin vaiheisiin ja tuloksiin sovelletaan kyseisessä jäsenvaltiossa voimassa olevia alaa koskevia määräyksiä ja säännöksiä, myös mahdollisia muutoksenhakukeinoja.

11. Nimittävä viranomainen voi myöntää valtuutuksen asianomaiselle henkilölle, jos jäsenvaltioiden toimivaltaiset kansalliset viranomaiset antavat myönteisen lausunnon.

12. Jos toimivaltaiset kansalliset viranomaiset antavat kielteisen lausunnon, asianomaiselle henkilölle ilmoitetaan siitä ja tämä voi pyytää, että nimittävä viranomainen kuulee häntä. Nimittävä viranomainen voi, jos hän pitää sitä tarpeellisena, pyytää toimivaltaisia kansallisia viranomaisia antamaan luovutettavissaan olevia tarkempia tietoja. Jos kielteinen lausunto vahvistetaan, valtuutusta ei voida myöntää.

13. Henkilölle, joka on 4 ja 5 kohdan mukaisesti saanut valtuutuksen, annetaan tämän oikeuden myöntämisen yhteydessä ja tämän jälkeen määräajoin ohjeet turvaluokiteltujen tietojen suojaamisesta ja siitä, miten tämä varmistetaan. Asianomainen allekirjoittaa vakuutuksen siitä, että on saanut ohjeet ja että hän sitoutuu noudattamaan niitä.

14. Nimittävä viranomainen toteuttaa tarvittavat toimenpiteet tämän jakson täytäntöönpanemiseksi ja erityisesti ne toimenpiteet, joilla säännellään oikeutta tutustua valtuutuksen saaneista henkilöistä laadittuun luetteloon.

15. Nimittävä viranomainen voi poikkeuksellisesti ja yksikön tarpeiden niin vaatiessa myöntää ennen 7 kohdassa tarkoitetun luotettavuusselvityksen saamista, ilmoitettuaan asiasta ennakolta kansallisille toimivaltaisille viranomaisille ja edellyttäen, että nämä eivät ole kuukauden kuluessa esittäneet huomautuksia, väliaikaisen valtuutuksen enintään kuudeksi kuukaudeksi.

16. Täten myönnetyt väliaikaiset valtuutukset eivät oikeuta saamaan TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoa; tällaisen tiedon saanti on rajattu virkamiehille, joista on tosiasiassa tehty luotettavuusselvitys 7 kohdan mukaisesti myönteisin tuloksin. Ennen luotettavuusselvityksen saamista TRÈS SECRET UE / EU TOP SECRET -turvaluokan luotettavuusselvitykseen määrätyille virkamiehille voidaan myöntää väliaikainen valtuutus saada SECRET UE- ja sitä alemman turvaluokan tietoa.

VII JAKSO

EU:N TURVALUOKITELTAVAN AINEISTON VALMISTELU, JAKELU, LÄHETTÄMINEN, VARASTOINTI JA HÄVITTÄMINEN

Sisällysluettelo

Sivu

Yleiset määräykset

I luku EU:n turvaluokiteltujen asiakirjojen valmistelu ja jakelu 23

II luku EU:n turvaluokiteltujen asiakirjojen lähettäminen 23

III luku Sähköiset ja muut tekniset lähetyskeinot 26

IV luku EU:n turvaluokitelluista asiakirjoista tehdyt ylimääräiset jäljennökset, käännökset ja otteet 26

V luku EU:n turvaluokitellun aineiston inventointi, tarkastukset, säilytys ja hävittäminen 26

VI luku Neuvostolle osoitettuihin asiakirjoihin sovellettavat erityissäännöt 28

Yleiset määräykset

Tässä osassa esitellään yksityiskohtaisesti EU:n turvaluokiteltavien asiakirjojen valmistelu-, jakelu-, lähettämis-, varastointi- ja hävittämistoimenpiteet sellaisina kuin ne määritellään jakson I liitteessä olevan otsakkeen "Turvallisuutta koskevat perusperiaatteet ja vähimmäisstandardit" 3 kohdan a alakohdassa. Tätä käytetään tapauskohtaisesti ja aineiston tyypistä riippuen viitekohtana, kun on kyse näiden menetelmien käyttöönottamisesta muun EU:n turvaluokiteltavan aineiston osalta.

I luku

EU:n turvaluokiteltujen asiakirjojen valmistelu ja jakelu

VALMISTELU

1. EU:n turvaluokituksia ja merkintöjä sovelletaan siten kuin II jaksossa on vahvistettu, ne merkitään jokaisen sivun ylä- ja alareunan keskelle ja jokainen sivu numeroidaan. Jokaiseen EU:n turvaluokiteltuun asiakirjaan merkitään viitenumero ja päivämäärä. TRÈS SECRET UE / EU TOP SECRET- ja SECRET UE -turvaluokan asiakirjojen osalta tämä viitenumero merkitään jokaiselle sivulle. Jos näitä jaetaan useina käännöksinä, merkitään kuhunkin niistä käännöksen numero ensimmäiselle sivulle asiakirjan sivumäärän lisäksi. Kaikki liitteet ja lisäykset luetellaan CONFIDENTIEL UE- tai tätä ylemmän turvaluokan asiakirjan ensimmäisellä sivulla.

2. CONFIDENTIEL UE- tai sitä ylemmän turvaluokan asiakirjoja saavat kirjoittaa koneella, kääntää, varastoida, valokopioida, jäljentää magneettisesti tai kuvata mikrofilmille ainoastaan henkilöt, joilla on valtuutus päästä vähintään kyseessä olevan asiakirjan turvaluokan tasoiseen EU:n turvaluokiteltavaan tietoon, paitsi tämän osan 27 kohdassa kuvatussa erityistapauksessa.

   Turvaluokiteltavien asiakirjojen tuottamista tietokoneella sääntelevät määräykset ovat XI jaksossa.

JAKELU

3. EU:n turvaluokiteltavaa tietoa jaetaan vain henkilöille, joilla on siihen valtuutus ja joille on tehty asianmukainen luotettavuusselvitys. Alkuperäisen jakelun määrittää tietojen luovuttaja.

4. TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjat kierrätetään TRÈS SECRET UE / EU TOP SECRET -turvaluokan rekisterinpitäjien kautta (ks. VIII jakso). TRÈS SECRET UE / EU TOP SECRET -turvaluokan viestien osalta, toimivaltainen kirjaamo voi valtuuttaa viestintäkeskuksen päällikön tuottamaan vastaanottajien luettelossa mainitun määrän käännöksiä.

5. Alkuperäinen vastaanottaja voi jakaa SECRET UE- ja sitä alemman turvaluokan asiakirjoja edelleen muille vastaanottajille tarpeellisuusperiaatteen pohjalta. Luovuttaneiden viranomaisten on kuitenkin selkeästi ilmoitettava varoituksista, joita he haluavat määrätä. Aina kun tällaisista varoituksista määrätään, vastaanottajat voivat jakaa asiakirjoja edelleen vain luovuttaneen viranomaisen luvalla.

6. Laitoksen kirjaamo kirjaa jokaisen CONFIDENTIEL UE- ja sitä ylemmän turvaluokan asiakirjan sen saapuessa laitokseen tai lähtiessä laitoksesta. Kirjattavista tiedoista (viitteet, päivämäärä ja soveltuvin osin käännöksen numero) on voitava tunnistaa asiakirja ja ne merkitään päiväkirjaan tai viedään erityiselle suojatulle tietovälineelle.

II luku

EU:n turvaluokiteltujen asiakirjojen lähettäminen

PAKKAUS

7. CONFIDENTIEL UE- tai sitä ylemmän turvaluokan asiakirjat lähetetään tukevissa, läpinäkymättömissä kaksinkertaisissa voimapaperikirjekuorissa. Sisempään kirjekuoreen merkitään asianmukainen EU:n turvaluokka sekä mikäli mahdollista, vastaanottajan työnimike ja osoite täydellisinä.

8. Ainoastaan rekisterin valvontavirkailija tai hänen sijaisensa voi avata sisemmän kirjekuoren ja kuitata sisällä olevat asiakirjat vastaanotetuiksi, ellei kirjekuorta ole osoitettu yksittäiselle henkilölle. Tällaisessa tapauksessa asianmukaisessa rekisterissä merkitään kirjekuoren saapumisaika, ja ainoastaan henkilö, jolle se on osoitettu, voi avata sisemmän kirjekuoren ja kuitata sisällä olevat asiakirjat vastaanotetuiksi.

9. Sisempään kirjekuoreen laitetaan kuitti. Kuittiin, jota ei tarvitse turvaluokitella, merkitään asiakirjan viitenumero, päivämäärä ja käännöksen numero, mutta ei koskaan sen sisältämää asiaa.

10. Sisempi kirjekuori suljetaan ulompaan kirjekuoreen, johon merkitään pakkausnumero kuittausta varten. Missään tapauksessa turvaluokkaa ei saa merkitä ulompaan kirjekuoreen.

11. CONFIDENTIEL UE- tai sitä ylemmän turvaluokan asiakirjoista kuriireille ja läheteille annetaan kuitti pakkausnumeroita vastaan.

LÄHETTÄMINEN RAKENNUSTEN TAI RAKENNUSRYHMIEN SISÄLLÄ

12. Määrätyn rakennuksen tai rakennusryhmän sisällä turvaluokiteltavia asiakirjoja voidaan kuljettaa suljetussa kuoressa, johon on merkitty ainoastaan vastaanottajan nimi, sillä ehdolla, että sitä kuljettaa henkilö, jolla on asiakirjojen turvaluokkaa vastaava valtuutus.

EU:N ASIAKIRJOJEN LÄHETTÄMINEN VALTION SISÄLLÄ

13. Valtion sisällä TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjoja saa lähettää ainoastaan virallisen lähettipalvelun tai TRÈS SECRET UE / EU TOP SECRET -turvaluokan valtuutuksen saaneiden henkilöiden kautta.

14. Aina kun käytetään lähettipalvelua TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjan lähettämiseksi rakennuksen tai rakennusryhmän rajojen ulkopuolelle, noudatetaan tässä luvussa olevia määräyksiä pakkaamisen ja kuittaamisen osalta. Jakeluyksiköiden henkilöstö järjestetään varmistaen, että TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjoja sisältävät pakkaukset pysyvät vastuunalaisen viranomaisen välittömässä valvonnassa kaiken aikaa.

15. Poikkeuksellisesti muut virkailijat kuin lähetit voivat viedä TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjoja rakennuksen tai rakennusryhmän ulkopuolelle käytettäväksi kokouksissa ja keskusteluissa edellyttäen, että:

   a) kantajalla on valtuutus päästä TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoon,

   b) kuljetustapa on kansallisten ERITTÄIN SALAINEN -asiakirjojen lähettämistä koskevien kansallisten sääntöjen mukainen,

   c) virkailija ei missään olosuhteissa jätä TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjoja vartioimatta;

   d) toteutetaan sellaiset järjestelyt, että täten siirrettävistä asiakirjoista tehty luettelo tulee kirjatuksi sen TRÈS SECRET UE / EU TOP SECRET -turvaluokan rekisteriin, jossa asiakirjoja pidetään, ja että ne tulevat viedyiksi päiväkirjaan sekä että niitä palautettaessa niiden yhtäpitävyys tulee tarkastetuksi.

16. Määrätyn valtion sisällä SECRET UE- ja CONFIDENTIEL UE -turvaluokan asiakirjoja voidaan lähettää postitse, jos tällainen menettely on sallittu kansallisten sääntöjen mukaan ja jos se tapahtuu kyseisten säännösten määräysten mukaisesti, tai sellaisten lähettipalveluiden tai henkilöiden kautta, joilla on valtuutus päästä EU:n turvaluokiteltuun tietoon.

17. Kunkin jäsenvaltion tai EU:n hajautetun erillisviraston olisi laadittava ohjeet EU:n turvaluokiteltujen asiakirjojen henkilökohtaisesta kuljettamisesta näiden asetusten pohjalta. Kuljetuksesta vastaavaa on vaadittava lukemaan ja allekirjoittamaan nämä ohjeet. Erityisesti ohjeissa on tehtävä selväksi, että kaikissa tapauksissa:

   a) kuljetuksesta vastaavan on pidettävä asiakirjat hallussaan siihen asti, kunnes ne ovat turvallisessa säilössä IV jakson mukaisesti;

   b) asiakirjoja on vartioitava julkisissa kulkuneuvoissa tai yksityisissä ajoneuvoissa tai ravintoloiden tai hotellien kaltaisissa paikoissa. Niitä ei saa varastoida hotellien kassakaappeihin tai jättää vartioimatta hotellihuoneisiin;

   c) asiakirjojen lukeminen lentokoneiden tai junien kaltaisilla julkisilla paikoilla on kielletty.

LÄHETTÄMINEN JÄSENVALTIOSTA TOISEEN

18. CONFIDENTIEL UE- tai sitä korkeamman turvaluokan aineisto olisi kuljetettava jäsenvaltiosta toiseen diplomaatti- tai sotilaskuriirilla.

19. Kuitenkin SECRET UE- tai CONFIDENTIEL UE -turvaluokan aineiston henkilökohtainen kuljettaminen voidaan sallia, jos kuljetusjärjestelyin voidaan varmistaa, että aineisto ei voi joutua sivullisille.

20. Kansalliset turvallisuusviranomaiset voivat antaa luvan henkilökohtaiseen kuljettamiseen silloin kun diplomaatti- tai sotilaskuriiri ei ole käytettävissä tai jos näiden kuriirien käytöstä saattaisi seurata viive, joka voisi haitata EU:n toimia ja aiottu vastaanottaja tarvitsee aineiston kiireellisesti. Kunkin jäsenvaltion olisi laadittava ohjeet muiden kuin diplomaattisen tai sotilaallisen kuriirin suorittamasta kansainvälisestä SECRET UE- ja sitä alemman turvaluokan aineiston henkilökohtaisesta kuljettamisesta. Ohjeissa on edellytettävä, että:

a) kuljetuksesta vastaavalle on tehty jäsenvaltioiden myöntämä asianmukainen valtuutus;

b) kaikki näin kuljetettu aineisto viedään rekisteriin asianmukaisessa toimistossa tai rekisterinpitäjän luona;

c) EU:n aineistoa sisältävissä pakkauksissa tai laukuissa on oltava virallinen sinetti tullitarkastusten estämiseksi tai rajoittamiseksi sekä osoitelippu, jossa on yhteystiedot ja ohjeet löytäjälle;

d) kuljetuksesta vastaavalla on oltava mukanaan kaikkien EU-valtioiden hyväksymä kuriiritodistus ja/tai työmääräys tunnistetiedoissa tarkoitetun pakkauksen kuljettamiseen;

e) minkään EU:n ulkopuolisen valtion kautta tai sen rajan yli ei saa kulkea matkustettaessa maitse, ellei lähettävällä valtiolla ole erityisiä takuita kyseisen valtion taholta;

f) kuljetuksesta vastaavan matkasuunnitelmien on oltava päämäärien, matkustusreittien ja käytettävien kulkuneuvojen osalta EU:n asetusten mukaisia tai — mikäli kansalliset asetukset tämän osalta ovat tiukempia — näiden asetusten mukaisia;

g) kuljetuksesta vastaavan on pidettävä aineisto koko ajan hallussaan, kunnes se varastoidaan IV jaksossa olevien turvallista säilyttämistä koskevien määräysten mukaisesti;

h) aineistoa ei saa jättää vartioimatta julkisiin tai yksityisiin ajoneuvoihin tai ravintoloiden tai hotellien kaltaisiin paikkoihin. Sitä ei saa varastoida hotellien kassakaappeihin tai jättää vartioimatta hotellihuoneisiin;

i) jos kuljetettava aineisto sisältää asiakirjoja, näitä ei saa lukea julkisilla paikoilla (esim. lentokoneissa, junissa jne.).

Turvaluokiteltavaa aineistoa kuljettamaan määrätyn henkilön on luettava ja allekirjoitettava turvaohjeet, jotka sisältävät vähintään edellä luetellut ohjeet ja menettelytavat, joita on noudatettava hätätapauksessa tai tulliviranomaisten tai lentoturvallisuusviranomaisten vaatiessa turvaluokiteltavan aineiston sisältämän pakkauksen avaamista.

RESTREINT UE -TURVALUOKAN ASIAKIRJOJEN LÄHETTÄMINEN

21. RESTREINT UE -turvaluokan asiakirjojen lähettämisestä ei ole erityisiä määräyksiä, paitsi että lähetettäessä on varmistettava, että asiakirjat eivät voi joutua sivullisille.

KURIIRIEN TURVALLISUUS

22. Kaikkien SECRET UE- ja CONFIDENTIEL UE -turvaluokan asiakirjojen kuljettamista varten palkattujen kuriirien ja lähettien on läpäistävä asianmukainen luotettavuusselvitys.

III luku

Sähköiset ja muut tekniset lähetyskeinot

23. Tietoliikenteen turvaamismenetelmien tarkoituksena on varmistaa EU:n turvaluokitellun tiedon suojattu lähettäminen. Tällaisen EU:n turvaluokitellun tiedon lähettämiseen sovellettavia yksityiskohtaisia sääntöjä käsitellään XI jaksossa.

24. CONFIDENTIEL UE- ja SECRET UE -turvaluokan tietoa saa siirtää ainoastaan valtuutettujen tietoliikennekeskusten ja -verkostojen ja/tai -päätteiden ja -järjestelmien kautta.

IV luku

EU:n turvaluokitelluista asiakirjoista tehdyt ylimääräiset jäljennökset, käännökset ja otteet

25. Vain tietojen luovuttaja antaa valtuutuksen TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjojen jäljentämiseen tai kääntämiseen.

26. Jos henkilön, jolla ei ole TRÈS SECRET UE / EU TOP SECRET -turvaluokan valtuutusta tarvitsee sellaista tietoa, joka ei ole turvaluokiteltu siitä huolimatta, että se esiintyy TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjassa, TRÈS SECRET UE / EU TOP SECRET -turvaluokan rekisteristä vastaava virkamies voidaan valtuuttaa ottamaan tarpeellisen määrän otteita kyseisestä asiakirjasta. Samalla hänen on toteutettava tarpeelliset toimet sen varmistamiseksi, että nämä otteet turvaluokitellaan asianmukaisesti.

27. Vastaanottaja voi jäljentää tai kääntää SECRET UE- ja sitä alemman turvaluokan asiakirjoja kansallisten turvallisuutta koskevien asetusten puitteissa sillä ehdolla, että yleisen valtuutuksen periaatetta noudatetaan tarkasti. Alkuperäiseen asiakirjaan sovellettavia turvatoimia sovelletaan myös siitä tehtyihin jäljennöksiin ja/tai käännöksiin. EU:n hajautetuissa erillisvirastoissa noudatetaan näitä turvallisuussääntöjä.

V luku

EU:n turvaluokitellun aineiston inventointi, tarkastukset, säilytys ja hävittäminen

INVENTOINNIT JA TARKASTUKSET

28. Joka vuosi kukin VIII jaksossa tarkoitettu TRÈS SECRET UE / EU TOP SECRET -turvaluokan kirjaamo toteuttaa TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjojen yksityiskohtaisen inventoinnin VIII jakson 9—11 jakson asetusten mukaisesti. TRÈS SECRET UE / EU TOP SECRET -turvaluokkaa alemmat EU:n turvaluokitellut asiakirjat tarkastetaan sisäisesti kansallisten suuntaviivojen mukaisesti sekä neuvoston pääsihteeristön tai EU:n hajautettujen erillisvirastojen osalta korkeana edustajana toimivan pääsihteerin ohjeiden mukaisesti.

Tässä yhteydessä asiakirjojen haltijoilla on tilaisuus ottaa kantaa siihen:

a) alennetaanko tai poistetaanko määrättyjen asiakirjojen turvaluokitus;

b) mitä asiakirjoja tuhotaan.

