►**B**

KOMISSION PÄÄTÖS,

tehty 29 päivänä marraskuuta 2001,

komission sisäisten menettelysääntöjen muuttamisesta

(tiedoksiannettu numerolla K(2001) 3031)

(2001/844/EY, EHTY, Euratom)

(EYVL L 317, 3.12.2001, s. 1)

Muutettu:

		virallinen lehti		
		N:o	sivu	päivämäärä
►**M1**	Komission päätös 2005/94/EY, Euratom, tehty 3 päivänä helmikuuta 2005	L 31	66	4.2.2005
►**M2**	Komission päätös 2006/70/EY, Euratom, tehty 31 päivänä tammikuuta 2006	L 34	32	7.2.2006
►**M3**	Komission päätös 2006/548/EY, Euratom, tehty 2 päivänä elokuuta 2006	L 215	38	5.8.2006

▼B

KOMISSION PÄÄTÖS,

tehty 29 päivänä marraskuuta 2001,

komission sisäisten menettelysääntöjen muuttamisesta

(tiedoksiannettu numerolla K(2001) 3031)

(2001/844/EY, EHTY, Euratom)

EUROOPAN YHTEISÖJEN KOMISSIO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen ja erityisesti sen 218 artiklan 2 kohdan,

ottaa huomioon Euroopan hiili- ja teräsyhteisön perustamissopimuksen ja erityisesti sen 16 artiklan,

ottaa huomioon Euroopan atomienergiayhteisön perustamissopimuksen ja erityisesti sen 131 artiklan,

ottaa huomioon Euroopan unionista tehdyn sopimuksen ja erityisesti sen 28 artiklan 1 kohdan ja 41 artiklan 1 kohdan,

ON PÄÄTTÄNYT SEURAAVAA:

1 artikla

Lisätään tämän päätöksen liitteenä olevat komission turvallisuussäännökset komission sisäisten menettelysääntöjen liitteeksi.

2 artikla

Tämä päätös tulee voimaan päivänä, jona se julkaistaan *Euroopan yhteisöjen virallisessa lehdessä*.

Sitä sovelletaan 1 päivästä joulukuuta 2001.

▼B

LIITE

KOMISSION TURVALLISUUSSÄÄNNÖKSET

Sekä katsoo seuraavaa:

(1) Komission toimintojen kehittämiseksi luottamuksellisuutta edellyttävillä aloilla on asianmukaista ottaa käyttöön kattava komissiota, muita toimielimiä, Euroopan yhteisöjen perustamissopimuksella tai Euroopan unionista tehdyllä sopimuksella taikka niiden nojalla perustettuja elimiä, toimistoja ja virastoja, jäsenvaltioita sekä kaikkia muita Euroopan unionin turvaluokitellun tiedon, jäljempänä ”EU:n turvaluokiteltu tieto”, vastaanottajia koskeva turvallisuusjärjestelmä.

(2) Näin perustetun turvallisuusjärjestelmän tehokkuuden varmistamiseksi komissio antaa EU:n turvaluokitellun tiedon ainoastaan sellaisten ulkopuolisten elinten käyttöön, jotka antavat takeet siitä, että ne ovat toteuttaneet kaikki tarvittavat toimenpiteet näitä säännöksiä ehdottomasti vastaavien sääntöjen soveltamiseksi.

(3) Näiden säännösten soveltaminen ei rajoita Euroopan ydinenergiayhteisön perustamissopimuksen 24 artiklan soveltamisesta 31 päivänä heinäkuuta 1958 annetun asetuksen N:o 3 ([1]), salassapidettävien tilastotietojen luovuttamisesta Euroopan yhteisöjen tilastotoimistolle 11 päivänä kesäkuuta 1990 annetun neuvoston asetuksen (ETY) N:o 1588/90 ([2]) ja tietojenkäsittelyjärjestelmien suojaamisesta 23 päivänä marraskuuta 1995 tehdyn komission päätöksen K (95) 1510 lopullinen soveltamista.

(4) Komission turvallisuusjärjestelmä perustuu neuvoston turvallisuussääntöjen vahvistamisesta 19 päivänä maaliskuuta 2001 tehdyssä neuvoston päätöksessä 2001/264/EY ([3]) esitettyihin periaatteisiin unionin päätöksentekomenettelyn kitkattoman toiminnan varmistamiseksi.

(5) Komissio korostaa sitä, että muut toimielimet on tarvittaessa saatava mukaan noudattamaan niitä luottamuksellisuutta koskevia sääntöjä ja vaatimuksia, jotka ovat välttämättömiä unionin ja sen jäsenvaltioiden etujen suojelemiseksi.

(6) Komissio tunnustaa tarpeen luoda komission oma turvallisuusjärjestelmä ottaen huomioon kaikki turvallisuuteen liittyvät tekijät ja komission erityisluonne toimielimenä.

(7) Näiden säännösten soveltaminen ei rajoita perustamissopimuksen 255 artiklan ja Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi 30 päivänä toukokuuta 2001 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1049/2001 ([4]) säännösten soveltamista.

▼M2

(8) Nämä säännökset eivät kuitenkaan rajoita yhteisön perustamissopimuksen 286 artiklan ja yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 soveltamista,

▼B

1 artikla

Komission turvallisuussäännöt vahvistetaan liitteessä.

2 artikla

1. Turvallisuusasioista vastaava komission jäsen toteuttaa asianmukaiset toimenpiteet sen varmistamiseksi, että komissiossa työskentelevät komission virkamiehet ja muu henkilöstö sekä komissiossa avustajina toimivat henkilöt noudattavat 1 artiklassa tarkoitettuja sääntöjä käsitellessään EU:n turvaluokiteltua tietoa ja että näitä sääntöjä noudatetaan kaikissa komission toimitiloissa, myös unionin alueella sijaitsevissa edustustoissa ja toimistoissa sekä yhteisön ulkopuolisissa maissa toimivissa lähetystöissä, ja että myös komission ulkopuoliset toimeksisaajat noudattavat niitä.

▼M3

Kun komission ja ulkopuolisen toimeksisaajan tai tuensaajan väliseen sopimukseen tai tukisopimukseen liittyy EU:n turvaluokitellun tiedon käsittelyä toimeksisaajan tai tuensaajan toimitiloissa, asianmukaisten toimenpiteiden, jotka mainitun

([1]) EYVL N:o 17, 6.10.1958, s. 406/58.
([2]) EYVL L 151, 15.6.1990, s. 1.
([3]) EYVL L 101, 11.4.2001, s. 1.
([4]) EYVL L 145, 31.5.2001, s. 43.

▼**M3**

ulkopuolisen toimeksisaajan tai tuensaajan on toteutettava 1 artiklassa tarkoitettujen sääntöjen noudattamisen varmistamiseksi EU:n turvaluokiteltua tietoa käsiteltäessä, on oltava erottamaton osa sopimusta tai tukisopimusta.

▼**B**

2. Jäsenvaltiot, muut toimielimet, perustamissopimuksilla taikka niiden nojalla perustetut elimet, toimistot ja virastot voivat saada EU:n turvaluokiteltua tietoa sillä edellytyksellä, että ne varmistavat, että kun EU:n turvaluokiteltua tietoa käsitellään, niiden yksiköissä ja toimitiloissa sovelletaan 1 artiklassa tarkoitettuja sääntöjä ehdottomasti vastaavia sääntöjä, erityisesti kun tämä koskee seuraavia henkilöitä:

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

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

c) EU:n turvaluokiteltua tietoa käsittelevät ulkopuoliset toimeksisaajat ja komennuksella olevat työntekijät.

3 artikla

Yhteisön ulkopuoliset maat, kansainväliset järjestöt ja muut elimet voivat saada EU:n turvaluokiteltua tietoa sillä edellytyksellä, että ne varmistavat, että tällaista tietoa käsiteltäessä noudatetaan 1 artiklassa tarkoitettuja sääntöjä ehdottomasti vastaavia sääntöjä.

4 artikla

Turvallisuusasioista vastaava komission jäsen voi toteuttaa liitteessä olevan II osan mukaisia toimenpiteitä noudattaen liitteessä olevassa I osassa olevia turvallisuutta koskevia perusperiaatteita ja vähimmäisvaatimuksia.

5 artikla

Näillä säännöksillä korvataan niiden soveltamispäivästä alkaen

a) Euroopan unionin toiminnan yhteydessä tuotettuun tai välitettyyn turvaluokiteltuun tietoon sovellettavista turvatoimista 30 päivänä marraskuuta 1994 tehty komission päätös K(94) 3282;

b) lupamenettelystä, jolla Euroopan komission virkamiehet ja muuhun henkilöstöön kuuluvat voidaan oikeuttaa komission hallussa olevien luokiteltujen tietojen saamiseen, 25 päivänä helmikuuta 1999 tehty komission päätös K (1999) 423.

6 artikla

Näiden säännösten soveltamispäivästä alkaen kaikki komission hallussa ennen kyseistä päivämäärää oleva turvaluokiteltu tieto, Euratomin turvaluokiteltua tietoa lukuun ottamatta,

a) jos se on komission tuottamaa, luokitellaan järjestelmällisesti uudelleen turvaluokkana ”►**M1** RESTREINT UE ◄”, jollei sen kirjoittaja päätä antaa sille uutta luokitusta 31 päivään tammikuuta 2002 mennessä. Tällaisissa tapauksissa kirjoittajan on ilmoitettava asiasta kaikille asianomaisen asiakirjan vastaanottajille;

b) jos se on tuotettu komission ulkopuolella, säilyttää alkuperäisen turvaluokituksensa, minkä johdosta sitä pidetään samantasoisena EU:n turvaluokiteltuna tietona, jollei kirjoittaja suostu turvaluokan poistamiseen tai alentamiseen.

▼B

LIITE

TURVALLISUUSSÄÄNNÖT

Sisällysluettelo

▼B

16 TURVALUOKAT, -OSOITTIMET JA -MERKINNÄT

16.1. **Luokitteluasteet**

16.2. **Turvaosoittimet**

16.3. **Merkinnät**

16.4. **Turvaluokan merkintätapa**

16.5. **Turvaosoittimien merkintätapa**

17 TURVALUOKITTELUN HALLINNOINTI

17.1. **Yleistä**

17.2. **Turvaluokituksen soveltaminen**

17.3. **Turvaluokan alentaminen ja poistaminen**

18 FYYSINEN TURVALLISUUS

18.1. **Yleistä**

18.2. **Turvallisuutta koskevat vaatimukset**

18.3. **Fyysiset turvatoimet**

18.3.1. *Turva-alueet*

18.3.2. *Hallinnollinen alue*

18.3.3. *Tulo- ja lähtötarkastukset*

18.3.4. *Vartiointikierrokset*

18.3.5. *Turvalliset säilytyspaikat ja kassaholvit*

18.3.6. *Lukot*

18.3.7. *Avainten ja yhdistelmien valvonta*

18.3.8. *Tunkeutumisen havaitsemislaitteet*

18.3.9. *Hyväksytty laitteisto*

18.3.10. *Kopio- ja faksilaitteiden fyysinen suojaus*

18.4. **Suojautuminen salakatselulta ja salakuuntelulta**

18.4.1. *Salakatselu*

18.4.2. *Salakuuntelu*

18.4.3. *Sähköisten laitteiden ja äänityslaitteiden tuominen*

18.5. **Teknisesti suojatut alueet**

19 TIEDONSAANTITARPEEN PERIAATETTA JA EU:N HENKILÖSTÖN LUOTETTAVUUSSELVITYSTÄ KOSKEVAT YLEISET SÄÄNNÖT

19.1. **Yleistä**

19.2. **TRES SECRET UE/EU TOP SECRET -turvaluokan tietoon pääsyä koskevat erityissäännöt**

19.3 **SECRET UE- ja CONFIDENTIEL UE -turvaluokan tietoon pääsyä koskevat erityissäännöt**

19.4. **RESTREINT UE -turvaluokan tietoon pääsyä koskevat erityissäännöt**

19.5. **Henkilösiirrot**

19.6. **Erityisohjeet**

▼B

20 KOMISSION VIRKAMIESTEN JA MUUN HENKILÖSTÖN LUOTETTAVUUSSELVITYSMENETTELY

21 EU:N TURVALUOKITELTUJEN ASIAKIRJOJEN VALMISTELU, JAKELU JA LÄHETTÄMINEN, KURIIREIHIN SOVELLETTAVAT TURVATOIMET, YLIMÄÄRÄISET KOPIOT, KÄÄNNÖKSET JA OTTEET

21.1. **Valmistelu**

21.2. **Jakelu**

21.3. **EU:n turvaluokiteltujen asiakirjojen lähettäminen**

21.3.1. *Pakkaukset ja kuitit*

21.3.2. *Lähettäminen kiinteistöjen tai kiinteistöryhmien sisällä*

21.3.3. *Lähettäminen valtion sisällä*

21.3.4. *Lähettäminen valtiosta toiseen*

21.3.5. *RESTREINT UE -asiakirjojen lähettäminen*

21.4. **Kuriireihin sovellettavat turvatoimet**

21.5. **Sähköiset ja muut tekniset lähetyskeinot**

21.6. **EU:n turvaluokitelluista asiakirjoista tehdyt ylimääräiset kopiot, käännökset ja otteet**

22 EU:N TURVALUOKITELLUN TIEDON REKISTERIT, INVENTOINNIT, TARKASTUKSET, SÄILYTTÄMINEN ARKISTOISSA JA HÄVITTÄMINEN

22.1. **EU turvaluokitellun tiedon paikallisrekisterit**

22.2. **TRES SECRET UE/EU TOP SECRET -rekisteri**

22.2.1. *Yleistä*

22.2.2. *TRES SECRET UE/EU TOP SECRET -keskusrekisteri*

22.2.3. *TRES SECRET UE/EU TOP SECRET -alarekisterit*

22.3. **EU:n turvaluokiteltujen asiakirjojen inventointi ja tarkastukset**

22.4. **EU:n turvaluokitellun tiedon säilyttäminen arkistoissa**

22.5. **EU:n turvaluokiteltujen asiakirjojen hävittäminen**

22.6. **Hävittäminen hätätapauksissa**

23 KOMISSION TILOJEN ULKOPUOLELLA JÄRJESTETTÄVIÄ KOKOUKSIA, JOISSA KÄSITELLÄÄN EU:N TURVALUOKITELTUA TIETOA, KOSKEVAT TURVATOIMET

23.1. **Yleistä**

23.2. **Vastuualueet**

23.2.1. ► **M2** *Komission turvallisuudesta vastaava linja* ◄

23.2.2. *Kokouksen turvavastaava (MSO)*

23.3. **Turvatoimet**

23.3.1. *Turva-alueet*

23.3.2. *Kulkuluvat*

23.3.3. *Kuvan- ja äänentallennuslaitteiston tarkastaminen*

23.3.4. *Salkkujen, kannettavien tietokoneiden ja pakettien tarkastus*

23.3.5. *Tekninen suojaus*

▼B

23.3.6. *Valtuuskuntien asiakirjat*

23.3.7. *Asiakirjojen säilyttäminen turvallisessa paikassa*

23.3.8. *Tilojen tarkastus*

23.3.9. *EU:n turvaluokiteltujen asiakirjojen hävittäminen*

24 EU:N TURVALUOKITELLUN TIEDON TURVALLISUUDEN RIKKOMINEN JA VAARANTAMINEN

24.1. **Määritelmät**

24.2. **Turvallisuuden vaarantumisesta raportoiminen**

24.3. **Oikeustoimet**

25 TIETO- JA TIETOLIIKENNEJÄRJESTELMISSÄ KÄSITELTÄVÄN EU:N TURVALUOKITELLUN TIEDON SUOJAUS

25.1. **Johdanto**

25.1.1. *Yleistä*

25.1.2. *Järjestelmiin kohdistuvat uhat ja järjestelmien haavoittuvuus*

25.1.3. *Turvatoimien päätarkoitus*

25.1.4. *Järjestelmäkohtainen turvavaatimusilmoitus (SSRS)*

25.1.5. *Turvallisuuden takaavat toimintatavat*

25.2. **Määritelmät**

25.3. **Turvallisuusvastuut**

25.3.1. *Yleistä*

25.3.2. *Turvallisuusjärjestelyt hyväksyvä viranomainen (SAA)*

25.3.3. *Tietoturvaviranomainen (IA)*

25.3.4. *Tekninen järjestelmävastaava (TSO)*

25.3.5. *Sisältövastaava (IO)*

25.3.6. *Käyttäjät*

25.3.7. *Tietoturvaa koskeva koulutus*

25.4. **Muut kuin tekniset turvatoimet**

25.4.1. *Henkilöstön luotettavuus*

25.4.2. *Fyysinen turvallisuus*

25.4.3. *Järjestelmän käytön valvonta*

25.5. **Tekniset turvatoimet**

25.5.1. *Tietoturva*

25.5.2. *Tietojen valvonta ja tilivelvollisuus tiedoista*

25.5.3. *Siirrettävien tietovälineiden käsittely ja valvonta*

25.5.4. *Tietovälineiden luokituksen poistaminen ja tietovälineiden tuhoaminen*

25.5.5. *Tietoliikenneturvallisuus*

25.5.6. *Turvallisuus asennuksen yhteydessä ja säteilyturvallisuus*

25.6. **Turvallisuus käsittelyn aikana**

25.6.1. *Turvallisuusmenettelyt (SecOP:t)*

▼B

25.6.2. *Ohjelmistojen suojaus / konfiguraation hallinta*

25.6.3. *Tuhoisien ohjelmisto- tai tietokonevirusten tarkistaminen*

25.6.4. *Huolto*

25.7. **Hankinnat**

25.7.1. *Yleistä*

25.7.2. *Hyväksyminen*

25.7.3. *Arviointi ja varmentaminen*

25.7.4. *Turvallisuusominaisuuksien rutiinitarkastukset pysyvää hyväksymistä varten*

25.8. **Tilapäinen tai satunnainen käyttö**

25.8.1. *Mikrotietokoneiden tai henkilökohtaisten tietokoneiden suojaus*

25.8.2. *Yksityisen atk-laitteiston käyttö komission virallisessa työskentelyssä*

25.8.3. *Sopimuspuolten omistamien tai jäsenvaltioiden toimittamien atk-laitteiden käyttö komission virallisessa työskentelyssä*

26 EU:N TURVALUOKITELLUN AINEISTON LUOVUTTAMINEN YHTEISÖN ULKOPUOLISILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE

26.1.1. *EU:n turvaluokitellun tiedon luovuttamista koskevat periaatteet*

26.1.2. *Tasot*

26.1.3. *Turvallisuussopimukset*

LISÄYS 1: KANSALLISTEN TURVALLISUUSLUOKITUSTEN VERTAILU

LISÄYS 2: LUOKITTELUOHJEET

LISÄYS 3: OHJEET EU:N TURVALUOKITELLUN TIEDON LUOVUTTAMISESTA YHTEISÖN ULKOPUOLISILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE: 1 TASON YHTEISTYÖ

LISÄYS 4: OHJEET EU:N TURVALUOKITELLUN TIEDON LUOVUTTAMISESTA YHTEISÖN ULKOPUOLISILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE: 2 TASON YHTEISTYÖ

LISÄYS 5: OHJEET EU:N TURVALUOKITELLUN TIEDON LUOVUTTAMISESTA YHTEISÖN ULKOPUOLISILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE: 3 TASON YHTEISTYÖ

LISÄYS 6: LYHENNELUETTELO

▼B

I OSA: TURVALLISUUTTA KOSKEVAT PERUSPERIAATTEET JA VÄHIMMÄISVAATIMUKSET

1. JOHDANTO

Näillä säännöksillä säädetään niistä turvallisuutta koskevista perusperiaatteista ja vähimmäisvaatimuksista, joita kaikissa komission työpaikoissa on noudatettava asianmukaisella tavalla ja joita kaikkien EU:n turvaluokitellun tiedon vastaanottajien on noudatettava, jotta turvallisuus on taattu ja voidaan olla vakuuttuneita siitä, että yhteiset suojausvaatimukset on vahvistettu.

2. YLEISET PERIAATTEET

Komission turvallisuuspolitiikka on olennainen osa komission yleistä sisäistä hallintopolitiikkaa, ja se pohjautuu näin ollen komission yleistä politiikkaa koskeviin periaatteisiin.

Näihin periaatteisiin kuuluvat laillisuus, avoimuus, tilintekovelvollisuus ja toissijaisuus (suhteellisuus).

Laillisuus merkitsee tarvetta pitäytyä tiukasti oikeudellisessa kehyksessä turvallisuustoimia toteutettaessa ja tarvetta noudattaa oikeudellisia vaatimuksia. Se merkitsee myös sitä, että turvallisuusalalla vastuun on perustuttava asianmukaisiin oikeudellisiin säännöksiin. Henkilöstösääntöjen säännöksiä sovelletaan kokonaisuudessaan ja erityisesti sovelletaan henkilöstösääntöjen 17 artiklaa, joka koskee henkilöstön velvollisuutta toimia harkitsevaisesti komissioon liittyvän tiedon suhteen, ja kurinpitomenettelyä koskevaa VI osastoa. Laillisuus merkitsee myös sitä, että komission vastuulle tulevaa turvallisuuden vaarantamista on käsiteltävä johdonmukaisesti kurinpitomenettelyä koskevan komission politiikan kanssa ja yhteistyötä jäsenvaltioiden kanssa rikosoikeuden alalla koskevan komission politiikan kanssa.

Avoimuus merkitsee, että kaikkien turvallisuutta koskevien sääntöjen ja säännösten on oltava selkeitä, eri yksiköiden ja alojen on oltava tasapainossa (fyysinen turvallisuus vs. tietojen suojaaminen jne.) ja turvatietoisuuspolitiikan on oltava johdonmukaista ja jäsentynyttä. Turvatoimien toteuttamisesta tarvitaan myös selkeitä kirjallisia ohjeita.

Tilintekovelvollisuus merkitsee, että turvallisuusalan vastuualueet määritellään selkeästi. Lisäksi se merkitsee tarvetta testata säännöllisesti, onko vastuu kannettu asianmukaisella tavalla.

Toissijaisuus tai suhteellisuus merkitsee, että turvallisuudesta huolehditaan alimmalla mahdollisella tasolla sekä mahdollisimman lähellä pääosastoja ja komission yksiköitä. Se merkitsee myös sitä, että turvallisuustoimet rajoitetaan ainoastaan niihin osa-alueisiin, joilla niitä todella tarvitaan. Se merkitsee myös sitä, että turvatoimien on oltava oikeassa suhteessa suojattaviin etuihin ja niihin kohdistuviin todellisiin tai mahdollisiin uhkiin. Näin puolustautuminen aiheuttaa kaikkein vähiten häiriöitä.

3. TURVALLISUUDEN PERUSTEET

Taattu turvallisuus perustuu seuraaviin seikkoihin:

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

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

   2) hallituksille ja sitä kautta komissiolle annetaan tietoa ja neuvoja turvallisuusuhkien luonteesta ja keinoista suojautua niitä vastaan.

b) Jokaisessa jäsenvaltiossa ja komissiossa on tekninen tietoturvaviranomainen (INFOSEC authority), jonka vastuulla on työskennellä turvallisuusviranomaisten kanssa tietojen ja neuvojen antamiseksi turvallisuutta uhkaavista teknisistä seikoista ja keinoista suojautua niitä vastaan.

c) Hallitusten yksiköt ja virastot sekä Euroopan unionin toimielinten asianomaiset yksiköt tekevät säännöllistä yhteistyötä, jotta päätettäisiin ja tarvittaessa suositeltaisiin,

   1) mitä henkilöitä, tietoja ja resursseja on suojeltava; ja

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

d) ►M2 Komission turvallisuudesta vastaavan linjan ◄ ja muiden Euroopan unionin toimielinten turvallisuusyksiköiden ja NATO:n turvallisuustoimiston (NOS) välinen tiivis yhteistyö.