EU:N TURVALUOKITELLUN TIEDON SÄILYTTÄMINEN ARKISTOISSA

29. Varastointiongelmien minimoimiseksi kaikkien rekisterien valvontavirkailijoilla on valtuudet tallentaa TRÈS SECRET UE / EU TOP SECRET-, SECRET UE- ja CONFIDENTIEL UE -turvaluokan asiakirjoja mikrofilmille tai muulla tavoin varastoida sähköisesti tai optisin välinein arkistointia varten edellyttäen, että:

a) henkilöstöllä, joka suorittaa mikrofilmitallentamisen/varastoinnin, on voimassa oleva valtuutus käsitellä asianmukaisen turvaluokan tietoa;

b) mikrofilmi/varastointivälineet suojataan yhtä huolellisesti kuin alkuperäiset asiakirjat;

c) kaikesta TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjojen mikrofilmitallentamisesta/varastoinnista ilmoitetaan tietojen luovuttajalle;

d) yksittäiset filmirullat tai muut tallennusvälineet sisältävät ainoastaan saman TRÈS SECRET UE / EU TOP SECRET-, SECRET UE- tai CONFIDENTIEL UE -turvaluokan asiakirjoja;

e) TRÈS SECRET UE / EU TOP SECRET- tai SECRET UE -turvaluokan asiakirjojen mikrofilmitallennuksesta/varastoimisesta ilmoitetaan selkeästi vuosittaisessa inventoinnissa käytettävässä luettelossa;

f) alkuperäiset mikrofilmille tallennetut tai muuten varastoidut asiakirjat hävitetään jäljempänä 31—36 kohdassa olevien asetusten mukaisesti.

30. Nämä säännöt soveltuvat myös kaikkiin muihin kansallisen turvallisuusviranomaisen valtuuttamiin varastointikeinoihin kuten sähkömagneettiselle ja optiselle levykkeelle tallentamiseen.

EU:N TURVALUOKITELTUJEN ASIAKIRJOJEN TAVANOMAINEN HÄVITTÄMINEN

31. EU:n turvaluokiteltujen asiakirjojen tarpeettoman kasaantumisen välttämiseksi ne asiakirjat, joiden niitä hallinnoivan laitoksen päällikkö katsoo olevan vanhentuneita ja joita hän katsoo olevan liikaa, hävitetään niin pian kuin se on käytännössä mahdollista seuraavalla tavalla:

a) TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjojen hävittäminen voidaan tehdä ainoastaan niistä vastaavassa keskusrekisterissä. Jokainen hävitetty asiakirja merkitään hävittämisluetteloon, jonka allekirjoittavat TRÈS SECRET UE / EU TOP SECRET -turvaluokan valvontavirkailija sekä hävittämisen todistava virkailija, jolla on TRÈS SECRET UE / EU TOP SECRET -turvaluokan valtuutus. Tämä kirjataan päiväkirjaan.

b) Rekisterissä säilytetään hävittämistodistus yhdessä jakelulistan kanssa kymmenen vuoden ajan. Käännökset toimitetaan tietojen luovuttajalle tai asianmukaiselle keskuskirjaamolle ainoastaan erikseen pyydettäessä.

c) TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjat, mukaan lukien kaikki TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjojen valmistelusta aiheutuva turvaluokiteltu jäte, kuten vialliset käännökset, luonnokset, koneella kirjoitetut muistiinpanot ja hiilipaperit hävitetään TRÈS SECRET UE / EU TOP SECRET -turvaluokan valtuutuksen saaneen viranomaisen valvonnassa polttamalla, silppuamalla, repimällä tai muulla tavoin saattamalla tunnistamattomaan muotoon, josta niitä ei voi palauttaa ennalleen.

32. SECRET UE -turvaluokan asiakirjojen hävittämisen suorittaa kyseisistä asiakirjoista vastaava rekisteri luotettavuusselvityksen läpikäyneen henkilön valvonnassa käyttäen jotakin 31 kohdan c alakohdassa osoitettua menetelmää. Hävitetyt TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjat luetteloidaan hävittämistodistuksiin, jotka allekirjoitetaan ja jotka rekisteri säilyttää yhdessä jakelulistan kanssa vähintään kolmen vuoden ajan.

33. CONFIDENTIEL UE -turvaluokan asiakirjojen hävittämisen suorittaa kyseisistä asiakirjoista vastaava rekisteri luotettavuusselvityksen läpikäyneen henkilön valvonnassa käyttäen jotakin 31 kohdan c alakohdassa mainittua menetelmää. Niiden hävittäminen kirjataan kansallisten asetusten mukaisesti ja neuvoston pääsihteeristön tai EU:n hajautettujen erillisvirastojen tapauksessa korkeana edustajana toimivan pääsihteerin ohjeiden mukaisesti.

34. RESTREINT UE -turvaluokan asiakirjojen hävittämisen suorittaa kyseisistä asiakirjoista vastaava kirjaamo tai niiden käyttäjä kansallisten asetusten mukaisesti ja neuvoston pääsihteeristön tai EU:n hajautettujen erillisvirastojen tapauksessa korkeana edustajana toimivan pääsihteerin ohjeiden mukaisesti.

HÄVITTÄMINEN HÄTÄTAPAUKSISSA

35. Neuvoston pääsihteeristö, jäsenvaltiot ja EU:n hajautetut erillisvirastot laativat paikallisiin olosuhteisiin pohjautuvat suunnitelmat EU:n turvaluokitellun aineiston suojaamiseksi kriisitilanteissa mukaan lukien mahdolliset suunnitelmat hävittämistä ja evakuointia varten hätätapauksissa; kukin niistä julkaisee organisaationsa puitteissa tarpeelliseksi katsotut ohjeet sen estämiseksi, että EU:n turvaluokiteltava aineisto joutuisi sivullisille.

36. Järjestelyt SECRET UE- ja CONFIDENTIEL UE -turvaluokan aineiston suojaamiseksi ja/tai hävittämiseksi kriisitilanteessa eivät saa missään olosuhteissa vaikuttaa haitallisesti TRÈS SECRET UE / EU TOP SECRET -turvaluokan aineiston suojaamiseen tai hävittämiseen, mukaan lukien salauslaitteisto, jonka käsittely on kaikkia muita tehtäviä kiireellisempi. Salauslaitteisto suojataan ja hävitetään hätätapauksessa noudattaen *ad hoc* -ohjeita.

VI luku

Neuvostolle osoitettuihin asiakirjoihin sovellettavat erityissäännöt

37. Luokiteltujen tietojen toimisto seuraa neuvoston pääsihteeristössä SECRET UE- tai CONFIDENTIEL UE -turvaluokkien tietoja, jotka sisältyvät neuvostolle osoitettuihin asiakirjoihin.

Henkilöstö- ja hallintoasiain pääjohtajan alaisuudessa luokiteltujen tietojen toimisto:

a) hoitaa kirjaamista, monentamista, kääntämistä, siirtämistä, lähettämistä ja hävittämistä koskevia toimenpiteitä;

b) pitää ajantasaista luetteloa turvaluokiteltavista tiedoista;

c) tiedustelee säännöllisin väliajoin tietojen lähettäjiltä, onko tietojen suojaus samassa luokassa edelleen tarpeen;

d) määrittelee yhteistyössä turvallisuusyksikön kanssa tietojen luokituksessa ja luokituksen poistamisessa sovellettavat käytännön menettelytavat.

38. Luokiteltujen tietojen toimisto pitää yllä seuraavat tiedot sisältävää rekisteriä:

a) turvaluokiteltavan tiedon valmistumispäivämäärä;

b) luokka;

c) luokan voimassaolon päättymispäivä;

d) lähettäjän nimi ja osasto;

e) vastaanottaja/t sekä tämän/näiden järjestysnumerot;

f) asia;

g) numero;

h) jaettujen kappaleiden lukumäärä;

i) neuvostolle toimitetun turvaluokiteltavan tiedon inventaarioiden valmistelut;

j) turvaluokiteltavan tiedon luokan poistamisesta tai alentamisesta pidettävä luettelo.

39. Tämän jakson I—V luvuissa määrätyt yleiset säännöt soveltuvat neuvoston pääsihteeristön luokiteltujen tietojen toimistoon, ellei niitä muuteta tässä luvussa määrätyillä erityissäännöillä.

VIII JAKSO

TRÈS SECRET UE / EU TOP SECRET -REKISTERIT

1. TRÈS SECRET UE / EU TOP SECRET -rekistereiden tarkoituksena on varmistaa, että TRÈS SECRET UE / EU TOP SECRET -asiakirjojen tallennus, käsittely ja jakelu toteutetaan turvamääräysten mukaisesti. TRÈS SECRET UE / EU TOP SECRET -rekisterin johtaja toimii kussakin jäsenvaltiossa ja neuvoston pääsihteeristössä ja tarvittaessa EU:n hajautetuissa virastoissa TRÈS SECRET UE / EU TOP SECRET -valvontaviranomaisena.

2. Keskusrekisterit toimivat pääasiallisina tietoja vastaanottavina ja luovuttavina viranomaisina jäsenvaltioissa, neuvoston pääsihteeristössä ja sellaisissa EU:n hajautetuissa virastoissa, joihin kyseisiä rekistereitä on perustettu, sekä tarvittaessa muissa EU:n toimielimissä, kansainvälisissä järjestöissä ja kolmansissa valtioissa, joiden kanssa neuvosto on sopinut luokiteltujen tietojen vaihtamista koskevista turvamenettelyistä.

3. Tarvittaessa perustetaan alarekistereitä, jotka vastaavat TRÈS SECRET UE / EU TOP SECRET -asiakirjojen sisäisestä hallinnoinnista; kyseisissä rekistereissä pidetään ajantasaiset tiedot alarekisterissä olevien asiakirjojen liikkeistä.

4. TRÈS SECRET UE / EU TOP SECRET -alarekisterit perustetaan I jaksossa esitetyn mukaisesti vastauksena pitkäaikaisiin tarpeisiin, ja ne liitetään TRÈS SECRET UE / EU TOP SECRET -keskusrekisteriin. Jos TRÈS SECRET UE / EU TOP SECRET -asiakirjoja tarvitaan vain väliaikaisesti ja satunnaisesti, ne voidaan luovuttaa ilman TRÈS SECRET UE / EU TOP SECRET -alarekisterin perustamista edellyttäen, että on olemassa määräyksiä sen varmistamiseksi, että kyseiset asiakirjat ovat edelleen asianomaisen TRÈS SECRET UE / EU TOP SECRET -rekisterin valvonnassa ja että kaikkia fyysisen ja henkilöstön turvallisuuden suojausta koskevia toimenpiteitä noudatetaan.

5. TRÈS SECRET UE / EU TOP SECRET -asiakirjoja ei voida toimittaa suoraan saman TRÈS SECRET UE / EU TOP SECRET -keskusrekisterin alarekisteristä toiseen ilman keskusrekisterin nimenomaista hyväksyntää.

6. Muiden kuin samaan keskusrekisteriin liittyvien alarekistereiden välinen TRÈS SECRET UE / EU TOP SECRET -asiakirjojen vaihto on ohjattava TRÈS SECRET UE / EU TOP SECRET -keskusrekistereiden kautta.

TRÈS SECRET UE / EU TOP SECRET -KESKUSREKISTERIT

7. TRÈS SECRET UE / EU TOP SECRET -keskusrekisterin valvontaviranomaisena toimivan johtajan tehtävänä on:

   a) toimittaa TRÈS SECRET UE / EU TOP SECRET -asiakirjoja VII jaksossa olevien määräysten mukaisesti;

   b) ylläpitää luetteloa kaikista keskusrekisterin alaisista TRÈS SECRET UE / EU TOP SECRET -alarekistereistä sekä näiden valvontaviranomaisiksi nimettyjen henkilöiden ja heidän valtuutettujen sijaistensa nimistä ja allekirjoituksista;

   c) säilyttää kuittaustiedot kaikista keskusrekisterin luovuttamista TRÈS SECRET UE / EU TOP SECRET -asiakirjoista;

   d) pitää kirjaa keskusrekisterissä olevista ja sen jakamista TRÈS SECRET UE / EU TOP SECRET -asiakirjoista;

   e) ylläpitää ajantasaista luetteloa kaikista sellaisista TRÈS SECRET UE / EU TOP SECRET -keskusrekistereistä ja niiden valvontaviranomaisiksi nimettyjen henkilöiden ja heidän valtuutettujen sijaistensa nimistä ja allekirjoituksista, joiden kanssa keskusrekisterin johtaja on yleensä tekemisissä;

   f) suojelee fyysisesti kaikkia rekisterissä olevia TRÈS SECRET UE / EU TOP SECRET -asiakirjoja IV jaksossa olevien määräysten mukaisesti.

TRÈS SECRET UE / EU TOP SECRET -ALAREKISTERIT

8. TRÈS SECRET UE / EU TOP SECRET -alarekisterin valvontaviranomaisena toimivan johtajan tehtävänä on:

   a) toimittaa TRÈS SECRET UE / EU TOP SECRET -asiakirjoja VII jaksossa ja VIII jakson 5 ja 6 kohdassa olevien määräyksien mukaisesti;

b) ylläpitää ajantasaista luetteloa kaikista henkilöistä, joilla on valtuudet saada hänen valvonnassaan olevia TRÈS SECRET UE / EU TOP SECRET -tietoja;

c) toimittaa TRÈS SECRET UE / EU TOP SECRET -asiakirjoja niiden luovuttajan ohjeiden tai tarpeellisuusperiaatteen mukaisesti tarkistettuaan ensin, että vastaanottajasta on tehty vaadittu luotettavuusselvitys;

d) ylläpitää ajantasaiset tiedot kaikista TRÈS SECRET UE / EU TOP SECRET -asiakirjoista, joiden hallussapitoa tai jakelua hän valvoo tai jotka on toimitettu muihin TRÈS SECRET UE / EU TOP SECRET -rekistereihin, sekä säilyttää kuittaustiedot kyseisistä asiakirjoista;

e) ylläpitää ajantasaista luetteloa niistä TRÈS SECRET UE / EU TOP SECRET -rekistereistä, joiden kanssa hänellä on valtuudet vaihtaa TRÈS SECRET UE / EU TOP SECRET -asiakirjoja, ja kyseisten rekistereiden valvontaviranomaisina toimivien henkilöiden ja heidän valtuutettujen sijaistensa nimistä ja allekirjoituksista;

f) suojelee fyysisesti kaikkia rekisterissä olevia TRÈS SECRET UE / EU TOP SECRET -asiakirjoja IV jaksossa olevien määräysten mukaisesti.

INVENTOINTI

9. TRÈS SECRET UE / EU TOP SECRET -rekisteri luetteloi vuosittain yksityiskohtaisesti kaikki TRÈS SECRET UE / EU TOP SECRET -asiakirjat, joista se on tilivelvollinen. Asiakirja on luetteloitava, jos se on fyysisesti rekisterissä tai jos rekisterissä on sen TRÈS SECRET UE / EU TOP SECRET -rekisterin kuittaus vastaanotosta, jonne asiakirja on siirretty, todistus asiakirjan hävittämisestä taikka määräys kyseisen asiakirjan luokittelun alentamisesta tai poistamisesta.

10. Alarekistereiden on toimitettava vuosittaisen luettelointinsa tulokset siihen keskusrekisteriin, jonka alaisia ne ovat, tiettyyn kyseisen keskusrekisterin määräämään päivään mennessä.

11. Kansallisten turvallisuusviranomaisten, kuten myös niiden EU:n toimielinten, kansainvälisten järjestöjen ja niiden EU:n hajautettujen virastojen, joihin perustettu TRÈS SECRET UE / EU TOP SECRET -keskusrekisteri, on toimitettava TRÈS SECRET UE / EU TOP SECRET -keskusrekisterissä suoritettujen vuosittaisten luettelointien tulokset korkeana edustajana toimivalle pääsihteerille viimeistään kunkin vuoden 1 päivänä huhtikuuta.

IX JAKSO

NEUVOSTON ULKOPUOLELLA JÄRJESTETTÄVIEN JA ERITTÄIN ARKALUONTEISIA ASIOITA KÄSITTELEVIEN ERITYISKOKOUSTEN YHTEYDESSÄ SOVELLETTAVAT TURVATOIMET

YLEISTÄ

1. Järjestettäessä Eurooppa-neuvoston tai neuvoston istuntoja, ministerikokouksia tai muita tärkeitä kokouksia Brysselissä ja Luxemburgissa sijaitsevien neuvoston tilojen ulkopuolella ja käsiteltävien asioiden tai tietojen arkaluonteisuuteen liittyvien turvavaatimusten sitä edellyttäessä on toteutettava seuraavat turvatoimet. Kyseiset toimet koskevat ainoastaan EU:n luokiteltujen tietojen suojelua. Myös muita turvatoimia saattaa olla tarpeen suunnitella.

VASTUUALUEET

Isäntäjäsenvaltiot

2. Jäsenvaltion, jonka alueella kokous on määrä järjestää (isäntäjäsenvaltio), on vastattava yhteistyössä neuvoston pääsihteeristön turvallisuusyksikön kanssa Eurooppa-neuvoston ja neuvoston istuntojen sekä ministerikokousten ja muiden tärkeiden kokousten turvallisuudesta sekä valtuuskuntien tärkeimpien jäsenten ja heidän henkilöstönsä fyysisestä turvallisuudesta.

Turvallisuuden suojelun osalta on erityisesti varmistettava, että:

a) turvallisuusuhkiin ja turvallisuuden vaarantaviin tapahtumiin varautumiseksi laaditaan suunnitelmia. Kyseisissä suunnitelmissa on otettava erityisesti huomioon se, että EU:n luokiteltuja tietoja on voitava toimistotiloissa säilyttää turvallisessa paikassa;

b) toteutetaan toimenpiteitä, jotta EU:n luokiteltuja tietoja koskevien viestien vastaanottamiseen ja toimittamiseen on mahdollista käyttää neuvoston tietoliikennejärjestelmää. Isäntäjäsenvaltion on myös pyydettäessä annettava käyttöön turvallisia puhelinjärjestelmiä.

Jäsenvaltiot

3. Jäsenvaltioiden viranomaisten on toteutettava tarvittavat toimet sen varmistamiseksi, että:

a) jäsenvaltioiden valtuuskuntien jäsenille annetaan asianmukaiset todistukset luotettavuusselvityksistä tarvittaessa joko merkkeinä tai faksilla joko suoraan kokouksen turvallisuusvastaavalle tai neuvoston pääsihteeristön turvallisuusyksikön välityksellä;

b) tiedottavat erityisistä uhkista isäntäjäsenvaltion viranomaisille ja tarvittaessa neuvoston pääsihteeristön turvallisuusyksikölle asianmukaisten toimien toteuttamiseksi.

Kokouksen turvallisuuspäällikkö

4. On nimettävä kokouksen turvallisuudesta vastaava henkilö, joka valmistelee ja valvoo yleisiä sisäisiä turvatoimenpiteitä sekä koordinoi niitä muiden asiaankuuluvien turvaviranomaisten kanssa. Hänen toteuttamiensa toimien olisi yleensä liityttävä:

a) i) kokouspaikkaa koskeviin turvatoimiin, jotta kokous voidaan järjestää ilman kokouksessa mahdollisesti käytettävien EU:n luokiteltujen tietojen turvallisuuden vaarantavia tapahtumia;

ii) kokouspaikalle, valtuuskuntien tiloihin ja kokoussaleihin pääsyyn oikeutetun henkilöstön tarkastamiseen ja laitteiston tarkistamiseen;

iii) jatkuvaan koordinointiin isäntäjäsenvaltion toimivaltaisten viranomaisten sekä neuvoston pääsihteeristön turvallisuusyksikön kanssa;

b) kokousasiakirjoihin liitettäviin turvaohjeisiin ottaen asianmukaisesti huomioon näissä turvallisuussäännöissä esitetyt vaatimukset ja muut tarpeellisiksi katsotut turvaohjeet.

Neuvoston pääsihteeristön turvallisuusyksikkö

5. Neuvoston pääsihteeristön turvallisuusyksikön on toimittava turvallisuusasioiden neuvontajana kokousta valmisteltaessa; turvallisuusyksikön olisi osallistuttava kokouksen valmisteluun auttamalla ja antamalla neuvoja kokouksen turvallisuuspäällikölle ja tarvittaessa valtuuskunnille.