▼B

4. TIETOTURVAN PERIAATTEET

4.1. **Tavoitteet**

Tietoturvan olennaisimmat tavoitteet ovat seuraavat:

a) EU:n turvaluokitellun tiedon suojaaminen vakoilulta, vaarantamiselta ja luvattomalta ilmitulolta;

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

c) komission toimitilojen, joissa EU:n tietoa säilytetään, suojaaminen sabotoinnilta ja tahalliselta vahingoittamiselta;

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

4.2. **Määritelmät**

Näissä säännöissä:

a) Ilmaisulla ’EU:n turvaluokiteltu tieto’ tarkoitetaan mitä tahansa tietoa tai aineistoa, jonka luvaton ilmitulo vahingoittaisi jollakin tavalla EU:n tai jonkin sen jäsenvaltion etuja riippumatta siitä, onko tällainen tieto peräisin EU:n sisältä vai onko se saatu jäsenvaltioilta, yhteisön ulkopuolisilta valtioilta vai kansainvälisiltä järjestöiltä.

b) Ilmaisulla ’asiakirja’ tarkoitetaan 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.

c) Ilmaisulla ’aineisto’ tarkoitetaan edellä b alakohdassa määriteltyä asiakirjaa sekä mitä tahansa joko tuotettua tai tuotannossa olevaa laitetta.

d) Ilmaisulla ’tiedonsaantitarve’ tarkoitetaan yksittäisen työntekijän tarvetta päästä tutustumaan EU:n turvaluokiteltuun tietoon jonkin toimen tai tehtävän hoitamiseksi.

e) ’Valtuutuksella’ tarkoitetaan ►**M2** komission turvallisuudesta vastaavan linjan johtajan ◄ päätöstä myöntää yksittäiselle henkilölle oikeus tutustua EU:n turvaluokiteltuun tietoon tiettyyn tasoon saakka kansallisten turvallisuusviranomaisten kansallisen lainsäädännön nojalla tekemän luotettavuusselvityksen antaman myönteisen tuloksen perusteella.

f) Ilmaisulla ’turvaluokitus’ tarkoitetaan tarkoituksenmukaisen turvallisuustason määrittämistä tiedoille, joiden luvaton ilmitulo saattaisi haitata komission tai jäsenvaltioiden etuja.

g) Ilmaisulla ’turvaluokan alentaminen’ (downgrading) tarkoitetaan salassapitotason alentamisesta johtuvaa luokan muuttamista.

h) Ilmaisulla ’turvaluokan poistaminen’ (declassification) tarkoitetaan minkä tahansa turvaluokan poistamista.

i) Ilmaisulla ’luovuttaja’ tarkoitetaan turvaluokitellun asiakirjan asianmukaisesti hyväksyttyä kirjoittajaa. Komission yksiköiden päälliköt voivat sallia henkilöstönsä kirjoittavan EU:n turvaluokiteltua tietoa.

j) Ilmaisulla ’komission yksiköt’ tarkoitetaan kaikkia komission eritasoisia toimija palveluyksiköitä, myös komission jäsenten kabinetteja, kaikissa toimipaikoissa, mukaan luettuna Yhteinen tutkimuskeskus, unionin alueella sijaitsevat edustustot ja toimistot sekä yhteisön ulkopuolisissa maissa toimivat lähetystöt.

4.3. **Turvaluokitus**

a) 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 yli- ja aliluokituksen välttämiseksi.

b) Nämä periaatteet voidaan toteuttaa turvaluokittelujärjestelmällä: suunniteltaessa ja järjestettäessä toimia vakoilun, sabotoinnin, terrorismin ja muiden uhkien torjumiseksi on noudatettava vastaavaa luokittelujärjestelmää, jotta tärkeimpiä toimitiloja, joissa turvaluokiteltua tietoa säilytetään, ja näiden tilojen herkimpiä alueita suojeltaisiin tehokkaimmin.

c) Tietojen luovuttaja vastaa yksinomaisesti tietojen luokittelusta.

d) Turvaluokituksen taso saa perustua yksinomaan tietojen sisältöön.

▼B

e) Jos tietoja ryhmitellään yhteen, kokonaisuuteen sovelletaan yksittäisten tietojen vaatimaa korkeinta turvaluokitusta. Tietokokonaisuudelle voidaan kuitenkin antaa korkeampi turvaluokitus kuin sen yksittäisille osille.

f) Turvaluokitus annetaan vain tarvittaessa ja tarvittavan pitkäksi aikaa.

4.4. **Turvatoimien tavoitteet**

Turvatoimet/turvatoimilla

a) koskevat kaikkia, joilla on pääsy turvaluokiteltuun tietoon, turvaluokiteltua tietoa sisältäviin tietovälineisiin, kaikkiin toimitiloihin, joissa tällaisia tietoja säilytetään, ja tärkeisiin laitteisiin;

b) on suunniteltava niin, että niiden avulla voidaan paljastaa ja vapauttaa tehtävistään tai siirtää muihin tehtäviin henkilöt, joiden aseman vuoksi turvaluokitellun tiedon ja laitteiden, joissa sitä säilytetään, turvallisuus voisi vaarantua;

c) on estettävä luvaton pääsy turvaluokiteltuun tietoon ja laitteisiin, joissa sitä säilytetään;

d) on varmistettava se, että turvaluokiteltua tietoa levitetään ainoastaan tiedonsaantitarpeen periaatteen pohjalta: tämä on olennaista kaikkien turvallisuusnäkökohtien kannalta;

e) 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 turvaluokiteltuja vai eivät. Tämä koskee erityisesti sähkömagneettisesti säilytettäviä, käsiteltäviä tai lähetettäviä tietoja.

5. TURVALLISUUSJÄRJESTELYT

5.1. **Yhteiset vähimmäisvaatimukset**

Komissio varmistaa, että kaikki EU:n turvaluokitellun tiedon vastaanottajat, jotka toimivat toimielimessä tai sen valtuuttamina, eli kaikki osastot ja toimeksisaajat noudattavat turvallisuutta koskevia yhteisiä vähimmäisvaatimuksia, jotta voidaan luottaa siihen, että EU:n turvaluokiteltua tietoa käsitellään kaikkialla yhtä huolellisesti. Vähimmäisvaatimuksiin on kuuluttava arviointiperusteet henkilöstön luotettavuuden selvittämiseksi ja menettelyt EU:n turvaluokitellun tiedon suojaamiseksi.

Komissio antaa ulkopuolisille elimille pääsyn EU:n turvaluokiteltuun tietoon ainoastaan sillä edellytyksellä, että ne varmistavat, että EU:n turvaluokiteltua tietoa käsiteltäessä noudatetaan ainakin vähimmäisvaatimuksia ehdottomasti vastaavia säännöksiä.

▼M3

Tällaisia vähimmäisvaatimuksia on sovellettava myös silloin, kun komissio antaa sopimuksella tai tukisopimuksella yrityksille tai muille yksiköille tehtäviä, joihin liittyy ja/tai jotka sisältävät EU:n turvaluokitellun tiedon käsittelyä; nämä yhteiset vähimmäisvaatimukset sisältyvät II osan 27 jaksoon.

▼B

5.2. **Järjestelyt**

Turvallisuudesta huolehditaan komissiossa kahdella eri tasolla:

a) Koko komission tasolla toimii ►M2 komission turvallisuudesta vastaava linja ◄, johon sijoittuu turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) (SAA toimii myös salausasioista vastaavana viranomaisena (Crypto Authority eli CrA) ja TEMPEST-viranomaisena), tietoturvaviranomainen (INFOSEC Authority eli IA) sekä yksi tai useampi EU:n turvaluokitellun tiedon keskusrekisteri (Central EUCI Registries), jossa puolestaan toimii yksi tai useampi rekisterin valvontavastaava (Registry Control Officer eli RCO).

b) Komission yksiköissä turvallisuudesta vastaavat yksi tai useampi paikallinen turvavastaava (Local Security Officers eli LSO), yksi tai useampi keskustietojärjestelmien tietoturvavastaava (Central Information Security Officer eli CISO), paikallistietojärjestelmien tietoturvavastaava (Local Informatics Security Officer eli LISO) ja EU:n turvaluokitellun tiedon paikallisrekisterit (Local EU Classified Information Registries), joissa toimii yksi tai useampi rekisterin valvontavastaava.

c) Turvallisuusalan keskuselimet antavat ohjeistusta kyseisen alan paikalliselimille.

▼B

6. HENKILÖSTÖN LUOTETTAVUUS

6.1. **Henkilöstön luotettavuuden selvittäminen**

Kaikkien, jotka pyytävät saada ►M1 CONFIDENTIEL UE ◄ -turvaluokan 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 turvaluokiteltua tietoa 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 sellainen, että hänen käsiteltäväkseen voidaan epäilyksettä uskoa turvaluokiteltua tietoa; tai

c) hän saattaa olla altis ulkoiselle tai muista lähteistä peräisin olevalle painostukselle.

Erityisen perusteellisesti on tarkastettava sellaisten henkilöiden luotettavuus,

d) joille on tarkoitus sallia pääsy ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoihin;

e) jotka ovat sellaisessa asemassa, että heidän tehtäviinsä kuuluu päästä säännöllisesti huomattavaan määrään ►M1 SECRET UE ◄ -turvaluokan tietoja;

f) joilla on tehtäviensä vuoksi oikeus päästä turvattuihin 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.

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

6.2. **Luotettavuusselvitysrekisteri**

Kaikkien komission yksiköiden, joissa käsitellään EU:n turvaluokiteltua tietoa tai joissa käytetään turvattuja tieto- ja tietoliikennejärjestelmiä, on pidettävä rekisteriä palvelukseen otetun henkilöstön luotettavuusselvityksistä. Luotettavuusselvitys on tarvittaessa tarkistettava sen varmistamiseksi, että se on kyseisen henkilön kulloistenkin tehtävien kannalta riittävä. Luotettavuusselvitys on tarkistettava uudelleen ensisijaisen kiireellisesti, jos saadaan uusia tietoja, joiden mukaan henkilön työskentely turvaluokitellun tiedon parissa ei enää ole turvallisuusetujen mukaista. Komission yksikön paikallinen turvavastaava pitää kirjaa alaansa kuuluvista luotettavuusselvityksistä.

6.3. **Henkilöstölle annettavat turvallisuusohjeet**

Henkilöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voisivat päästä turvaluokiteltuun tietoon, on annettava heti aluksi ja säännöllisin väliajoin tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyistä. Tällaisen henkilöstön on vakuutettava kirjallisesti, että he ovat lukeneet turvallisuussäännökset ja ymmärtävät ne täysin.

6.4. **Johdon velvollisuudet**

Johdon velvollisuus on tietää, ketkä kyseisen johdon alaisuudessa olevasta henkilöstöstä työskentelevät turvaluokitellun tiedon parissa tai voivat päästä turvattuihin tieto- ja tietoliikennejärjestelmiin, ja johdon on pidettävä kirjaa ja raportoitava kaikista tapahtumista tai ilmeisistä puutteista, jotka voivat vaikuttaa turvallisuuteen.

6.5. **Henkilöstön oikeudellinen asema turvallisuusasioissa**

On otettava käyttöön menettelyt sen varmistamiseksi, että henkilöä koskevien kielteisten seikkojen tullessa ilmi määritellään, onko hän tekemisissä turvaluokitellun tiedon kanssa tai sallitaanko hänen päästä turvattuihin tieto- ja tietoliikennejärjestelmiin ja onko ►M2 komission turvallisuudesta vastaavalle linjalle ◄ ilmoitettu asiasta. Jos henkilön todetaan olevan turvallisuusriski, häntä on estettävä suorittamasta tehtäviä, joissa hän voi vaarantaa turvallisuuden, tai hänet on siirrettävä suorittamaan muita tehtäviä.

7. FYYSINEN TURVALLISUUS

7.1. **Suojauksen tarve**

EU:n turvaluokitellun tiedon suojaamiseksi sovellettavien fyysisten turvatoimien taso on suhteutettava säilytettävän tiedon ja aineiston turvaluokkaan, määrään ja uhkaan. Kaikkien EU:n turvaluokiteltua tietoa hallussaan pitävien on noudatettava

▼B

yhdenmukaista käytäntöä tietojen luokittelun osalta ja yhteisiä suojausstandardeja suojausta edellyttävän tiedon ja aineiston säilyttämisen, siirron ja levittämisen osalta.

7.2. **Tarkastukset**

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

7.3. **Kiinteistöjen turvallisuus**

Kiinteistöt, joissa on EU:n turvaluokiteltua tietoa tai turvattuja tieto- ja tietoliikennejärjestelmiä, on suojeltava, jottei niihin pääse luvatta. Suojellaanko EU:n turvaluokiteltua tietoa esimerkiksi varustamalla sen säilytystilojen 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 kyseisen tiedon ja aineiston turvalliselta säilytyspaikalta edellytetään; ja

c) itse kiinteistön fyysisistä ominaisuuksista ja sijainnista.

Myös tieto- ja tietoliikennejärjestelmien suojauksen luonne määräytyy sen mukaan, kuinka tärkeinä tietoja pidetään ja kuinka pahoja vahinkoja turvallisuuden vaarantumisesta koituisi riippuen sen kiinteistön fyysisistä ominaisuuksista ja sijainnista, joissa järjestelmät ovat, ja järjestelmän sijainnista kiinteistössä.

7.4. **Varautumissuunnitelmat**

Turvaluokitellun tiedon suojauksesta paikallisen tai kansallisen hätätilan aikana on laadittava ennakkoon yksityiskohtaiset suunnitelmat.

8. TIETOTURVA

Tietoturva (Infosec) liittyy turvatoimien määrittämiseen ja soveltamiseen käsiteltävän, tallennettavan tai välitettävän EU:n turvaluokitellun tiedon suojaamiseksi tietoliikenne-, tieto- ja muissa sähköisissä järjestelmissä tahattomilta ja tahallisilta toimilta, jotta tietojen luotettavuus, eheys ja käytettävyys säilyvät. On toteutettava asiaan kuuluvia vastatoimia, jotta valtuuttamattomat käyttäjät eivät pääse EU:n turvaluokiteltuun tietoon ja jotta valtuutetuilta käyttäjiltä ei evätä siihen pääsyä ja jotta EU:n turvaluokiteltua tietoa ei turmella, luvatta muuteta tai poisteta.

9. SABOTOINNIN JA MUUNLAISEN TAHALLISEN VAHINGOITTAMISEN TORJUNTA

Turvaluokiteltua tietoa säilyttävien tärkeiden laitteiden suojelemiseksi toteutetut fyysiset varotoimet ovat paras suoja sabotointia ja muunlaista tahallista vahingoittamista vastaan, eikä niitä voi korvata tehokkaasti henkilöstön luotettavuuden selvittämisellä. Toimivaltaista kansallista elintä pyydetään toimittamaan tietoja vakoilusta, sabotoinnista, terrorismista ja muusta haitallisesta toiminnasta.

10. TURVALUOKITELLUN TIEDON LUOVUTTAMINEN YHTEISÖN ULKOPUOLISILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE

Komission kollegio tekee päätöksen komissiossa pidettävän EU:n turvaluokitellun tiedon luovuttamisesta yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille. Jos luovutettavaksi haluttujen tietojen alkuperäinen luovuttaja ei ole komissio, komission on ensin saatava luovuttajan suostumus luovutukselle. Jos luovuttajaa ei tiedetä, komissio ottaa luovuttajan vastuun itselleen.

Jos komissio vastaanottaa turvaluokiteltua tietoa yhteisön ulkopuolisilta valtioilta, kansainvälisiltä järjestöiltä tai muilta kolmansilta osapuolilta, tiedot on suojattava niiden turvaluokkaa ja näissä säännöksissä vahvistettuja EU:n turvaluokiteltua tietoa koskevia vaatimuksia vastaavalla tavalla, tai sellaisia tätä tiukempia vaatimuksia vastaavalla tavalla, joita tiedot luovuttava kolmas osapuoli saattaa edellyttää. Keskinäiset tarkastukset ovat mahdollisia.

Edellä esitetyt periaatteet on pantava täytäntöön II osassa olevassa 26 jaksossa ja lisäyksissä 3, 4 ja 5 esitettyjen yksityiskohtaisten säännösten mukaisesti.

II OSA: TURVALLISUUSJÄRJESTELYT KOMISSIOSSA

▼B

11. TURVALLISUUSASIOISTA VASTAAVA KOMISSION JÄSEN

Turvallisuusasioista vastaava komission jäsen

a) toteuttaa komission turvallisuuspolitiikkaa;

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

c) käsittelee tiiviissä yhteistyössä jäsenvaltioiden kansallisten turvallisuusviranomaisten (tai muiden asiaan kuuluvien viranomaisten) kanssa komission turvallisuuspolitiikan muuttamiseen liittyviä kysymyksiä.

Turvallisuusasioista vastaavan komission jäsenen vastuulla on erityisesti

a) koordinoida kaikkia komission toimintoihin liittyviä turvallisuusasioita;

b) osoittaa jäsenvaltioiden nimetyille turvallisuusviranomaisille pyyntö tehdä luotettavuusselvitys komission palveluksessa olevista henkilöistä 20 jakson mukaisesti;

c) tutkia tai määrätä tutkimaan jokainen sellainen EU:n turvaluokitellun tiedon vuoto, joka on alustavan näytön perusteella tapahtunut komissiossa;

d) pyytää asiaankuuluvia turvallisuusviranomaisia käynnistämään tutkinta, jos EU:n turvaluokiteltua tietoa on ilmeisesti vuotanut komission ulkopuolella, ja koordinoida tutkimuksia, jos asiaa käsittelee useampi turvallisuusviranomainen;

e) toteuttaa EU:n turvaluokitellun tiedon suojaamiseksi tehtyjen turvajärjestelyjen määräaikaistarkastuksia;

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

g) valvoa jatkuvasti komission turvallisuuspolitiikkaa ja -menettelyjä ja laatia pyynnöstä aiheellisia suosituksia. Turvallisuusasioista vastaava komission jäsen esittää tältä osin komissiolle ►**M2** komission turvallisuudesta vastaavan linjan ◄ laatiman vuotuisen tarkastussuunnitelman.

12. KOMISSION TURVALLISUUSASIOIDEN NEUVONANTAJARYHMÄ

On perustettava komission turvallisuusasioiden neuvonantajaryhmä. Se koostuu turvallisuusasioista vastaavasta komission jäsenestä tai hänen edustajastaan, joka toimii puheenjohtajana, sekä kunkin jäsenvaltion kansallisten turvallisuusviranomaisten edustajista. Muiden Euroopan unionin toimielinten edustajia voidaan myös kutsua. Myös asianomaisia EY:n ja EU:n erillisvirastojen edustajia voidaan kutsua ryhmän kokouksiin, jos niissä käsitellään niitä koskevia kysymyksiä.

Komission turvallisuusasioiden neuvonantajaryhmä kokoontuu sen puheenjohtajan tai kenen tahansa jäsenen pyynnöstä. Ryhmän tehtävänä on tarkastella ja arvioida kaikkia merkityksellisiä turvallisuusasioita ja esittää komissiolle tarvittaessa suosituksia.

▼M2

13. KOMISSION TURVALLISUUSLAUTAKUNTA

On perustettava komission turvallisuuslautakunta. Siihen kuuluvat henkilöstön ja hallinnon pääosaston pääjohtaja, joka toimii lautakunnan puheenjohtajana, yksi turvallisuusasioista vastaavan komission jäsenen kabinetin jäsen, yksi komission puheenjohtajan kabinetin jäsen, apulaispäällikkö, joka toimii komission kriisinhallintaryhmän puheenjohtajana, oikeudellisen yksikön, ulkosuhteiden pääosaston, oikeus-, vapaus- ja turvallisuusasioiden pääosaston, yhteisen tutkimuskeskuksen, tietotekniikan pääosaston ja sisäisen tarkastuksen toimialan pääjohtajat ja komission turvallisuudesta vastaavan linjan johtaja tai heidän edustajansa. Muita komission virkamiehiä voidaan kutsua kokouksiin. Lautakunnan tehtävänä on arvioida turvatoimia komissiossa ja antaa tämän alan suosituksia turvallisuusasioista vastaavalle komission jäsenelle.

▼B

14. ►**M2** KOMISSION TURVALLISUUDESTA VASTAAVA LINJA ◄

Täyttääkseen 11 jaksossa mainitut velvoitteensa turvallisuusasioista vastaavalla komission jäsenellä on oltava käytössään ►**M2** komission turvallisuudesta vastaava linja ◄ turvatoimien koordinoimiseksi, johtamiseksi ja täytäntöönpanemiseksi.

►**M2** Komission turvallisuudesta vastaavan linjan johtaja ◄ on turvallisuusasioista vastaavan komission jäsenen tärkein neuvonantaja turvallisuusasioissa, ja hän toimii turvallisuusasioiden neuvonantajaryhmän sihteerinä. Hän johtaa turvallisuussääntöjen ajan tasalle saattamista ja koordinoi turvatoimia jäsenvaltioiden

▼B

toimivaltaisten viranomaisten kanssa ja tarvittaessa turvallisuussopimusten kautta komission kanssa yhteydessä olevien kansainvälisten järjestöjen kanssa. Tältä osin hän toimii yhteyshenkilönä.

►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ vastaa komissioon hankittavien tietojärjestelmien ja -verkkojen hyväksymisestä. ►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ päättää yhdessä jäsenvaltioiden asianomaisten kansallisten turvallisuusviranomaisten kanssa sellaisten tietojärjestelmien ja -verkkojen hyväksymisestä, jotka koskevat komissiota ja EU:n turvaluokitellun tiedon muita vastaanottajia.

15. TURVALLISUUSTARKASTUKSET

►M2 Komission turvallisuudesta vastaava linja ◄ toteuttaa EU:n turvaluokitellun tiedon suojaamiseksi tehtyjen turvajärjestelyjen määräaikaistarkastuksia.

►M2 Komission turvallisuudesta vastaavaa linjaa ◄ voivat avustaa näissä tehtävissä EU:n turvaluokiteltua tietoa hallussaan pitävien muiden Euroopan unionin toimielinten turvallisuusyksiköt ja jäsenvaltioiden kansalliset turvallisuusviranomaiset ([1]).

Jäsenvaltion pyynnöstä jäsenvaltion kansalliset viranomaiset voivat tarkastaa EU:n turvaluokiteltua tietoa komission sisällä yhdessä ►M2 komission turvallisuudesta vastaavan linjan ◄ kanssa yhteisestä sopimuksesta.

16. TURVALUOKAT, -OSOITTIMET JA -MERKINNÄT

16.1. **Luokitteluasteet** ([2])

Tiedot jaetaan seuraaviin turvaluokkiin (ks. myös lisäys 2):

►M1 TRES 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.

►M1 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.

►M1 CONFIDENTIEL UE ◄: Tätä turvaluokkaa sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo saattaisi haitata Euroopan unionin tai sen yhden tai useamman jäsenvaltion etuja.

►M1 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.

Muita turvaluokkia ei sallita.

16.2. **Turvaosoittimet**

Turvaluokituksen kelpoisuuden rajaamiseksi (turvaluokitellun tiedon osalta tämä merkitsee turvaluokituksen automaattista alentamista tai poistamista) voidaan käyttää sovittua turvaosoitinta. Turvaosoitin on joko ”UNTIL … (aika/päivämäärä)” tai ”UNTIL … (tapahtuma)”.

Jos turvaluokittelun mukaisen käsittelyn lisäksi tarvitaan rajoitettua jakelua ja erityiskäsittelyä, käytetään muita turvaosoittimia, kuten CRYPTO, tai jotain muuta EU:ssa hyväksyttyä erityistä turvaosoitinta.

Turvaosoittimia voidaan käyttää ainoastaan jonkin turvaluokan kanssa.

16.3. **Merkinnät**

Asiakirjaan voidaan tehdä merkintä, jolla osoitetaan asiakirjan kattama ala tai tiedonsaantitarpeeseen perustuva erityisjakelu. Samoin muuhun kuin turvaluokiteltuun tietoon voidaan tehdä merkintä turvaluokitetun osuuden loppumisesta.

Merkintä ei ole turvaluokka, eikä sitä voida käyttää sellaisena.

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

16.4. **Turvaluokan merkintätapa**

Turvaluokka merkitään seuraavia merkintätapoja käyttäen:

([1]) Sanotun kuitenkaan rajoittamatta vuonna 1961 tehdyn diplomaattisia suhteita koskevan Wienin yleissopimuksen ja Euroopan yhteisöjen erioikeuksista ja vapauksista 8 päivänä huhtikuuta 1965 tehdyn pöytäkirjan soveltamista.

([2]) Ks. lisäyksessä 1 oleva EU:n, NATOn, WEU:n ja jäsenvaltioiden turvaluokittelua koskeva vertailutaulukko.

▼B

a) ►M1 RESTREINT UE ◄ -turvaluokan asiakirjoihin mekaanisesti tai sähköisesti;

b) ►M1 CONFIDENTIEL UE ◄ -turvaluokan asiakirjoihin mekaanisesti tai käsin tai painamalla asiakirja esileimatulle kirjatulle paperille;

c) ►M1 SECRET UE ◄- ja ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokkien asiakirjoihin mekaanisesti tai käsin.