6. Jokaisen kokoukseen osallistuvan valtuuskunnan on nimettävä turvallisuuspäällikkö, joka vastaa valtuuskuntaa koskevista turvallisuusasioista ja on yhteydessä kokouksen turvallisuuspäällikköön sekä tarvittaessa neuvoston pääsihteeristön turvallisuusyksikön edustajaan.

TURVATOIMET

Suojatut alueet

7. Seuraavat alueet olisi määriteltävä:

   a) II luokan suojattu alue, johon kuuluvat tarvittaessa asiakirjojen valmisteluhuone, neuvoston pääsihteeristön tilat ja kopiointilaitteet, sekä valtuuskuntien tilat;

   b) I luokan suojattu alue, johon kuuluvat kokoussali sekä tulkkien ja ääniteknikkojen työtilat;

   c) hallinnolliset alueet, joihin kuuluvat lehdistötilat, hallinnointiin, ruokailuun ja yöpymiseen käytettävät tilat, lehdistökeskuksen välittömässä läheisyydessä sijaitseva alue sekä kokouspaikka.

Kulkuluvat

8. Kokouksen turvallisuuspäällikön on toimitettava asianmukaiset kulkuluvat, joita valtuuskunnat ovat pyytäneet tarpeidensa mukaisesti. Tarvittaessa voidaan eritellä ne suojatut alueet, joille kulkuluvan haltijalla on oikeus päästä.

9. Kokouksen turvaohjeistuksessa on vaadittava, että kaikkien asianomaisten henkilöiden on pidettävä kokouspaikalla ollessaan aina kulkulupansa näkyvästi esillä, jotta turvahenkilöstö voi tarvittaessa tarkastaa ne.

10. Kokouspaikalle olisi päästettävä mahdollisimman vähän henkilöitä, joilla ei ole kulkulupaa. Valtuuskunnat, jotka haluavat tavata vierailijoita kokouksen aikana, on ilmoitettava tästä kokouksen turvallisuuspäällikölle. Vierailijoille on annettava erillinen vierailijakulkulupa. Tässä yhteydessä on täytettävä vierailijalomake, johon merkitään vierailijan nimi sekä tavattavan henkilön nimi. Vierailijalla on oltava aina mukanaan joko turvamies tai tavattava henkilö. Saattavan henkilön on pidettävä vierailijalomake mukanaan ja palautettava se yhdessä vierailijakulkuluvan kanssa turvahenkilöstölle, kun vierailija poistuu kokouspaikalta.

Kuvan- ja äänentallennuslaitteiston tarkastaminen

11. Kameroita ja äänityslaitteita ei saa tuoda I luokan suojatulle alueelle lukuun ottamatta valokuvaajien ja ääniteknikkojen tuomia laitteita, joille kokouksen turvallisuuspäällikkö on antanut asiaankuuluvat luvat.

Salkkujen, kannettavien tietokoneiden ja pakettien tarkastus

12. Henkilöt, joilla on kulkulupa suojatulle alueelle, voivat yleensä tuoda salkkunsa ja kannettavat tietokoneensa (ainoastaan omalla virtalähteellä) ilman, että niitä tarkastetaan. Valtuuskunnille tarkoitetut paketit on tarkastettava joko siten, että valtuuskunnan turvallisuuspäällikkö tarkastaa paketit, ne läpivalaistaan erityislaitteistoa käyttäen tai turvallisuushenkilöstö avaa ne tarkastusta varten. Salkkujen ja pakettien tarkastukseen voidaan määrätä tiukempia toimenpiteitä, jos kokouksen turvallisuuspäällikkö katsoo sen tarpeelliseksi.

Tekninen suojaus

13. Turvallisuusteknikot voivat suojata teknisesti kokoussalin, ja he voivat myös suorittaa televalvontaa kokouksen aikana.

Valtuuskuntien asiakirjat

14. Valtuuskunnat ovat vastuussa EU:n luokiteltujen asiakirjojen viemisestä kokouksiin ja niistä pois. Valtuuskunnat vastaavat myös kyseisten asiakirjojen todentamisesta ja suojaamisesta sinä aikana, kun niitä käytetään valtuuskunnille osoitetuissa tiloissa. Isäntäjäsenvaltiota saatetaan pyytää kuljettamaan luokiteltuja asiakirjoja kokouspaikalle ja sieltä pois.

Asiakirjojen säilyttäminen turvallisessa paikassa

15. Jolleivat neuvoston pääsihteeristö, komissio tai valtuuskunnat voi säilyttää luokiteltuja asiakirjojaan hyväksyttyjen normien mukaisesti, ne voivat kuittausta vastaan jättää kyseiset asiakirjat sinetöidyssä kirjekuoressa kokouksen turvallisuuspäällikölle, joka säilyttää ne hyväksyttyjen normien mukaisesti.

Tilojen tarkastus

16. Kokouksen turvallisuuspäällikkö huolehtii siitä, että neuvoston pääsihteeristön ja valtuuskuntien tilat tarkastetaan jokaisen työpäivän jälkeen sen varmistamiseksi, että kaikkia EU:n luokiteltuja tietoja säilytetään turvallisessa paikassa. Ellei näin ole, turvallisuuspäällikkö toteuttaa tarvittavat toimenpiteet.

EU:n luokiteltujen asiakirjojen hävittäminen

17. Kaikkia tarpeettomia asiakirjoja on käsiteltävä EU:n luokiteltuina tietoina. Neuvoston pääsihteeristölle ja valtuuskunnille on annettava jätepaperikorit tai -pussit. Ennen kuin neuvoston pääsihteeristö ja valtuuskuntien jäsenet poistuvat niille osoitetuista tiloista, niiden on toimitettava tarpeettomat asiakirjat kokouksen turvallisuuspäällikölle, joka huolehtii niiden sääntöjen mukaisesta hävittämisestä.

18. Kokouksen päätyttyä kaikkia neuvoston pääsihteeristön tai valtuuskuntien hallussa olevia tarpeettomia asiakirjoja on käsiteltävä jätteenä. Neuvoston pääsihteeristön ja valtuuskuntien tilat on tarkastettava perinpohjaisesti ennen kokouksen turvajärjestelyjen poistamista. Asiakirjat, joiden vastaanotosta on vaadittu kuittaus, on hävitettävä VII jaksossa esitetyllä tavalla.

X JAKSO

EU:N LUOKITELTUJEN TIETOJEN TURVALLISUUDEN RIKKOMINEN JA VAARANTAMINEN

1. Tietoturvallisuutta rikotaan, jos neuvoston tai kansallisia turvasääntöjä ei noudateta tai niitä laiminlyödään, mistä saattaa aiheutua vahinkoa tai vaaraa EU:n luokitelluille tiedoille.

2. EU:n luokiteltujen tietojen turvallisuus vaarantuu, jos kyseiset tiedot ovat joutuneet kokonaisuudessaan tai osittain henkilöille, joita ei ole valtuutettu käsittelemään niitä, eli joiden luotettavuutta ei ole selvitetty asianmukaisella tavalla tai joilla ei ole tietojen käsittelyn edellyttämiä valtuuksia, tai jos on todennäköistä, että tiedot ovat joutuneet kyseisille henkilöille.

3. EU:n luokiteltujen tietojen turvallisuus voi vaarantua huolimattomuuden, välinpitämättömyyden tai harkitsemattomuuden seurauksena, EU:hun tai sen jäsenvaltioihin kohdistuvan, EU:n luokiteltuja tietoja koskevan toiminnan vuoksi tai muuta haitallista toimintaa harjoittavien järjestöjen vuoksi.

4. Henkilöille, joiden edellytetään käsittelevän EU:n luokiteltuja tietoja, on selvitettävä perusteellisesti, mitä turvatoimia on sovellettava, mitä vaaroja on harkitsemattomasta keskustelusta ja mikä on heidän suhteensa tiedotusvälineisiin. Heidän on oltava tietoisia siitä, että mistä tahansa heidän tietoonsa tulleesta tietoturvallisuuden vaarantavasta rikkomuksesta on ilmoitettava välittömästi jäsenvaltion tai sen toimielimen tai viraston turvallisuusviranomaiselle, jonka palveluksessa he ovat.

5. Kun turvallisuusviranomainen havaitsee tai saa tiedon EU:n luokiteltujen tietojen turvallisuuden rikkomisesta tai EU:n luokitellun aineiston katoamisesta tai häviämisestä, ryhtyy se pikaisiin toimiin, jotta voidaan:

   a) selvittää tosiseikat;

   b) arvioida tapahtunut vahinko ja minimoida sen vaikutukset;

   c) estää tapahtuman toistuminen;

   d) ilmoittaa asiaankuuluville viranomaisille turvallisuusmääräysten rikkomisen vaikutuksista.

   Tässä yhteydessä on annettava seuraavat tiedot:

   i) kuvaus kyseessä olevista tiedoista ja niiden luokituksesta, viite- ja kopionumero, päivämäärä, tietojen luovuttaja, asia ja soveltamisala;

   ii) lyhyt kuvaus olosuhteista, joissa tietoturvallisuutta on rikottu, sekä päivämäärä ja ajankohta, jona tietojen turvallisuus saattoi vaarantua;

   iii) ilmoitus tietojen luovuttajalle mahdollisesti annetusta ilmoituksesta.

6. Saatuaan ilmoituksen tietoturvallisuuden mahdollisesta rikkomisesta kunkin turvallisuusviranomaisen velvollisuutena on raportoida tapahtumasta välittömästi seuraavaa menettelyä noudattaen: EU TOP SECRET -alarekisteri raportoi asian neuvoston pääsihteeristön turvallisuusyksikölle EU TOP SECRET -keskusrekisterin välityksellä; jos EU:n luokiteltujen tietojen turvallisuus on vaarantunut jonkin jäsenvaltion toimivaltaan kuuluvalla alalla, kyseisen jäsenvaltion on raportoitava neuvoston pääsihteeristön turvallisuusyksikölle kansallisen turvallisuusviranomaisen välityksellä 5 kohdassa esitetyn mukaisesti.

7. Jos kyseessä on RESTREINT UE -tietoja, asiasta on raportoitava ainoastaan, jos tapauksessa on jotain epätavanomaista.

8. Saatuaan tiedon tietoturvallisuuden rikkomisesta korkeana edustajana toimiva pääsihteeri

   a) ilmoittaa asiasta viranomaiselle, joka kyseiset luokitellut tiedot on luovuttanut;

   b) pyytää asianomaisia turvallisuusviranomaisia aloittamaan tutkintatoimet;

   c) koordinoi tutkintaa, jos asia koskee useampaa kuin yhtä turvallisuusviranomaista;

d) hankkii selvityksen olosuhteista, joissa tietoturvallisuutta on rikottu, päivämäärästä ja ajankohdasta, jona tietojen turvallisuus saattoi vaarantua ja jona rikkomus havaittiin, sekä tarkan kuvauksen kyseessä olevan aineiston sisällöstä ja luokituksesta. Lisäksi olisi raportoitava EU:n tai sen yhden tai useamman jäsenvaltion eduille aiheutuneesta vahingosta tai tapahtuman toistumisen estämiseksi toteutetuista toimista.

9. Viranomaisen, jolta tiedot ovat peräisin, on myös tiedotettava asiasta asianosaisille ja annettava niille asianmukaiset ohjeet.

10. Henkilölle, joka on vastuussa EU:n luokiteltujen tietojen turvallisuuden vaarantamisesta, voidaan määrätä kurinpitoseuraamus asiaankuuluvien sääntöjen ja määräysten mukaisesti. Kurinpitoseuraamus ei rajoita oikeutta ryhtyä oikeustoimiin.

XI JAKSO

TIETO- JA TIETOLIIKENNEJÄRJESTELMISSÄ KÄSITELTÄVIEN TIETOJEN SUOJAUS

Sisällysluettelo

		Sivu
I luku	Johdanto	37
II luku	Määritelmät	38
III luku	Turvallisuusvastuut	41
IV luku	Muut kuin tekniset turvatoimet	42
V luku	Tekniset turvatoimet	43
VI luku	Turvallisuus käsittelyn aikana	45
VII luku	Hankinnat	45
VIII luku	Väliaikainen tai tilapäinen käyttö	46

I luku

Johdanto

YLEISTÄ

1. Tässä jaksossa käsiteltävää turvallisuuspolitiikkaa ja -vaatimuksia sovelletaan kaikkiin tieto- ja tietoliikennejärjestelmiin ja -verkkoihin (jäljempänä JÄRJESTELMÄT), joissa käsitellään CONFIDENTIEL UE- tai sitä luottamuksellisempia tietoja.

2. Myös RESTREINT UE -tietoja käsitteleville JÄRJESTELMILLE on kehitettävä turvatoimet tällaisten tietojen luottamuksellisuuden suojaamiseksi. Kaikki JÄRJESTELMÄT edellyttävät turvatoimia järjestelmien ja niiden sisältämien tietojen eheyden ja käytettävyyden suojaamiseksi. Nimetty turvallisuusjärjestelyt hyväksyvä viranomainen (Security Accreditation Authority, SAA) määrittelee näihin järjestelmiin sovellettavat turvatoimet, jotka ovat oikeassa suhteessa arvioituun riskiin ja näissä turvallisuussäännöissä esitetyn politiikan mukaisia.

3. Sulautettuja tietotekniikkajärjestelmiä sisältävien anturijärjestelmien suojaus määritellään niiden järjestelmien yleisessä yhteydessä, joihin ne kuuluvat, käyttäen mahdollisimman laajalti tämän jakson soveltuvia määräyksiä.

JÄRJESTELMIIN KOHDISTUVAT UHAT JA JÄRJESTELMIEN HAAVOITTUVUUS

4. Yleisesti ottaen uhka voidaan määritellä mahdollisuudeksi turvallisuuden tahattomaan tai tahalliseen vaarantamiseen. JÄRJESTELMIEN osalta tällainen vaarantaminen tapahtuu silloin, kun yksi tai useampi luottamuksellisuuden, eheyden tai käytettävyyden ominaisuuksista häviää. Haavoittuvuus voidaan määritellä valvonnan riittämättömyydeksi tai puuttumiseksi, jonka vuoksi jokin erityinen kohde helpommin joutuu tai voi joutua uhan alaiseksi. Haavoittuvuus voi olla valvonnan laiminlyöntiä, tai se voi liittyä puutteellisuuteen valvonnan tehokkuudessa, täydellisyydessä tai johdonmukaisuudessa. Haavoittuvuus voi olla luonteeltaan teknistä, menettelyihin liittyvää tai toiminnallista.

5. Nopeasti toimivia hakuja, viestintää ja käyttöä varten suunnitelluissa JÄRJESTELMISSÄ käsiteltävät EU:n turvaluokitellut ja -luokittelemattomat keskitetyssä muodossa olevat tiedot ovat alttiina monille riskeille. Näitä ovat luvattomien käyttäjien pääsy tietoihin tai päinvastaisesti pääsyn epääminen luvan saaneilta käyttäjiltä. Riskejä ovat myös tietojen luvaton paljastaminen, turmeleminen, muuttaminen tai poistaminen. Lisäksi monimutkaiset ja joskus herkät laitteet ovat kalliita ja niitä on usein vaikea korjata tai uusia nopeasti. Sen vuoksi tällaiset JÄRJESTELMÄT ovat houkuttelevia kohteita tiedonkeruutoimille ja sabotoinnille erityisesti, jos turvatoimia pidetään tehottomina.

TURVATOIMET

6. Tässä jaksossa käsiteltävien turvatoimien päätarkoituksena on suojata tiedot luvattomalta paljastamiselta (luottamuksellisuuden häviämiseltä) ja varmistaa tietojen eheys ja käytettävyys. Jotta EU:n turvaluokiteltuja tietoja käsittelevälle JÄRJESTELMÄLLE saataisiin asianmukainen turvallisuussuoja, on määriteltävä kunkin JÄRJESTELMÄN osalta tavanomaista turvallisuutta koskevat asianmukaiset standardit ja asianmukaiset erityiset turvallisuusmenettelyt ja -tekniikat.

7. On määriteltävä ja pantava täytäntöön asianmukaiset turvatoimet turvallisen ympäristön luomiseksi JÄRJESTELMÄN toiminnalle. Näitä toimia sovelletaan fyysisiin tekijöihin, henkilöstöön, muihin kuin teknisiin menettelyihin sekä tietojen ja tietoliikenteen turvallisuuden varmistaviin toimintatapoihin.

8. Tarpeellisuusperiaatteen täytäntöönpanemiseksi ja luvattoman tiedon paljastamisen ehkäisemiseksi tai havaitsemiseksi on edellytettävä turvatoimia (laitteiston ja ohjelmiston turvallisuusominaisuudet). Turvamääräyksiä laadittaessa määritellään, kuinka laajalti turvatoimia tarvitaan. Hyväksymismenettelyssä määritellään, että on olemassa näiden turvatoimien tarvetta vastaava riittävä varmuustaso.

JÄRJESTELMÄKOHTAINEN TURVAVAATIMUSILMOITUS

9. Kaikkien CONFIDENTIEL UE- tai sitä luottamuksellisempia tietoja käsittelevien JÄRJESTELMIEN osalta vaaditaan järjestelmäkohtainen turvavaatimusilmoitus (SYSTEM-Specific Security Requirement Statement, SSRS), jonka tekee tietotekniikkajärjestelmän käyttöviranomainen (IT System Operational Authority, ITSOA) tarvittaessa projektihenkilöstön ja tietoturvaviranomaisen tuella ja jonka turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) hyväksyy. Järjestelmäkohtainen turvavaatimusilmoitus vaaditaan myös silloin, kun turvallisuusjärjestelyt hyväksyvä viranomainen katsoo, että RESTREINT UE -tietojen tai luokittelemattomien tietojen käytettävyys ja eheys ovat uhattuina.

10. Järjestelmäkohtainen turvavaatimusilmoitus (SSRS) on laadittava mahdollisimman varhaisessa vaiheessa projektin alussa, ja sitä on kehitettävä ja paranneltava projektin edetessä, jotta se täyttää eri tehtävät projektin ja JÄRJESTELMÄN elinkaaren eri vaiheissa.

11. Järjestelmäkohtainen turvavaatimusilmoitus (SSRS) on tietotekniikkajärjestelmän käyttöviranomaisen (ITSOA) ja turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) välinen sitova sopimus, jonka perusteella JÄRJESTELMÄ hyväksytään.

12. Järjestelmäkohtainen turvavaatimusilmoitus (SSRS) on täydellinen ja täsmällinen selvitys noudatettavista turvallisuusperiaatteista ja yksityiskohtaisista turvallisuusvaatimuksista. Se perustuu neuvoston turvallisuuspolitiikkaan ja riskinarviointiin, tai sitä edellyttävät käyttöympäristöä koskevat parametrit, henkilöstön luotettavuusselvityksen alin taso, käsiteltävän tiedon korkein turvaluokitus, turvallisuuden takaava toimintatapa tai käyttäjävaatimukset. Järjestelmäkohtainen turvavaatimusilmoitus (SSRS) on erottamaton osa projektia koskevaa dokumentaatiota, joka toimitetaan asianmukaisille viranomaisille hyväksyttäväksi teknisten, rahoituksellisten ja turvallisuusnäkökohtien osalta. Lopullisessa muodossaan järjestelmäkohtaisesta turvavaatimusilmoituksesta (SSRS) käy täysin selville, mihin JÄRJESTELMÄN turvallisuus perustuu.

TURVALLISUUDEN TAKAAVAT TOIMINTATAVAT

13. Kaikki CONFIDENTIEL UE- tai sitä luottamuksellisempia tietoja käsittelevät JÄRJESTELMÄT on hyväksyttävä käytettäväksi jollain, tai jos eri aikoina esitettävät vaatimukset sitä edellyttävät, usealla seuraavalla toimintatavalla tai niitä vastaavilla kansallisilla tavoilla:

a) yleisvaltuutus;

b) korkean turvallisuuden takaava toimintatapa;

c) monitasoinen turvallisuuden takaava toimintatapa.