16.5. **Turvaosoittimien merkintätapa**

Turvaosoittimet merkitään heti turvaluokan jälkeen samoilla menetelmillä kuin itse turvaluokat.

17. TURVALUOKITTELUN HALLINNOINTI

17.1. **Yleistä**

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

Tietojen luovuttaja vastaa yksin tietojen luokittelusta ja mahdollisesta myöhemmästä turvaluokan alentamisesta tai poistamisesta.

Komission virkamiehet ja muuhun henkilöstöön kuuluvat luokittelevat tiedot ja alentavat tai poistavat turvaluokan yksikkönsä päällikön ohjeiden mukaan tai hänen suostumuksellaan.

Turvaluokiteltujen asiakirjojen käsittelyä koskevien yksityiskohtaisten menettelyjen vahvistamisella on pyritty varmistamaan, että asiakirjat suojataan niiden sisältämien tietojen edellyttämällä tavalla.

Niiden henkilöiden lukumäärä, joilla on oikeus laatia ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan asiakirjoja, on pidettävä mahdollisimman alhaisena ja heidän nimensä on pidettävä ►M2 komission turvallisuudesta vastaavan linjan ◄ laatimassa luettelossa.

17.2. **Turvaluokituksen soveltaminen**

Asiakirjan turvaluokka on määriteltävä sen sisällön arkaluonteisuuden mukaan 16 jakson määritelmän mukaisesti. On tärkeää, että luokittelua käytetään oikein ja rajoitetusti. Tämä koskee erityisesti ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokkaa.

Luokiteltavaksi tarkoitetun asiakirjan luovuttajan on pidettävä mielessä edellä mainitut säännöt ja vältettävä yli- ja aliluokittelua.

Luokitteluohjeet ovat lisäyksessä 2.

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

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.

Asiakirjojen saamista yleisön tutustuttavaksi säännellään edelleen asetuksella (EY) N:o 1049/2001.

17.3. **Turvaluokan alentaminen ja poistaminen**

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 luovuttajan on ilmoitettava vastaanottajille muutoksesta, ja näiden on puolestaan ilmoitettava muutoksesta kaikille myöhemmille vastaanottajille, joille he ovat lähettäneet asiakirjan tai sen kopion.

Mahdollisuuksien mukaan asiakirjan luovuttajat ilmoittavat turvaluokitellussa asiakirjassa päivämäärän, ajanjakson tai tapahtuman, jonka jälkeen asiakirjan sisällön turvaluokka voidaan alentaa tai poistaa. Muussa tapauksessa he tarkistavat asiakirjan vähintään joka viides vuosi varmistaakseen, onko alkuperäinen luokitus tarpeellinen.

▼B

18. FYYSINEN TURVALLISUUS

18.1. **Yleistä**

Fyysisten turvatoimien pääasiallisena tavoitteena on estää sivullisten henkilöiden pääsy EU:n turvaluokiteltuun tietoon ja/tai aineistoon, estää välineiden ja muun omaisuuden varkaudet ja vaurioituminen sekä estää henkilöstöön, muihin työntekijöihin ja vierailijoihin kohdistuva häirintä ja kaikenlaiset muunlaiset vihamieliset reaktiot.

18.2. **Turvallisuutta koskevat vaatimukset**

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

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

a) tiedon ja/tai aineiston turvaluokittelu;

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.

Sovellettavilla fyysisillä turvatoimilla on pyrittävä:

a) epäämään tunkeutuminen salaa tai väkisin;

b) ehkäisemään, estämään ja havaitsemaan epärehellisten henkilöiden toimet;

c) estämään niiden, joilla ei ole tarvetta saada tietoja, pääsy EU:n turvaluokitettuun tietoon.

18.3. **Fyysiset turvatoimet**

18.3.1. *Turva-alueet*

Alueiden, joissa ►**M1** CONFIDENTIEL UE ◄- turvaluokan tai sitä korkeamman turvaluokan tietoa käsitellään ja säilytetään, on oltava järjestelyiltään ja rakenteeltaan sellaisia, että ne vastaavat jotakin seuraavista:

a) Turvaluokan I turva-alue: alue, jossa ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan tietoa käsitellään tai säilytetään 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 että ulos on valvottua;

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

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

b) Turvaluokan II turva-alue: alue, jossa ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan tietoa käsitellään tai säilytetään siten, että tieto voidaan suojata sivullisilta sisäisesti asennetuin tarkastuksin, esim. tilat, joissa on yksiköitä, joissa ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tietoa käsitellään tai varastoidaan säännöllisesti. Tällaiselta alueelta edellytetään:

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

   ii) kulunvalvontajärjestelmää, joka sallii alueelle saattajatta 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.

18.3.2. *Hallinnollinen alue*

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 ►**M1** RESTREINT UE ◄ -turvaluokan tietoa ja turvaluokittelematonta tietoa voidaan käsitellä ja varastoida hallinnollisilla alueilla.

▼B

18.3.3. *Tulo- ja lähtötarkastukset*

Pääsyä turvaluokkien I ja II turva-alueille valvotaan kulkuluvin tai kaiken alueella tavallisesti työskentelevän henkilöstön osalta henkilökohtaisesti tunnistamalla. On myös luotava vierailijoiden tarkastamiseksi järjestelmä, 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 korkeassa asemassa olevien henkilöiden vierailuiden aikana.

18.3.4. *Vartiointikierrokset*

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.

18.3.5. *Turvalliset säilytyspaikat ja kassaholvit*

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

— Luokka A: kansallisesti ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tiedon varastoimiseen hyväksyttyjä säilytyspaikkoja turvaluokkien I ja II turva-alueilla,

— Luokka B: kansallisesti ►**M1** SECRET UE ◄- ja ►**M1** CONFIDENTIEL UE ◄ -turvaluokkien tiedon varastoimiseen hyväksyttyjä säilytyspaikkoja turvaluokkien I ja II turva-alueilla,

— Luokka C: ainoastaan ►**M1** RESTREINT UE ◄ -turvaluokan tiedon varastoimiseen soveltuvaa kalustoa.

Turvajärjestelyt hyväksyvän viranomaisen on varmennettava sellaisten turvaluokkien I ja II turva-alueille rakennettujen kassaholvien osalta ja turvaluokan I turva-alueiden, joissa ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan tietoa varastoidaan avoimille hyllyille tai pannaan näytteille taulukkoihin, karttoihin jne., osalta, että seinien, lattioiden, sisäkattojen, lukittavan oven tai lukittavien ovien suojaus on yhtäläinen saman turvaluokan tiedon varastoimiseen hyväksytyn turvallisen säilytyspaikan kanssa.

18.3.6. *Lukot*

Turvallisissa säilytyspaikoissa ja kassaholveissa, joissa EU:n turvaluokiteltavaa tietoa säilytetään, 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 kalustolle.

18.3.7. *Avainten ja yhdistelmien valvonta*

Turvallisten säilytyspaikkojen avaimia ei saa viedä pois komission kiinteistöistä. Valtuutuksen saaneet henkilöt opettelevat ulkoa turvallisten säilytyspaikkojen numeroyhdistelmät. Hätätapauksia varten asianomaisen komission yksikön paikallinen turvavastaava 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.

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

a) uuden säilytyspaikan vastaanoton yhteydessä;

b) aina henkilöstön vaihtuessa;

c) aina vaaratilanteen tai sen epäilyksen ilmetessä;

d) mieluummin kuuden ja vähintään kahdentoista kuukauden välein.

18.3.8. *Tunkeutumisen havaitsemislaitteet*

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

▼B

18.3.9. *Hyväksytty laitteisto*

►M2 Komission turvallisuudesta vastaava linja ◄ ylläpitää ajan tasalla olevia luetteloita niiden suojauslaitteiden tyypeistä ja malleista, jotka se on hyväksynyt turvaluokitellun tiedon suojaamiseen vaihtelevissa erityisolosuhteissa ja erityisedellytysten mukaisesti. ►M2 Komission turvallisuudesta vastaava linja ◄ perustaa nämä luettelot muun muassa kansallisilta turvallisuusviranomaisilta saatuun tietoon.

18.3.10. *Kopio- ja faksilaitteiden fyysinen suojaus*

Kopio- ja faksilaitteet suojataan fyysisesti tarpeellisissa määrin sen varmistamiseksi, että vain valtuutetut henkilöt voivat käyttää niitä turvaluokitellun tiedon käsittelemiseksi ja että kaikki turvaluokitellut tuotteet ovat asianmukaisesti valvottuja.

18.4. **Suojautuminen salakatselulta ja salakuuntelulta**

18.4.1. *Salakatselu*

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

18.4.2. *Salakuuntelu*

Yksiköt ja alueet, joilla ►M1 SECRET UE ◄ -turvaluokan tai sitä korkeamman turvaluokan tiedosta keskustellaan säännöllisesti, suojataan tahatonta ja tahallista salakuunteluyritystä vastaan riskiarvioinnin niin vaatiessa. Tällaisten yritysten riskiarviointi on ►M2 komission turvallisuudesta vastaavan linjan ◄ vastuulla sen kuultua tarvittaessa kansallista turvallisuusviranomaista.

18.4.3. *Sähköisten laitteiden ja äänityslaitteiden tuominen*

Turva-alueille ja teknisesti suojatuille alueille ei saa tuoda matkapuhelimia, henkilökohtaisessa käytössä olevia tietokoneita, äänityslaitteita, kameroita tai muita sähköisiä laitteita tai äänityslaitteita ilman ►M2 komission turvallisuudesta vastaavan linjan johtajan ◄ lupaa.

Sen määrittämiseksi, millaisia suojaustoimenpiteitä on toteutettava tahattomalle salakuuntelulle (esim. seinien, ovien, lattioiden ja kattojen eristäminen, paljastavien virtauksien mittaus) tai tahalliselle salakuuntelulle (esim. mikrofonien etsintä) alttiissa tiloissa, ►M2 komission turvallisuudesta vastaava linja ◄ voi pyytää apua kansallisten turvallisuusviranomaisten asiantuntijoilta.

Samoin, olosuhteiden niin vaatiessa, kansallisten turvallisuusviranomaisten tekniset turvallisuusasiantuntijat voivat ►M2 komission turvallisuudesta vastaavan linjan johtajan ◄ pyynnöstä tarkastaa telelaitteet ja kaikki sähköiset tai elektroniset toimistolaitteet, joita käytetään ►M1 SECRET UE ◄ -turvaluokan tai sitä korkeamman turvaluokan kokouksissa.

18.5. **Teknisesti suojatut alueet**

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.

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, ettei teknisesti suojatuille alueille saa asentaa tietoliikenneyhteyksiä ilman asianmukaisen viranomaisen antamaa ennakkolupaa.

19. TIEDONSAANTITARPEEN PERIAATETTA JA EU:N HENKILÖSTÖN LUOTETTAVUUSSELVITYSTÄ KOSKEVAT YLEISET SÄÄNNÖT

19.1. **Yleistä**

Pääsy EU:n turvaluokiteltuun tietoon myönnetään vain henkilöille, joiden on tarpeen saada tällaista tietoa voidakseen suorittaa velvollisuutensa tai tehtävänsä. Pääsy ►M1 TRES SECRET UE/EU TOP SECRET ◄-, ►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -turvaluokan tietoon myönnetään vain henkilöille, joille on tehty asianmukainen luotettavuusselvitys.

Vastuu tiedonsaantitarpeen määrittämisestä on yksiköllä, johon kyseinen henkilö aiotaan palkata.

Henkilöstön luotettavuusselvitystä koskevasta pyynnöstä vastaa kukin yksikkö.

▼B

Tämän jälkeen myönnetään ”EU:n henkilöstön luotettavuustodistus”, josta ilmenee sen turvaluokitellun tiedon turvaluokka, johon luotettavuusselvityksen läpikäynyt henkilö valtuutetaan pääsemään, sekä valtuutuksen päättymispäivä.

Tiettyä turvaluokkaa koskeva EU:n henkilöstön luotettavuustodistus voi antaa haltijalle valtuutuksen päästä alemman turvaluokan tietoon.

Muilla henkilöillä kuin virkamiehillä tai muulla henkilöstöllä, kuten ulkopuolisilla toimeksisaajilla, asiantuntijoilla tai konsulteilla, 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 EU:n henkilöstön luotettavuustodistus ja heille on selvitettävä heidän turvallisuusvastuunsa.

Yleisön oikeudesta saada tietoa säädetään asetuksessa (EY) N:o 1049/2001.

19.2. ►M1 **TRES SECRET UE/EU TOP SECRET** ◄ **-turvaluokan tietoon pääsyä koskevat erityissäännöt**

Kaikki henkilöt, joiden on päästävä ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoon, on ennen tällaiseen tietoon pääsyä seulottava.

Turvallisuusasioista vastaava komission jäsen nimittää kaikki henkilöt, joiden on päästävä ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoon, ja heidän nimensä merkitään asianmukaiseen ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisteriin.►M2 Komission turvallisuudesta vastaava linja ◄ perustaa tämän rekisterin ja ylläpitää sitä.

Ennen ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoon pääsyä kaikkien henkilöiden on allekirjoitettava todistus siitä, että heille on selvitetty komission turvallisuusmenettelyt ja että he ymmärtävät täysin erityisen velvollisuutensa suojata ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tiedon sekä EU:n säännöissä ja kansallisessa lainsäädännössä tai hallinnollisissa säännöissä vahvistetut seuraamukset turvaluokitellun tiedon joutumisesta sivullisille joko tarkoituksellisesti tai laiminlyönnin seurauksena.

►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoon pääsyyn oikeutettujen henkilöiden osallistuessa kokouksiin tai muihin vastaaviin tilaisuuksiin sen yksikön tai elimen, jossa kyseinen henkilö työskentelee, toimivaltainen valvontavastaava ilmoittaa kokouksen järjestävälle elimelle, onko kyseisille henkilöille myönnetty tällainen valtuutus.

Kaikkien niiden henkilöiden, jotka eivät enää työskentele ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoon pääsyä edellyttävissä tehtävissä, nimet poistetaan ►M1 TRES SECRET UE/EU TOP SECRET ◄ -luettelosta. Lisäksi kaikkia tällaisia henkilöitä muistutetaan uudelleen erityisestä velvollisuudestaan suojata ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tiedot. He allekirjoittavat myös vakuutuksen siitä, että he eivät käytä tai välitä eteenpäin hallussaan olevaa ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoa.

19.3. ►M1 **SECRET UE** ◄**- ja** ►M1 **CONFIDENTIEL UE** ◄ **-turvaluokan tietoon pääsyä koskevat erityissäännöt**

Kaikki henkilöt, joiden on päästävä ►M1 SECRET UE ◄- tai ►M1 CONFIDENTIEL UE ◄ -turvaluokan tietoon, on ensin seulottava asianmukaisen turvaluokan mukaisesti.

Kaikille henkilöille, joiden on päästävä ►M1 SECRET UE ◄- tai ►M1 CONFIDENTIEL UE ◄ -turvaluokan tietoon, on selvitettävä asianmukaiset turvallisuussäännökset ja heidän on oltava tietoisia laiminlyönnin seuraamuksista.

►M1 SECRET UE ◄- tai ►M1 CONFIDENTIEL UE ◄ -turvaluokan tietoon pääsyyn oikeutettujen henkilöiden osallistuessa kokouksiin tai muihin vastaaviin tilaisuuksiin sen elimen, jossa kyseinen henkilö työskentelee, turvavastaava ilmoittaa kokouksen järjestävälle elimelle, onko kyseisille henkilöille myönnetty tällainen valtuutus.

19.4. ►M1 **RESTREINT UE** ◄ **-turvaluokan tietoon pääsyä koskevat erityissäännöt**

Henkilöille, joilla on pääsy ►M1 RESTREINT UE ◄ -turvaluokan tietoon, selvitetään turvallisuussäännöt ja laiminlyönnin seuraamukset.

19.5. **Henkilösiirrot**

Kun henkilöstön jäsen siirretään pois tehtävästä, joka edellyttää EU:n turvaluokitellun aineiston käsittelyä, rekisterinpitäjä valvoo, että kyseinen aineisto siirretään asianmukaisesti lähtevältä virkamieheltä saapuvalle virkamiehelle.

Kun henkilöstön jäsen siirretään toiseen tehtävään, joka edellyttää EU:n turvaluokitellun aineiston käsittelyä, paikallinen turvavastaava antaa hänelle tarvittavat selvitykset.

▼B

19.6. **Erityisohjeet**

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

a) harkitsemattoman keskustelun aiheuttamat turvallisuusriskit;

b) käytettävät varotoimet suhteessa tiedotusvälineisiin ja eturyhmien edustajiin;

c) tiedustelupalvelujen Euroopan unioniin 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 vakoilua.

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

Komissiolla ei ole turvallisuussäännöksiä EU:n turvaluokiteltuun tietoon pääsyyn oikeutettujen henkilöiden yksityisen matkustamisen osalta mihinkään kohteeseen. ►**M2** Komission turvallisuudesta vastaava linja ◄ selvittää kuitenkin vastuualueeseensa kuuluville virkamiehille ja muulle henkilöstölle matkustussäännökset, joita heihin saatetaan soveltaa.

20. KOMISSION VIRKAMIESTEN JA MUUN HENKILÖSTÖN LUOTETTAVUUSSELVITYSMENETTELY

a) Komission hallussa olevaa turvaluokiteltua tietoa saavat ainoastaan ne komission virkamiehet ja muu henkilöstö tai muut komissiossa työskentelevät henkilöt, joiden on tehtäviensä ja yksikön tarpeiden vuoksi saatava tutustua niihin tai voitava käsitellä niitä.

b) Saadakseen ►**M1** TRES SECRET UE/EU TOP SECRET ◄-, ►**M1** SECRET UE ◄- ja ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tietoja a kohdassa tarkoitetuilla henkilöillä on oltava tämän jakson c ja d kohdassa tarkoitetun menettelyn mukaisesti annettu valtuutus.

c) Valtuutus annetaan ainoastaan henkilöille, joista jäsenvaltioiden toimivaltaiset kansalliset viranomaiset (kansalliset turvallisuusviranomaiset) ovat tehneet luotettavuusselvityksen i—n kohdassa tarkoitetun menettelyn mukaisesti.

d) ►**M2** Komission turvallisuudesta vastaavan linjan johtaja ◄ vastaa a, b ja c kohdassa tarkoitettujen valtuutusten myöntämisestä.

e) Päällikkö myöntää valtuutuksen saatuaan i—n kohdan mukaisesti suoritettuun luotettavuusselvitykseen perustuvan jäsenvaltioiden kansallisten toimivaltaisten viranomaisten lausunnon.

f) ►**M2** Komission turvallisuudesta vastaava linja ◄ pitää ajantasaista luetteloa komission eri yksiköiden kaikista arkaluontoisista tehtävistä ja henkilöistä, joille on myönnetty (väliaikainen) valtuutus.

g) Valtuutus on voimassa viisi vuotta, mutta ei kuitenkaan kauemmin kuin henkilö on tehtävissä, joiden perusteella valtuutus myönnettiin. Valtuutuksen voimassaoloa voidaan jatkaa e kohdassa säädettyä menettelyä noudattaen.

h) ►**M2** Komission turvallisuudesta vastaavan linjan johtaja ◄ voi peruuttaa valtuutuksen, jos hän katsoo siihen olevan perusteita. Päätös valtuutuksen peruuttamisesta ilmoitetaan kyseiselle henkilölle, joka voi pyytää, että ►**M2** komission turvallisuudesta vastaavan linjan johtaja ◄ kuulee häntä, sekä toimivaltaiselle kansalliselle viranomaiselle.

i) Luotettavuusselvitys tehdään ►**M2** komission turvallisuudesta vastaavan linjan johtajan ◄ pyynnöstä yhteistyössä kyseisen henkilön kanssa. Luotettavuusselvityksen tekevä toimivaltainen kansallinen viranomainen on jokin sen jäsenvaltion viranomaisista, jonka kansalainen kyseinen henkilö on. Kun kyseinen henkilö ei ole EU:n jäsenvaltion kansalainen, ►**M2** komission turvallisuudesta vastaavan linjan johtaja ◄ pyytää luotettavuusselvitystä siltä EU:n jäsenvaltiolta, jossa henkilön kotipaikka tai tavanomainen oleskelupaikka on.

j) Luotettavuusselvitystä varten kyseisen henkilön on täytettävä henkilötietolomake.

k) ►**M2** Komission turvallisuudesta vastaavan linjan johtaja ◄ yksilöi pyynnössään niiden tietojen tyypin ja turvaluokan, jotka kyseinen henkilö työssään saa tietoonsa, jotta toimivaltaiset kansalliset viranomaiset voivat tehdä luotettavuusselvityksen ja antaa lausunnon kyseiselle henkilölle annettavan valtuutuksen asianmukaista tasoa varten.

▼B

l) Luotettavuutta koskevan selvitysmenettelyn kaikkiin vaiheisiin ja tuloksiin sovelletaan kyseisessä jäsenvaltiossa voimassa olevia asiaa koskevia sääntöjä ja asetuksia mahdolliset muutoksenhakukeinot mukaan luettuina.

m) ►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ voi myöntää valtuutuksen kyseiselle henkilölle, jos jäsenvaltion toimivaltaiset kansalliset viranomaiset antavat myönteisen lausunnon.

n) Jos toimivaltaiset kansalliset viranomaiset antavat kielteisen lausunnon, kyseiselle henkilölle ilmoitetaan siitä ja hän voi pyytää, että ►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ kuulee häntä. ►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ voi tarvittaessa pyytää toimivaltaisia kansallisia viranomaisia antamaan tarkempia tietoja. Jos kielteinen lausunto vahvistetaan, valtuutusta ei voida myöntää.

o) Henkilöille, jotka ovat saaneet valtuutuksen d ja e kohdan mukaisesti, annetaan valtuutuksen myöntämisen yhteydessä ja tämän jälkeen määräajoin tarvittavat ohjeet turvaluokiteltujen tietojen suojaamisesta ja siitä, miten tämä varmistetaan. Nämä henkilöt allekirjoittavat vakuutuksen siitä, että he ovat saaneet ohjeet ja että he sitoutuvat noudattamaan niitä.

p) ►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ toteuttaa tarvittavat toimenpiteet tämän jakson säännösten täytäntöönpanemiseksi ja erityisesti ne toimenpiteet, joilla säännellään oikeutta tutustua valtuutuksen saaneista henkilöistä laadittuun luetteloon.

q) ►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ voi poikkeuksellisesti ja yksikön tarpeiden niin vaatiessa myöntää ennen i 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.

r) Tällä tavoin myönnetyt väliaikaiset valtuutukset eivät oikeuta saamaan ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoa; tällaisen tiedon saanti on rajoitettu virkamiehiin, joista on tehty i kohdan mukainen luotettavuusselvitys, jonka tulokset ovat olleet myönteiset. Ennen luotettavuusselvityksen tulosten saamista ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan luotettavuusselvitykseen määrätyille virkamiehille voidaan myöntää väliaikainen valtuutus saada ►M1 SECRET UE ◄- ja sitä alemman turvaluokan tietoa.

21. EU:n TURVALUOKITELTUJEN ASIAKIRJOJEN VALMISTELU, JAKELU JA LÄHETTÄMINEN, KURIIREIHIN SOVELLETTAVAT TURVATOIMET, YLIMÄÄRÄISET KOPIOT, KÄÄNNÖKSET JA OTTEET

21.1. **Valmistelu**

1. EU:n turvaluokituksia sovelletaan 16 jaksossa vahvistetulla tavalla. ►M1 CONFIDENTIEL UE ◄- ja sitä luottamuksellisempi turvaluokitus merkitään jokaisen sivun ylä- ja alareunan keskelle ja jokainen sivu numeroidaan. Jokaiseen EU:n turvaluokiteltuun asiakirjaan merkitään viitenumero ja päivämäärä. ►M1 TRES SECRET UE/EU TOP SECRET ◄- ja ►M1 SECRET UE ◄ -asiakirjoihin viitenumero merkitään jokaiselle sivulle. Jos asiakirjoja on jaossa useita kopioita, jokaiseen kopioon merkitään kopionumero ensimmäiselle sivulle asiakirjan sivumäärän lisäksi. Kaikki liitteet ja lisäykset luetellaan ►M1 CONFIDENTIEL UE ◄- ja sitä luottamuksellisemman turvaluokan asiakirjan ensimmäisellä sivulla.

2. ►M1 CONFIDENTIEL UE ◄- ja sitä luottamuksellisemman 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 turvaluokiteltuun tietoon.