II luku

Määritelmät

LISÄMERKINNÄT

14. Jos turvaluokittelun mukaisen käsittelyn lisäksi tarvitaan rajoitettua jakelua ja erityiskäsittelyä varten vielä muita merkintöjä, käytetään merkintää CRYPTO tai jotain muuta EU:ssa hyväksyttyä erityistä käsittelymerkintää.

15. YLEISVALTUUTUKSELLA tarkoitetaan toimintatapaa, jossa KAIKKIEN JÄRJESTELMÄÄN pääsevien luotettavuus selvitetään JÄRJESTELMÄSSÄ käsiteltäviä tietoja koskevan korkeimman turvaluokan mukaan ja kaikilla on yleinen valtuutus päästä KAIKKIIN JÄRJESTELMÄSSÄ käsiteltäviin tietoihin.

Huomautuksia:

1. Yleisvaltuutus merkitsee sitä, että turvallisuusominaisuuksilta ei edellytetä tietojen erottelua JÄRJESTELMÄN sisällä.

2. Muiden turvallisuusominaisuuksien (kuten fyysinen turvallisuus, henkilöstöturvallisuus ja menettelyihin liittyvä turvallisuus) on oltava JÄRJESTELMÄSSÄ käsiteltävien tietojen korkeimman turvaluokan ja kaikkien tietoluokkavaatimusten mukaisia.

16. KORKEAN TURVALLISUUSTASON TAKAAVALLA TOIMINTATAVALLA tarkoitetaan toimintatapaa, jossa kaikkien JÄRJESTELMÄÄN pääsevien luotettavuus selvitetään JÄRJESTELMÄSSÄ käsiteltäviä tietoja koskevan korkeimman turvaluokan mukaan, mutta KAIKILLA EI ole yleisvaltuutusta päästä JÄRJESTELMÄSSÄ käsiteltyihin tietoihin.

Huomautuksia:

1. Yleisvaltuutuksen puuttuminen merkitsee sitä, että turvallisuusominaisuuksilta edellytetään sitä, että pääsy JÄRJESTELMÄN tietoihin on valikoivaa ja tiedot erotellaan järjestelmässä.

2. Muiden turvallisuusominaisuuksien (kuten fyysinen turvallisuus, henkilöstöturvallisuus ja menettelyihin liittyvä turvallisuus) on oltava JÄRJESTELMÄSSÄ käsiteltävien tietojen korkeimman turvaluokan ja kaikkien tietoluokkavaatimusten mukaisia.

3. Kaikki tämän toimintatavan mukaisesti JÄRJESTELMÄSSÄ käsiteltävät tai käytettävät tiedot ja tietojen tulostus on suojattava ikään kuin ne kuuluisivat kulloiseenkin tietoluokkaan ja edellyttäisivät korkeinta turvaluokkaa, kunnes ne määritellään toisin, paitsi jos jotain muuta merkintätapaa pidetään tarpeeksi luotettavana.

17. MONITASOISELLA TURVALLISUUDEN TAKAAVALLA TOIMINTATAVALLA tarkoitetaan toimintatapaa, jossa KAIKKIEN JÄRJESTELMÄÄN pääsevien luotettavuutta EI selvitetä JÄRJESTELMÄSSÄ käsiteltäviä tietoja koskevan korkeimman turvaluokan mukaan ja jossa KAIKILLA EI ole yleisvaltuutusta päästä JÄRJESTELMÄSSÄ käsiteltäviin tietoihin.

Huomautuksia:

1. Tämän toimintatavan mukaan voidaan nykyään käsitellä tietoja, joilla on erilaisia turvaluokkia ja jotka kuuluvat eri tietoluokkiin.

2. Se, että kaikkien luotettavuutta ei selvitetä korkeimman turvaluokan mukaan ja yleisvaltuutusta ei ole, merkitsee, että turvallisuusominaisuuksilta edellytetään, että pääsy JÄRJESTELMÄN tietoihin on valikoivaa ja tiedot erotellaan järjestelmässä.

18. TIETOTURVALLISUUS (INFOSEC) tarkoittaa turvatoimien soveltamista tietoliikenne-, tieto- ja muissa sähköisissä järjestelmissä käsiteltävien, tallennettavien tai siirrettävien tietojen suojaamiseksi tahattomasti tai tarkoituksellisesti aiheutetulta luottamuksellisuuden, eheyden ja käytettävyyden menettämiseltä, ja itse järjestelmien eheyden ja käytettävyyden menettämiseltä. Tietoturvallisuustoimenpiteitä ovat tietojen, siirron, lähettämisen ja salauksen turvallisuuden suojaaminen sekä tietoihin ja JÄRJESTELMÄÄN kohdistuvien uhkien havaitseminen, dokumentointi ja torjunta.

19. TIETOJÄRJESTELMÄTURVALLISUUS (COMPUTER SECURITY eli COMPUSEC) tarkoittaa laitteiston, valmisohjelmiston ja ohjelmiston turvaominaisuuksien soveltamista tietojärjestelmässä suojautumiseksi tietojen luvattomalta paljastamiselta, käsittelyltä, muuttamiselta tai poistamiselta tai palvelujen epäämiseltä tai näiden estämiseksi.

20. TIETOTURVATUOTTEELLA (COMPUTER SECURITY PRODUCT) tarkoitetaan yleistä tuotetta, joka sisällytetään tietojärjestelmään käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden tehostamiseksi tai varmistamiseksi.

21. TIETOLIIKENNETURVALLISUUDELLA (COMMUNICATIONS SECURITY eli COMSEC) tarkoitetaan turvatoimien soveltamista tietoliikenteeseen luvattoman pääsyn estämiseksi sellaiseen arvokkaaseen tietoon, jota voidaan saada seuraamalla tai analysoimalla tietoliikennettä, tai tietoliikenteen tietojen luotettavuuden takaamiseksi.

Huomautus:

Tällaiset toimet kattavat salauksen, siirron ja lähettämisen turvallisuuden sekä myös menettelyjen, fyysisen, henkilöstö-, asiakirjojen ja tietojen turvallisuuden.

22. ARVIOINNILLA (EVALUATION) tarkoitetaan sitä, että asiaankuuluva viranomainen suorittaa yksityiskohtaisen teknisen tutkimuksen JÄRJESTELMÄN turvallisuusnäkökohdista tai salaus- tai tietoturvatuotteesta.

Huomautuksia:

1. Arvioinnissa tutkitaan, onko vaadittava turvallisuustoiminta olemassa, aiheutuuko siitä haitallisia sivuvaikutuksia ja onko kyseinen toiminta suojattu luvattomalta muuttamiselta.

2. Arvioinnissa määritellään, missä määrin JÄRJESTELMÄN tai tietoturvatuotteen turvavaatimukset täyttyvät, ja vahvistetaan JÄRJESTELMÄN tai salauksen tai tietoturvatuotteen luotettavan toiminnan luotettavuustaso.

23. VARMENTAMISELLA (CERTIFICATION) tarkoitetaan riippumattoman tahon tarkastuksen ja arvioinnin tulosten pohjalta annettavaa virallista lausuntoa siitä, missä määrin JÄRJESTELMÄ on turvallisuusvaatimusten mukainen tai tietoturvatuote ennalta määriteltyjen turvallisuusvaatimusten mukainen.

24. HYVÄKSYMISELLÄ (ACCREDITATION) tarkoitetaan JÄRJESTELMÄLLE myönnettävää lupaa ja hyväksyntää käsitellä käyttöympäristössään EU:n turvaluokiteltuja tietoja.

Huomautus:

Hyväksyminen olisi tehtävä sen jälkeen, kun kaikki asiaankuuluvat turvatoimet on pantu täytäntöön ja on saavutettu riittävä järjestelmäresurssien suojaustaso. Hyväksymisen olisi perustuttava järjestelmäkohtaiseen turvavaatimusilmoitukseen ja sisällettävä seuraavat seikat:

a) järjestelmän hyväksymisen tavoite, erityisesti se, mikä on käsiteltävän tiedon turvaluokitus ja mitä järjestelmän tai verkon turvallisuuden takaavaa toimintatapaa ehdotetaan;

b) riskinhallinta-arviointi, jossa esitetään uhat ja heikot kohdat ja toimet niiden torjumiseksi;

c) turvallisuusmenettelyt (SecOP:t), joihin kuuluu yksityiskohtainen kuvaus ehdotetuista toimista (esimerkiksi toimintatavat ja toiminnat) ja kuvaus JÄRJESTELMÄN turvallisuusominaisuuksista, joihin hyväksyminen perustuu;

d) suunnitelma turvallisuusominaisuuksien täytäntöönpanemiseksi ja ylläpitämiseksi;

e) järjestelmän tai verkon turvallisuuden ensimmäistä ja jatkossa suoritettavaa tarkastusta, arviointia ja hyväksymistä koskeva suunnitelma;

f) tarvittaessa todistus ja muut hyväksymisasiakirjat.

25. TIETOTEKNIIKKAJÄRJESTELMÄLLÄ (IT SYSTEM) tarkoitetaan tietojenkäsittelytoimintaan tarkoitettuja laitteita, menetelmiä ja menettelyjä sekä tarvittaessa henkilöstöä.

Huomautuksia:

1. Tässä tarkoitetaan laitteita, jotka on konfiguroitu käsittelemään tietoja järjestelmässä.

2. Tällaisen järjestelmän avulla voidaan toteuttaa hakuja, ohjausta, valvontaa, tietoliikennettä sekä tieteellisiä tai hallinnollisia sovellutuksia, mukaan lukien tekstinkäsittely.

3. Järjestelmän rajat määritellään yleensä siten, että järjestelmä on yhden ainoan tietotekniikkajärjestelmän käyttöviranomaisen (ITSOA) valvonnassa.

4. Tietotekniikkajärjestelmään voi kuulua alajärjestelmiä, joista jotkut ovat nekin tietotekniikkajärjestelmiä.

26. TIETOTEKNIIKKAJÄRJESTELMÄN TURVALLISUUSOMINAISUUUKSIIN (IT SYSTEM SECURITY FEATURES) kuuluvat kaikki laitteistoa, valmisohjelmistoa ja ohjelmistoa koskevat toiminnot, piirteet ja ominaisuudet, käyttömenettelyt, tilivelvollisuusmenettelyt, pääsyn valvonta, laitetila, etäpäätteen/työaseman sijoituspaikka, hallinnolliset puitteet, fyysiset rakenteet ja laitteet sekä henkilöstöä ja tietoliikennettä koskeva valvonta, joita tarvitaan tietotekniikkajärjestelmässä käsiteltävien turvaluokiteltujen tietojen hyväksyttävää suojaustasoa varten.

27. TIETOVERKOLLA (IT NETWORK) tarkoitetaan tietojen vaihtoa varten toisiinsa liitettyjen tietotekniikkajärjestelmien maantieteellisesti hajautettua organisaatiota, johon kuuluvat toisiinsa liitettyjen tietotekniikkajärjestelmien osat ja niiden rajapinta tieto- tai tietoliikenneverkkoihin.

Huomautuksia:

1. Tietoverkko voi käyttää yhden tai useamman tietoliikenneverkon palveluja ja se voidaan liittää toiseen verkkoon tietojenvaihtoa varten; useat tietoverkot voivat käyttää yhteisen tietoliikenneverkon palveluja.

2. Tietoverkkoa kutsutaan ”lähiverkoksi”, jos siinä liitetään useita tietokoneita toisiinsa samassa sijaintipaikassa.

28. TIETOVERKON TURVALLISUUSOMINAISUUDET käsittävät verkon muodostavien yksittäisten tietotekniikkajärjestelmien turvallisuusominaisuudet ja verkkoon sellaisenaan liittyvät lisäkomponentit ja -tekijät (esimerkiksi verkkoviestintä, turvatunnistus, merkintäjärjestelmät ja -menettelyt, pääsynvalvonta, ohjelmat ja kirjausketjut), joita tarvitaan turvaluokiteltujen tietojen hyväksyttävää suojaustasoa varten.

29. LAITETILA (IT AREA) tarkoittaa tilaa, jossa on yksi tai useampi tietokone, niiden paikalliset oheis- ja tallennusyksiköt, ohjausyksiköt sekä niille tarkoitettu verkko- ja tietoliikennelaitteisto.

Huomautus:

Tähän eivät kuulu paikat, joihin on sijoitettu etäoheislaitteet tai etäpäätteet/työasemat, vaikka ne olisikin liitetty laitetilan laitteisiin.

30. TYÖASEMAN SIJOITUSPAIKALLA tarkoitetaan paikkaa, johon on sijoitettu tietokonelaitteisto, sen paikalliset oheislaitteet tai etäpäätteet/työasemat sekä näihin liittyvä laitetilasta erillään oleva tietoliikennelaitteisto.

31. SÄHKÖHÄIRIÖILTÄ SUOJAUTUMISELLA tarkoitetaan turvatoimia, joiden tarkoituksena on suojata laitteistoa tai tietoliikenneinfrastruktuureja tahattomista elektromagneettisista päästöistä aiheutuvalta turvaluokiteltujen tietojen vaarantumiselta.

III luku

Turvallisuusvastuut

YLEISTÄ

32. Edellä 1 jakson 4 kohdassa tarkoitettu turvakomitea vastaa myös tietoturva-asioista. Turvakomitea järjestää toimintansa siten, että se voi antaa asiantuntija-apua edellä mainituissa asioissa.

33. Turvallisuudesta vastaavan kansallisen viranomaisen ja/tai neuvoston pääsihteeristön turvallisuusyksikön on ryhdyttävä välittömästi toimiin turvallisuusongelmien ilmetessä (poikkeukselliset tapahtumat, rikkomukset jne.). Kaikista ongelmista on tiedotettava neuvoston pääsihteeristön turvallisuusyksikölle.

34. Korkeana edustajana toimiva pääsihteeri tai tarvittaessa EU:n hajautetun viraston päällikkö perustaa INFOSEC-toimiston antamaan turvallisuusviranomaiselle neuvoja JÄRJESTELMIEN osaksi tarkoitettujen erityisten turvallisuusominaisuuksien täytäntöönpanemiseksi ja valvomiseksi.

TURVALLISUUSJÄRJESTELYT HYVÄKSYVÄ VIRANOMAINEN (SECURITY ACCREDITATION AUTHORITY, SAA)

35. Turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) voi olla

— kansallinen turvallisuusviranomainen,

— korkeana edustajana toimivan pääsihteerin nimeämä viranomainen,

— EU:n hajautetun viraston turvallisuusviranomainen, tai

— näiden valtuutettu/nimetty edustaja hyväksyttävästä JÄRJESTELMÄSTÄ riippuen.

36. Turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) vastaa siitä, että JÄRJESTELMÄT ovat neuvoston turvallisuuspolitiikan mukaiset. Yksi hänen tehtäviään on myöntää JÄRJESTELMÄLLE hyväksyntä käsitellä EU:n turvaluokiteltuja tietoja määrätyllä luokittelutasolla järjestelmän käyttöympäristössä. Neuvoston pääsihteeristön ja tarvittaessa EU:n hajautettujen virastojen osalta tämä turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) vastaa turvallisuudesta korkeana edustajana toimivan pääsihteerin tai hajautettujen virastojen päälliköiden puolesta.

Neuvoston pääsihteeristön turvallisuusjärjestelyt hyväksyvä viranomainen on toimivaltainen kaikkien neuvoston pääsihteeristön tiloissa käytettävien JÄRJESTELMIEN osalta. Jäsenvaltiossa käytettävät JÄRJESTELMÄT ja niiden osat kuuluvat kyseisen jäsenvaltion toimivallan piiriin. JÄRJESTELMÄN eri osien tullessa neuvoston pääsihteeristön ja muiden turvallisuusjärjestelyt hyväksyvien viranomaisten toimivallan piiriin kaikki osapuolet nimeävät yhteisen hyväksymislautakunnan, jota neuvoston pääsihteeristön turvallisuusjärjestelyt hyväksyvä viranomainen koordinoi.

TIETOTURVAVIRANOMAINEN (INFOSEC AUTHORITY)

37. Tietoturvaviranomainen vastaa tietoturvatoimiston toiminnasta. Neuvoston pääsihteeristön ja tarvittaessa EU:n hajautettujen virastojen osalta tietoturvaviranomainen

— antaa teknistä neuvontaa ja apua turvallisuusjärjestelyt hyväksyvälle viranomaiselle (SAA),

— auttaa järjestelmäkohtaisen turvavaatimusilmoituksen (SSRS) kehittämisessä,

— huolehtii järjestelmäkohtaisen turvavaatimusilmoituksen (SSRS) tarkistamisesta sen varmistamiseksi, että se on näiden turvallisuussääntöjen sekä tietoturvapolitiikkoja ja -arkkitehtuuria koskevien asiakirjojen mukainen,

— osallistuu tarvittaessa hyväksymislautakuntiin/asiantuntijaryhmiin ja antaa hyväksymistä koskevia tietoturvasuosituksia turvallisuusjärjestelyt hyväksyvälle viranomaiselle,

— antaa apua tietoturvaa koskevan koulutuksen järjestämisessä,

— antaa teknistä neuvontaa tietoturvaan liittyvien poikkeuksellisten tapahtumien tutkinnassa, ja

— vahvistaa tekniset ohjeet sen varmistamiseksi, että käytetään vain luvallisia ohjelmia.

TIETOTEKNIIKKAJÄRJESTELMÄN KÄYTTÖVIRANOMAINEN (IT SYSTEM OPERATIONAL AUTHORITY, ITSOA)

38. Tietoturvaviranomainen valtuuttaa mahdollisimman varhaisessa vaiheessa tietotekniikkajärjestelmän käyttöviranomaisen (ITSOA) vastaamaan JÄRJESTELMÄN valvonnan ja erityisten turvaominaisuuksien täytäntöönpanosta ja toiminnasta. Vastuuta laajennetaan koko JÄRJESTELMÄN elinkaaren ajan projektin suunnitteluvaiheesta järjestelmän lopulliseen toimintavalmiuteen saakka.

39. Tietojärjestelmäviranomainen vastaa kaikista osaksi koko JÄRJESTELMÄÄ tarkoitetuista turvatoimista. Tähän vastuuseen kuuluu turvallisuuden varmistavien toimintatapojen (SecOP:t) valmistelu. Tietotekniikkajärjestelmän käyttöviranomainen (ITSOA) määrittelee JÄRJESTELMÄN toimittajalta edellytettävät turvallisuusstandardit ja -käytännöt.

40. Tietotekniikkajärjestelmän käyttöviranomainen (ITSOA) voi tarvittaessa siirtää osan toimivallastaan esimerkiksi tietoturvasta vastaavalle virkamiehelle ja tietoturvasta vastaavalle paikalliselle virkamiehelle. Yksi ainoa henkilö voi vastata eri tietoturvatehtävistä.

KÄYTTÄJÄT

41. Kaikki käyttäjät vastaavat siitä, että heidän toimintansa ei haittaa heidän käyttämänsä JÄRJESTELMÄN turvallisuutta.

TIETOTURVALLISUUTTA KOSKEVA KOULUTUS

42. Tietoturvallisuudesta järjestetään eri tasoista koulutusta tarvittaessa eri henkilöstöryhmille neuvoston pääsihteeristössä, EU:n hajautetuissa virastoissa tai jäsenvaltioiden ministeriöissä.

IV luku

Muut kuin tekniset turvatoimet

HENKILÖSTÖTURVALLISUUS

43. JÄRJESTELMÄN käyttäjien luotettavuus selvitetään ja heille annetaan heidän erityisessä järjestelmässään käsiteltävien tietojen luokittelun ja sisällön mukainen valtuutus. Oikeus käyttää tiettyjä järjestelmän turvallisuuteen liittyviä laitteita tai pääsy tiettyihin järjestelmän turvallisuutta koskeviin tietoihin voi edellyttää erityistä neuvoston menettelyjen mukaista luotettavuusselvitystä.

44. Turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) määrittelee kaikki arkaluonteiset tehtävät sekä niistä huolehtivilta henkilöiltä vaadittavan luotettavuusselvityksen ja valvonnan tason.