3. Turvaluokiteltujen asiakirjojen tuottamista tietokoneella koskevat säännökset ovat 25 jaksossa.

21.2. **Jakelu**

1. EU:n turvaluokiteltua tietoa jaetaan vain henkilöille, joiden on tarpeen saada tällaista tietoa ja joille on tehty asianmukainen luotettavuusselvitys. Alkuperäisen jakelun määrittää tietojen luovuttaja.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjat kulkevat ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisterien kautta (katso 22.2 jakso). ►M1 TRES SECRET UE/EU TOP SECRET ◄ -viestien toimivaltainen rekisteri voi valtuuttaa viestintäkeskuksen päällikön ottamaan vastaanottajaluettelossa mainitun määrän kopioita.

3. Alkuperäinen vastaanottaja voi jakaa ►M1 SECRET UE ◄- ja sitä alemman turvaluokan asiakirjoja edelleen muille vastaanottajille tiedonsaantitarpeen periaatetta noudattaen. Tiedot luovuttaneiden viranomaisten on kuitenkin

▼B

annettava selkeästi tiedoksi mahdollisesti sovellettavat varoitukset. Jos tällaisia varoituksia sovelletaan, vastaanottajat voivat jakaa asiakirjoja edelleen vain tiedot luovuttaneiden viranomaisten valtuutuksella.

4. EU:n turvaluokitellun tiedon paikallisrekisterin yksiköt kirjaavat jokaisen ►M1 CONFIDENTIEL UE ◄- ja sitä luottamuksellisemman turvaluokan asiakirjan sen saapuessa pääosastoon tai yksikköön tai lähtiessä niistä. Asiakirjat on voitava tunnistaa kirjattavien tietojen (viitteet, päivämäärä ja tarvittaessa kopionumero) perusteella. Nämä tiedot merkitään päiväkirjaan tai tallennetaan erityiselle suojatulle tietovälineelle (katso 22.1 jakso).

21.3. **EU:n turvaluokiteltujen asiakirjojen lähettäminen**

21.3.1. *Pakkaukset ja kuitit*

1. ►M1 CONFIDENTIEL UE ◄- ja sitä luottamuksellisemman turvaluokan asiakirjat lähetetään kahdessa sisäkkäisessä, tukevassa ja läpinäkymättömässä kirjekuoressa. Sisempään kirjekuoreen merkitään asianmukainen EU:n turvaluokka ja mahdollisuuksien mukaan vastaanottajan täydellinen työnimike ja osoite.

2. Ainoastaan rekisterin valvontavastaava (katso 22.1 osasto) tai hänen sijaisensa saa avata sisemmän kirjekuoren ja kuitata sisällä olevat asiakirjat vastaanotetuiksi, ellei kirjekuorta ole osoitettu yksittäiselle henkilölle. Tällaisessa tapauksessa asianmukainen rekisteri (katso 22.1 jakso) kirjaa kirjekuoren saapuneeksi ja ainoastaan henkilö, jolle se on osoitettu, voi avata sisemmän kirjekuoren ja kuitata sisällä olevat asiakirjat vastaanotetuiksi.

3. Vastaanottokuitti sijoitetaan sisempään kirjekuoreen. Kuittiin, jota ei tarvitse turvaluokitella, merkitään asiakirjan viitenumero, päivämäärä ja kopionumero, mutta ei koskaan asiakirjan aihetta.

4. Sisempi kirjekuori suljetaan ulompaan kirjekuoreen, johon merkitään pakkausnumero kuittausta varten. Turvaluokkaa ei saa missään nimessä merkitä ulompaan kirjekuoreen.

5. ►M1 CONFIDENTIEL UE ◄- ja sitä luottamuksellisemman turvaluokan asiakirjoista annetaan kuriireille ja läheteille kuitti pakkausnumeroita vastaan.

21.3.2. *Lähettäminen kiinteistöjen tai kiinteistöryhmien sisällä*

Turvaluokiteltuja asiakirjoja voidaan kuljettaa tietyn kiinteistön tai kiinteistöryhmän sisällä suljetussa kirjekuoressa, johon on merkitty ainoastaan vastaanottajan nimi, jos kirjekuoren kuljettaa henkilö, jolla on asiakirjojen turvaluokkaa vastaava valtuutus.

21.3.3. *Lähettäminen valtion sisällä*

1. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja saa lähettää valtion sisällä ainoastaan virallisen lähettipalvelun tai ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valtuutuksen saaneiden henkilöiden välityksellä.

2. Kun käytetään lähettipalvelua ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjan lähettämiseksi kiinteistön tai kiinteistöryhmän ulkopuolelle, on noudatettava tämän luvun pakkausta ja kuitteja koskevia säännöksiä. Lähettipalvelujen henkilöstön avulla on pystyttävä varmistamaan, että ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja sisältävät pakkaukset ovat vastuuhenkilön välittömässä valvonnassa kaiken aikaa.

3. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja voivat viedä kiinteistön tai kiinteistöryhmän ulkopuolelle poikkeuksellisesti muut henkilöt kuin lähetit käytettäväksi kokouksissa ja keskusteluissa, jos

   a) asiakirjojen viejällä on valtuutus päästä ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoihin;

   b) kuljetustapa on ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen lähettämistä koskevien sääntöjen mukainen;

   c) asiakirjojen viejä ei missään vaiheessa jätä ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja vartioimatta;

   d) on olemassa järjestelyt sen varmistamiseksi, että ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisteri pitää tällä tavoin kuljetuista asiakirjoista luetteloa ja että ne merkitään päiväkirjaan. Asiakirjojen palauttamisen yhteydessä niiden vastaavuus rekisterin kanssa on tarkastettava.

4. ►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -asiakirjoja voidaan lähettää tietyn valtion sisällä postitse, jos tällainen lähetystapa sallitaan kansallisessa lainsäädännössä ja lähetys on tämän lainsäädännön mukainen, tai lähettipalvelun taikka henkilöiden, joilla on valtuutus päästä EU:n turvaluokiteltuun tietoon, välityksellä.

▼B

5. ►M2 Komission turvallisuudesta vastaava linja ◄ laatii näiden sääntöjen perusteella ohjeet EU:n turvaluokiteltujen asiakirjojen kuljettamisesta henkilökohtaisesti. Asiakirjojen viejän on luettava ja allekirjoitettava nämä ohjeet. Ohjeissa on erityisesti tehtävä selväksi se, että

   a) viejän on pidettävä asiakirjat hallussaan siihen asti kun ne ovat turvallisessa paikassa 18 jakson mukaisesti;

   b) asiakirjoja ei saa jättää vartioimatta julkisissa tai yksityisissä kulkuneuvoissa tai ravintoloiden taikka hotellien kaltaisissa paikoissa. Asiakirjoja ei saa säilyttää hotellien kassakaapeissa tai jättää vartioimatta hotellihuoneisiin;

   c) asiakirjoja ei saa lukea lentokoneiden tai junien kaltaisissa julkisissa paikoissa.

21.3.4. *Lähettäminen valtiosta toiseen*

1. ►M1 CONFIDENTIEL UE ◄ ja sitä luotettavamman turvaluokan aineisto on kuljetettava jäsenvaltiosta toiseen diplomaatti- tai sotilaskuriirilla.

2. ►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -aineiston henkilökohtainen kuljettaminen voidaan kuitenkin sallia, jos kuljetusjärjestelyin voidaan varmistaa, että aineisto ei voi joutua sivullisille.

3. Turvallisuusasioista vastaava komission jäsen voi antaa luvan henkilökohtaiseen kuljettamiseen, jos diplomaatti- tai sotilaskuriiri ei ole käytettävissä tai näiden kuriirien käyttö voisi johtaa viivästyksiin, jotka voisivat haitata EU:n toimia, ja vastaanottaja tarvitsee aineiston kiireellisesti. ►M2 Komission turvallisuudesta vastaava linja ◄ laatii ohjeet ►M1 SECRET UE ◄- ja sitä alemman turvaluokan aineiston kansainvälisestä kuljettamisesta henkilökohtaisesti silloin, kun siitä huolehtivat muut kuin diplomaatti- tai sotilaskuriirit. Ohjeissa on edellytettävä, että

   a) asiakirjojen viejän luotettavuus on selvitetty asianmukaisesti;

   b) kaikesta tällä tavoin kuljetetusta aineistosta pidetään kirjaa asianmukaisessa yksikössä tai rekisterissä;

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

   d) asiakirjojen viejällä on mukanaan kaikkien EU:n jäsenvaltioiden hyväksymä kuriiritodistus ja/tai työmääräys, joka antaa hänelle valtuudet kyseisen pakkauksen kuljettamiseen;

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

   f) asiakirjojen viejän matkasuunnitelmat ovat määräpaikan, matkustusreittien ja käytettävien kulkuneuvojen osalta EU:n sääntöjen mukaiset tai, jos kansallinen lainsäädäntö on tiukempi, sen mukaiset;

   g) asiakirjojen viejän on pidettävä asiakirjat hallussaan, ellei niiden turvallista säilyttämistä voida taata 18 jakson säännösten 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 (esimerkiksi lentokoneissa, junissa jne.).

4. Turvaluokiteltua aineistoa kuljettamaan nimetyn henkilön on luettava ja allekirjoitettava turvaohjeet, jotka sisältävät vähintään edellä luetellut ohjeet ja menettelytavat, joita on noudatettava hätätapauksessa taikka tulli- tai lentoturvallisuusviranomaisten vaatiessa turvaluokitellun aineiston sisältämän pakkauksen avaamista.

21.3.5. ►M1 *RESTREINT UE* ◄ *-asiakirjojen lähettäminen*

►M1 RESTREINT UE ◄ -asiakirjojen lähettämisestä ei ole muita erityisiä säännöksiä kuin että niitä lähetettäessä on varmistettava, että asiakirjat eivät voi joutua sivullisille.

21.4. **Kuriireihin sovellettavat turvatoimet**

Kaikkien ►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -asiakirjojen kuljettamista varten palkattujen kuriirien ja lähettien on läpäistävä asianmukainen luotettavuusselvitys.

21.5. **Sähköiset ja muut tekniset lähetyskeinot**

1. Tietoliikennettä koskevien turvatoimien tavoitteena on varmistaa EU:n turvaluokitellun tiedon suojattu lähettäminen. Tällaisen EU:n turvaluokitellun tiedon lähettämiseen sovellettavia yksityiskohtaisia sääntöjä käsitellään 25 jaksossa.

▼B

2. ►M1 CONFIDENTIEL UE ◄- ja ►M1 SECRET UE ◄ -turvaluokan tietoa saa siirtää ainoastaan hyväksyttyjen tietoliikennekeskusten ja -verkkojen ja/tai -päätteiden ja -järjestelmien kautta.

21.6. **EU:n turvaluokitelluista asiakirjoista tehdyt ylimääräiset kopiot, käännökset ja otteet**

1. Ainoastaan tietojen alkuperäinen luovuttaja voi antaa luvan ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen kopiointiin tai kääntämiseen.

2. Jos henkilö, jolla ei ole ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valtuutusta, tarvitsee tietoa, jota ei ole turvaluokiteltu siitä huolimatta, että se esiintyy ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjassa, ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisterin esimies (katso 22.2 jakso) voidaan valtuuttaa laatimaan asiakirjasta tarvittava määrä otteita. Samalla hänen on toteutettava tarvittavat toimet sen varmistamiseksi, että nämä otteet turvaluokitellaan asianmukaisesti.

3. Vastaanottaja voi kopioida tai kääntää ►M1 SECRET UE ◄- ja sitä alemman turvaluokan asiakirjoja turvallisuussäännösten mukaisesti, jos tiedonsaantitarpeen periaatetta noudatetaan tiukasti. Alkuperäiseen asiakirjaan sovellettavia turvatoimia sovelletaan myös siitä tehtyihin kopioihin ja/tai käännöksiin.

22. EU:N TURVALUOKITELLUN TIEDON REKISTERIT, INVENTOINNIT, TARKASTUKSET, SÄILYTTÄMINEN ARKISTOISSA JA HÄVITTÄMINEN

22.1. **EU turvaluokitellun tiedon paikallisrekisterit**

1. Komission kussakin yksikössä on tarpeen mukaan yksi tai useampi EU:n turvaluokitellun tiedon paikallisrekisteri, joka vastaa ►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -asiakirjojen kirjaamiseen, kopiointiin, lähettämiseen, arkistointiin ja hävittämiseen liittyvistä tehtävistä.

2. Jos jossain yksikössä ei ole EU:n turvaluokitellun tiedon paikallisrekisteriä, pääsihteeristön EU:n turvaluokitellun tiedon paikallisrekisteri toimi tällaisena rekisterinä.

3. EU:n turvaluokitellun tiedon paikallisrekisterit raportoivat sen yksikön esimiehelle, jolta he saavat ohjeensa. Näiden rekisterien esimiehenä toimii rekisterin valvontavastaava.

4. Paikallinen turvavastaava valvoo, että nämä paikallisrekisterit noudattavat EU:n turvaluokiteltujen asiakirjojen käsittelyä koskevia säännöksiä ja asianmukaisia turvatoimia.

5. EU:n turvaluokitellun tiedon paikallisrekistereissä työskenteleville henkilöille on annettava valtuudet EU:n turvaluokiteltuun tietoon pääsemiseksi 20 jakson mukaisesti.

6. Asianmukaisen yksikön esimiehen alaisuudessa toimivat EU:n turvaluokitellun tiedon paikallisrekisterit

   a) hoitavat kirjaamista, kopiointia, kääntämistä, siirtämistä, lähettämistä ja hävittämistä koskevia tehtäviä;

   b) pitävät ajantasaista luetteloa turvaluokitelluista tiedoista;

   c) tiedustelevat säännöllisin väliajoin tietojen lähettäjiltä, onko tietojen suojaus samassa luokassa edelleen tarpeen.

7. EU:n turvaluokiteltujen tietojen paikallisrekisterit pitävät seuraavat tiedot sisältävää rekisteriä:

   a) turvaluokitellun tiedon valmistelupäivä;

   b) turvaluokitus;

   c) turvaluokituksen voimassaolon päättymispäivä;

   d) lähettäjän nimi ja yksikkö;

   e) vastaanottaja/t sekä tämän/näiden järjestysnumerot;

   f) aihe;

   g) numero;

   h) jaettujen kopioiden lukumäärä;

   i) yksikölle toimitetun turvaluokitellun tiedon inventaarioiden valmistelut;

   j) turvaluokitellun tiedon luokan poistamisesta tai alentamisesta pidettävä luettelo.

8. Edellä olevan 21 jakson yleisiä sääntöjä sovelletaan EU:n turvaluokitellun tiedon komission paikallisrekistereihin, ellei niitä muuteta tässä jaksossa vahvistetuilla erityissäännöillä.

▼B

22.2. ►M1 **TRES SECRET UE/EU TOP SECRET** ◄ **-rekisteri**

22.2.1. *Yleistä*

1. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen keskusrekisteri vastaa ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen kirjaamisesta, käsittelystä ja jakelusta näiden turvallisuussäännösten mukaisesti. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisterin esimiehenä toimii ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen rekisterin valvontavastaava.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen keskusrekisteri toimii pääasiallisena tietoja vastaanottavana ja luovuttavana tahona komissiossa. Se hoitaa tätä tehtävää myös sellaisten muiden EU:n toimielinten, jäsenvaltioiden, kansainvälisten järjestöjen ja yhteisön ulkopuolisten valtioiden puolesta, joiden kanssa komissio on tehnyt sopimuksen turvaluokiteltujen tietojen vaihtamista koskevista turvamenettelyistä.

3. Tarvittaessa perustetaan alarekistereitä, jotka vastaavat ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen sisäisestä hallinnoinnista. Alarekistereihin tallennetaan ajantasaiset tiedot alarekisterissä olevien asiakirjojen liikkeistä.

4. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -alarekisterit perustetaan 22.2.3 jakson mukaisesti pitkäaikaisten tarpeiden perusteella, ja ne liitetään ►M1 TRES SECRET UE/EU TOP SECRET ◄ -keskusrekisteriin. Jos ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja tarvitaan vain väliaikaisesti ja satunnaisesti, ne voidaan luovuttaa ilman ►M1 TRES SECRET UE/EU TOP SECRET ◄ -alarekisterin perustamista edellyttäen, että on olemassa säännöt sen varmistamiseksi, että kyseiset asiakirjat ovat edelleen asianmukaisen ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisterin valvonnassa ja että kaikkia henkilöstön ja fyysiseen turvallisuuteen liittyviä näkökohtia noudatetaan.

5. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja ei voida toimittaa suoraan saman ►M1 TRES SECRET UE/EU TOP SECRET ◄ -keskusrekisterin alarekisteristä toiseen ilman keskusrekisterin nimenomaista hyväksyntää.

6. Muiden kuin samaan keskusrekisteriin liitettyjen alarekistereiden välinen ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen vaihto on ohjattava ►M1 TRES SECRET UE/EU TOP SECRET ◄ -keskusrekistereiden kautta.

22.2.2. ►M1 *TRES SECRET UE/EU TOP SECRET* ◄ *-keskusrekisteri*

►M1 TRES SECRET UE/EU TOP SECRET ◄ -keskusrekisterin esimiehenä toimivan valvontavastaavan tehtävänä on

a) toimittaa ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja 21.3 jakson säännösten mukaisesti;

b) pitää luetteloa kaikista keskusrekisterin alaisista ►M1 TRES SECRET UE/EU TOP SECRET ◄ -alarekistereistä sekä näiden valvontavastaaviksi nimettyjen henkilöiden ja heidän valtuutettujen sijaistensa nimistä ja allekirjoituksista;

c) säilyttää kuitit kaikista keskusrekisterin luovuttamista ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoista;

d) pitää kirjaa keskusrekisterissä olevista ja sen jakamista ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoista;

e) pitää ajantasaista luetteloa kaikista ►M1 TRES SECRET UE/EU TOP SECRET ◄ -keskusrekistereistä, joiden kanssa hän on yleensä tekemisissä, sekä näiden valvontavastaaviksi nimettyjen henkilöiden ja heidän valtuutettujen sijaistensa nimistä ja allekirjoituksista;

f) suojata fyysisesti kaikkia rekisterissä olevia ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja 18 jakson säännösten mukaisesti.

22.2.3. ►M1 *TRES SECRET UE/EU TOP SECRET* ◄ *-alarekisterit*

►M1 TRES SECRET UE/EU TOP SECRET ◄ -alarekisterin esimiehenä toimivan valvontavastaavan tehtävänä on

a) toimittaa ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja 21.3 jakson säännösten mukaisesti;

b) pitää ajantasaista luetteloa kaikista henkilöistä, joilla on valtuudet saada hänen valvonnassaan olevia ►M1 TRES SECRET UE/EU TOP SECRET ◄ -tietoja;

c) toimittaa ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja niiden luovuttajan ohjeiden tai tiedonsaantitarpeen periaatteen mukaisesti varmistettuaan ensin, että vastaanottajasta on tehty vaadittu luotettavuusselvitys;

▼B

d) ylläpitää ajantasaisia tietoja kaikista ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoista, joiden säilyttämistä tai liikkeitä hän valvoo tai jotka on toimitettu muihin ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekistereihin, sekä säilyttää kyseisiä asiakirjoja koskevat kuitit;

e) pitää ajantasaista luetteloa niistä ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekistereistä, joiden kanssa hänellä on valtuudet vaihtaa ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja, sekä näiden valvontavastaaviksi nimettyjen henkilöiden ja heidän valtuutettujen sijaistensa nimistä ja allekirjoituksista;

f) suojata fyysisesti kaikkia rekisterissä olevia ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoja 18 jakson säännösten mukaisesti.

22.3. **EU:n turvaluokiteltujen asiakirjojen inventointi ja tarkastukset**

1. Tässä jaksossa tarkoitettu kukin ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisteri tekee vuosittain ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen yksityiskohtaisen inventoinnin. Asiakirja katsotaan asianmukaisesti rekisteröidyksi, jos se on fyysisesti rekisterissä tai jos rekisterissä on sen ►M1 TRES SECRET UE/EU TOP SECRET ◄ -rekisterin kuittaus, jonne asiakirja on siirretty, todistus asiakirjan hävittämisestä taikka ohjeet kyseisen asiakirjan luokittelun alentamisesta tai poistamisesta. Rekisterit ilmoittavat vuotuisen inventoinnin tulokset turvallisuusasioista vastaavalle komission jäsenelle kunkin vuoden 1 päivään huhtikuuta mennessä.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -alarekisterit ilmoittavat vuotuisen inventoinnin tulokset keskusrekisterille, jonka alaisia ne ovat, keskusrekisterin määrittämään päivään mennessä.

3. ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokkaa alemmille EU:n turvaluokitelluille asiakirjoille tehdään sisäinen tarkastus turvallisuusasioista vastaavan komission jäsenen antamien ohjeiden mukaisesti.

4. Tässä yhteydessä asiakirjojen haltijoilla on tilaisuus ottaa kantaa siihen

   a) alennetaanko tai poistetaanko tiettyjen asiakirjojen turvaluokitus;

   b) mitä asiakirjoja tuhotaan.

22.4. **EU:n turvaluokitellun tiedon säilyttäminen arkistoissa**

1. EU:n turvaluokiteltu tieto varastoidaan siten, että noudatetaan kaikkia 18 jaksossa lueteltuja asianmukaisia vaatimuksia.

2. Varastointiongelmien minimoimiseksi kaikkien rekisterien valvontavastaavilla on valtuudet tallentaa ►M1 TRES SECRET UE/EU TOP SECRET ◄-, ►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -asiakirjoja mikrofilmille tai varastoida ne muulla tavoin sähköisesti tai optisin välinein arkistointia varten edellyttäen, että:

   a) henkilöstöllä, joka huolehtii mikrofilmauksesta/varastointiin liittyvistä toimista, on voimassa oleva valtuutus käsitellä asianmukaisen turvaluokan tietoa;

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

   c) ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen mikrofilmauksesta/varastoinnista ilmoitetaan alkuperäisen tiedon luovuttajalle;

   d) yksittäiset filmirullat tai muut tallennusvälineet sisältävät ainoastaan saman turvaluokan ►M1 TRES SECRET UE/EU TOP SECRET ◄-, ►M1 SECRET UE ◄- tai ►M1 CONFIDENTIEL UE ◄ -asiakirjoja;

   e) ►M1 TRES SECRET UE/EU TOP SECRET ◄- tai ►M1 SECRET UE ◄ -asiakirjojen mikrofilmauksesta/varastoinnista ilmoitetaan selkeästi vuosittaisessa inventoinnissa käytettävässä luettelossa;

   f) alkuperäiset mikrofilmille tallennetut tai muuten varastoidut asiakirjat hävitetään 22.5 jaksossa vahvistettujen sääntöjen mukaisesti.

3. Näitä sääntöjä sovelletaan myös kaikkiin muihin hyväksyttyihin varastointikeinoihin, kuten sähkömagneettiselle ja optiselle levykkeelle tallentamiseen.

22.5. **EU:n turvaluokiteltujen asiakirjojen hävittäminen**

1. EU:n turvaluokiteltujen asiakirjojen tarpeettoman kasautumisen välttämiseksi asiakirjat, joita kyseisen säilytyspaikan esimies pitää vanhentuneita ja joita on liikaa, hävitetään mahdollisimman pian seuraavalla tavalla:

   a) ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjat voidaan hävittää ainoastaan niistä vastaavassa keskusrekisterissä. Kukin hävitetty asiakirja merkitään hävittämistodistukseen, jonka allekirjoittavat ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valvontavastaava sekä hävittämisen todistava henkilö, jolla on ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valtuutus. Päiväkirjaan tehdään asiaa koskeva merkintä.

▼B

b) Rekisteri säilyttää hävittämistodistukset ja jakeluluettelot kymmenen vuoden ajan. Kopiot toimitetaan alkuperäisen tiedon luovuttajalle tai asianmukaiselle keskusrekisterille ainoastaan erillisestä pyynnöstä.

c) ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjat, mukaan lukien kaikki ►M1 TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen valmistelusta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja levykkeet hävitetään ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valvontavastaavan valvonnassa polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei niitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa.

2. ►M1 SECRET UE ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun henkilön valvonnassa käyttäen jotakin 1 kohdan c alakohdassa tarkoitettua menetelmää. Hävitetyt ►M1 SECRET UE ◄ -asiakirjat kirjataan allekirjoitettaviin hävittämistodistuksiin, jotka rekisteri säilyttää yhdessä jakeluluetteloiden kanssa vähintään kolmen vuoden ajan.