45. JÄRJESTELMÄ määritellään ja suunnitellaan niin, että tehtävät ja vastuut voidaan jakaa käyttäjien kesken siten, etteivät järjestelmän turvallisuutta koskevat avainkohdat ole täydellisesti yhden henkilön tiedossa ja valvonnassa. Tavoitteena olisi oltava, että tarvitaan vähintään kaksi yhteistyössä toimivaa henkilöä, jotta järjestelmään tai verkkoon voidaan tehdä muutoksia tai tahallisia vahinkoja.

FYYSINEN TURVALLISUUS

46. Edellä 29 ja 30 kohdassa määritellyt laitetilat ja etäpääte-/työasematilat, joissa käsitellään tietotekniikkavälineillä CONFIDENTIEL UE- tai sitä luottamuksellisempia tietoja tai joissa voidaan päästä tällaisiin tietoihin, vahvistetaan EU:n I tai II luokan turva-alueiksi tai tarvittaessa näitä vastaaviksi kansallisiksi turva-alueiksi.

47. Sellaisia laitetiloja ja etäpääte-/työasematiloja, joissa voidaan muuttaa JÄRJESTELMÄN turvallisuutta, käyttää useampi kuin yksi toimivaltainen virkamies/muu henkilöstön jäsen.

JÄRJESTELMÄN KÄYTÖN VALVONTA

48. Tieto ja aineisto, joilla voidaan valvoa järjestelmän käyttöä, on suojattava järjestelyin, jotka ovat järjestelmässä oleviin tietoihin sovellettavan korkeimman turvaluokan ja luokkamäärittelyn mukaiset.

49. Käytön valvontaa koskeva tieto ja aineisto tuhotaan 61 ja 63 kohdan mukaisesti, kun niitä ei enää käytetä tähän tarkoitukseen.

V luku

Tekniset turvatoimet

TIETOTURVA

50. Tietojen luovuttajan velvollisuutena on oltava kaikkien tietoja sisältävien asiakirjojen yksilöiminen ja luokittelu, olivat asiakirjat sitten paperitulosteena tai atk-tallenteena. Turvaluokka on merkittävä paperitulosteen jokaisen sivun ylä- ja alareunaan. Tulosteella (sekä paperitulosteissa että atk-tallenteissa) on oltava sama turvaluokka kuin sen tuottamisessa käytettyjen tietojen korkein turvaluokka. Myös JÄRJESTELMÄN käyttötapa voi vaikuttaa kyseisen järjestelmän tulosteiden luokitteluun.

51. Organisaation ja sen tiedonomistajien on otettava huomioon yksittäisten tietojen yhdistämiskysymykset ja yhdistetyistä tiedoista mahdollisesti tehtävät johtopäätökset sekä määritettävä, onko korkeampi turvaluokka kaikkien tietojen kannalta tarkoituksenmukaista.

52. Se, että tieto voi olla tiivistettynä, siirrettävässä muodossa tai missä tahansa binäärisessä esitysmuodossa, ei anna turvallisuuden suojausta eikä näin ollen saisi vaikuttaa tietojen luokitteluun.

53. Kun tieto siirretään JÄRJESTELMÄSTÄ toiseen, se on suojattava siirron aikana ja vastaanottavassa JÄRJESTELMÄSSÄ tiedon alkuperäisen turvaluokituksen ja luokan edellyttämällä tavalla.

54. Kaikkia tietovälineitä on käsiteltävä tallennetun tiedon korkeimman luokituksen tai välineen tunnisteen mukaisesti, ja ne on aina suojattava asianmukaisella tavalla.

55. EU:n turvaluokiteltujen tietojen rekisteröimiseen käytetyn tietovälineen, jota voidaan käyttää uudelleen, on säilytettävä korkein luokitus, joka sen sisältämällä tiedolla on koskaan ollut, kunnes kyseisten tietojen luokitus on asianmukaisesti alennettu tai poistettu ja väline tämän mukaisesti luokiteltu uudelleen tai kunnes välineen luokitus on poistettu tai väline on tuhottu hyväksytyllä neuvoston pääsihteeristön tai kansallisella menettelyllä (ks. 61—63 kohta).

TIETOJEN VALVONTA JA TILIVELVOLLISUUS TIEDOISTA

56. SECRET UE -turvaluokan ja sitä korkeampiin tietoihin pääsystä on pidettävä kirjaa automaattisten (kirjausketjujen) tai manuaalisten lokitiedostojen avulla. Tietojen säilyttämisessä on noudatettava näitä turvallisuussääntöjä.

57. Laitetilassa säilytettäviä EU:n turvaluokiteltuja tulosteita voidaan käsitellä yhtenä luokiteltuna tietona eikä niitä tarvitse rekisteröidä, jos tuloste on tunnistettu, merkitty luokituksella ja sitä valvotaan asianmukaisella tavalla.

58. Jos tuloste on peräisin EU:n turvaluokiteltuja tietoja käsittelevästä JÄRJESTELMÄSTÄ ja siirretty laitetilasta työaseman sijoituspaikkaan, on työasemalla tuotetun tulosteen valvontaa varten otettava käyttöön menettelyjä, jotka turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) on hyväksynyt. Jos kyseessä on vähintään SECRET UE -turvaluokan luokiteltu aineisto, on menettelyjä käyttöön otettaessa annettava erityisohjeistusta tietoihin liittyvästä tilivelvollisuudesta.

SIIRRETTÄVIEN TIETOVÄLINEIDEN KÄSITTELY JA VALVONTA

59. CONFIDENTIEL UE -turvaluokan ja sitä korkeammalle luokiteltuja tietovälineitä käsitellään kuten aineistoa, ja yleisiä sääntöjä noudatetaan. Tunnistus- ja luokitusmerkinnät on mukautettava välineen fyysisiin ominaisuuksiin, jotta väline olisi selvästi tunnistettavissa.

60. Käyttäjien on vastattava siitä, että EU:n turvaluokitellut tiedot tallennetaan tietovälineille, joilla on asianmukainen luokitusmerkintä ja suojaus. Sen varmistamiseksi, että EU:n tiedot tallennetaan luokituksesta riippumatta tietovälineille näiden turvallisuussääntöjen mukaisesti, on otettava käyttöön menettelyjä.

TIETOVÄLINEIDEN LUOKITUKSEN POISTAMINEN JA NIIDEN TUHOAMINEN

61. EU:n turvaluokiteltujen tietojen tallentamiseen käytettyjen tietovälineiden luokka voidaan alentaa tai poistaa, jos sovelletaan hyväksyttyjä neuvoston pääsihteeristön tai kansallisia menettelyjä.

62. TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoja tai erityisluokan tietoja sisältäneiden tietovälineiden luokitusta ei saa poistaa eikä niitä saa käyttää uudelleen.

63. Jos tietovälineen luokitusta ei voida poistaa tai sitä ei voida käyttää uudelleen, se on tuhottava hyväksytyllä neuvoston pääsihteeristön tai kansallisella menettelyllä.

TIETOLIIKENNETURVALLISUUS

64. Kun EU:n turvaluokiteltuja tietoja siirretään sähkömagneettisesti, on toteutettava erityistoimenpiteitä siirtojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi. Turvallisuusjärjestelmät hyväksyvän viranomaisen (SAA) on asetettava vaatimukset siirtojen suojaamiseksi jäljittämiseltä ja salakuuntelulta. Jossakin tietoliikennejärjestelmässä siirrettävät tiedot on suojattava luottamuksellisuuden, eheyden ja käytettävyyden edellyttämien vaatimusten pohjalta.

65. Kun luottamuksellisuuden, eheyden ja käytettävyyden suojaus edellyttää salausmenetelmiä, turvallisuusjärjestelmät hyväksyvän viranomaisen (SAA) on hyväksyttävä nämä menetelmät tai niissä käytettävät tuotteet nimenomaan tätä tarkoitusta varten.

66. SECRET UE -turvaluokan tai sitä korkeamman luokan tiedon luottamuksellisuus on siirron aikana suojattava salausmenetelmillä tai tuotteilla, jotka neuvosto on hyväksynyt turvakomiteansa suosituksesta. CONFIDENTIEL UE- tai RESTREINT-luokan tiedon luottamuksellisuus on siirron aikana suojattava salausmenetelmillä tai tuotteilla, jotka on hyväksynyt neuvoston korkeana edustajana toimiva pääsihteeri neuvoston turvakomitean suosituksesta tai jokin jäsenvaltio.

67. EU:n turvaluokiteltujen tietojen siirtoa koskevat yksityiskohtaiset säännöt annetaan erityisessä turvallisuusohjeessa, jonka neuvosto on hyväksynyt turvakomiteansa suosituksesta.

68. Poikkeusoloissa EU:n turvaluokituksen mukaan merkinnällä RESTREINT UE-, CONFIDENTIEL UE- tai SECRET UE -turvaluokkien tietoja voidaan siirtää selkotekstinä edellyttäen, että kussakin tapauksessa tähän annetaan nimenomainen lupa. Tällaisia poikkeusoloja ovat seuraavat:

a) uhkaava tai todellinen kriisitilanne, konflikti tai sotatilanne;

b) kun tietojen nopea toimittaminen on ensiarvoisen tärkeää, eikä salakirjoitusvälineitä ole saatavilla ja katsotaan, että jos siirrettäviä tietoja ei voida käyttää ajoissa, se vaikuttaa toimintaan haitallisesti.

69. JÄRJESTELMÄN on ehdottomasti pystyttävä tarvittaessa estämään pääsy EU:n turvaluokiteltuihin tietoihin joltakin työasemalta tai kaikista alijärjestelmistä joko kytkemällä ne fyysisesti irti tai sellaisten ohjelman erityisominaisuuksien avulla, jotka turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) on hyväksynyt.

TURVALLISUUS ASENNUKSEN YHTEYDESSÄ JA SÄTEILYTURVALLISUUS

70. JÄRJESTELMIEN ensimmäisestä asennuksesta ja niihin tehtävistä huomattavista muutoksista on tehtävä sopimus, jonka mukaan asennuksen suorittavat asentajat, joista on tehty luotettavuusselvitys. Toimintaa valvovat jatkuvasti tehtävään erikoistuneet työntekijät, joilla luotettavuusselvityksen perusteella on pääsy EU:n turvaluokiteltuihin tietoihin tasolla, joka vastaa sitä korkeinta luokkaa, jolla varustettuja tietoja JÄRJESTELMÄN on määrä tallentaa ja käsitellä.

71. Kaikki laitteet asennetaan noudattaen neuvoston harjoitettavaa turvallisuutta koskevaa toimintapolitiikkaa.

72. JÄRJESTELMÄT, jotka käsittelevät CONFIDENTIEL UE- tai sitä korkeamman turvaluokan tietoja, on suojattava siten, että haitallinen säteily, jonka tutkimuksesta ja hallinnasta käytetään nimitystä TEMPEST, ei voi uhata niiden turvallisuutta.

73. Neuvoston pääsihteeristön turvallisuusviranomaisen nimeämän TEMPEST-viranomaisen on tarkastettava ja hyväksyttävä toimenpiteet, joilla neuvoston pääsihteeristön ja EU:n hajautettuihin erillisvirastoihin asennetut laitteet suojataan sähköhäiriöiltä. EU:n turvaluokiteltuja tietoja käsittelevät kansalliset laitteistot hyväksyy tunnustettu kansallinen TEMPEST-hyväksyntäviranomainen.

VI luku

Turvallisuus käsittelyn aikana

TURVALLISUUDEN VARMISTAVAT TOIMINTATAVAT

74. Turvallisuuden varmistavissa toimintatavoissa (SecOP) määritellään turvallisuuskysymyksissä noudatettavat periaatteet, toimintatavat ja työntekijöiden vastuu. Turvallisuuden varmistavat toimintatavat on laadittava ITSOA:n vastuulla.

OHJELMISTOJEN SUOJAUS / ASETUSTEN HALLINTA

75. Sovellusohjelmien turvallisuuden suojaus on määritettävä sen perusteella, millaiseksi ohjelman turvaluokittelu on arvioitu eikä niinkään sen perusteella, millaiseksi ohjelman käsittelemien tietojen luokittelu on arvioitu. Käytössä olevat ohjelmaversiot olisi tarkistettava säännöllisesti niiden eheyden ja moitteettoman toiminnan varmistamiseksi.

76. Uusia tai muutettuja ohjelmaversioita ei pitäisi käyttää EU:n turvaluokiteltujen tietojen käsittelyssä ennen kuin ITSOA on tarkistanut ne.

TUHOISTEN OHJELMISTO- TAI TIETOKONEVIRUSTEN TARKISTAMINEN

77. Mahdolliset tuhoisat ohjelmisto- tai tietokonevirukset on tarkistettava määräajoin SAA:n vaatimusten mukaisesti.

78. Kaikki neuvoston pääsihteeristöön, EU:n erillisvirastoihin tai jäsenvaltioihin tulevat tietovälineet olisi tarkistettava tuhoisien ohjelmisto- tai tietokonevirusten varalta ennen niiden käyttämistä JÄRJESTELMÄSSÄ.

HUOLTO

79. Sellaisten JÄRJESTELMIEN säännöllistä tai tarvittaessa tapahtuvaa huoltoa koskevissa sopimuksissa ja menettelyissä, joista on tehty järjestelmäkohtainen turvavaatimusilmoitus (SSRS), on mainittava laitetilassa käyvää huoltohenkilöstöä ja sen varusteita koskevat vaatimukset ja järjestelyt.

80. Vaatimukset on mainittava selvästi järjestelmäkohtaisessa turvavaatimusilmoituksessa, ja menettelyt on mainittava selvästi turvallisuuden varmistavissa toimintatavoissa (SecOP). Etäyhteydellä tapahtuvaa vian määritystä vaativa sopimushuolto sallitaan vain poikkeustilanteissa tiukassa turvallisuusvalvonnassa ja ainoastaan SAA:n suostumuksella.

VII luku

Hankinnat

81. Hankittavassa JÄRJESTELMÄSSÄ käytettävien turvatuotteiden on joko oltava arvioituja ja varmennettuja tai niiden on oltava parhaillaan arviointi- tai varmennelaitoksen arvioitavana ja varmennettavana noudattaen kansainvälisesti tunnustettuja kriteerejä (esim. yleiset tietoturvallisuuden arviointiperusteet, ISO 15408).

82. Päätettäessä siitä, kannattaako välineitä, etenkin tietovälineitä, vuokrata vai ostaa, olisi muistettava, että EU:n turvaluokiteltujen tietojen käsittelemiseen käytettyjä välineitä ei voida päästää asianmukaisella tavalla turvallisen ympäristön ulkopuolelle ennen kuin niiden luokitus on poistettu turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) suostumuksella ja että suostumusta ei aina voi saada.

HYVÄKSYMINEN

83. Turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) on hyväksyttävä kaikki JÄRJESTELMÄT, joista on annettava järjestelmäkohtainen turvavaatimusilmoitus (SSRS) ennen EU:n turvaluokiteltujen tietojen käsittelyä, SSRS:n, turvallisuuden varmistavien toimintatapojen (SecOP:t) ja kaikkien muiden asiaa koskevien asiakirjojen sisältämien tietojen perusteella. Alijärjestelmät ja työaseman sijoituspaikat on hyväksyttävä osana kaikkia JÄRJESTELMIÄ, joihin ne ovat yhteydessä. Jos JÄRJESTELMÄÄ käytetään sekä neuvostossa että muissa organisaatioissa, neuvoston pääsihteeristön ja asiasta vastaavien turvallisuusviranomaisten on yhdessä sovittava hyväksymisestä.

84. Hyväksymisprosessissa voidaan edetä yksittäiseen JÄRJESTELMÄÄN soveltuvan ja turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) määrittelemän hyväksymisstrategian mukaisesti.

ARVIOINTI JA VARMENTAMINEN

85. JÄRJESTELMÄN laitteistojen, kiinteiden ohjelmistojen ja ohjelmien turvallisuusominaisuudet on arvioitava ja varmennettava sellaisiksi, että ne pystyvät suojaamaan tietoa aiotulla luokitustasolla.

86. Arviointi- ja varmennusvaatimukset on esitettävä järjestelmäsuunnitelmassa ja selvästi mainittava järjestelmäkohtaisessa turvavaatimusilmoituksessa (SSRS).

87. Teknisesti pätevän henkilöstön, josta on asianmukaisesti tehty luotettavuusselvitys ja joka toimii tietotekniikkajärjestelmän käyttöviranomaisen (ITSOA) nimissä, on suoritettava arviointi ja varmentaminen hyväksyttyjen ohjeiden mukaisesti.

88. Työtiimit voidaan muodostaa jonkin jäsenvaltion nimetystä arviointi- tai varmenneviranomaisesta tai tämän nimetyistä edustajista, esimerkiksi pätevästä tavarantoimittajasta, josta on tehty luotettavuusselvitys.

89. Arviointi- ja varmennusastetta voidaan vähentää (esim. vain integrointi), jos JÄRJESTELMISSÄ käytetään olemassa olevia kansallisesti arvioituja ja varmennettuja tietoturvatuotteita.

TURVALLISUUSOMINAISUUKSIEN RUTIINITARKASTUKSET PYSYVÄÄ HYVÄKSYMISTÄ VARTEN

90. Tietotekniikkajärjestelmän käyttöviranomaisen (ITSOA) on otettava käyttöön rutiinitarkastukset, joilla on varmistettava, että kaikki JÄRJESTELMÄN turvallisuusominaisuudet pätevät edelleen.

91. Muutokset, joiden perusteella hyväksyminen olisi suoritettava uudelleen tai jotka edellyttäisivät turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) edeltävää suostumusta, on selkeästi yksilöitävä ja mainittava järjestelmäkohtaisessa turvavaatimusilmoituksessa (SSRS). Jos JÄRJESTELMÄSSÄ tapahtuu muutoksia, sitä korjataan tai siinä esiintyy häiriöitä, tietotekniikkajärjestelmän käyttöviranomaisen (ITSOA) on huolehdittava siitä, että se tarkastetaan turvallisuusominaisuuksien moitteettoman toiminnan varmistamiseksi. JÄRJESTELMÄN jatkuva hyväksyminen riippuu tavallisesti siitä, että tarkastukset on tyydyttävästi tehty.

92. Turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) on tarkastettava määräajoin kaikki JÄRJESTELMÄT, joihin on liitetty turvallisuusominaisuuksia. JÄRJESTELMÄT, jotka käsittelevät TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoja tai tietoja, joissa on lisämerkintöjä, on tarkastettava vähintään kerran vuodessa.

VIII luku

Tilapäinen tai satunnainen käyttö

MIKROTIETOKONEIDEN TAI HENKILÖKOHTAISTEN TIETOKONEIDEN SUOJAUS

93. Mikrotietokoneiden tai henkilökohtaisten tietokoneiden (PC:t), joissa on kiintolevy (tai muu katkeamaton muistiväline) ja jotka toimivat erillisinä tai verkotetussa kokoonpanossa, sekä kannettavien atk-laitteiden (esimerkiksi kannettavat PC:t ja sähköiset muistikirjamikrot), joissa on kovalevy, katsotaan olevan levykkeitä tai muita siirrettäviä atk-tallennevälineitä vastaavia tietovälineitä.

94. Kyseisten laitteiden käyttö, käsittely, varastointi ja kuljettaminen on suojattava tavalla, joka vastaa niillä tallennettavan tai käsiteltävän tiedon korkeinta luokitusta (ennen luokituksen laskemista tai poistamista hyväksyttyjen menettelyjen mukaisesti).

YKSITYISEN ATK-LAITTEISTON KÄYTTÖ NEUVOSTON TYÖSKENTELYSSÄ

95. Yksityisten siirrettävien atk-tallennevälineiden, ohjelmistojen ja atk-laitteiston (esimerkiksi PC:t ja kannettavat atk-laitteet), joissa on tallennusmahdollisuus, käyttö EU:n luokiteltujen tietojen käsittelemiseen on kielletty.

96. Yksityisiä laitteita, ohjelmistoja ja tiedotusvälineitä ei saa tuoda niille I tai II luokan alueille, joilla käsitellään EU:n luokiteltuja tietoja, ilman neuvoston pääsihteeristön turvallisuusyksikön päällikön tai jonkin jäsenvaltion ministeriön tai vastaavan EU:n hajautetun viraston johtajan lupaa.

SOPIMUSPUOLTEN TAI JÄSENVALTIOIDEN TOIMITTAMIEN ATK-LAITTEIDEN KÄYTTÖ NEUVOSTON VIRALLISESSA TYÖSKENTELYSSÄ

97. Neuvoston pääsihteeristön turvallisuusyksikön päällikkö, jäsenvaltion ministeriön tai vastaavan EU:n hajautetun viraston johtaja voi antaa luvan käyttää sopimuspuolten omistamia atk-laitteita. Neuvoston pääsihteeristön tai EU:n hajautetun viraston henkilöstö voi myös saada luvan käyttää jäsenvaltioiden toimittamia atk-laitteita ja ohjelmistoja; tällöin atk-laitteet on saatettava asianmukaisesti neuvoston pääsihteeristön valvontaan. Jos atk-laitteita on määrä käyttää EU:n luokiteltujen tietojen käsittelyssä, on molemmissa tapauksissa kuultava asiaankuuluvaa turvallisuusjärjestelyt hyväksyvää viranomaista (SAA) sen varmistamiseksi, että kyseisten laitteiden INFOSEC-tekijät otetaan asianmukaisesti huomioon ja että niitä sovelletaan asianmukaisella tavalla.

XII JAKSO

EU:N LUOKITELTUJEN TIETOJEN LUOVUTTAMINEN KOLMANSILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE

EU:N LUOKITELTUJEN TIETOJEN LUOVUTTAMISTA KOSKEVAT PERIAATTEET

1. Neuvosto päättää EU:n luokiteltujen tietojen luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille seuraavin perustein:

   — kyseisten tietojen laatu ja sisältö,

   — vastaanottajan tehtävien mukainen valtuutus,

   — EU:lle koituvien etujen arviointi.

   EU:n luokiteltuja tietoja luovuttaneelta jäsenvaltiolta pyydetään suostumus tietojen edelleen luovuttamiseen.

2. Päätökset tehdään tapauskohtaisesti seuraavin perustein:

   — taso, jolla yhteistyötä halutaan tehdä asianomaisten kolmansien valtioiden ja kansainvälisten järjestöjen kanssa,

   — kyseisten valtioiden ja järjestöjen luotettavuus — luotettavuutta arvioidaan kyseisille valtioille tai järjestöille luovutettaviin EU:n luokiteltuihin tietoihin sovellettavan turvallisuuden tason ja kyseisissä valtioissa ja järjestöissä sekä EU:ssa sovellettavien turvamääräysten johdonmukaisuuden perusteella; neuvoston turvakomitea antaa neuvostolle asiasta teknisen lausuntonsa.

3. Hyväksyessään EU:n luokitellut tiedot kolmannet valtiot tai kansainväliset järjestöt takaavat sen, että tietoja ei käytetä muuhun kuin tietojen luovuttamisen tai vaihtamisen perusteena olevaan tarkoitukseen ja että ne suojelevat kyseisiä tietoja neuvoston edellyttämällä tavalla.

TASOT

4. Neuvoston päätettyä, että luokiteltuja tietoja voidaan luovuttaa jollekin valtiolle tai kansainväliselle järjestölle tai että niitä voidaan vaihtaa jonkin valtion tai kansainvälisen järjestön kanssa, se tekee päätöksen tasosta, jolla yhteistyötä voidaan tehdä. Yhteistyön taso riippuu erityisesti kyseisessä valtiossa tai järjestössä sovellettavasta turvallisuuspolitiikasta ja turvamääräyksistä.

5. Yhteistyö on kolmitasoista:

   1 taso

   Yhteistyö sellaisten kolmansien valtioiden tai kansainvälisten järjestöjen kanssa, joiden turvallisuuspolitiikka ja turvamääräykset ovat hyvin lähellä EU:n turvallisuuspolitiikkaa ja turvamääräyksiä.

   2 taso

   Yhteistyö sellaisten kolmansien valtioiden tai kansainvälisten järjestöjen kanssa, joiden turvallisuuspolitiikka ja turvamääräykset poikkeavat huomattavasti EU:n turvallisuuspolitiikasta ja turvamääräyksistä.

   3 taso

   Satunnainen yhteistyö sellaisten kolmansien valtioiden tai kansainvälisten järjestöjen kanssa, joiden turvallisuuspolitiikkaa ja turvamääräyksiä ei voida arvioida.

6. Turvamääräykset, joita muokataan tapauskohtaisesti uudelleen neuvoston turvakomitean antaman teknisen lausunnon perusteella ja joita tietojen vastaanottajia pyydetään soveltamaan niille luovutettavien luokiteltujen tietojen suojelemiseksi, määräytyvät kyseessä olevan yhteistyön tason mukaisesti. Kyseiset menettelyt ja turvamääräykset esitetään yksityiskohtaisesti lisäyksissä 4, 5 ja 6.

SOPIMUKSET

7. Neuvoston tehtyä päätöksen, jonka mukaan luokiteltujen tietojen vaihtoon EU:n ja kolmansien valtioiden tai kansainvälisten järjestöjen välillä on pysyvä tai pitkäaikainen tarve, se laatii kyseisten valtioiden tai järjestöjen kanssa sopimuksia luokiteltujen tietojen vaihtoa koskevista turvamenettelyistä, joissa määritellään yhteistyön tarkoitus ja kyseisten tietojen suojelua koskevat vastavuoroiset määräykset.

8. Luokiteltujen tietojen vaihtoa koskevista turvamenettelyistä tehtävä sopimus voidaan satunnaisen 3 tasolla tehtävän yhteistyön osalta, joka on kestoltaan ja tarkoitukseltaan rajallista, korvata yksinkertaisella yhteisymmärryspöytäkirjalla, jossa määritellään niiden luokiteltujen tietojen laatu, joita on määrä vaihtaa, sekä kyseisiä tietoja koskevat vastavuoroiset velvoitteet edellyttäen, että kyseisten tietojen luokittelu ole RESTREINT UE -luokkaa korkeampi.

9. Turvakomitea hyväksyy ehdotukset turvamenettelyistä tehtäviksi sopimuksiksi tai yhteisymmärryspöytäkirjoiksi ennen niiden antamista neuvoston päätettäviksi.

10. Kansallisten turvallisuusviranomaisten on annettava korkeana edustajana toimivalle pääsihteerille kaikki tarvittava apu sen varmistamiseksi, että luovutettavia tietoja käytetään ja suojellaan turvamenettelyistä tehtyjen sopimusten tai yhteisymmärryspöytäkirjojen määräysten mukaisesti.

Lisäys 1

Kansalliset turvallisuusviranomaiset

BELGIA

Ministère des Affaires Etrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité — A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
P. 32-2-501 85 14
F. 32-2-501 80 58
Teleksi: 21376
Sähkeosoite: Direction de Sécurité A01 — MINAFET

TANSKA

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
P. 45-33 14 88 88
F. 45-38 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø.
P. 45-33 32 55 66
F. 45-33 93 13 20

SAKSA

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
P. 49-30-39 81 15 28
F. 49-30-39 81 16 10

KREIKKA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ - Β' Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020-Χολαργός (Αθήνα)
Ελλαδα
Τηλέφωνα: 00 30-1-655 22 03 (ώρες γραφείου)
00 30-1-655 22 05 (εικοσιτετάωρο)
Φαξ: 00 30-1-642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR. / SEC.)
STG 1020, Holargos — Athens
Greece
P. 00 30-1-655 22 03 (toimistoaikana)
00 30-1-655 22 05 (24 tuntia)
F. 00 30-1-642 69 40

ESPANJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E-28023 Madrid
P. 34-91-372 57 07
F. 34-91-372 58 08
Sähköposti: nsa-sp@areatec.com

RANSKA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
P. 33-0-144 18 81 80
F. 33-0-144 18 82 00
Teleksi: SEGEDEFNAT 200019
Sähkeosoite: SEGEDEFNAT PARIS

IRLANTI

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
P. 353-1-478 08 22
F. 353-1-478 14 84

ITALIA

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
P. 39-06-627 47 75
F. 39-06-614 33 97
Teleksi: 623876 AQUILA 1
Sähkeosoite: ess: PCM-ANS-UCSI-ROMA

LUXEMBURG

Autorité Nationale de Sécurité
Ministère d'Etat
Boîte Postale 2379
L-1023 Luxembourg
P. 352-478 22 10 keskus
352-478 22 35 suora
F. 352-478 22 43
352-478 22 71
Teleksi: 3481 SERET LU
Sähkeosoite: MIN D'ETAT — ANS

ALANKOMAAT

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
P. 31-70-320 44 00
F. 31-70-320 07 33
Teleksi: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-2500 ES Den Haag
P. 31-70-318 70 60
F. 31-70-318 79 51

ITÄVALTA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
P. 43-1-531 15 34 64
F. 43-1-531 8 52 19

PORTUGALI

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
P. 351-21-301 55 10
351-21-301 00 01, alanumero 20 45 37
F. 351-21-302 03 50

SUOMI

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
P. 358-9-13 41 53 38
F. 358-9-13 41 53 03

RUOTSI

Utrikesdepartementet
SSSB
S-103 39 Stockholm
P. 46-8-405 54 44
F. 46-8-723 11 76

YHDISTYNYT KUNINGASKUNTA

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1 AH
P. 44-20-72 70 87 51
F. 44-20-76 30 14 28
Sähkeosoite: UK Delegation to Security Policy Dept FCO, marked (in Box 5656 for DIR/5).

Lisäys 2

Kansallisten turvallisuusluokitusten vertailu

EU:n luokitus	Très secret UE/EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
Naton luokitus ([1])				
WEU:n luokitus	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Saksa	STRENG GEHEIM	GEHEIM	VS ([2]) - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Itävalta	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgia	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Tanska	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Espanja	Secreto	Reservado	Confidencial	Difusion Limitada
Suomi	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Ranska	Très Secret Défense ([3])	Secret Défense	Confidentiel Défense	Diffusion restreinte
Kreikka	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Irlanti	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Alankomaat	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Portugali	Muito Secreto	Secreto	Confidencial	Reservado
Yhdistynyt kuningaskunta	Top Secret	Secret	Confidential	Restricted
Ruotsi	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

([1]) Nato: vastaavuus Naton luokitustasojen kanssa vahvistetaan Euroopan unionin ja Naton välistä turvallisuussopimusta koskevien neuvottelujen yhteydessä.
([2]) Saksa: VS = Verschlusssache.
([3]) Ranska: Hallituksen prioriteetteja koskeva "Très Secret Défense" -luokitus voidaan muuttaa ainoastaan pääministerin luvalla.

Lisäys 3

Luokitteluohjeet

Tämä ohje on suuntaa antava eikä sitä saa tulkita niin, että se muuttaa jaksoissa II ja III annettuja sisältöä koskevia määräyksiä.

Luokitus	Milloin	Kuka	Merkinnät	Siirto alempaan turvaluokkaan/julkistaminen/hävittäminen	
				Kuka	Milloin
TRÈS SECRET UE/ EU TOP SECRET: Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo voisi poikkeuksellisen vakavasti vaarantaa Euroopan unionin tai yhden tai useamman jäsenvaltion olennaista etua [II jakson 1 kohta].	Kun TRÈS SECRET UE/EU TOP SECRET -aineiston julkistaminen todennäköisesti — uhkaisi suoraan EU:n, jäsenvaltion tai ystävällismielisen maan sisäistä vakautta — vahingoittaisi poikkeuksellisen vakavasti suhteita ystävällismielisiin hallituksiin — aiheuttaisi suoraan laajamittaisen ihmishenkien menetyksen — vahingoittaisi poikkeuksellisen vakavasti jäsenvaltioiden tai muiden avunantajien joukkojen operatiivista tehokkuutta tai turvallisuutta tai äärettömän arvokkaiden turvallisuus- tai tiedusteluoperaatioiden jatkuvaa tehokkuutta — vahingoittaisi pitkällä aikavälillä EU:n tai jäsenvaltion taloutta.	Jäsenvaltiot: asianmukaisesti valtuutetut henkilöt (tietojen luovuttajat) [III jakson 4 kohta]; neuvoston pääsihteeristö: asianmukaisesti valtuutetut henkilöt (tietojen luovuttajat) [III jakson 4 kohta], korkeana edustajana toimiva pääsihteeri ja varapääsihteeri. Tietojen luovuttajat ilmoittavat päivämäärän tai ajanjakson, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai julkistaa. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [III jakson 10 kohta].	TRÈS SECRET UE/EU TOP SECRET -luokitusta sovelletaan TRES SECRET UE/EU TOP SECRET -asiakirjoihin, ja soveltuvilta osin lisätään puolustusasioihin viittaava merkintä ESDP mekaanisesti ja käsin [II jakson 8 kohta]. EU:n luokitus ilmoitetaan kaikkien sivujen ylä- ja alareunassa keskellä ja kaikki sivut numeroidaan. Kaikissa asiakirjoissa on viitenumero ja päivämäärä; viitenumero ilmoitetaan kaikilla sivuilla. Jos asiakirjasta jaetaan useita kappaleita, jokaisessa on kappalenumero, joka merkitään ensimmäiselle sivulle kokonaissivumäärän kanssa. Kaikki liitteet ja lisäykset luetellaan ensimmäisellä sivulla [VII jakson 1 kohta].	Julkistamisesta tai siirrosta alempaan turvaluokkaan voi päättää ainoastaan tietojen luovuttaja tai YUTP:n korkeana edustajana toimiva pääsihteeri, joka ilmoittaa muutoksesta kaikille myöhemmille vastaanottajille, joille asiakirja on lähetetty tai kopioitu [VIII jakson 9 kohta]. TRÈS SECRET UE/EU TOP SECRET -asiakirjojen hävittäminen tapahtuu niistä vastaavan keskusrekisterin tai alarekisterin toimesta. Kaikki hävitetyt asiakirjat kirjataan hävittämistodistukseen, jonka allekirjoittaa TRÈS SECRET UE/EU TOP SECRET -valvontavirkamies ja hävittämisen todistajana toimiva virkamies, jolla on oikeus käsitellä TRÈS SECRET UE/EU TOP SECRET -asiakirjoja. Päiväkirjaan tehdään asiaa koskeva merkintä. Rekisteri säilyttää hävittämistodistukset ja jakeluluettelot kymmenen vuotta [VII jakson 31 kohta].	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [VII jakson 31 kohta]. TRÈS SECRET UE/EU TOP SECRET -asiakirjat, mukaan lukien kaikki TRÈS SECRET UE/EU TOP SECRET -asiakirjojen laatimisesta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja hiilipaperi, hävitetään TRÈS SECRET UE/EU TOP SECRET virkamiehen valvonnassa polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei sitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa [VII jakson 31 kohta].

Luokitus	Milloin	Kuka	Merkinnät	Siirto alempaan turvaluokkaan/julkistaminen/hävittäminen	
				Kuka	Milloin
SECRET UE: Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo voisi vakavasti vahingoittaa Euroopan unionin tai yhden tai useamman jäsenvaltion olennaista etua [II jakson 2 kohta].	Kun SECRET UE -aineiston julkistaminen todennäköisesti — aiheuttaisi kansainvälisiä jännitteitä — vahingoittaisi vakavasti suhteita ystävällismielisiin hallituksiin — uhkaisi ihmishenkiä suoraan tai vaarantaisi vakavasti yleisen järjestyksen tai yksilön turvallisuuden tai vapauden — vahingoittaisi vakavasti jäsenvaltioiden tai muiden avunantajien joukkojen operatiivista tehokkuutta tai turvallisuutta tai erittäin arvokkaiden turvallisuus- tai tiedusteluoperaatioiden jatkuvaa tehokkuutta — aiheuttaisi huomattavaa aineellista vahinkoa EU:n tai jäsenvaltion rahoitukseen, rahaan, talouteen tai kauppaan liittyville eduille.	Jäsenvaltiot: valtuutetut henkilöt (tietojen luovuttajat) [III jakson 2 kohta]; neuvoston pääsihteeristö ja EU:n hajautetut erillisvirastot: valtuutetut henkilöt (tietojen luovuttajat) [III jakson 2 kohta], pääjohtajat, korkeana edustajana toimiva pääsihteeri ja varapääsihteeri. Tietojen luovuttajat ilmoittavat päivämäärän tai ajanjakson, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai julkistaa. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [III jakson 10 kohta].	SECRET UE -luokitusta sovelletaan SECRET UE -asiakirjoihin, ja soveltuvilta osin lisätään puolustusasioihin viittaava merkintä ESDP mekaanisesti ja käsin [II jakson 8 kohta]. EU:n luokitus ilmoitetaan kaikkien sivujen ylä- ja alareunassa keskellä ja kaikki sivut numeroidaan. Kaikissa asiakirjoissa on viitenumero ja päivämäärä; viitenumero ilmoitetaan kaikilla sivuilla. Jos asiakirjasta jaetaan useita kopioita, jokaisessa on kopionumero, joka merkitään ensimmäiselle sivulle kokonaissivumäärän kanssa. Kaikki liitteet ja lisäykset luetellaan ensimmäisellä sivulla [VII jakson 1 kohta].	Julkistamisesta tai siirrosta alempaan turvaluokkaan voi päättää ainoastaan tietojen luovuttaja tai YUTP:n korkeana edustajana toimiva pääsihteeri, joka ilmoittaa muutoksesta kaikille myöhemmille vastaanottajille, joille asiakirja on lähetetty tai kopioitu [III jakson 9 kohta]. SECRET UE -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun virkamiehen valvonnassa. Hävitetyt SECRET UE -asiakirjat kirjataan allekirjoitettaviin hävittämistodistuksiin, jotka rekisteri säilyttää hävittämislomakkeiden kanssa vähintään kolme vuotta [VII jakson 32 kohta].	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [VII jakson 31 kohta]. SECRET UE -asiakirjat, mukaan lukien kaikki SECRET UE -asiakirjojen laatimisesta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja hiilipaperi, hävitetään polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei sitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa [VII jakson 31 ja 32 kohta].

Luokitus	Milloin	Kuka	Merkinnät	Siirto alempaan turvaluokkaan/julkistaminen/hävittäminen	
				Kuka	Milloin
CONFIDENTIEL UE: Tätä luokitusta sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton paljastaminen vahingoittaisi Euroopan unionin tai yhden tai useamman jäsenvaltion olennaista etua [II jakson 3 kohta].	Kun CONFIDENTIEL UE -aineiston julkistaminen todennäköisesti — vahingoittaisi aineellisesti diplomaattisuhteita eli aiheuttaisi muodollisen protestin tai muita pakotteita — vaarantaisi yksilön turvallisuuden tai vapauden — vahingoittaisi jäsenvaltioiden tai muiden avunantajien joukkojen operatiivista tehokkuutta tai turvallisuutta tai arvokkaiden turvallisuus tai tiedusteluoperaatioiden tehokkuutta — heikentäisi merkittävästi tärkeiden järjestöjen taloudellista elinkelpoisuutta — haittaisi vakavien rikosten tutkimista tai helpottaisi niiden tekemistä — vahingoittaisi EU:n tai jäsenvaltion rahoitukseen, rahaan, talouteen tai kauppaan liittyviä etuja — haittaisi vakavasti tärkeiden EU:n politiikkojen kehittämistä tai toteuttamista — estäisi tai muuten merkittävästi keskeyttäisi merkittäviä EU:n toimia.	Jäsenvaltiot: valtuutetut henkilöt (tietojen luovuttajat) [III jakson 2 kohta]; neuvoston pääsihteeristö ja EU:n hajautetut erillisvirastot: valtuutetut henkilöt (tietojen luovuttajat) [III jakson 2 kohta], pääjohtajat, korkeana edustajana toimiva pääsihteeri ja varapääsihteeri. Tietojen luovuttajat ilmoittavat päivämäärän tai ajanjakson, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai julkistaa. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [III jakson 10 kohta].	CONFIDENTIEL UE -luokitusta sovelletaan CONFIDENTIEL UE -asiakirjoihin, ja soveltuvilta osin lisätään puolustusasioihin viittaava merkintä ESDP mekaanisesti ja käsin tai painamalla ennalta leimattuun, rekisteröityyn paperiin [II jakson 8 kohta]. EU:n luokitus ilmoitetaan kaikkien sivujen ylä- ja alareunassa keskellä ja kaikki sivut numeroidaan. Kaikissa asiakirjoissa on viitenumero ja päivämäärä. Kaikki liitteet ja lisäykset luetellaan ensimmäisellä sivulla [VII jakson 1 kohta].	Julkistamisesta tai siirrosta alempaan turvaluokkaan voi päättää ainoastaan tietojen luovuttaja tai YUTP:n korkeana edustajana toimiva pääsihteeri tai varapääsihteeri, joka ilmoittaa muutoksesta kaikille myöhemmille vastaan-ottajille, joille asiakirja on lähetetty tai kopioitu [III jakson 9 kohta]. CONFIDENTIEL UE -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun virkamiehen valvonnassa. Hävittäminen kirjataan kansallisten sääntöjen mukaisesti ja, jos kyseessä on neuvoston pääsihteeristö tai EU:n hajautettu erillisvirasto, korkeana edustajana toimivan pääsihteerin ohjeiden mukaisesti [VII jakson 33 kohta].	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [VII jakson 31 kohta]. CONFIDENTIEL UE -asiakirjat, mukaan lukien kaikki CONFIDENTIEL UE -asiakirjojen laatimisesta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja hiilipaperi, hävitetään polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei sitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa [VII jakson 31 ja 33 kohta].