3. ►M1 CONFIDENTIEL UE ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun henkilön valvonnassa käyttäen jotakin 1 kohdan c alakohdassa tarkoitettua menetelmää. Niiden hävittäminen kirjataan turvallisuusasioista vastaavan komission jäsenen antamien ohjeiden mukaisesti.

4. ►M1 RESTREINT UE ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin tai käyttäjän toimesta turvallisuusasioista vastaavan komission jäsenen antamien ohjeiden mukaisesti.

22.6. **Hävittäminen hätätapauksissa**

1. Komission yksiköt laativat paikallisiin olosuhteisiin perustuvat suunnitelmat EU:n turvaluokitellun aineiston suojaamiseksi kriisitilanteissa mukaan luettuina mahdolliset suunnitelmat hävittämistä ja evakuointia varten hätätapauksissa. Ne julkaisevat tarpeellisiksi katsomansa ohjeet sen estämiseksi, että EU:n turvaluokiteltua aineistoa joutuisi sivullisille.

2. Järjestelyt►M1 SECRET UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -aineiston suojaamiseksi ja/tai hävittämiseksi kriisitilanteessa eivät saa missään olosuhteissa vaikuttaa haitallisesti ►M1 TRES SECRET UE/EU TOP SECRET ◄ -aineiston suojaamiseen tai hävittämiseen, jonka käsittely on kaikkia muita tehtäviä kiireellisempi, salauslaitteet mukaan luettuina.

3. Salauslaitteet suojataan ja hävitetään hätätapauksessa noudattaen erityisohjeita.

4. Ohjeita on säilytettävä paikalla suljetussa kirjekuoressa. Myös hävittämiskeinoja/välineitä on oltava saatavilla.

23. KOMISSION TILOJEN ULKOPUOLELLA JÄRJESTETTÄVIÄ KOKOUKSIA, JOISSA KÄSITELLÄÄN EU:N TURVALUOKITELTUA TIETOA, KOSKEVAT TURVATOIMET

23.1. **Yleistä**

Järjestettäessä komission kokouksia tai muita tärkeitä kokouksia komission tilojen ulkopuolella ja käsiteltävien asioiden tai tietojen arkaluonteisuuteen liittyvien turvavaatimusten sitä edellyttäessä on toteutettava jäljempänä kuvaillut turvatoimet. Kyseiset toimet koskevat ainoastaan EU:n turvaluokitellun tiedon suojelua. Myös muita turvatoimia saattaa olla tarpeen suunnitella.

23.2. **Vastuualueet**

23.2.1. ►M2 *Komission turvallisuudesta vastaava linja* ◄

►M2 Komission turvallisuudesta vastaava linja ◄ toimii yhteistyössä sen jäsenvaltioiden toimivaltaisten viranomaisten kanssa, jonka alueella kokous järjestetään (isäntäjäsenvaltio) taatakseen komission kokouksen tai muun tärkeän kokouksen sekä valtuuskuntien jäsenten ja heidän henkilöstönsä turvallisuuden. 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 turvaluokiteltuja asiakirjoja on voitava toimistotiloissa säilyttää turvallisessa paikassa;

b) Toteutetaan toimenpiteitä, jotta EU:n turvaluokiteltujen viestien vastaanottamiseen ja toimittamiseen on mahdollista käyttää komission tietoliikennejärjestelmää. Isäntäjäsenvaltiota pyydetään myös tarvittaessa antamaan käyttöön turvattuja puhelinjärjestelmiä.

►M2 Komission turvallisuudesta vastaavan linjan ◄ on toimittava turvallisuusasioiden neuvonantajana kokousta valmisteltaessa; turvallisuustoimiston olisi osallistuttava kokouksen valmisteluun auttamalla ja antamalla neuvoja kokouksen turvavastaavalle ja tarvittaessa valtuuskunnille.

▼B

Jokaista kokoukseen osallistuvaa valtuuskuntaa pyydetään nimeämään turvavastaava, joka vastaa valtuuskuntaa koskevista turvallisuusasioista ja on yhteydessä kokouksen turvavastaavaan sekä tarvittaessa ►M2 komission turvallisuudesta vastaavan linjan ◄ edustajaan.

23.2.2. *Kokouksen turvavastaava (MSO)*

On nimettävä kokouksen turvavastaava, joka valmistelee ja valvoo yleisiä sisäisiä turvatoimia sekä koordinoi niitä muiden asiaankuuluvien turvaviranomaisten kanssa. Kokouksen turvavastaavan toteuttamien toimien on yleensä liityttävä:

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

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

c) jatkuvaan koordinointiin isäntäjäsenvaltion toimivaltaisten viranomaisten sekä ►M2 komission turvallisuudesta vastaavan linjan ◄ kanssa;

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

23.3. **Turvatoimet**

23.3.1. *Turva-alueet*

Seuraavat turva-alueet on määriteltävä:

a) II luokan turva-alue, johon kuuluvat tarvittaessa asiakirjojen valmisteluhuone, komission tilat ja kopiointilaitteet sekä valtuuskuntien tilat;

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

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

23.3.2. *Kulkuluvat*

Kokouksen turvavastaavan on toimitettava asianmukaiset kulkuluvat, joita valtuuskunnat ovat pyytäneet tarpeidensa mukaisesti. Tarvittaessa voidaan eritellä ne turva-alueet, joille kulkuluvan haltijalla on oikeus päästä.

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

Kokouspaikalle on päästettävä mahdollisimman vähän henkilöitä, joilla ei ole kulkulupaa. Kokouksen turvavastaava antaa kansallisille valtuuskunnille ainoastaan näiden pyynnöstä luvan vastaanottaa kokouksen aikana vierailijoita. 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.

23.3.3. *Kuvan- ja äänentallennuslaitteiston tarkastaminen*

Kameroita ja äänityslaitteita ei saa tuoda I luokan turva-alueelle lukuun ottamatta niiden valokuvaajien ja ääniteknikkojen tuomia laitteita, joille kokouksen turvavastaava on antanut asiaankuuluvat luvat.

23.3.4. *Salkkujen, kannettavien tietokoneiden ja pakettien tarkastus*

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

23.3.5. *Tekninen suojaus*

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

▼B

23.3.6. *Valtuuskuntien asiakirjat*

Valtuuskunnat ovat vastuussa EU:n turvaluokiteltujen 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 turvaluokiteltuja asiakirjoja kokouspaikalle ja sieltä pois.

23.3.7. *Asiakirjojen säilyttäminen turvallisessa paikassa*

Jolleivät komissio tai valtuuskunnat voi säilyttää turvaluokiteltuja asiakirjojaan hyväksyttyjen normien mukaisesti, ne voivat kuittausta vastaan jättää kyseiset asiakirjat sinetöidyssä kirjekuoressa kokouksen turvavastaavalle, joka säilyttää ne hyväksyttyjen normien mukaisesti.

23.3.8. *Tilojen tarkastus*

Kokouksen turvavastaava huolehtii siitä, että komission ja valtuuskuntien tilat tarkastetaan jokaisen työpäivän jälkeen sen varmistamiseksi, että kaikkia EU:n turvaluokiteltuja asiakirjoja säilytetään turvallisessa paikassa. Ellei näin ole, turvavastaavan on toteutettava tarvittavat toimenpiteet.

23.3.9. *EU:n turvaluokiteltujen asiakirjojen hävittäminen*

Kaikkia tarpeettomia asiakirjoja on käsiteltävä EU:n turvaluokiteltuina tietoina. Komissiolle ja valtuuskunnille on annettava jätepaperikorit tai -pussit. Ennen kuin komission ja valtuuskuntien jäsenet poistuvat niille osoitetuista tiloista, niiden on toimitettava tarpeettomat asiakirjat kokouksen turvavastaavalle, joka huolehtii niiden sääntöjen mukaisesta hävittämisestä.

Kokouksen päätyttyä kaikkia komission tai valtuuskuntien hallussa olevia tarpeettomia asiakirjoja on käsiteltävä jätteenä. Komission ja valtuuskuntien tilat on tarkastettava perinpohjaisesti ennen kokouksen turvajärjestelyjen poistamista. Asiakirjat, joiden vastaanotosta on vaadittu kuittaus, on hävitettävä 22.5 jaksossa esitetyllä tavalla.

24. EU:N TURVALUOKITELLUN TIEDON TURVALLISUUDEN RIKKOMINEN JA VAARANTAMINEN

24.1. **Määritelmät**

Tietoturvallisuutta rikotaan, jos komission turvamääräyksiä ei noudateta tai niitä laiminlyödään, mistä saattaa aiheutua vahinkoa tai vaaraa EU:n turvaluokitellulle tiedolle.

EU:n turvaluokiteltujen 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 tiedonsaantitarvetta, tai jos on todennäköistä, että tiedot ovat joutuneet kyseisille henkilöille.

EU:n turvaluokitellun tiedon turvallisuus voi vaarantua huolimattomuuden, välinpitämättömyyden tai harkitsemattomuuden seurauksena, EU:hun tai sen jäsenvaltioihin kohdistuvan, EU:n turvaluokiteltua tietoa koskevan toiminnan vuoksi tai muuta haitallista toimintaa harjoittavien järjestöjen vuoksi.

24.2. **Turvallisuuden vaarantumisesta raportoiminen**

Kaikille henkilöille, joiden edellytetään käsittelevän EU:n turvaluokiteltua tietoa, on selvitettävä perusteellisesti heidän vastuunsa tällä alalla. Heidän on raportoitava viipymättä mistä tahansa heidän tietoonsa tulleesta turvallisuusmääräysten rikkomisesta.

Kun paikallinen turvavastaava tai kokouksen turvavastaava havaitsee tai saa tiedon EU:n turvaluokitellun tiedon turvallisuuden rikkomisesta tai EU:n turvaluokitellun aineiston katoamisesta tai häviämisestä, hänen on ryhdyttävä pikaisiin toimiin, jotta voidaan:

a) säilyttää todistusaineisto,

b) selvittää tosiseikat,

c) arvioida tapahtunut vahinko ja minimoida sen vaikutukset,

d) estää tapahtuman toistuminen,

e) ilmoittaa asiaankuuluville viranomaisille turvallisuusmääräysten rikkomisen vaikutuksista.

Tässä yhteydessä on annettava seuraavat tiedot:

i) kuvaus kyseessä olevista tiedoista ja niiden turvaluokituksesta, 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;

▼B

iii) ilmoitus tietojen luovuttajalle mahdollisesti annetusta ilmoituksesta.

Saatuaan ilmoituksen tietoturvallisuuden mahdollisesta rikkomisesta kunkin turvallisuusviranomaisen velvollisuutena on raportoida tapahtumasta viipymättä ►M2 komission turvallisuudesta vastaavalle linjalle ◄.

Jos kyse on ►M1 RESTREINT UE ◄ -tiedosta, asiasta on raportoitava ainoastaan, jos tapauksessa on jotain epätavanomaista.

Saatuaan tiedon tietoturvallisuuden rikkomisesta turvallisuusasioista vastaava komission jäsen

a) ilmoittaa asiasta viranomaiselle, joka kyseisen turvaluokitellun tiedon 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 turvaluokituksesta. Lisäksi on raportoitava EU:n tai sen yhden tai useamman jäsenvaltion eduille aiheutuneesta vahingosta tai tapahtuman toistumisen estämiseksi toteutetuista toimista.

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

24.3. **Oikeustoimet**

Henkilölle, joka on vastuussa EU:n turvaluokitellun tiedon turvallisuuden vaarantamisesta, voidaan määrätä kurinpitoseuraamus asiaankuuluvien sääntöjen ja asetusten, erityisesti henkilöstösääntöjen VI osaston mukaisesti. Kurinpitoseuraamus ei rajoita oikeutta ryhtyä myöhemmin oikeustoimiin.

Turvallisuusasioista vastaavan komission jäsenen on asianmukaisesti perustelluissa tapauksissa toteutettava 24.2 jaksossa mainitun raportin perusteella kaikki tarvittavat toimet, jotta toimivaltaiset kansalliset viranomaiset voivat aloittaa rikosoikeudelliset menettelyt.

25. TIETO- JA TIETOLIIKENNEJÄRJESTELMISSÄ KÄSITELTÄVÄN EU:N TURVALUOKITELLUN TIEDON SUOJAUS

25.1. **Johdanto**

25.1.1. *Yleistä*

Turvallisuuspolitiikkaa ja -vaatimuksia sovelletaan kaikkiin tieto- ja tietoliikennejärjestelmiin ja -verkkoihin (jäljempänä 'järjestelmät'), joissa käsitellään ►M1 CONFIDENTIEL UE ◄ -turvaluokan tai sitä luottamuksellisempia tietoja. Niitä sovelletaan täydennyksenä tietojenkäsittelyjärjestelmien suojaamisesta 23 päivänä marraskuuta 1995 tehtyyn komission päätökseen K(95) 1510 lopullinen.

Myös ►M1 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.

Komission tietotekniikkaan soveltama turvallisuuspolitiikka koostuu seuraavista seikoista:

— Se on erottamaton osa yleistä turvallisuutta ja täydentää kaikkia tietoturvaan sekä henkilöstön luotettavuuteen ja fyysiseen turvallisuuteen liittyviä näkökohtia.

— Vastuunjako teknisten järjestelmävastaavien, teknisiin järjestelmiin tallennetun tai niissä käsiteltävän EU:n turvaluokitellun tiedon sisältövastaavien, tietotekniikan turvallisuusasiantuntijoiden ja käyttäjien kesken.

— Kunkin tietotekniikkajärjestelmän turvallisuusperiaatteiden ja -vaatimusten kuvaus.

— Nimetyn viranomaisen näille periaatteille ja vaatimuksille antama hyväksyntä.

— Laitetilaan kohdistuvien erityisuhkien ja järjestelmien haavoittuvuuden huomioon ottaminen.

25.1.2. *Järjestelmiin kohdistuvat uhat ja järjestelmien haavoittuvuus*

Uhka voidaan määritellä mahdollisuudeksi turvallisuuden tahattomaan tai tahalliseen vaarantamiseen. Järjestelmien osalta tällainen vaarantaminen tapahtuu silloin, kun yksi tai useampi luottamuksellisuuden, eheyden tai käytettävyyden

▼B

ominaisuuksista häviää. Haavoittuvuus voidaan määritellä valvonnan riittämättömyydeksi tai puuttumiseksi, jonka vuoksi jokin erityinen kohde helpommin joutuu tai voi joutua uhan alaiseksi.

Nopeasti toimivia hakuja, viestintää ja käyttöä varten suunnitelluissa järjestelmissä käsiteltävä EU:n turvaluokiteltu ja -luokittelematon keskitetyssä muodossa oleva tieto on alttiina monille uhkille. Näitä ovat sivullisten 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 vaihtaa nopeasti.

25.1.3. *Turvatoimien päätarkoitus*

Tässä jaksossa käsiteltävien turvatoimien päätarkoituksena on suojata EU:n turvaluokiteltu tieto luvattomalta paljastamiselta (luottamuksellisuuden häviämiseltä) ja varmistaa tietojen eheys ja käytettävyys. Jotta EU:n turvaluokiteltua tietoa käsittelevälle järjestelmälle saataisiin asianmukainen turvallisuussuoja, ►**M2** komission turvallisuudesta vastaavan linjan ◄ on täsmennettävä kunkin järjestelmän osalta tavanomaista turvallisuutta koskevat asianmukaiset vaatimukset ja asianmukaiset erityiset turvallisuusmenettelyt ja -tekniikat.

25.1.4. *Järjestelmäkohtainen turvavaatimusilmoitus (SSRS)*

Kaikkien ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä luottamuksellisempia tietoja käsittelevien järjestelmien osalta vaaditaan järjestelmäkohtainen turvavaatimusilmoitus, jonka tekee tekninen järjestelmävastaava (katso 25.3.4 jakso) ja sisältövastaava (katso 25.3.5 jakso) tarvittaessa projektihenkilöstön ja ►**M2** komission turvallisuudesta vastaavan linjan ◄ (joka toimii tietoturvaviranomaisena, katso 25.3.3 jakso) tuella ja jonka turvallisuusjärjestelyt hyväksyvä viranomainen (katso 25.3.2 jakso) hyväksyy.

Järjestelmäkohtainen turvavaatimusilmoitus vaaditaan myös silloin, kun turvallisuusjärjestelyt hyväksyvä viranomainen katsoo, että ►**M1** RESTREINT UE ◄ -tietojen tai luokittelemattomien tietojen käytettävyys ja eheys ovat uhattuina.

Järjestelmäkohtainen turvavaatimusilmoitus 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.

25.1.5. *Turvallisuuden takaavat toimintatavat*

Kaikki ►**M1** CONFIDENTIEL UE ◄ -turvaluokan 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, ja

c) monitasoinen turvallisuuden takaava toimintatapa.

25.2. **Määritelmät**

'Hyväksymisellä' (accreditation) tarkoitetaan järjestelmälle myönnettävää lupaa ja hyväksyntää käsitellä käyttöympäristössään EU:n turvaluokiteltua tietoa.

Huomautus:

Hyväksyminen olisi tehtävä sen jälkeen, kun kaikki asiaankuuluvat turvamenettelyt 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 varmentamista koskeva suunnitelma, ja

f) tarvittaessa varmennus ja muut hyväksymisasiakirjat.

▼B

’Keskustietojärjestelmien tietoturvavastaavalla’ (Central Information Security Officer eli CISO) tarkoitetaan tietotekniikan keskusyksikön virkailijaa, joka koordinoi ja valvoo keskitettyjen järjestelmien turvatoimia.

’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.

’Tietoliikenneturvallisuudella’ (communications security eli COMSEC) tarkoitetaan turvatoimien soveltamista tietoliikenteeseen, jotta voidaan estää sivullisten pääsy sellaiseen arvokkaaseen tietoon, jota voidaan saada seuraamalla tai analysoimalla tietoliikennettä, tai taata tietoliikenteen tietojen luotettavuus.

Huomautus:

Tällaiset toimet kattavat salauksen, siirron ja lähettämisen turvallisuuden sekä myös menettelyjen turvallisuuden, fyysisen turvallisuuden, henkilöstön luotettavuuden, asiakirjojen turvallisuuden ja tietojärjestelmäturvallisuuden.

’Tietojärjestelmäturvallisuus’ (computer security eli COMPUSEC) tarkoittaa laitteiston, valmisohjelmiston ja ohjelmiston turvaominaisuuksien soveltamista tietojärjestelmässä, jotta tietojen luvattomalta paljastamiselta, käsittelyltä, muuttamiselta tai poistamiselta tai palvelujen epäämiseltä voidaan suojautua taikka nämä voidaan estää.

’Tietoturvatuotteella’ (computer security product) tarkoitetaan yleistä tietoturvatuotetta, joka sisällytetään tietojärjestelmään käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden tehostamiseksi tai varmistamiseksi.

’Yleisvaltuutuksella’ tarkoitetaan toimintatapaa, jossa KAIKKIEN järjestelmään pääsevien luotettavuus selvitetään järjestelmässä käsiteltäviä tietoja koskevan korkeimman turvaluokan mukaan ja jossa kaikki tarvitsevat pääsyn KAIKKIIN järjestelmässä käsiteltäviin tietoihin.

Huomautuksia:

(1) Yleinen tiedonsaantitarve merkitsee sitä, että tietojärjestelmän turvallisuusominaisuuksilta ei edellytetä tietojen erottelua järjestelmän sisällä.

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

’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 salaus- tai tietoturvatuotteen luotettavan toiminnan luotettavuustaso.

’Sisältövastaavalla’ (Information Owner eli IO) tarkoitetaan viranomaista (yksikön esimiestä), joka on vastuussa tietojen tuottamisesta, käsittelystä ja käytöstä ja joka päättää siitä, kenellä on oikeus saada näitä tietoja.

’Tietoturvalla’ (information security eli INFOSEC) tarkoitetaan turvatoimien soveltamista tietoliikenne- ja tietojärjestelmissä sekä 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.

’Tietoturvatoimenpiteitä’ ovat tietojärjestelmien, siirron, lähettämisen ja salauksen turvallisuuden suojaaminen sekä tietoihin ja järjestelmiin kohdistuvien uhkien havaitseminen, dokumentointi ja torjunta.

’Laitetilalla’ (IT Area) tarkoitetaan tilaa, jossa on yksi tai useampi tietokone, niiden paikalliset oheis- ja tallennusyksiköt, ohjausyksiköt sekä niille tarkoitettu verkko- ja tietoliikennelaitteisto.

Huomautus:

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

▼B

’Tietoverkolla’ (IT Network) tarkoitetaan tietojen vaihtoa varten toisiinsa liitettyjen tietotekniikkajärjestelmien sijaintipaikaltaan 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.

’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 turvaluokitellun tiedon hyväksyttävää suojaustasoa varten.

’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 teknisen järjestelmävastaavan valvonnassa.

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

’Tietotekniikkajärjestelmän turvallisuusominaisuuksiin’ (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 käsiteltävän turvaluokitellun tiedon hyväksyttävää suojaustasoa varten.

’Paikallistietojärjestelmien tietoturvavastaavalla’ (Local Informatics Security Officer eli LISO) tarkoitetaan komission yksikön virkamiestä, joka vastaa oman alansa turvatoimien koordinoinnista ja valvonnasta.

’Monitasoisella turvallisuuden takaavalla toimintatavalla’ tarkoitetaan toimintatapaa, jossa KAIKKIEN järjestelmään pääsevien luotettavuutta EI selvitetä järjestelmässä käsiteltäviä tietoja koskevan korkeimman turvaluokan mukaan ja jossa KAIKKI järjestelmään pääsevät EIVÄT tarvitse pääsyä 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 yleistä tiedonsaantitarvetta ei ole, merkitsee, että turvallisuusominaisuuksilta edellytetään, että pääsy järjestelmän tietoihin on valikoivaa ja tiedot erotellaan järjestelmässä.

’Etäpäätteen/työaseman sijoituspaikalla’ tarkoitetaan paikkaa, johon on sijoitettu tietokonelaitteisto, sen paikalliset oheislaitteet tai päätteet/työasemat sekä näihin liittyvä laitetilasta erillään oleva tietoliikennelaitteisto.

’Turvallisuusmenettelyillä’ tarkoitetaan teknisten järjestelmävastaavien tuottamia menettelyjä, joissa määritellään turvallisuuskysymyksissä noudatettavat periaatteet, toimintatavat ja työntekijöiden vastuu.

’Monitasoisella turvallisuuden takaavalla toimintatavalla’ tarkoitetaan toimintatapaa, jossa KAIKKIEN järjestelmään pääsevien luotettavuus selvitetään järjestelmässä käsiteltäviä tietoja koskevan korkeimman turvaluokan mukaan mutta jossa KAIKKI järjestelmään pääsevät EIVÄT tarvitse pääsyä järjestelmässä käsiteltäviin tietoihin.

Huomautuksia:

(1) Yleisen tiedonsaantitarpeen puuttuminen merkitsee sitä, että tietojärjestelmän turvallisuusominaisuuksilta edellytetään, että pääsy järjestelmän tietoihin on valikoivaa ja tiedot erotellaan järjestelmässä.

▼B

(2) Muiden turvallisuusominaisuuksien (kuten fyysinen turvallisuus, henkilöstön luotettavuus 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, siihen asti kun ne määritellään toisin, paitsi jos jotain muuta merkintätapaa pidetään tarpeeksi luotettavana.

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

'Teknisellä järjestelmävastaavalla' (Technical Systems Owner eli TSO) tarkoitetaan järjestelmän luomisesta, ylläpidosta, toiminnasta ja sulkemisesta vastuussa olevaa viranomaista.

'Sähköhäiriöiltä suojautumisella' (Tempest) tarkoitetaan turvatoimia, joiden tarkoituksena on suojata laitteistoa tai tietoliikenneinfrastruktuureja tahattomista elektromagneettisista päästöistä ja johtavuudesta aiheutuvalta turvaluokitellun tiedon vaarantumiselta.

25.3. **Turvallisuusvastuut**

25.3.1. *Yleistä*

Komission turvallisuusasioiden neuvonantajaryhmän neuvonantovastuut, jotka on määritelty 12 jaksossa, sisältävät tietoturvaa koskevat kysymykset. Kyseinen ryhmä järjestää toimintansa siten, että se voi antaa asiantuntija-apua edellä mainituissa asioissa.

►**M2** Komission turvallisuudesta vastaava linja ◄ vastaa tämän luvun säännöksiin perustuvien yksityiskohtaisten tietoturvasäännösten antamisesta.