Luokitus	Milloin	Kuka	Merkinnät	Siirto alempaan turvaluokkaan/julkistaminen/hävittäminen	
				Kuka	Milloin
RESTREINT UE: Tätä luokitusta sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton paljastaminen voisi olla Euroopan unionin tai yhden tai useamman jäsenvaltion edun vastaista [II jakson 4 kohta].	Kun RESTREINT UE -merkityn aineiston julkistaminen todennäköisesti — vaikuttaisi haitallisesti diplomaattisuhteisiin — aiheuttaisi yksilöille merkittävää hätää — vaikeuttaisi jäsenvaltioiden tai muiden avunantajien joukkojen operatiivisen tehokkuuden tai turvallisuuden ylläpitämistä — aiheuttaisi yksilöille tai yhtiöille taloudellista tappiota tai helpottaisi laittoman voiton tai edun saamista — estäisi yrityksiä säilyttämästä kolmansien osapuolten luovuttamien tietojen luottamuksellisuuden — aiheuttaisi tietojen paljastamista koskevien rajoitusten rikkomisen — haittaisi rikosten tutkimista tai helpottaisi niiden tekemistä — asettaisi EU:n tai jäsenvaltiot epäedulliseen asemaan kauppaa tai politiikkaa koskevissa neuvotteluissa — haittaisi EU:n politiikkojen tehokasta kehittämistä tai toteuttamista — haittaisi EU:n asianmukaista hallintoa ja sen toimia.	Jäsenvaltiot: valtuutetut henkilöt (tietojen luovuttajat) [III jakson 2 kohta]; neuvoston pääsihteeristö ja EU:n hajautetut erillisvirastot: valtuutetut henkilöt (tietojen luovuttajat) [III jakson 2 kohta], pääjohtajat, korkeana edustajana toimiva pääsihteeri ja varapääsihteeri. Tietojen luovuttajat ilmoittavat päivämäärän tai ajanjakson, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai julkistaa. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [III jakson 10 kohta].	RESTREINT UE -luokitusta sovelletaan RESTREINT UE -asiakirjoihin, ja soveltuvilta osin lisätään puolustusasioihin viittaava merkintä ESDP mekaanisesti tai elektronisesti [II jakson 8 kohta]. EU:n luokitus ilmoitetaan kaikkien sivujen ylä- ja alareunassa keskellä ja kaikki sivut numeroidaan. Kaikissa asiakirjoissa on viitenumero ja päivämäärä [VII jakson 1 kohta].	Julkistamisesta tai siirrosta alempaan turvaluokkaan voi päättää ainoastaan tietojen luovuttaja tai YUTP:n korkeana edustajana toimiva pääsihteeri, joka ilmoittaa muutoksesta kaikille myöhemmille vastaanottajille, joille asiakirja on lähetetty tai kopioitu [III jakson 9 kohta]. RESTREINT UE -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun virkamiehen valvonnassa. Hävittäminen kirjataan kansallisten sääntöjen mukaisesti ja, jos kyseessä on neuvoston pääsihteeristö tai EU:n hajautettu erillisvirasto, korkeana edustajana toimivan pääsihteerin ohjeiden mukaisesti [VII jakson 34 kohta].	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [VII jakson 31 kohta].

Lisäys 4

Ohjeet EU:n turvaluokitellun aineiston luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille

1 tason yhteistyö

MENETTELY

1. Vain neuvostolla on toimivalta luovuttaa EU:n turvaluokiteltua tietoa valtioille, jotka eivät ole allekirjoittaneet sopimusta Euroopan unionista tai muille kansainvälisille järjestöille, joilla on vastaava turvallisuuspolitiikka ja turvallisuusmääräykset kuin EU:lla.

2. Neuvosto voi delegoida päätöksen luovuttaa turvaluokiteltua tietoa. Neuvoston valtuutuksessa todetaan luovutettavissa olevan tiedon laatu ja sen turvaluokka-aste, joka ei tavallisesti ole CONFIDENTIEL UE -turvaluokkaa korkeampi.

3. Sillä edellytyksellä, että turvallisuussopimus hyväksytään, asianosaisten valtioiden tai kansainvälisten järjestöjen turvallisuudesta vastaavat elimet osoittavat korkeana edustajana toimivalle pääsihteerille EU:n turvaluokitellun tiedon luovuttamista koskevat pyynnöt, joissa on mainittava luovutuksen tarkoitus ja luovutettavan turvaluokitellun tiedon laatu.

   Myös jäsenvaltio tai EU:n hajautettu erillisvirasto, joka katsoo EU:n turvaluokitellun tiedon luovuttamisen olevan suotavaa, voi esittää pyynnön; sen on mainittava tällaisen pyynnön tavoitteet ja EU:lle koituva hyöty sekä eriteltävä luovutettavan tiedon laatu ja turvaluokka.

4. Neuvoston pääsihteeristö käsittelee pyynnöt ja tässä tarkoituksessa:

   — kysyy luovutettavan tiedon alunperin luovuttaneen jäsenvaltioiden tai tarvittaessa EU:n hajautetun erillisviraston kantaa,

   — luo tarpeelliset yhteydet edunsaajina olevien valtioiden tai kansainvälisten järjestöjen turvallisuudesta vastaaviin elimiin tarkistaakseen, että niiden turvallisuuspolitiikka ja turvallisuusmääräykset riittävät varmistamaan luovutettavan turvaluokitellun tiedon suojaamisen näiden turvallisuussääntöjen mukaisesti,

   — pyytävät jäsenvaltioiden kansallisten turvallisuusviranomaisten teknistä lausuntoa edunsaajina olevien valtioiden tai kansainvälisten elinten luotettavuudesta.

5. Neuvoston pääsihteeristö toimittaa pyynnön ja turvallisuusyksikön lausunnon edelleen neuvostolle päätöstä varten.

TURVALLISUUTTA KOSKEVAT SÄÄNNÖT, JOITA EDUNSAAJIEN ON SOVELLETTAVA

6. Korkeana edustajana toimiva pääsihteeri antaa edunsaajina oleville valtioille tai kansainvälisille järjestöille tiedon EU:n turvaluokitellun tiedon luovuttamisen hyväksymistä koskevasta neuvoston päätöksestä ja toimittaa eteenpäin tarpeelliseksi katsotun kappalemäärän näitä turvallisuussääntöjä. Jos pyyntö on jäsenvaltion esittämä, kyseinen valtio antaa edunsaajalle tiedon hyväksytystä luovutuksesta.

   Luovutuspäätös tulee voimaan vasta, kun edunsaajat ovat antaneet kirjallisen vakuutuksen siitä, että ne:

   — käyttävät tietoa ainoastaan sovittuihin tarkoituksiin,

   — suojaavat tiedon näiden turvallisuussääntöjen ja erityisesti jäljempänä mainittujen erityismääräysten mukaisesti.

7. *Henkilöstö*

   a) EU:n turvaluokiteltuun tietoon pääsevien virkamiesten määrä rajataan tarpeellisuusperiaatteen pohjalta tiukasti niihin henkilöihin, joiden tehtävät edellyttävät pääsyä kyseiseen tietoon.

b) Kaikilla viranomaisilla ja kansalaisilla, jotka valtuutetaan pääsemään EU:n turvaluokiteltuun tietoon, on oltava joko asianmukaisen turvaluokan luotettavuustodistus tai vastaava luotettavuusselvitys, jonka heidän oman maansa hallitus on myöntänyt.

8. *Asiakirjojen lähettäminen*

a) Käytännön menettelytavat asiakirjojen lähettämiseksi päätetään sopimuksen mukaan neuvoston turvamääräysten VII jakson määräysten pohjalta. Niissä täsmennetään erityisesti ne rekisterin pitäjät, joille EU:n turvaluokiteltu tieto on lähetettävä.

b) Jos turvaluokiteltuun tietoon, jonka luovuttamisen neuvosto on valtuuttanut, sisältyy TRÈS SECRET UE / EU TOP SECRET -turvaluokan tietoa, edunsaajana olevan valtion tai kansainvälisen järjestön on perustettava keskustoimisto EU-asioiden rekisteröintiä varten ja tarvittaessa alarekistereitä EU-asioiden rekisteröintiä varten. Näitä rekisterin pitäjiä hallinnoidaan näiden turvallisuussääntöjen VIII jakson määräysten mukaisesti.

9. *Rekisteröinti*

Välittömästi rekisterin pitäjän vastaanotettua CONFIDENTIEL UE- tai sitä korkeamman turvaluokan EU:n asiakirjan, se merkitsee asiakirjan järjestön hallinnoimaan erityiseen rekisteriin, jossa on sarakkeet, joihin merkitään vastaanottopäivämäärä, asiakirjaa koskevia tietoja (päivämäärä, viitenumero ja käännöksen numero), asiakirjan turvaluokitusaste, otsikko, vastaanottajan nimi ja ammattinimike, kuitin palautuspäivämäärä sekä päivämäärä, jona asiakirja palautetaan EU:n luovuttajalle tai hävitetään.

10. *Hävittäminen*

a) EU:n turvaluokitellut asiakirjat hävitetään näiden turvallisuussääntöjen VI jaksossa määrättyjen ohjeiden mukaisesti. Käännökset TRÈS SECRET UE / EU TOP SECRET- ja SECRET UE -turvaluokan asiakirjojen hävittämistodistuksista lähetetään asiakirjat toimittaneelle EU:n rekisterin pitäjälle.

b) EU:n turvaluokitellut asiakirjat sisällytetään edunsaajina olevien elinten hätätapauksessa suoritettavaa hävittämistä koskeviin suunnitelmiin.

11. *Asiakirjojen suojaaminen*

Toteutetaan kaikki asianmukaiset toimet sen estämiseksi, että sivulliset henkilöt pääsisivät EU:n turvaluokiteltuun tietoon.

12. *Jäljennökset, käännökset ja otteet*

CONFIDENTIEL UE- tai SECRET UE -turvaluokan asiakirjasta ei saa tehdä valokopiota tai käännöstä tai ottaa siitä poimintoja ilman asianomaisen turvallisuudesta vastaavan järjestön päällikön valtuutusta, joka kirjaa ja tarkistaa kyseiset jäljennökset, käännökset tai otteet ja leimaa ne tarvittaessa.

TRÈS SECRET UE / EU TOP SECRET -turvaluokan asiakirjan monentamisen tai kääntämisen voi valtuuttaa ainoastaan luovuttava viranomainen, joka vahvistaa valtuutettujen käännösten määrän; jos luovuttavaa viranomaista ei pystytä määrittämään, pyyntö toimitetaan edelleen neuvoston pääsihteeristön turvallisuusyksikölle.

13. *Turvallisuuden vaarantuminen*

Jos turvallisuus on vaarantunut tai sen epäillään vaarantuneen EU:n turvaluokitellun asiakirjan osalta, on välittömästi suoritettava seuraavat toimet edellyttäen, että turvallisuussopimus on tehty:

a) tehdään tutkimus turvallisuuden vaarantumiseen johtaneiden olosuhteiden osoittamiseksi;

b) annetaan neuvoston pääsihteeristön turvallisuusyksikölle, kansalliselle turvallisuusviranomaiselle ja luovuttaneelle viranomaiselle asia tiedoksi, tai mainitaan selkeästi, että viimeksi mainitulle ei ole tietoa annettu, mikäli näin ei ole tehty;

c) toteutetaan toimia turvallisuuden vaarantumisen vaikutusten minimoimiseksi;

d) selvitetään ja toteutetaan toimenpiteitä tapahtuneen toistumisen välttämiseksi;

e) toteutetaan kaikki neuvoston pääsihteeristön turvallisuusyksikön suosittelemat toimenpiteet tapahtuneen toistumisen estämiseksi.

14. *Tarkastukset*

Neuvoston pääsihteeristön turvallisuusyksikön sallitaan, asianomaisten valtioiden tai kansainvälisten järjestöjen kanssa tehtävän sopimuksen perusteella, suorittaa luovutetun EU:n turvaluokitellun tiedon suojaamisessa käytettyjen toimenpiteiden tehokkuuden arviointi.

15. *Raportointi*

Sillä edellytyksellä, että turvallisuussopimus tehdään, ja niin kauan kuin määrätyllä valtiolla tai kansainvälisellä järjestöllä on hallussaan EU:n turvaluokiteltua tietoa, sen on toimitettava tiedon luovuttamista koskevaa valtuutusta annettaessa määrättyyn päivämäärään mennessä, vuosittainen raportti, jossa vahvistetaan, että näitä turvallisuussääntöjä on noudatettu.

Lisäys 5

Ohjeet EU:n turvaluokitellun aineiston luovuttamisesta kolmansille valtioille tai kansainvälisille järjestöille

2 tason yhteistyö

MENETTELYT

1. Vain neuvostolla on toimivalta luovuttaa EU:n turvaluokiteltua tietoa kolmansille valtioille tai kansainvälisille järjestöille, joilla on selvästi erilainen turvallisuuspolitiikka ja turvallisuusmääräykset kuin EU:lla. Periaatteessa luovuttaminen on rajattu SECRET UE- ja sitä alemman turvaluokan tietoon; luovutettavaan tietoon ei sisällytetä erityisesti jäsenvaltioille varattua kansallista tietoa eikä erityismerkinnöin varustettua EU:n turvaluokiteltua tietoa.

2. Neuvosto voi delegoida päätöksen luovuttaa turvaluokiteltua tietoa; valtuutuksessa todetaan 1 kohdassa määriteltyjen rajojen puitteissa luovutettavissa olevan tiedon laatu ja sen turvaluokitus, joka ei voi olla RESTREINT UE -turvaluokkaa korkeampi.

3. Sillä edellytyksellä, että turvallisuussopimus on tehty, asianosaisten valtioiden tai kansainvälisten järjestöjen turvallisuudesta vastaavat elimet osoittavat korkeana edustajana toimivalle pääsihteerille EU:n turvaluokitellun tiedon luovuttamista koskevat pyynnöt, joissa on mainittava luovutuksen tarkoitus sekä luovutettavan tiedon laatu ja turvaluokitusaste.

   Myös jäsenvaltio tai EU:n hajautettu erillisvirasto, joka katsoo EU:n turvaluokitellun tiedon luovuttamisen olevan suotavaa, voi esittää pyynnön; sen on mainittava tällaisen luovuttamisen tarkoitus ja siitä EU:lle koituva hyöty sekä eriteltävä luovutettavan tiedon laatu ja turvaluokka.

4. Neuvoston pääsihteeristö käsittelee pyynnöt ja tässä tarkoituksessa:

   — kysyy luovutettavan tiedon alunperin luovuttaneen jäsenvaltion tai tarvittaessa EU:n hajautetun erillisviraston mielipidettä,

   — luo alustavat yhteydet edunsaajina olevien valtioiden tai kansainvälisten järjestöjen turvallisuudesta vastaaviin elimiin tiedon hankkimiseksi niiden turvallisuuspolitiikasta ja turvallisuusmääräyksistä ja erityisesti vertailevan taulukon laatimiseksi EU:ssa ja asianosaisessa valtiossa tai kansainvälisessä järjestössä sovellettavista turvaluokituksista,

   — järjestää neuvoston turvakomitean kokouksen tai tekee tiedusteluja, hiljaisen hyväksynnän menettelyllä mikäli tarpeellista, jäsenvaltioiden kansallisilta turvallisuusviranomaisilta, jotta turvakomitealta saataisiin tekninen lausunto.

5. Neuvoston turvakomitean tekninen lausunto koskee seuraavia asioita:

   — edunsaajina olevien valtioiden tai kansainvälisten järjestöjen luotettavuus, jotta voitaisiin arvioida turvallisuusriskit, joille EU tai sen jäsenvaltiot asettavat itsensä alttiiksi,

   — arviointi edunsaajien kyvystä suojata EU:n luovuttamaa turvaluokiteltua tietoa,

   — ehdotuksia käytännön menettelytavoiksi (esimerkiksi lyhennettyjen tekstiversioiden toimittaminen), jotka koskevat lähetettävien EU:n turvaluokiteltujen tiedon ja asiakirjojen käsittelyä (EU:n turvaluokkaotsikoiden säilyttäminen tai poistaminen, erityismerkinnät jne.) ([1]),

   — siirtäminen alempaan turvaluokkaan tai luokituksen poistaminen luovuttavan viranomaisen toimesta ennen kuin tieto luovutetaan edunsaajina oleville valtioille tai kansainvälisille järjestöille.

([1]) Tällöin luovuttavan viranomaisen on välttämätöntä soveltaa III jakson 9 kohdassa määriteltyä menettelyä kaikkien EU:ssa liikkeelle pantujen jäljennösten osalta.

6. Korkeana edustajana toimiva pääsihteeri toimittaa pyynnön ja neuvoston pääsihteeristön turvallisuusyksikön hankkiman neuvoston turvakomitean teknisen lausunnon edelleen neuvostolle päätöstä varten.

TURVALLISUUTTA KOSKEVAT SÄÄNNÖT, JOITA EDUNSAAJIEN ON SOVELLETTAVA

7. Korkeana edustajana toimiva pääsihteeri antaa edunsaajina oleville valtioille tai kansainvälisille järjestöille EU:n turvaluokitellun tiedon luovuttamisen hyväksymistä koskevasta neuvoston päätöksestä sekä toimittaa niille vertailevan taulukon EU:ssa ja asianosaisissa valtioissa tai kansainvälisissä järjestöissä sovellettavista turvaluokituksista. Jos pyyntö on jäsenvaltion esittämä, kyseinen valtio antaa edunsaajalle tiedon hyväksytystä luovutuksesta.

Luovutuspäätös tulee voimaan vasta kun edunsaajat ovat antaneet kirjallisen vakuutuksen siitä, että ne:

— käyttävät tietoa ainoastaan sovittuihin tarkoituksiin,

— suojaavat tiedon neuvoston määräämien sääntöjen mukaisesti.

8. Ellei neuvosto, saatuaan neuvoston turvakomitean teknisen lausunnon, päätä erityisestä menettelytavasta EU:n turvaluokiteltujen asiakirjojen käsittelemiseksi (poistetaan maininta EU:n turvaluokasta, erityismerkinnät jne.), laaditaan seuraavanlaiset suojaamista koskevat säännöt.

Siinä tapauksessa sääntöjä on mukautettava.