►**M2** Komission turvallisuudesta vastaavan linjan ◄ on ryhdyttävä välittömästi toimiin turvallisuusongelmien ilmetessä (poikkeukselliset tapahtumat, rikkomukset jne.).

►**M2** Komission turvallisuudesta vastaavassa linjassa ◄ on tietoturvayksikkö.

25.3.2. *Turvallisuusjärjestelyt hyväksyvä viranomainen (SAA)*

►**M2** Komission turvallisuudesta vastaavan linjan johtajaan ◄ toimii komission turvallisuusjärjestelyt hyväksyvänä viranomaisena (SAA). SAA on vastuuviranomainen yleisen turvallisuuden alalla sekä tieto- ja tietoliikenneturvallisuuden, salauksen turvallisuuden ja sähköhäiriöiltä suojautumisen erikoisaloilla.

SAA vastaa siitä, että järjestelmät ovat komission turvallisuuspolitiikan mukaiset. Yksi hänen tehtäviään on myöntää järjestelmälle hyväksyntä käsitellä EU:n turvaluokiteltua tietoa määrätyllä luokittelutasolla järjestelmän käyttöympäristössä.

Komission turvallisuusjärjestelyt hyväksyvä viranomainen on toimivaltainen kaikkien komission tiloissa käytettävien järjestelmien osalta. Järjestelmän eri osien tullessa komission ja muiden turvallisuusjärjestelyt hyväksyvien viranomaisten toimivallan piiriin kaikki asianomaiset osapuolet voivat nimetä yhteisen hyväksymislautakunnan, jota komission turvallisuusjärjestelyt hyväksyvä viranomainen koordinoi.

25.3.3. *Tietoturvaviranomainen (IA)*

►**M2** Komission turvallisuudesta vastaavan linjan ◄ tietoturvayksikön päällikkö toimii komission tietoturvaviranomaisena. 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 tietoturvaan liittyvien toimintaperiaatteiden ja arkkitehtuuria koskevien asiakirjojen mukainen,

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

▼B

— antaa apua tietoturvaa koskevan koulutuksen järjestämisessä,

— antaa teknistä neuvontaa tietoturvaan liittyvien poikkeuksellisten tapahtumien tutkinnassa,

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

25.3.4. *Tekninen järjestelmävastaava (TSO)*

Tekninen järjestelmävastaava on vastuussa järjestelmän valvonnan ja erityisten turvaominaisuuksien täytäntöönpanosta ja toiminnasta. Keskitettyjä järjestelmiä varten on nimitettävä keskustietojärjestelmien tietoturvavastaava (CISO). Kukin yksikkö nimeää tarvittaessa paikallistietojärjestelmien tietoturvavastaavan (LISO). Teknisen järjestelmävastaavan vastuulla on turvallisuusmenettelyjen (SecOP:ien) luominen, ja vastuuta laajennetaan koko järjestelmän elinkaaren ajan projektin suunnitteluvaiheesta järjestelmän lopulliseen toimintavalmiuteen saakka.

Tekninen järjestelmävastaava määrittelee järjestelmän toimittajalta edellytettävät turvallisuusstandardit ja -käytännöt.

Tekninen järjestelmävastaava voi tarvittaessa siirtää osan toimivallastaan paikallistietojärjestelmien tietoturvavastaavalle. Yksi ainoa henkilö voi vastata eri tietoturvatehtävistä.

25.3.5. *Sisältövastaava (IO)*

Sisältövastaava on vastuussa niistä EU:n turvaluokitelluista tiedoista (ja muista tiedoista) jotka tallennetaan ja joita käsitellään ja tuotetaan teknisissä järjestelmissä. Hänen on määriteltävä vaatimukset näihin järjestelmissä oleviin tietoihin pääsemiseksi. Hän voi siirtää tämän vastuun alallaan toimivalle informaatikolle tai tietokannanhoitajalle.

25.3.6. *Käyttäjät*

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

25.3.7. *Tietoturvaa koskeva koulutus*

Tietoturvaa koskevaa koulutusta on tarjottava kaikille sitä tarvitseville henkilöstön jäsenille.

25.4. **Muut kuin tekniset turvatoimet**

25.4.1. *Henkilöstön luotettavuus*

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 komission menettelyjen mukaista luotettavuusselvitystä.

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

Järjestelmät 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.

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

Järjestelmän turva-asetusten muuttamiseen tarvitaan vähintään kaksi siihen oikeutettua henkilöstön jäsentä, jotka työskentelevät yhdessä.

25.4.2. *Fyysinen turvallisuus*

Laitetilat ja etäpäätteen/työaseman sijoituspaikat (sellaisina kuin ne on määritelty 25.2 jaksossa), joissa käsitellään tietotekniikkavälineillä ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä luottamuksellisempia tietoja tai joissa voidaan päästä tällaisiin tietoihin, vahvistetaan EU:n I tai II luokan turva-alueiksi.

25.4.3. *Järjestelmän käytön valvonta*

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

Käytön valvontaa koskeva tieto ja aineisto tuhotaan jakson 25.5.4 mukaisesti kun niitä ei enää käytetä tähän tarkoitukseen.

▼B

25.5. **Tekniset turvatoimet**

25.5.1. *Tietoturva*

Tietojen luovuttajan velvollisuutena on kaikkien tietoja sisältävien asiakirjojen yksilöiminen ja luokittelu, olivatpa 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.

Komission yksiköiden ja niissä olevien tiedon hallussapitäjien on otettava huomioon yksittäisten tietojen yhdistämiskysymykset ja yhdistetyistä tiedoista mahdollisesti tehtävät johtopäätökset sekä määritettävä, onko korkeampi turvaluokka kaikkien tietojen kannalta tarkoituksenmukaista.

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

Kun tieto siirretään järjestelmästä toiseen, se on suojattava siirron aikana ja vastaanottavassa järjestelmässä tiedon alkuperäisen turvaluokituksen ja luokan edellyttämällä tavalla.

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

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 turvallisuusjärjestelyt hyväksyvän viranomaisen hyväksymän menettelyn mukaisesti (katso 25.5.4).

25.5.2. *Tietojen valvonta ja tilivelvollisuus tiedoista*

►**M1** SECRET UE ◄ -turvaluokan ja sitä korkeampiin tietoihin pääsystä on pidettävä kirjaa automaattisten (kirjausketjujen) tai manuaalisten lokitiedostojen avulla. Tietojen säilyttämisessä on noudatettava näitä turvallisuussääntöjä.

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

Jos tuloste on peräisin EU:n turvaluokiteltua tietoa käsittelevästä järjestelmästä ja siirretty laitetilasta etäpäätteen/työaseman sijoituspaikkaan, on työasemalla tuotetun tulosteen valvontaa ja tietojenkeruuta varten otettava käyttöön menettelyjä, jotka turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) on hyväksynyt. Jos kyseessä on vähintään ►**M1** SECRET UE ◄ -turvaluokan luokiteltu aineisto, on menettelyjä käyttöön otettaessa annettava erityisohjeistusta tietoihin liittyvästä tilivelvollisuudesta.

25.5.3. *Siirrettävien tietovälineiden käsittely ja valvonta*

►**M1** CONFIDENTIEL UE ◄ -turvaluokan ja sitä korkeammalle luokiteltuja tietovälineitä käsitellään kuten aineistoa, ja yleisiä sääntöjä noudatetaan. Tunnistus- ja turvaluokitusmerkinnät on mukautettava välineen fyysisiin ominaisuuksiin, jotta ne olisivat selvästi tunnistettavissa.

Käyttäjien on vastattava siitä, että EU:n turvaluokiteltu tieto 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.

25.5.4. *Tietovälineiden luokituksen poistaminen ja tietovälineiden tuhoaminen*

EU:n turvaluokiteltujen tietojen tallentamiseen käytettyjen tietovälineiden luokka voidaan alentaa tai poistaa turvallisuusjärjestelyt hyväksyvän viranomaisen hyväksymän menettelyn mukaisesti.

►**M1** TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoja tai erityisluokan tietoja sisältäneiden tietovälineiden luokitusta ei saa poistaa eikä tietovälineitä saa käyttää uudelleen.

Jos tietovälineen luokitusta ei voida poistaa tai sitä ei voida käyttää uudelleen, se on tuhottava edellä mainitun menettelyn mukaisesti.

25.5.5. *Tietoliikenneturvallisuus*

►**M2** Komission turvallisuudesta vastaavan linjan johtaja ◄ on salausasioista vastaava viranomainen.

▼B

Kun EU:n turvaluokiteltua tietoa siirretään sähkömagneettisesti, on toteutettava erityistoimenpiteitä siirtojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi. Turvallisuusjärjestelmät hyväksyvän viranomaisen (SAA) on määriteltävä vaatimukset siirtojen suojaamiseksi jäljittämiseltä ja salakuuntelulta. Tietoliikennejärjestelmissä siirrettävät tiedot on suojattava siten, että vaatimus luottamuksellisuudesta, eheydestä ja käytettävyydestä täyttyy.

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

►**M1** SECRET UE ◄ -turvaluokan tai sitä korkeamman luokan tiedon luottamuksellisuus on siirron aikana suojattava salausmenetelmillä tai tuotteilla, jotka turvallisuusasioista vastaava komission jäsen on hyväksynyt kuultuaan komission turvallisuusasioiden neuvonantajaryhmää. ►**M1** CONFIDENTIEL UE ◄- tai ►**M1** RESTREINT UE ◄ -turvaluokan tietojen luottamuksellisuus on siirron aikana suojattava salausmenetelmillä tai tuotteilla, jotka komission salausasioista vastaava viranomainen on hyväksynyt kuultuaan komission turvallisuusasioiden neuvonantajaryhmää.

EU:n turvaluokitellun tiedon siirtoa koskevat yksityiskohtaiset säännöt annetaan erityisessä turvallisuusohjeessa, jonka ►**M2** komission turvallisuudesta vastaava linja ◄ on hyväksynyt kuultuaan komission turvallisuusasioiden neuvonantajaryhmää.

Poikkeusoloissa ►**M1** RESTREINT UE ◄-, ►**M1** CONFIDENTIEL UE ◄- tai ►**M1** 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; ja

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.

Järjestelmän on ehdottomasti pystyttävä tarvittaessa estämään pääsy EU:n turvaluokiteltuihin tietoihin joltakin työasemalta/etäpäätteeltä joko kytkemällä ne fyysisesti irti tai sellaisten ohjelmiston erityisominaisuuksien avulla, jotka turvallisuusjärjestelyt hyväksyvä viranomainen (SAA) on hyväksynyt.

25.5.6. *Turvallisuus asennuksen yhteydessä ja säteilyturvallisuus*

Järjestelmien ensimmäisestä asennuksesta ja niihin tehtävistä huomattavista muutoksista on tehtävä sopimus, jonka mukaan asennuksen suorittavat asentajat, joista on tehty luotettavuusselvitys. Toimintaa valvovat jatkuvasti teknisesti pätevät työntekijät, joilla luotettavuusselvityksen perusteella on pääsy EU:n turvaluokiteltuihin tietoihin. Tämän pääsyn on oltava tasolla, joka vastaa sitä korkeinta luokkaa, jonka tietoja järjestelmän on määrä tallentaa ja käsitellä.

Järjestelmät, jotka käsittelevät ►**M1** CONFIDENTIEL UE ◄- tai sitä korkeamman turvaluokan tietoja, on suojattava siten, että haitallinen säteily ja/tai johtavuus, joiden tutkimuksesta ja hallinnasta käytetään nimitystä ”Tempest” ei voi uhata niiden turvallisuutta.

Tempest-viranomaisen on tarkastettava ja hyväksyttävä toimenpiteet, joilla laitteet suojataan sähköhäiriöiltä (katso 25.3.2).

25.6. **Turvallisuus käsittelyn aikana**

25.6.1. *Turvallisuusmenettelyt (SecOP:t)*

Turvallisuusmenettelyissä (SecOP:t) määritellään turvallisuuskysymyksissä noudatettavat periaatteet, toimintatavat ja työntekijöiden vastuu. Turvallisuusmenettelyt on laadittava teknisen järjestelmävastaavan (TSO) vastuulla.

25.6.2. *Ohjelmistojen suojaus / konfiguraation hallinta*

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 ohjelmistoversiot on tarkistettava säännöllisesti niiden eheyden ja moitteettoman toiminnan varmistamiseksi.

Uusia tai muutettuja ohjelmistoversioita ei saa käyttää EU:n turvaluokitellun tiedon käsittelyssä ennen kuin TSO on tarkistanut ne.

25.6.3. *Tuhoisien ohjelmisto- tai tietokonevirusten tarkistaminen*

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

▼B

Kaikki komissioon saapuvat tietovälineet on tarkistettava tuhoisien ohjelmisto- tai tietokonevirusten varalta ennen niiden käyttämistä järjestelmässä.

25.6.4. *Huolto*

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.

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

25.7. **Hankinnat**

25.7.1. *Yleistä*

Hankittavassa järjestelmässä käytettävien turvatuotteiden on joko oltava arvioituja ja varmennettuja tai niiden on oltava parhaillaan jonkin EU:n jäsenvaltion arviointi- tai varmennelaitoksen arvioitavana ja varmennettavana noudattaen kansainvälisesti tunnustettuja kriteerejä (esim. yleiset tietoturvallisuuden arviointiperusteet, ISO 15408). Erityismenettelyihin vaaditaan hankintoja ja sopimuksia käsittelevän neuvoa-antavan komitean (ACPC) hyväksyntä.

Päätettäessä siitä, kannattaako välineitä, etenkin tietovälineitä, vuokrata vai ostaa, on muistettava, että EU:n turvaluokitellun tiedon käsittelemiseen käytettyjä välineitä ei voida päästää pois asianmukaisesti turvatusta ympäristöstä ennen kuin luokitus on poistettu turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) suostumuksella ja että suostumusta ei aina voi saada.

25.7.2. *Hyväksyminen*

Turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) on hyväksyttävä kaikki järjestelmät, joista on annettava järjestelmäkohtainen turvavaatimusilmoitus (SSRS) ennen EU:n turvaluokitellun tiedon käsittelyä, SSRS:n, turvallisuusmenettelyjen (SecOP:t) ja kaikkien muiden asiaa koskevien asiakirjojen sisältämien tietojen perusteella. Alijärjestelmät ja etäpäätteet/työasemat on hyväksyttävä osana kaikkia järjestelmiä, joihin ne ovat yhteydessä. Jos järjestelmää käytetään sekä komissiossa että muissa organisaatioissa, komission ja asiasta vastaavien turvallisuusviranomaisten on yhdessä sovittava hyväksymisestä.

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

25.7.3. *Arviointi ja varmentaminen*

Järjestelmän laitteistojen, valmisohjelmistojen ja ohjelmistojen turvallisuusominaisuudet on arvioitava ja varmennettava sellaisiksi, että ne pystyvät suojaamaan tietoa aiotulla turvaluokitustasolla.

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

Teknisesti pätevän henkilöstön, josta on asianmukaisesti tehty luotettavuusselvitys ja joka toimii teknisen järjestelmävastaavan (TSO) nimissä, on suoritettava arviointi ja varmentaminen hyväksyttyjen ohjeiden mukaisesti.

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

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

25.7.4. *Turvallisuusominaisuuksien rutiinitarkastukset pysyvää hyväksymistä varten*

Teknisen järjestelmävastaavan (TSO) on otettava käyttöön rutiinitarkastukset, joilla on varmistettava, että kaikki järjestelmän turvallisuusominaisuudet pätevät edelleen.

Muutokset, joiden perusteella hyväksyminen olisi suoritettava uudelleen tai jotka edellyttäisivät turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) ennakkohyväksyntää, on selkeästi yksilöitävä ja mainittava järjestelmäkohtaisessa turvavaatimusilmoituksessa (SSRS). Jos järjestelmässä tapahtuu muutoksia, sitä korjataan tai siinä esiintyy häiriöitä, teknisen järjestelmävastaavan (TSO) on huolehdittava siitä, että se tarkastetaan turvallisuusominaisuuksien moitteettoman toiminnan varmistamiseksi. Järjestelmän hyväksynnän säilyminen riippuu tavallisesti siitä, että tarkastukset on tyydyttävästi tehty.

▼B

Turvallisuusjärjestelyt hyväksyvän viranomaisen (SAA) on tarkastettava määräajoin kaikki järjestelmät, joihin on liitetty turvallisuusominaisuuksia. Järjestelmät, jotka käsittelevät ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoja, on tarkastettava vähintään kerran vuodessa.

25.8. **Tilapäinen tai satunnainen käyttö**

25.8.1. *Mikrotietokoneiden tai henkilökohtaisten tietokoneiden suojaus*

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.

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

25.8.2. *Yksityisen atk-laitteiston käyttö komission virallisessa työskentelyssä*

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

Yksityisiä laitteita, ohjelmistoja ja tietovälineitä ei saa tuoda niille I tai II luokan alueille, joilla käsitellään EU:n turvaluokiteltua tietoa, ilman ►M2 komission turvallisuudesta vastaavan linjan johtajan ◄ kirjallista lupaa. Tämä lupa voidaan antaa ainoastaan teknisistä syistä poikkeustapauksissa.

25.8.3. *Sopimuspuolten omistamien tai jäsenvaltioiden toimittamien atk-laitteiden käyttö komission virallisessa työskentelyssä*

►M2 Komission turvallisuudesta vastaavan linjan johtaja ◄ voi antaa luvan käyttää sopimuspuolten omistamia atk-laitteita ja ohjelmistoja komission virallista työskentelyä tukevissa organisaatioissa. Myös jäsenvaltioiden toimittamien atk-laitteiden käyttö voidaan sallia; tällöin atk-laitteet on saatettava asianmukaisesti komission valvontaan. Jos atk-laitteita on määrä käyttää EU:n turvaluokitellun tiedon käsittelyssä, molemmissa tapauksissa on kuultava turvallisuusjärjestelyt hyväksyvää viranomaista (SAA) sen varmistamiseksi, että kyseisten laitteiden tietoturvatekijät otetaan asianmukaisesti huomioon ja että niitä sovelletaan asianmukaisella tavalla.

26. EU:N TURVALUOKITELLUN AINEISTON LUOVUTTAMINEN YHTEISÖN ULKOPUOLISILLE VALTIOILLE TAI KANSAINVÄLISILLE JÄRJESTÖILLE

26.1.1. *EU:n turvaluokitellun tiedon luovuttamista koskevat periaatteet*

Komissio päättää kollegiona EU:n turvaluokitellun tiedon luovuttamisesta yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille seuraavin perustein:

— kyseisten tietojen laatu ja sisältö,

— vastaanottajan tiedonsaantitarve,

— EU:lle koituvien etujen arviointi.

EU:n turvaluokitellun tiedon luovuttajalta pyydetään suostumus tietojen luovuttamiseen.

Päätökset tehdään tapauskohtaisesti seuraavin perustein:

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

— kyseisten valtioiden ja järjestöjen luotettavuus — luotettavuutta arvioidaan kyseisille valtioille tai järjestöille luovutettavaan EU:n turvaluokiteltuun tietoon sovellettavan turvallisuuden tason ja kyseisissä valtioissa ja järjestöissä sekä EU:ssa sovellettavien turvamääräysten johdonmukaisuuden perusteella; komission turvallisuusasioiden neuvonantajaryhmä antaa komissiolle asiasta teknisen lausuntonsa.

Ottaessaan EU:n turvaluokitellun tiedon vastaan yhteisön ulkopuoliset 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 komission edellyttämällä tavalla.

▼B

26.1.2. *Tasot*

Komission 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.

Yhteistyö on kolmitasoista:

1 taso

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

2 taso

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

3 taso

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

Menettelyt ja turvamääräykset, jotka esitellään yksityiskohtaisesti lisäyksissä 3, 4 ja 5, määräytyvät kunkin yhteistyön tason perusteella.

26.1.3. *Turvallisuussopimukset*

Komission tehtyä päätöksen, jonka mukaan luokiteltujen tietojen vaihtoon komission ja yhteisön ulkopuolisten valtioiden tai kansainvälisten järjestöjen välillä on pysyvä tai pitkäaikainen tarve, se laatii kyseisten valtioiden tai järjestöjen kanssa ”sopimuksia turvaluokiteltujen tietojen vaihtoa koskevista turvamenettelyistä”, joissa määritellään yhteistyön tarkoitus ja kyseisten tietojen suojelua koskevat vastavuoroiset säännöt.

Turvaluokiteltujen 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 ►**M1** RESTREINT UE ◄ -turvaluokkaa korkeampi.

Komission turvallisuusasioiden neuvonantajaryhmä hyväksyy luonnokset turvamenettelyistä tehtäviksi sopimuksiksi tai yhteisymmärryspöytäkirjoiksi ennen niiden antamista komission päätettäviksi.

Turvallisuusasioista vastaavan komission jäsenen on pyydettävä kansallisilta turvallisuusviranomaisilta kaikkea tarvittavaa apua sen varmistamiseksi, että luovutettavia tietoja käytetään ja suojellaan turvamenettelyistä tehtyjen sopimusten tai yhteisymmärryspöytäkirjojen määräysten mukaisesti.

▼M3

27. YRITYSTURVALLISUUTTA KOSKEVAT YHTEISET VÄHIMMÄISVAATIMUKSET

27.1. **Johdanto**

Tässä jaksossa käsitellään yritystoiminnan turvallisuusnäkökohtia, jotka koskevat pelkästään sellaisten sopimusten tai tukisopimusten neuvottelua ja tekemistä, joissa annettaviin tehtäviin liittyy ja/tai sisältyy EU:n turvaluokitellun tiedon käsittelyä, sekä yritysten tai muiden yksiköiden toteuttamaa tällaisten sopimusten täytäntöönpanoa, sekä myös EU:n turvaluokitellun tiedon luovuttamista tai käyttöä julkisia hankintoja koskevan tai ehdotuspyyntömenettelyn aikana (tarjouksentekovaiheessa ja sopimuksen tekemistä edeltävissä neuvotteluissa).

27.2. **Määritelmät**

Näissä vähimmäisvaatimuksissa tarkoitetaan:

a) ”turvaluokitellulla sopimuksella” mitä tahansa sopimusta tai tukisopimusta tuotteiden toimittamisesta, töiden suorittamisesta, rakennusten antamisesta käyttöön tai palvelujen tarjoamisesta, jonka täytäntöönpano edellyttää tai siihen liittyy EU:n turvaluokitellun tiedon käyttöä tai laatimista;

▼M3

b) ”turvaluokitellulla alihankintasopimuksella” toimeksisaajan tai tuensaajan toisen toimeksisaajan (toisin sanoen alihankkijan) kanssa tekemää sopimusta tuotteiden toimittamisesta, töiden suorittamisesta, rakennusten tai palvelujen tarjoamisesta, jonka täytäntöönpano edellyttää tai siihen liittyy EU:n turvaluokitellun tiedon käyttöä tai laatimista;

c) ”toimeksisaajalla” taloudellista toimijaa tai oikeushenkilöä, jolla on oikeuskelpoisuus tehdä sopimuksia tai olla tuensaaja;

d) ”nimetyllä turvallisuusviranomaisella (DSA)” EU:n jäsenvaltion kansalliselle turvallisuusviranomaiselle (NSA) vastuussa olevaa viranomaista, joka vastaa kaikkia yritysturvallisuuteen liittyviä asioita koskevasta kansallisesta politiikasta tiedottamisesta yrityksille ja muille yksiköille sekä ohjeiden ja avun antamisesta sen toteuttamisessa. Kansallinen turvallisuusviranomainen (NSA) voi hoitaa nimetyn turvallisuusviranomaisen (DSA) tehtävää;

e) ”laitoksen turvallisuusselvityksellä (FSC)” kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen antamaa hallinnollista päätöstä siitä, että tietty laitos kykenee tarjoamaan asianmukaisen turvallisuuden suojan EU:n tietyn turvaluokan turvaluokitellulle tiedolle ja että sen henkilöstön, jonka on tarpeen päästä käyttämään EU:n turvaluokiteltua tietoa, luotettavuus on selvitetty asiaankuuluvasti, ja että heille on selostettu EU:n turvaluokitellun tiedon käyttöön ja suojaamiseen liittyvät välttämättömät turvallisuusvaatimukset;

f) ”yrityksellä tai muulla yksiköllä” toimeksisaajaa tai alihankkijaa, joka osallistuu tavaroiden toimittamiseen, töiden suorittamiseen tai palvelujen tarjoamiseen; kyseessä voivat olla teolliset, kaupalliset, palvelu-, tiede-, tutkimus-, koulutus- tai kehitysalan yksiköt;

g) ”yritysturvallisuudella” suojaustoimenpiteiden ja –menettelyjen soveltamista tarkoituksena estää ja havaita toimeksisaajan tai alihankkijan sopimusta edeltävissä tai sopimusneuvotteluissa ja turvaluokiteltujen sopimusten yhteydessä käsittelemän EU:n turvaluokitellun tiedon katoaminen tai vaarantuminen sekä korjata tällaisen katoamisen tai vaarantumisen vaikutukset;

h) ”kansallisella turvallisuusviranomaisella (NSA)” EU:n jäsenvaltion viranomaista, jolla on perimmäinen vastuu EU:n turvaluokitellun tiedon suojaamisesta kyseisessä jäsenvaltiossa;

i) ”sopimuksen turvaluokituksen yleistasolla” koko sopimuksen tai tukisopimuksen turvaluokituksen määrittämistä sen perusteella, mille tasolle luokitellaan koko sopimuksen tai tukisopimuksen minkä tahansa osan mukaisesti laadittava, luovutettava tai käytettävä tai mahdollisesti laadittava, luovutettava tai käytettävä tieto ja/tai aineisto. Sopimuksen turvaluokituksen yleistaso ei voi olla matalampi kuin yhdenkään sen osan korkein turvaluokka, mutta voi olla korkeampi yhdistämisestä aiheutuvan vaikutuksen vuoksi;

j) ”turvallisuusnäkökohtia koskevalla kirjeellä (SAL)” hankintaviranomaisen antamia erityisiä sopimusehtoja, jotka muodostavat erottamattoman osan EU:n turvaluokitellun tiedon käyttöä tai tällaisen tiedon laadintaa käsittävää turvaluokiteltua sopimusta ja joissa määritellään turvaluokitellun sopimuksen turvallisuusvaatimukset tai osat, jotka edellyttävät turvallisuuden suojausta;

k) ”turvaluokitusohjeilla (SCG)” asiakirjaa, jossa kuvataan ohjelman, sopimuksen tai tukisopimuksen turvaluokiteltavat osat ja eritellään sovellettavat turvaluokitustasot. Turvaluokitusohjeita voidaan laajentaa koko ohjelman, sopimuksen tai tukisopimuksen voimassaolon ajan, ja tietojen osia voidaan luokitella uudelleen tai niiden turvaluokkaa alentaa. Turvaluokitusohjeiden on oltava osa turvallisuusnäkökohtia koskevaa kirjettä.