9. *Henkilöstö*

a) EU:n turvaluokiteltuun tietoon pääsevien virkamiesten määrä on rajattava tarpeellisuusperiaatteen pohjalta tiukasti niihin henkilöihin, joiden tehtävät edellyttävät pääsyä kyseiseen tietoon.

b) Kaikilla viranomaisilla ja kansalaisilla, jotka valtuutetaan pääsemään EU:n luovuttamaan turvaluokiteltuun tietoon, on oltava hyväksytty kansallinen luotettavuusselvitys tai kansallisen turvaluokitellun tiedon osalta valtuutus päästä tietoon asianmukaista EU:n turvaluokkaa vastaavalla tasolla, siten kuin se on määritelty vertailevassa taulukossa.

c) Nämä kansalliset luotettavuusselvitykset tai valtuutukset on toimitettava edelleen korkeana edustajana toimivalle pääsihteerille tiedoksi.

10. *Asiakirjojen lähettäminen*

a) Käytännön menettelytavat asiakirjojen lähettämiseksi sovitaan neuvoston pääsihteeristön turvallisuusyksikön ja vastaanottavien valtioiden tai kansainvälisten järjestöjen turvallisuudesta vastaavien elinten kesken EU:n neuvoston näiden asetusten VII jaksossa määrättyjen sääntöjen pohjalta. Niissä annetaan erityisesti tarkat osoitteet, joihin asiakirjat on toimitettava eteenpäin sekä EU:n turvaluokitellun tiedon lähettämisessä käytettävät kuriiri- tai postilaitokset.

b) CONFIDENTIEL UE- tai sitä korkeamman turvaluokan asiakirjat lähetetään kaksinkertaisissa kirjekuorissa. Sisempään kirjekuoreen merkitään ”UE” ja turvaluokka. Kuoreen laitetaan jokaisen turvaluokitellun asiakirjan osalta kuitti. Kuitissa, jota itseään ei turvaluokitella, mainitaan ainoastaan asiakirjan viitetiedot (sen viitenumero, päivämäärä ja käännöksen numero) ja kieli, jolla se on kirjoitettu mutta ei otsikkoa.

c) Sisempi kuori laitetaan ulompaan kirjekuoreen, johon merkitään pakkausnumero kuittausta varten. Ulompaan kirjekuoreen ei merkitä turvaluokkaa.

d) Kuriireille annetaan aina kuitti, josta ilmenee pakkauksen numero.

11. *Kirjaaminen saapumisen yhteydessä*

Vastaanottajavaltion kansallinen turvallisuusviranomainen tai sitä vastaava elin hallituksensa puolesta EU:n lähettämää turvaluokiteltua tietoa vastaanottavassa valtiossa tai vastaanottavan kansainvälisen järjestön turvallisuusyksikkö avaa erityisen rekisterin, johon kirjataan EU:n turvaluokiteltu tieto vastaanotetuksi. Rekisterissä on oltava sarakkeet, joihin merkitään vastaanottopäivämäärä, asiakirjaa koskevia tietoja (päivämäärä, viitenumero ja käännöksen numero), asiakirjan turvaluokka, otsikko, vastaanottajan nimi ja ammattinimike, kuitin palautuspäivämäärä sekä päivämäärä, jona asiakirja palautetaan EU:n luovuttajalle tai hävitetään.

12. *Asiakirjojen palauttaminen*

Vastaanottajan palauttaessa turvaluokitellun asiakirjan neuvostolle tai sen luovuttaneelle jäsenvaltiolle, sen on toimittava kohdassa 10 tarkoitetun menettelytavan mukaisesti.

13. *Suojaus*

a) Silloin kun asiakirjat eivät ole käytössä, ne varastoidaan turvalliseen säilytyspaikkaan, joka on hyväksytty saman turvaluokan kansallisesti luokitellun aineiston varastoimiseen. Turvallisessa säilytyspaikassa ei ole mitään merkintöjä, jotka viittaisivat sen sisältöön, johon pääsevät ainoastaan henkilöt, joilla on valtuutus käsitellä EU:n turvaluokiteltua tietoa. Käytettävien yhdistelmälukkojen numeroyhdistelmä annetaan ainoastaan niille valtion tai järjestön virkailijoille, joilla on valtuutus päästä turvallisessa säilytyspaikassa varastoitavaan EU:n turvaluokiteltuun tietoon ja se vaihdetaan kuuden kuukauden välein tai aikaisemmin virkailijan siirron, jonkin numeroyhdistelmän tuntevan virkailijan luotettavuusselvityksen peruuttamisen tai turvallisuuden vaarantumisen riskin yhteydessä.

b) Ainoastaan virkailijat, joilla on valtuutus päästä EU:n turvaluokiteltuun tietoon ja joiden on tarpeellista päästä siihen tietoon, saavat poistaa EU:n turvaluokiteltuja asiakirjoja turvallisesta säilytyspaikasta. He ovat vastuussa näiden asiakirjojen turvallisesta säilyttämisestä niin kauan, kun ne ovat heidän hallussaan ja erityisesti siitä, etteivät asiakirjat päädy sivulliselle. Heidän on myös varmistettava, että asiakirjat varastoidaan turvalliseen säilytyspaikkaan silloin, kun he ovat lopettaneet niihin tutustumisen, sekä työajan ulkopuolella.

c) CONFIDENTIEL UE- tai sitä korkeamman turvaluokan asiakirjasta ei saa tehdä valokopioita eikä poimintoja ilman neuvoston pääsihteeristön turvallisuusyksikön valtuutusta.

d) Menettelytapa asiakirjojen nopeaksi ja täydelliseksi hävittämiseksi hätätapauksissa on määriteltävä ja vahvistettava yhdessä neuvoston pääsihteeristön turvallisuusyksikön kanssa.

14. *Fyysinen turvallisuus*

a) Silloin kun ne eivät ole käytössä, EU:n turvaluokiteltujen asiakirjojen varastoimiseen käytettävät turvalliset säilytyspaikat pidetään lukittuina kaikkina aikoina.

b) Silloin kun kunnossapito- tai siivoushenkilöstön on tarpeellista tulla sisään huoneeseen tai työskennellä huoneessa, jossa on tällaisia turvallisia säilytyspaikkoja, on valtion tai järjestön turvallisuusyksikön jäsenen tai erityisesti kyseisen huoneen turvallisuuden valvonnasta vastaavan virkailijan seurattava heitä kaikkina aikoina.

c) Normaalin työajan ulkopuolella (öisin, viikonloppuisin ja juhlapyhinä) EU:n turvaluokiteltuja asiakirjoja sisältävät turvalliset säilytyspaikat suojataan joko vartioinnilla tai automaattisella hälytysjärjestelmällä.

15. *Turvallisuuden vaarantuminen*

Silloin kun on turvallisuus on vaarantunut tai sen epäillään vaarantuneen EU:n turvaluokitellun asiakirjan osalta, on välittömästi suoritettava seuraavat toimet:

a) toimitetaan välittömästi selostus tapahtuneesta neuvoston pääsihteeristön turvallisuusyksikölle tai aloitteen asiakirjojen edelleen lähettämisestä tehneen jäsenvaltion kansalliselle turvallisuusviranomaiselle (sekä käännös siitä neuvoston pääsihteeristön turvallisuusyksikölle);

b) suoritetaan tutkimus, jonka valmistuttua toimitetaan täydellinen selonteko turvallisuudesta vastaavalle elimelle (katso a) kohta edellä). Tämän jälkeen on toteutettava tarvittavat toimenpiteet tilanteen korjaamiseksi.

16. *Tarkastukset*

Neuvoston pääsihteeristön turvallisuusyksikön sallitaan, asianomaisten valtioiden tai kansainvälisten järjestöjen kanssa tehtävän sopimuksen perusteella, suorittaa luovutetun EU:n turvaluokitellun tiedon suojaamisessa käytettyjen toimenpiteiden tehokkuuden arviointi.

17. *Selonteko*

Niin kauan kuin valtiolla tai kansainvälisellä järjestöllä on hallussaan EU:n turvaluokiteltua tietoa, sen on toimitettava tiedon luovuttamista koskevaa valtuutusta annettaessa määrättyyn päivämäärään mennessä vuosittainen selonteko, jossa vahvistetaan että näitä turvallisuussääntöjä on noudatettu.

Lisäys 6

Ohjeet EU:n luokiteltujen tietojen luovuttamiseksi kolmansille valtioille tai kansainvälisille järjestöille

3 tason yhteistyö

MENETTELYT

1. Neuvosto saattaa ajoittain haluta tehdä tietyissä erityisolosuhteissa yhteistyötä sellaisten valtioiden tai järjestöjen kanssa, jotka eivät voi antaa näissä turvallisuussäännöissä vaadittuja varmistuksia. Kyseinen yhteistyö saattaa kuitenkin edellyttää EU:n luokiteltujen tietojen luovuttamista. Nimenomaan jäsenvaltioille tarkoitettuja kansallisia tietoja ei luovuteta.

2. Kyseisissä erityisolosuhteissa kolmansien valtioiden tai kansainvälisten järjestöjen esittämiä tai jäsenvaltioiden tai tarvittaessa EU:n hajautettujen erillisvirastojen ehdottamia pyyntöjä EU:n kanssa tehtävästä yhteistyöstä käsitellään asiaa ensin neuvostossa, joka pyytää tarvittaessa tiedot alunperin luovuttaneen jäsenvaltion tai hajautetun erillisviraston lausuntoa. Neuvosto harkitsee luokiteltujen tietojen luovuttamisen aiheellisuutta, arvioi edunsaajien valtuutuksia ja päättää, millaisia luokiteltuja tietoja voidaan luovuttaa.

3. Jos neuvosto puoltaa tietojen luovuttamista, korkeana edustajana toimivan pääsihteerin tehtävänä on kutsua koolle neuvoston turvakomitea tai tiedustella asiaa jäsenvaltioiden kansallisilta turvallisuusviranomaisilta tarvittaessa yksinkertaista kirjallista menettelyä noudattaen teknisen lausunnon saamiseksi turvakomitealta.

4. Neuvoston turvakomitean lausunto sisältää seuraavaa:

   a) EU:lle tai sen jäsenvaltioille aiheutuvien turvallisuusriskien arviointi;

   b) luovutettavissa olevien tietojen luokittelu ottaen tarvittaessa huomioon tietojen laadun;

   c) tiedot alunperin luovuttaneen viranomaisen suorittama luokittelun laskeminen tai poistaminen ennen tietojen luovuttamista edelleen asianomaisille maille tai kansainvälisille järjestöille ([1]);

   d) luovutettavien asiakirjojen käsittelymenettelyt (ks. 5 kohta jäljempänä);

   e) mahdolliset lähettämismenetelmät (esim. yleisten postipalvelujen käyttö, yleisten tai suojattujen teleliikennejärjestelmien käyttö, diplomaattiposti, kuriirit, joiden luotettavuus on selvitetty).

5. Tässä lisäyksessä tarkoitetuille valtioille tai järjestöille luovutettavat asiakirjat eivät periaatteessa sisällä lähdeviittauksia tai EU:n luokituksia. Neuvoston turvakomitea saattaa suositella käytettäväksi:

   — erityismerkintöjä tai koodinimeä,

   — erityistä luokittelumenetelmää, jossa tietojen arkaluonteisuus liittyy edunsaajan toimitusmenetelmiltä edellytettyihin valvontatoimenpiteisiin (ks. 14 kohdassa olevat esimerkit).

6. Neuvoston pääsihteeristön turvallisuusyksikkö toimittaa neuvoston turvalausunnon neuvostolle ja liittää siihen tarvittaessa ehdotuksen tehtävien suorittamisen edellyttämiksi valtuuksiksi, erityisesti kiireellisissä tilanteissa.

7. Neuvoston hyväksyttyä EU:n luokiteltujen tietojen luovuttamisen ja siihen liittyvät käytännön menettelyt, neuvoston pääsihteeristön turvallisuusyksikkö luo tarvittavat yhteydet asianomaisen valtion tai järjestön turvallisuusviranomaisiin aiottujen turvatoimenpiteiden soveltamisen helpottamiseksi.

([1]) Tämä edellyttää, että tiedot luovuttanut viranomainen soveltaa III jakson 9 kohdassa määriteltyä menettelyä kaikkiin EU:ssa jaettuihin kopioihin.

8. Neuvoston pääsihteeristön turvallisuusyksikkö jakaa kaikille jäsenvaltioille ja tarvittaessa asianomaisille EU:n hajautetuille erillisvirastoille taulukkomuotoisen yhteenvedon tietojen laadusta ja luokittelusta, jossa luetellaan ne järjestöt ja maat, joille kyseisiä tietoja voidaan luovuttaa neuvoston päätöksen mukaisesti.

9. Tiedot luovuttavan jäsenvaltion kansallinen turvallisuusviranomainen tai neuvoston pääsihteeristön turvallisuusyksikkö toteuttaa kaikki tarvittavat toimenpiteet, joilla helpotetaan mahdollisten vahinkojen arviointia ja menettelyjen tarkistamista.

10. Neuvostolle on ilmoitettava yhteistyön edellytyksissä tapahtuneista muutoksista.

TURVAMÄÄRÄYKSET, JOITA EDUNSAAJIEN ON NOUDATETTAVA

11. Neuvoston pääsihteeri ja korkea edustaja ilmoittaa edunsaajavaltioille tai kansainvälisille järjestöille neuvoston päätöksestä sallia EU:n luokiteltujen tietojen luovuttaminen sekä neuvoston turvakomitean ehdottamista ja neuvoston hyväksymistä yksityiskohtaisista suojelusäännöistä. Jos tietojen luovuttamista koskevan pyynnön on tehnyt jokin jäsenvaltio, kyseinen valtio ilmoittaa edunsaajavaltiolle tietojen luovuttamista koskevasta päätöksestä.

Päätös tulee voimaan vasta, kun edunsaajat ovat antaneet kirjallisen vakuutuksen, jonka mukaan ne:

— käyttävät tietoja ainoastaan neuvoston päätöksen mukaiseen yhteistyöhön,

— tarjoavat tiedoille neuvoston vaatiman suojan.

12. *Asiakirjojen lähettäminen*

a) Asiakirjojen lähettämistä koskevista käytännön menettelyistä sovitaan neuvoston pääsihteeristön turvallisuusyksikön ja vastaanottavien valtioiden tai kansainvälisten järjestöjen turvallisuuselinten kesken. Menettelyissä täsmennetään erityisesti tarkat osoitteet, joihin asiakirjat on toimitettava.

b) CONFIDENTIEL UE ja sitä korkeammalle luokitellut asiakirjat lähetetään kaksoiskuoressa. Sisimmässä kuoressa on sovittu erityismerkintä tai koodinimi sekä maininta asiakirjalle hyväksytystä erityisluokituksesta. Kutakin luokiteltua asiakirjaa varten liitetään kuittauslomake. Kuittauslomake, jota ei luokitella, sisältää ainoastaan asiakirjaa koskevia tietoja (viitenumero, päivämäärä, käännöksen numero) ja asiakirjan kielen, ei otsikkoa.

c) Sisempi kuori suljetaan tämän jälkeen toiseen ulompaan kuoreen, johon merkitään pakkausnumero kuittausta varten. Ulommaisessa kuoressa ei ole turvaluokkamerkintää.

d) Kuriireille on aina annettava kuitti, jossa on pakkausnumero.

13. *Kirjaaminen saapumisen yhteydessä*

Vastaanottajavaltion kansallinen turvallisuusviranomainen tai sitä vastaava elin hallituksensa puolesta EU:n lähettämän turvaluokiteltavan tiedon vastaanottavassa valtiossa tai vastaanottavan kansainvälisen järjestön turvallisuusyksikkö avaa erityisen rekisterin, johon kirjataan EU:n luokiteltu tieto sen vastaanottamisen yhteydessä. Rekisterissä on oltava sarakkeet, joihin merkitään vastaanottopäivämäärä, asiakirjaa koskevia tietoja (päivämäärä, viitenumero ja käännöksen numero), asiakirjan turvaluokitusaste, otsikko, vastaanottajan nimi tai ammattinimike, kuitin palautuspäivämäärä ja päivämäärä, jona kuitti on palautunut EU:hun sekä asiakirjan hävittämispäivämäärä.

14. *Vaihdettavien luokiteltujen tietojen käyttö ja suojelu*

a) SECRET UE -tason tietojen käsittelystä vastaavat erityisesti nimetyt viranomaiset, jotka on valtuutettu käsittelemään kyseiseen luokkaan kuuluvia tietoja. Tiedot on säilytettävä turvakaapeissa, jotka voidaan avata ainoastaan kyseisten tietojen käsittelyyn valtuutettujen henkilöiden toimesta. Tiloja, joissa kyseiset kaapit sijaitsevat, on valvottava jatkuvasti, ja on perustettava todentamisjärjestelmä sen varmistamiseksi, että kyseisiin tiloihin päästetään ainoastaan asianmukaisesti valtuutetut henkilöt. SECRET UE -tason tiedot toimitetaan joko diplomaattipostina tai turvallisia posti- tai teleliikennepalveluja käyttäen. SECRET UE -asiakirjasta voidaan ottaa käännös ainoastaan, jos tiedot alunperin luovuttanut viranomainen antaa tähän kirjallisen suostumuksen. Kaikki käännökset kirjataan ja niitä valvotaan. Kaikkia SECRET-asiakirjoja koskevista toimista on annettava kuitit.

b) CONFIDENTIEL UE -tason tietojen käsittelystä vastaavat asianmukaisesti nimetyt viranomaiset, jotka on valtuutettu saamaan asiaa koskevia tietoja. Asiakirjat on säilytettävä lukituissa turvakaapeissa valvotuissa tiloissa.

CONDIFENTIEL UE -luokan tiedot toimitetaan diplomaattipostina, sotilaspostina tai suojattuja teleliikennepalveluja käyttäen. Vastaanottaja voi ottaa asiakirjoista käännöksiä, joiden numero ja jakelu on kirjattava erityisiin rekistereihin.

c) RESTREINT UE -tason tietoja on käsiteltävä tiloissa, joihin valtuuttamattomat henkilöt eivät pääse, ja ne on säilytettävä lukitussa paikassa. Asiakirjat voidaan lähettää yleisiä postipalveluja käyttäen kirjattuna lähetyksenä kaksoiskuoressa ja kiireellisissä tapauksissa operaatioiden aikana suojaamattomia yleisiä teleliikennejärjestelmiä käyttäen. Vastaanottajat voivat ottaa asiakirjoista käännöksiä.

d) Luokittelemattomia tietoja ei tarvitse suojata erityistoimenpiteillä, ja niitä voidaan lähettää postissa ja yleisiä teleliikennejärjestelmiä käyttäen. Vastaanottajat voivat ottaa asiakirjoista käännöksiä.

15. *Hävittäminen*

Tarpeettomat asiakirjat on hävitettävä. RESTREINT UE- ja CONFIDENTIEL UE -tason asiakirjojen hävittäminen kirjataan asianmukaisesti erityisiin rekistereihin. SECRET UE -tason asiakirjoista annetaan hävittämistodistukset, joissa on kahden hävittämistä todistaneen henkilön allekirjoitus.

16. *Turvallisuuden vaarantuminen*

Jos CONFIDENTIEL UE- tai SECRET UE -tason tietojen turvallisuus vaarantuu tai jos turvallisuuden epäillään vaarantuneen, vastaanottaneen valtion kansallisen turvallisuusviranomaisen tai tiedot vastaanottaneen järjestön turvallisuuspäällikön on tutkittava olosuhteet, joissa turvallisuus vaarantui. Jos vaarantumisen syy saadaan selville tutkinnassa, tiedot alunperin luovuttaneelle viranomaiselle on tiedotettava asiasta. Jos riittämättömät menettelyt tai säilytysmenetelmät ovat olleet turvallisuuden vaarantumisen syynä, on toteutettava tarvittavat toimenpiteet kyseisten menettelyjen ja menetelmien korjaamiseksi. Korkeana edustajana toimiva pääsihteeri tai vaarantuneet tiedot luovuttaneen jäsenvaltion turvallisuusviranomainen voi pyytää edunsaajalta tarkempia tietoja tutkinnasta.