27.3. **Organisaatio**

a) Komissio voi antaa jäsenvaltiossa rekisteröidylle yritykselle tai muulle yksiköllе turvaluokitellulla sopimuksella tehtäviä, joihin liittyy ja/tai jotka sisältävät EU:n turvaluokitellun tiedon käsittelyä.

b) Komission on turvaluokiteltuja sopimuksia tehdessään varmistettava, että kaikkia näistä vähimmäisvaatimuksista johtuvia vaatimuksia noudatetaan.

c) Komission on otettava asianomainen kansallinen turvallisuusviranomainen tai kansalliset turvallisuusviranomaiset osalliseksi näiden yritysturvallisuutta koskevien vähimmäisvaatimusten soveltamista. Kansalliset turvallisuusviranomaiset voivat siirtää nämä tehtävät yhdelle tai useammalle nimetylle turvallisuusviranomaiselle (DSA).

d) Perimmäinen vastuu EU:n turvaluokitellun tiedon suojaamisesta yrityksissä tai muissa yksiköissä on kyseisten yksiköiden johdolla.

e) Tehtäessä turvaluokiteltua sopimusta tai alihankintasopimusta, joka kuuluu näiden vähimmäisvaatimusten soveltamisalaan, komission ja/tai kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen, tapauksen mukaan, on ilmoitettava asiasta viipymättä sen jäsenvaltion kansalliselle turvallisuusviranomaiselle tai nimetylle turvallisuusviranomaiselle, jossa toimeksisaaja tai alihankkija on rekisteröity.

▼M3

27.4. **Turvaluokitellut sopimukset ja tukipäätökset**

a) Sopimusten tai tukisopimusten turvaluokituksen yhteydessä on otettava huomioon seuraavat periaatteet:

— komissio määrittelee tarpeen mukaan turvaluokitellun sopimuksen osat, joiden suojaaminen ja sen myötä turvaluokittelu on tarpeen; tätä tehdessään sen on otettava huomioon tiedon luovuttajan ennen turvaluokitellun sopimuksen tekemistä tuotetulle tiedolle määrittämä alkuperäinen turvaluokitus;

— sopimuksen turvaluokituksen yleistaso ei voi olla matalampi kuin yhdenkään sen osan korkein turvaluokka;

— sopimukseen liittyvän toiminnan yhteydessä tuotetut EU:n turvaluokitellut tiedot luokitellaan turvaluokitusohjeiden mukaisesti;

— komissio on tarvittaessa vastuussa sopimuksen turvaluokituksen yleistason tai jonkin sen osan turvaluokituksen muuttamisesta tiedon alkuperäistä luovuttajaa kuullen sekä kaikille asianomaisille osapuolille tiedottamisesta;

— toimeksisaajalle tai alihankkijalle luovutettuja turvaluokiteltuja tietoja tai sopimukseen liittyvän toiminnan yhteydessä tuotettuja tietoja ei saa käyttää muuhun kuin turvaluokitellussa sopimuksessa määriteltyihin tarkoituksiin eikä niitä saa paljastaa kolmansille osapuolille ilman tiedon alkuperäisen luovuttajan kirjallista ennakkosuostumusta.

b) Komissio ja asianomaisten jäsenvaltioiden kansalliset turvallisuusviranomaiset ja/tai nimetyt turvallisuusviranomaiset ovat vastuussa sen varmistamisesta, että toimeksisaajat tai alihankkijat, joiden kanssa on tehty CONFIDENTIEL UE –turvaluokan tai sitä luottamuksellisemman turvaluokan tietoja käsittävä turvaluokiteltu sopimus, ryhtyvät kaikkiin tarvittaviin toimenpiteisiin tällaisen, niille turvaluokitellun sopimuksen kansallisten lakien ja asetusten mukaisen täytäntöönpanon yhteydessä luovutetun tai niiden tuottaman EU:n turvaluokitellun tiedon suojaamiseksi. Turvallisuusvaatimusten noudattamatta jättäminen saattaa johtaa turvaluokitellun sopimuksen irtisanomiseen.

c) Kaikille sellaisiin turvaluokiteltuihin sopimuksiin osallistuville yrityksille tai muille yksiköille, joihin liittyy pääsy CONFIDENTIEL UE –turvaluokan tai sitä luottamuksellisemman turvaluokan tietoihin, on oltava tehty kansallinen laitoksen turvallisuusselvitys (FSC). Jäsenvaltion kansallinen turvallisuusviranomainen ja/tai nimetty turvallisuusviranomainen tekee ja hyväksyy laitoksen turvallisuusselvityksen vahvistukseksi siitä, että laitos kykenee tarjoamaan ja takaamaan asianmukaisen turvallisuuden suojan asianomaiseen turvaluokkaan kuuluvalle EU:n turvaluokitellulle tiedolle.

d) Tehtäessä turvaluokiteltua sopimusta toimeksisaajan tai alihankkijan johdon nimittämä laitoksen turvavastaava (FSO) vastaa henkilöstön luotettavuusselvityksen (PSC) pyytämisestä kaikille jossakin EU:n jäsenvaltiossa rekisteröidyn yrityksen tai muun yksikön palveluksessa oleville henkilöille, joiden tehtävät turvaluokitellun sopimuksen mukaisesti edellyttävät pääsyä CONFIDENTIEL UE –turvaluokan tai sitä luottamuksellisemman turvaluokan tietoihin; selvityksen tekee kyseisen jäsenvaltion kansallinen turvallisuusviranomainen tai nimetty turvallisuusviranomainen kansallisten säännösten mukaisesti.

e) Turvaluokiteltujen sopimusten on sisällettävä 27 jakson 2 kohdan j alakohdassa määritelty turvallisuusnäkökohtia koskeva kirje (SAL). Turvallisuusnäkökohtia koskevan kirjeen on sisällettävä turvaluokitusohjeet.

f) Ennen turvaluokiteltua sopimusta koskevan neuvottelumenettelyn aloittamista komissio ottaa yhteyttä sen jäsenvaltion turvallisuusviranomaiseen tai nimettyyn turvallisuusviranomaiseen, jossa kyseiset yritykset tai muut yksiköt on rekisteröity, saadakseen vahvistuksen siitä, että niillä on voimassa oleva, sopimuksen turvaluokituksen tasoa vastaava laitoksen turvallisuusselvitys.

g) Hankintaviranomainen ei saa tehdä turvaluokiteltua sopimusta etusijalle asetetun taloudellisen toimijan kanssa ennen kuin on saanut laitoksen turvallisuusselvitystä koskevan voimassa olevan luotettavuustodistuksen.

h) Laitoksen turvallisuusselvitystä ei edellytetä sopimuksilta, joihin liittyvien tietojen turvaluokitus on RESTREINT UE, ellei jäsenvaltion kansallisissa laeissa ja asetuksissa sitä vaadita.

i) Turvaluokiteltuihin sopimuksiin liittyviin tarjouskilpailuihin on sisällyttävä määräys, jonka mukaan taloudellisen toimijan, joka ei tee tarjousta tai jota ei valita, on palautettava kaikki asiakirjat tietyn määräajan kuluessa.

j) Toimeksisaajien on mahdollisesti neuvoteltava turvaluokiteltuja alihankintasopimuksia eri tasoilla toimivien alihankkijoiden kanssa. Toimeksisaaja on vastuussa sen varmistamisesta, että kaikki alihankintatoiminta toteutetaan tähän jaksoon sisältyvien yhteisten vähimmäisvaatimusten mukaisesti. Toimeksisaaja ei kuitenkaan saa siirtää EU:n turvaluokiteltua tietoa tai aineistoa alihankkijalle ilman tiedon alkuperäisen luovuttajan kirjallista ennakkosuostumusta.

▼M3

k) Edellytykset, joiden mukaisesti toimeksisaaja voi teettää tehtäviä alihankintana, on määriteltävä tarjouskilpailussa tai ehdotuspyynnössä sekä turvaluokitellussa sopimuksessa. Alihankintasopimusta ei saa tehdä EU:n ulkopuoliseen valtioon rekisteröidyn yksikön kanssa ilman komission nimenomaista kirjallista suostumusta.

l) Komissio seuraa turvaluokitellun sopimuksen kaikkien turvallisuussäännösten noudattamista koko sen voimassaolon ajan yhdessä asianomaisen kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen kanssa. Kaikista turvallisuuteen liittyvistä tapahtumista on ilmoitettava näiden turvallisuussääntöjen II osan 24 jaksoon sisältyvien määräysten mukaisesti. Jos laitoksen turvallisuusselvitykseen tehdään muutoksia tai se peruutetaan, asiasta on ilmoitettava välittömästi komissiolle ja kaikille kansallisille turvallisuusviranomaisille tai nimetyille turvallisuusviranomaisille, joille se on annettu tiedoksi.

m) Kun turvaluokiteltu sopimus tai turvaluokiteltu alihankintasopimus irtisanotaan, komission ja/tai kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen, tapauksen mukaan, on ilmoitettava asiasta viipymättä sen jäsenvaltion kansalliselle turvallisuusviranomaiselle tai nimetylle turvallisuusviranomaiselle, jossa toimeksisaaja tai alihankkija on rekisteröity.

n) Toimeksisaajien ja alihankkijoiden on noudatettava edelleen tähän jaksoon sisältyviä yhteisiä vähimmäisvaatimuksia ja säilytettävä turvaluokitellun tiedon luottamuksellisuus turvaluokitellun sopimuksen tai turvaluokitellun alihankintasopimuksen irtisanomisen tai päättymisen jälkeen.

o) Turvallisuusnäkökohtia koskevassa kirjeessä tai muissa asian kannalta olennaisissa, turvallisuusvaatimuksia yksilöivissä säännöksissä annetaan erityiset määräykset turvaluokitellun tiedon hävittämisestä turvaluokitellun sopimuksen päättyessä.

p) Tässä jaksossa mainittuja velvoitteita ja edellytyksiä sovelletaan soveltuvin osin menettelyihin, joissa päätöksellä myönnetään tukia, ja erityisesti tällaisten tukien saajiin. Kaikki tuensaajan velvoitteet on esitettävä tukipäätöksessä.

27.5. **Vierailut**

Turvaluokiteltuihin sopimuksiin liittyvät komission henkilöstön vierailut jäsenvaltioissa toimiviin yrityksiin tai muihin yksiköihin, jotka panevat täytäntöön EU:n turvaluokiteltuja sopimuksia, on järjestettävä asianomaisen kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen kanssa. EU:n turvaluokiteltuun sopimukseen liittyvät yritysten tai muiden yksiköiden työntekijöiden vierailut on järjestettävä asianomaisten kansallisten turvallisuusviranomaisten tai nimettyjen turvallisuusviranomaisten kesken. EU:n turvaluokitellussa sopimuksessa mukana olevat kansalliset turvallisuusviranomaiset tai nimetyt turvallisuusviranomaiset voivat kuitenkin sopia menettelystä, jonka mukaan yritysten tai muiden yksiköiden työntekijöiden vierailut voidaan järjestää suoraan.

27.6. **EU:n turvaluokitellun tiedon lähettäminen ja kuljettaminen**

a) EU:n turvaluokitellun tiedon lähettämisen osalta sovelletaan näiden turvallisuussääntöjen II osan 21 jakson määräyksiä. Tällaisten määräysten täydentämiseksi sovelletaan jäsenvaltioissa voimassa olevia menettelyjä.

b) Turvaluokiteltuihin sopimuksiin liittyvän EU:n turvaluokitellun aineiston kansainväliset kuljetukset toteutetaan jäsenvaltioiden kansallisten menettelyjen mukaisesti. Kansainvälisten kuljetusten turvallisuusjärjestelyjä tarkasteltaessa sovelletaan seuraavia periaatteita:

   — Turvallisuus varmistetaan kuljetuksen kaikissa vaiheissa ja kaikissa olosuhteissa, lähtöpisteestä aina lopulliseen määränpäähän saakka.

   — Lähetyksen suojauksen taso määritellään siihen sisältyvän aineiston korkeimman turvaluokan mukaisesti.

   — Kuljetuksia hoitaville yrityksille tehdään tarvittaessa laitoksen turvallisuusselvitys. Tällaisessa tapauksessa lähetystä hoitavasta henkilöstöstä on oltava tehty turvallisuusselvitys tähän jaksoon sisältyvien yhteisten vähimmäisvaatimusten mukaisesti.

   — Matkat tehdään mahdollisuuksien mukaan suoraan yhdestä paikasta toiseen ja niin nopeasti kuin olosuhteet sallivat.

▼**M3**

— Reittien olisi kuljettava mahdollisuuksien mukaan pelkästään EU:n jäsenvaltioiden kautta. EU:n ulkopuolisten maiden kautta kulkevia reittejä olisi käytettävä ainoastaan silloin, kun sekä lähettäjän että vastaanottajan kotivaltion kansallinen turvallisuusviranomainen tai nimetty turvallisuusviranomainen on antanut siihen luvan.

— Ennen EU:n turvaluokitellun aineiston siirtämistä lähettäjä laatii kuljetussuunnitelman ja asianomainen kansallinen turvallisuusviranomainen tai nimetty turvallisuusviranomainen hyväksyy sen.

▼**M1**

Lisäys 1

KANSALLISTEN TURVALLISUUSLUOKITUSTEN VERTAILU

EU:n luokitus	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
WEU:n luokitus	FOCAL TOP SECRET	WEU SECRET	WEU CONFI-DENTIAL	WEU RESTRICTED
Euratomin luokitus	EURA TOP SECRET	EURA SECRET	EURA CONFI-DENTIAL	EURA RESTRICTED
NATOn luokitus	COSMIC TOP SECRET	NATO SECRET	NATO CONFI-DENTIAL	NATO RESTRICTED
Itävalta	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgia	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Kypros	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Tšekki	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Tanska	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Viro	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Saksa	Streng geheim	Geheim	VS [1] — Vertraulich	VS — Nur für den Dienstgebrauch
Kreikka	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Suomi	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Ranska	Très Secret Défense [2]	Secret Défense	Confidentiel Défense	
Irlanti	Top Secret	Secret	Confidential	Restricted
Italia	Segretissimo	Segreto	Riservatissimo	Riservato
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Liettua	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Unkari	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Alankomaat	Stg [3]. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Puola	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugali	Muito Secreto	Secreto	Confidencial	Reservado
Slovenia	Strogo tajno	Tajno	Zaupno	SVN Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Espanja	Secreto	Reservado	Confidencial	Difusión Limitada
Ruotsi	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

▼**M1**

Yhdistynyt kuningaskunta	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) Luokitusta ”Très Secret Défense”, joka kattaa hallituksen ensisijaiset kysymykset, voidaan muuttaa ainoastaan pääministerin luvalla.
([3]) Stg = staatsgeheim.

Lisäys 2

LUOKITTELUOHJEET

Tämä ohje on suuntaa antava eikä sitä saa tulkita niin, että se muuttaa 16, 17, 20 ja 21 jaksoissa annettuja sisältöä koskevia määräyksiä.

Luokitus	Milloin	Kuka	Merkinnät	Turvaluokan alentaminen / turvaluokan poistaminen / hävittäminen	
				Kuka	Milloin
►**M1** TRES SECRET UE/EU TOP SECRET ◄: Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo voisi poikkeuksellisen vakavasti vahingoittaa Euroopan unionin tai sen yhden tai useamman jäsenvaltion olennaisia etuja [16.1].	Kun "►**M1** TRES SECRET UE/EU TOP SECRET ◄" -aineiston julkistaminen todennäköisesti — uhkaisi suoraan EU:n, jäsenvaltion tai ystävällismielisen maan 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.	Asianmukaisesti valtuutetut henkilöt (tietojen luovuttajat), pääjohtajat, yksikönpäälliköt [17.1] Tietojen luovuttajat ilmoittavat päivämäärän, ajanjakson tai tapahtuman, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai turvaluokitus poistaa kokonaisuudessaan [16.2]. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [17.3].	►**M1** TRES SECRET UE/EU TOP SECRET ◄ -luokitus merkitään ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -asiakirjoihin, ja soveltuvilta osin lisätään turvasoitin ja/tai puolustusasioihin viittaava merkintä ESDP mekaanisesti ja käsin [16.4, 16.5, 16.3]. EU:n luokitus ja turvaosoitin 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 [21.1].	Turvaluokan poistamisesta tai alentamisesta voi päättää ainoastaan tietojen luovuttaja, joka ilmoittaa muutoksesta kaikille myöhemmille vastaanottajille, joille asiakirja on lähetetty tai kopioitu [17.3]. ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan keskusrekisterin tai alarekisterin toimesta. Jokainen hävitetty asiakirja merkitään hävittämisluetteloon, jonka allekirjoittavat ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valvontavastaava sekä hävittämisen todistava virkailija, jolla on ►**M1** TRES SECRET UE/EU TOP SECRET ◄ turvaluokan valtuutus. Päiväkirjaan tehdään asiaa koskeva merkintä. Rekisteri säilyttää hävittämistodistukset ja jakeluluettelot kymmenen vuotta [22.5].	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [22.5]. ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -asiakirjat, mukaan luettuina kaikki ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -asiakirjojen laatimisesta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja hiilipaperi, hävitetään ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan valvontavastaavan valvonnassa polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei niitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa [22.5].
►**M1** SECRET UE ◄: Tätä luokitusta sovelletaan ainoastaan sellaiseen tietoon ja aineistoon, jonka luvaton ilmitulo voisi vakavasti vahingoittaa	Kun ►**M1** SECRET UE ◄ -aineiston julkistaminen todennäköisesti — aiheuttaisi kansainvälisiä jännitteitä	Asianmukaisesti valtuutetut henkilöt (tietojen luovuttajat), pääjohtajat, yksikönpäälliköt [17.1]. Tietojen luovuttajat ilmoittavat	►**M1** SECRET UE ◄ -luokitus merkitään ►**M1** SECRET UE ◄ -asiakirjoihin, ja soveltuvilta osin lisätään turvaosoitin ja/tai	Turvaluokan poistamisesta tai alentamisesta voi päättää ainoastaan tietojen luovuttaja, joka ilmoittaa muutoksesta kaikille myöhemmille vastaa-	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [22.5]. ►**M1** SECRET UE ◄ -asiakirjat, mukaan luettuina kaikki

Luokitus	Milloin	Kuka	Merkinnät	Turvaluokan alentaminen / turvaluokan poistaminen / hävittäminen	
				Kuka	Milloin
Euroopan unionin tai yhden tai useamman jäsenvaltion olennaista etua [16.1].	— 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.	päivämäärän tai ajanjakson, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai turvaluokitus poistaa kokonaisuudessaan [16.2]. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [17.3].	puolustusasioihin viittaava merkintä ESDP mekaanisesti ja käsin [16.4, 16.5, 16.3]. EU:n luokitus ja turvaosoitin 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 [21.1].	nottajille, joille asiakirja on lähetetty tai kopioitu [17.3]. ►**M1** SECRET UE ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun virkamiehen valvonnassa. Hävitetyt ►**M1** SECRET UE ◄ -asiakirjat kirjataan allekirjoitettaviin hävittämistodistuksiin, jotka rekisteri säilyttää hävittämislomakkeiden kanssa vähintää kolme vuotta [22.5].	►**M1** SECRET UE ◄ -asiakirjojen laatimisesta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja hiilipaperi, hävitetään polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei niitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa [22.5].
►**M1** CONFIDENTIEL UE ◄: Tätä luokitusta sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton paljastaminen vahingoittaisi Euroopan unionin tai yhden tai useamman jäsenvaltion olennaista etua [16.1].	Kun ►**M1** 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	Asianmukaisesti valtuutetut henkilöt (tietojen luovuttajat), pääjohtajat ja yksikönpäälliköt [17.1]. Tietojen luovuttajat ilmoittavat päivämäärän tai ajanjakson, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai poistaa turvaluokka kokonaisuudessaan [16.2]. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [17.3].	►**M1** CONFIDENTIEL UE ◄ -luokitus merkitään ►**M1** CONFIDENTIEL UE ◄ -asiakirjoihin, ja soveltuvilta osin lisätään turvaosoitin ja/tai puolustusasioihin viittaava merkintä ESDP mekaanisesti ja käsin tai painamalla ennalta leimattuun, rekisteröityyn paperiin [16.4, 16.5, 16.3]. 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	Turvaluokan poistamisesta tai alentamisesta voi päättää ainoastaan tietojen luovuttaja, joka ilmoittaa muutoksesta kaikille myöhemmille vastaanottajille, joille asiakirja on lähetetty tai kopioitu [17.3]. ►**M1** CONFIDENTIEL UE ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin toimesta asiakirjojen käsittelyyn oikeutetun virkamiehen valvonnassa. Niiden hävittäminen kirjataan kansallisten asetusten mukaisesti ja komission tai EU:n hajautettujen erillisvirastojen tapauksessa ►**M2** turvallisuusasioista	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [22.5]. ►**M1** CONFIDENTIEL UE ◄ -asiakirjat, mukaan luettuina kaikki ►**M1** CONFIDENTIEL UE ◄ -asiakirjojen laatimisesta syntynyt luokiteltu jäte, kuten vialliset kopiot, luonnokset, muistiinpanot ja hiilipaperi, hävitetään polttamalla, silppuamalla, repimällä tai muuttamalla muuten sellaiseen muotoon, ettei niitä voida tunnistaa eikä palauttaa alkuperäiseen muotoonsa [22.5].

Luokitus	Milloin	Kuka	Merkinnät	Turvaluokan alentaminen / turvaluokan poistaminen / hävittäminen	
				Kuka	Milloin
	— 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.		[21.1].	vastaavan komission jäsenen ◄ ohjeiden mukaisesti [22.5].	
►**M1** RESTREINT UE ◄: Tätä luokitusta sovelletaan sellaiseen tietoon ja aineistoon, jonka luvaton paljastaminen voisi olla Euroopan unionin tai yhden tai useamman jäsenvaltion edun vastaista [16.1].	Kun ►**M1** RESTREINT UE ◄ -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 sitoumuksia säilyttää kolmansien osapuolten luovuttamien tietojen luottamuksellisuus	Asianmukaisesti valtuutetut henkilöt (tietojen luovuttajat), pääjohtajat, yksikönpäälliköt [17.1]. Tietojen luovuttajat ilmoittavat päivämäärän, ajanjakson tai tapahtuman, jolloin sisältö voidaan siirtää alempaan turvaluokkaan tai turvaluokka poistaa kokonaisuudessaan [16.2]. Muuten he tarkistavat asiakirjojen turvaluokituksen vähintään joka viides vuosi varmistaakseen, että alkuperäinen luokitus on tarpeen [17.3].	►**M1** RESTREINT UE ◄ -luokitus merkitään ►**M1** RESTREINT UE ◄ -asiakirjoihin, ja soveltuvilta osin lisätään turvaosoitin ja/tai puolustusasioihin viittaava merkintä ESDP mekaanisesti tai sähköisesti [16.4, 16.5, 16.3]. EU:n luokitus ja turvaosoitin ilmoitetaan ensimmäisen sivun yläreunassa ja kaikki sivut numeroidaan. Kaikissa asiakirjoissa on viitenumero ja päivämäärä [21.1].	Turvaluokan poistamisesta voi päättää ainoastaan tietojen luovuttaja, joka ilmoittaa muutoksesta kaikille myöhemmille vastaanottajille, joille asiakirja on lähetetty tai kopioitu [17.3]. ►**M1** RESTREINT UE ◄ -asiakirjojen hävittäminen tapahtuu niistä vastaavan rekisterin tai käyttäjän toimesta ►**M2** turvallisuusasioista vastaavalta komission jäseneltä ◄ saatujen ohjeiden mukaisesti [22.5].	Ylimääräiset kopiot ja asiakirjat, joita ei enää tarvita, on hävitettävä [22.5].

▼B

Luokitus	Milloin	Kuka	Merkinnät	Turvaluokan alentaminen / turvaluokan poistaminen / hävittäminen	
				Kuka	Milloin
	— 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 poliitikkojen tehokasta kehittämistä tai toteuttamista — haittaisi EU:n asianmukaista hallintoa ja sen toimia.				

▼B

Lisäys 3

Ohjeet EU:n turvaluokitellun tiedon luovuttamisesta yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille: 1 tason yhteistyö

MENETTELYT

1. Vain kollegiona toimivalla komissiolla on toimivalta luovuttaa EU:n turvaluokiteltua tietoa valtioille, jotka eivät ole Euroopan unionin jäseniä, tai muille kansainvälisille järjestöille, joilla on vastaava turvallisuuspolitiikka ja turvallisuusmääräykset kuin EU:lla.
2. Ennen turvallisuussopimuksen tekemistä turvallisuusasioista vastaava komission jäsen on toimivaltainen tarkastelemaan EU:n turvaluokitellun tiedon luovuttamista koskevia pyyntöjä.
3. Pyyntöjä tarkastellessaan hän
   — pyytää lausunnot luovutettavan EU:n turvaluokitellun tiedon alkuperäisiltä luovuttajilta,
   — 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 turvallisuussäännösten mukaisesti,
   — pyytää komission turvallisuusasioiden neuvonantajaryhmän lausuntoa edunsaajina olevien valtioiden tai kansainvälisten elinten luotettavuudesta.
4. Turvallisuusasioista vastaava komission jäsen toimittaa pyynnön ja komission turvallisuusasioiden neuvonantajaryhmän lausunnon komissiolle päätöksentekoa varten.

TURVALLISUUTTA KOSKEVAT SÄÄNNÖT, JOITA EDUNSAAJIEN ON SOVELLETTAVA

5. Turvallisuusasioista vastaava komission jäsen ilmoittaa edunsaajina oleville valtioille tai kansainvälisille järjestöille komission päätöksestä sallia EU:n turvaluokitellun tiedon luovuttaminen.
6. Luovutuspäätös tulee voimaan vasta, kun edunsaajat ovat antaneet kirjallisen vakuutuksen siitä, että ne:
   — käyttävät tietoa ainoastaan sovittuihin tarkoituksiin,
   — suojaavat tiedon näiden turvallisuussäännösten ja erityisesti jäljempänä mainittujen erityissääntöjen mukaisesti.
7. Henkilöstö
   a) EU:n turvaluokiteltuun tietoon pääsevien virkamiesten määrä on rajattava tiedonsaantitarpeen periaatteen pohjalta tiukasti niihin henkilöihin, joiden tehtävät edellyttävät pääsyä kyseiseen tietoon.
   b) Kaikilla viranomaisilla ja kansalaisilla, jotka valtuutetaan pääsemään ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan tietoon, on oltava joko asianmukaisen turvaluokan luotettavuustodistus tai vastaava luotettavuusselvitys, jonka heidän oman maansa hallitus on myöntänyt.
8. Asiakirjojen lähettäminen
   a) Asiakirjojen lähettämistä koskevista käytännön menettelyistä päätetään sopimuksella. Ennen tällaisen sopimuksen tekemistä sovelletaan 21 jakson säännöksiä. Sopimuksessa täsmennetään erityisesti ne rekisterin pitäjät, joille EU:n turvaluokiteltu tieto on lähetettävä.
   b) Jos turvaluokiteltuun tietoon, jonka luovuttamisen komissio on sallinut, sisältyy ►**M1** TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan tietoa, edunsaajana olevan valtion tai kansainvälisen järjestön on perustettava keskustoimisto EU-asioiden rekisteröintiä varten ja tarvittaessa alarekistereitä. Näiden rekisterien on sovellettava näiden turvallisuussäännösten osalta tiukasti 22 jaksossa määriteltyjä vastaavia säännöksiä.
9. Rekisteröinti

   Välittömästi rekisterin pitäjän vastaanotettua ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan EU:n asiakirjan, sen on merkittävä asiakirja järjestön hallinnoimaan erityiseen rekisteriin, jossa on sarakkeet, joihin merkitään vastaanottopäivämäärä, asiakirjaa koskevia tietoja (päivämäärä, viitenumero ja kopion numero), asiakirjan turvaluokka, otsikko, vastaanottajan nimi tai ammattinimike, kuitin palautuspäivämäärä sekä päivämäärä, jona asiakirja palautetaan EU:n luovuttajalle tai hävitetään.

▼B

10. Hävittäminen

a) EU:n turvaluokitellut asiakirjat on hävitettävä näiden turvallisuussäännösten 22 jaksossa esitettyjen ohjeiden mukaisesti. Kopiot ►M1 SECRET UE ◄- ja ►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan asiakirjojen hävittämistodistuksista on lähetettävä asiakirjat toimittaneelle EU:n rekisterin pitäjälle.

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

11. Asiakirjojen suojaaminen

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

12. Kopiot, käännökset ja otteet

►M1 CONFIDENTIEL UE ◄- tai ►M1 SECRET UE ◄ -turvaluokan asiakirjasta ei saa ottaa valokopiota tai tehdä käännöstä tai ottaa siitä poimintoja ilman asianomaisen turvallisuusyksikön esimiehen valtuutusta, joka kirjaa ja tarkistaa kyseiset kopiot, käännökset tai otteet ja leimaa ne tarvittaessa.

►M1 TRES SECRET UE/EU TOP SECRET ◄ -turvaluokan asiakirjan jäljentämisen tai kääntämisen voi sallia ainoastaan luovuttava viranomainen, joka vahvistaa sallittujen kopioiden määrän; jos luovuttavaa viranomaista ei pystytä määrittämään, pyyntö toimitetaan edelleen ►M2 komission turvallisuudesta vastaavalle linjalle ◄.

13. Turvallisuuden vaarantuminen

Silloin kun EU:n turvaluokitellun asiakirjan turvallisuus on vaarantunut tai sen epäillään vaarantuneen, on viipymättä suoritettava seuraavat toimet, jollei turvallisuussopimuksesta muuta johdu:

a) tehdään tutkimus turvallisuuden vaarantumiseen johtaneiden olosuhteiden osoittamiseksi;

b) annetaan ►M2 komission turvallisuudesta vastaavalle linjalle ◄, asiaankuuluvalle 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 estämiseksi;

e) toteutetaan kaikki ►M2 komission turvallisuudesta vastaavan linjan ◄ suosittelemat toimenpiteet tapahtuneen toistumisen estämiseksi.

14. Tarkastukset

►M2 Komission turvallisuudesta vastaavan linjan ◄ sallitaan asianomaisten valtioiden tai kansainvälisten järjestöjen kanssa tehtävän sopimuksen perusteella arvioida luovutetun EU:n turvaluokitellun tiedon suojaamisessa käytettyjen toimenpiteiden tehokkuus.

15. Raportointi

Jollei tehdystä turvallisuussopimuksesta muuta johdu, 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 turvallisuussäännöksiä on noudatettu.

▼B

Lisäys 4

Ohjeet EU:n turvaluokitellun tiedon luovuttamisesta yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille: 2 tason yhteistyö

MENETTELYT

1. Vain tiedon alkuperäisellä luovuttajalla on toimivalta luovuttaa EU:n turvaluokiteltua tietoa yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille, joilla on selvästi erilainen turvallisuuspolitiikka ja turvallisuusmääräykset kuin EU:lla. Kollegiona toimivalla komissiolla on toimivalta luovuttaa komissiossa tuotettua EU:n turvaluokiteltua tietoa.
2. Periaatteessa luovuttaminen on rajattu ►**M1** SECRET UE ◄ -turvaluokan ja sitä alemman turvaluokan tietoon; erityisin turvaosoittimin tai -merkinnöin suojattua turvaluokiteltua tietoa ei saa luovuttaa.
3. Ennen turvallisuussopimuksen tekemistä turvallisuusasioista vastaava komission jäsen on toimivaltainen tarkastelemaan EU:n turvaluokitellun tiedon luovuttamista koskevia pyyntöjä.
4. Pyyntöjä tarkastellessaan hän
   — pyytää lausunnot luovutettavan EU:n turvaluokitellun tiedon alkuperäisiltä luovuttajilta,
   — luo tarvittavat 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 komission turvallisuusasioiden neuvonantajaryhmän kokouksen tai tekee tiedusteluja, hiljaisen hyväksynnän menettelyllä mikäli tarpeellista, jäsenvaltioiden kansallisilta turvallisuusviranomaisilta, jotta komission turvallisuusasioiden neuvonantajaryhmältä saataisiin tekninen lausunto.
5. Komission turvallisuusasioiden neuvonantajaryhmän lausunto koskee seuraavia seikkoja:
   — 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 tietojen ja asiakirjojen käsittelyä (EU:n turvaluokkaotsikoiden säilyttäminen tai poistaminen, erityismerkinnät jne.),
   — siirtäminen alempaan turvaluokkaan tai luokituksen poistaminen ennen kuin tieto luovutetaan edunsaajina oleville valtioille tai kansainvälisille järjestöille.
6. Turvallisuusasioista vastaava komission jäsen toimittaa pyynnön ja komission turvallisuusasioiden neuvonantajaryhmän lausunnon komissiolle päätöksentekoa varten.

TURVALLISUUTTA KOSKEVAT SÄÄNNÖT, JOITA EDUNSAAJIEN ON SOVELLETTAVA

7. Turvallisuusasioista vastaava komission jäsen ilmoittaa edunsaajina oleville valtioille tai kansainvälisille järjestöille komission päätöksestä sallia EU:n turvaluokitellun tiedon luovuttaminen ja päätöstä koskevista rajoituksista.
8. Luovutuspäätös tulee voimaan vasta, kun edunsaajat ovat antaneet kirjallisen vakuutuksen siitä, että ne:
   — käyttävät tietoa ainoastaan sovittuihin tarkoituksiin,
   — suojaavat tiedon komission vahvistamien säännösten mukaisesti.
9. Ellei komissio, saatuaan komission turvallisuusasioiden neuvonantajaryhmän teknisen lausunnon, päätä erityisestä menettelytavasta EU:n turvaluokiteltujen asiakirjojen käsittelemiseksi (poistetaan maininta EU:n turvaluokasta, erityismerkinnät jne.), laaditaan seuraavanlaiset suojaamista koskevat säännöt.
10. Henkilöstö
    a) EU:n turvaluokiteltuun tietoon pääsevien virkamiesten määrä on rajattava tiedonsaantitarpeen periaatteen pohjalta tiukasti niihin henkilöihin, joiden tehtävät edellyttävät pääsyä kyseiseen tietoon.

▼B

b) Kaikilla viranomaisilla ja kansalaisilla, jotka valtuutetaan pääsemään komission luovuttamaan turvaluokiteltuun tietoon, on oltava hyväksytty kansallinen luotettavuusselvitys 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 ►M2 komission turvallisuudesta vastaavan linjan johtajalle ◄ tiedoksi.

11. Asiakirjojen lähettäminen

Asiakirjojen lähettämistä koskevista käytännön menettelyistä päätetään sopimuksella. Ennen tällaisen sopimuksen tekemistä sovelletaan 21 jakson säännöksiä. Sopimuksessa täsmennetään erityisesti ne rekisterin pitäjät, joille EU:n turvaluokiteltu tieto on lähetettävä eteenpäin sekä EU:n turvaluokitellun tiedon lähettämisessä käytettävät kuriiri- tai postilaitokset.

12. Kirjaaminen saapumisen yhteydessä

Vastaanottajavaltion kansallinen turvallisuusviranomainen tai sitä vastaava elin ottaa vastaan hallituksensa puolesta komission lähettämää turvaluokiteltua tietoa, 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 kopionumero), asiakirjan turvaluokka, otsikko, vastaanottajan nimi tai ammattinimike, kuitin palautuspäivämäärä sekä päivämäärä, jona asiakirja palautetaan EU:n luovuttajalle tai hävitetään.

13. Asiakirjojen palauttaminen

Kun vastaanottaja palauttaa turvaluokitellun asiakirjan komissiolle sen on toimittava edellä olevassa asiakirjojen lähettämissä koskevassa kohdassa tarkoitetun menettelytavan mukaisesti.

14. Suojaus

a) Silloin kun asiakirjat eivät ole käytössä, ne on varastoitava turvalliseen säilytyspaikkaan, joka on hyväksytty saman turvaluokan kansallisesti luokitellun aineiston varastoimiseen. Turvallisessa säilytyspaikassa ei saa olla mitään merkintöjä, jotka viittaisivat sen sisältöön. Sisältöön 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. Se on vaihdettava aikaisemmin, jos virkailija vaihtuu, jonkin numeroyhdistelmän tuntevan virkailijan luotettavuusselvitys peruutetaan tai havaitaan riski turvallisuuden vaarantumisesta.

b) Ainoastaan virkailijat, joilla on valtuutus päästä EU:n turvaluokiteltuun tietoon ja joiden on tarpeen saada kyseistä tietoa, 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 sitten, kun he ovat lopettaneet niihin tutustumisen, sekä työajan ulkopuolella.

c) ►M1 CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan asiakirjasta ei saa ottaa valokopioita eikä poimintoja ilman ►M2 komission turvallisuudesta vastaavan linjan ◄ lupaa.

d) Menettelytapa asiakirjojen nopeaksi ja täydelliseksi hävittämiseksi hätätapauksissa on määriteltävä ja vahvistettava yhdessä ►M2 komission turvallisuudesta vastaavan linjan ◄ kanssa.

15. Fyysinen turvallisuus

a) Silloin kun EU:n turvaluokitellut asiakirjat eivät ole käytössä, niiden 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, valtion tai järjestön turvallisuusyksikön jäsenen tai erityisesti kyseisen huoneen turvallisuuden valvonnasta vastaavan virkailijan on 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.

▼B

16. Turvallisuuden vaarantuminen

Silloin kun EU:n turvaluokitellun asiakirjan turvallisuus on vaarantunut tai sen epäillään vaarantuneen, on viipymättä toteutettava seuraavat toimet:

a) toimitetaan välittömästi selostus tapahtuneesta ►M2 komission turvallisuudesta vastaavalle linjalle ◄ tai aloitteen asiakirjojen edelleen lähettämisestä tehneen jäsenvaltion kansalliselle turvallisuusviranomaiselle (sekä kopio siitä ►M2 komission turvallisuudesta vastaavalle linjalle ◄);

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

17. Tarkastukset

►M2 Komission turvallisuudesta vastaavan linjan ◄ sallitaan asianomaisten valtioiden tai kansainvälisten järjestöjen kanssa tehtävän sopimuksen perusteella arvioida luovutetun EU:n turvaluokitellun tiedon suojaamisessa käytettyjen toimenpiteiden tehokkuus.

18. Raportointi

Jollei tehdystä turvallisuussopimuksesta, 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 turvallisuussäännöksiä on noudatettu.

▼B

Lisäys 5

Ohjeet EU:n turvaluokitellun tiedon luovuttamisesta yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille: 3 tason yhteistyö

MENETTELYT

1. Komissio 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 turvaluokiteltujen tietojen luovuttamista.

2. Vain tiedon alkuperäisellä luovuttajalla on toimivalta luovuttaa EU:n turvaluokiteltua tietoa yhteisön ulkopuolisille valtioille tai kansainvälisille järjestöille, joilla on selvästi erilainen turvallisuuspolitiikka ja turvallisuusmääräykset kuin EU:lla. Kollegiona toimivalla komissiolla on toimivalta luovuttaa komissiossa tuotettua EU:n turvaluokiteltua tietoa.

   Periaatteessa luovuttaminen on rajattu ►**M1** SECRET UE ◄ -turvaluokan ja sitä alemman turvaluokan tietoon; erityisin turvaosoittimin tai -merkinnöin suojattua turvaluokiteltua tietoa ei saa luovuttaa.

3. Komissio harkitsee luokiteltujen tietojen luovuttamisen aiheellisuutta, arvioi edunsaajien tiedonsaantitarvetta ja päättää, millaisia luokiteltuja tietoja voidaan luovuttaa.

4. Jos komissio puoltaa tietojen luovuttamista, turvallisuusasioista vastaava komission jäsen

   — pyytää lausunnot luovutettavan EU:n turvaluokitellun tiedon alkuperäisiltä luovuttajilta,

   — järjestää komission turvallisuusasioiden neuvonantajaryhmän kokouksen tai tekee tiedusteluja, hiljaisen hyväksynnän menettelyllä mikäli tarpeellista, jäsenvaltioiden kansallisilta turvallisuusviranomaisilta, jotta komission turvallisuusasioiden neuvonantajaryhmältä saataisiin tekninen lausunto.

5. Komission turvallisuusasioiden neuvonantajaryhmän lausunto koskee seuraavia seikkoja:

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

   b) luovutettavissa olevan tiedon turvaluokka-aste;

   c) siirtäminen alempaan turvaluokkaan tai luokituksen poistaminen ennen kuin tieto luovutetaan;

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

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

6. Tässä lisäyksessä tarkoitetuille valtioille tai järjestöille luovutettavat asiakirjat eivät periaatteessa sisällä lähdeviittauksia tai EU:n turvaluokituksia. Komission turvallisuusasioiden neuvonantajaryhmä saattaa suositella

   — erityismerkintöjä tai koodinimeä,

   — erityistä luokittelumenetelmää, jossa tietojen arkaluonteisuus liittyy edunsaajan käyttämiltä asiakirjojen toimitusmenetelmiltä edellytettyihin valvontatoimenpiteisiin.

7. ►**M2** Turvallisuusasioista vastaava komission jäsen ◄ toimittaa komission turvallisuusasioiden neuvonantajaryhmän lausunnon komissiolle päätöksentekoa varten.

8. Komission hyväksyttyä EU:n turvaluokitellun tiedon luovuttamisen ja siihen liittyvät käytännön menettelyt, ►**M2** komission turvallisuudesta vastaava linja ◄ luo tarvittavat yhteydet asianomaisen valtion tai järjestön turvallisuusviranomaisiin suunniteltujen turvatoimenpiteiden soveltamisen helpottamiseksi.

9. Turvallisuusasioista vastaava komission jäsen ilmoittaa jäsenvaltioille luovutettavan tiedon laadun ja turvaluokan sekä luettelee ne järjestöt ja maat, joille tieto voidaan luovuttaa komission päätöksen mukaisesti.

10. ►**M2** Komission turvallisuudesta vastaava linja ◄ toteuttaa kaikki tarvittavat toimenpiteet, joilla helpotetaan mahdollisten vahinkojen arviointia ja menettelyjen tarkistamista.

    Komission on tarkasteltava asiaa uudelleen aina kun yhteistyön edellytykset muuttuvat.

▼B

TURVALLISUUTTA KOSKEVAT SÄÄNNÖT, JOITA EDUNSAAJIEN ON SOVELLETTAVA

11. Turvallisuusasioista vastaava komission jäsen ilmoittaa edunsaajina oleville valtioille tai kansainvälisille järjestöille komission päätöksestä sallia EU:n turvaluokitellun tiedon luovuttaminen sekä komission turvallisuusasioiden neuvonantajaryhmän ehdottamista ja komission hyväksymistä yksityiskohtaisista suojelusäännöistä.

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

— käyttävät tietoja ainoastaan komission päätöksen mukaiseen yhteistyöhön,

— tarjoavat tiedoille komission vaatiman suojan.

13. Asiakirjojen lähettäminen

a) Asiakirjojen lähettämistä koskevista käytännön menettelyistä sovitaan ►**M2** komission turvallisuudesta vastaavan linjan ◄ ja vastaanottavien valtioiden tai kansainvälisten järjestöjen turvallisuuselinten kesken. Menettelyissä täsmennetään erityisesti tarkat osoitteet, joihin asiakirjat on toimitettava.

b) ►**M1** CONFIDENTIEL UE ◄ -turvaluokan tai sitä korkeamman turvaluokan asiakirjat lähetetään kahdessa sisäkkäisessä kirjekuoressa. Sisimmässä kuoressa on oltava sovittu erityismerkintä tai koodinimi sekä maininta asiakirjalle hyväksytystä erityisluokituksesta. Kuoreen on laitettava jokaisen turvaluokitellun asiakirjan osalta kuitti. Kuittauslomake, jota ei luokitella, sisältää ainoastaan asiakirjaa koskevia tietoja (viitenumero, päivämäärä, kopionumero) ja asiakirjan kielen, ei otsikkoa.

c) Sisempi kuori laitetaan ulompaan kirjekuoreen, johon merkitään pakkausnumero kuittausta varten. Ulommaisessa kuoressa ei ole turvaluokkamerkintää.

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

14. Kirjaaminen saapumisen yhteydessä

Vastaanottajavaltion kansallinen turvallisuusviranomainen tai sitä vastaava elin ottaa hallituksensa puolesta vastaan komission lähettämää turvaluokiteltua tietoa, 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 kopionumero), asiakirjan turvaluokka, otsikko, vastaanottajan nimi tai ammattinimike, kuitin palautuspäivämäärä ja päivämäärä, jona kuitti on palautunut EU:hun sekä asiakirjan hävittämispäivämäärä.

15. Vaihdettavien luokiteltujen tietojen käyttö ja suojelu

a) ►**M1** SECRET UE ◄ -tason tietojen käsittelystä vastaavat erityisesti nimetyt viranomaiset, jotka on valtuutettu käsittelemään kyseiseen luokkaan kuuluvia tietoja. Tiedot on säilytettävä turvakaapeissa, jotka ainoastaan kyseisten tietojen käsittelyyn valtuutetut henkilöt voivat avata. Tiloja, joissa kyseiset kaapit sijaitsevat, on valvottava jatkuvasti, ja on perustettava todentamisjärjestelmä sen varmistamiseksi, että kyseisiin tiloihin päästetään ainoastaan asianmukaisesti valtuutetut henkilöt. ►**M1** SECRET UE ◄ -tason tiedot on toimitettava joko diplomaattipostina tai suojattuja posti- tai teleliikennepalveluja käyttäen. ►**M1** SECRET UE ◄ -asiakirjasta voidaan ottaa kopio ainoastaan, jos tiedot alun perin luovuttanut viranomainen antaa tähän kirjallisen suostumuksen. Kaikki kopiot kirjataan ja niitä valvotaan. Kaikkia ►**M1** SECRET UE ◄ -asiakirjoja koskevista toimista on annettava kuitit.

b) ►**M1** CONFIDENTIEL UE ◄ -tason tietojen käsittelystä vastaavat asianmukaisesti nimetyt viranomaiset, jotka on valtuutettu saamaan asiaa koskevia tietoja. Asiakirjat on säilytettävä lukituissa turvakaapeissa valvotuissa tiloissa.

►**M1** CONFIDENTIEL UE ◄ -tason tiedot on toimittava diplomaattipostina, sotilaspostina tai suojattuja teleliikennepalveluja käyttäen. Vastaanottaja voi ottaa asiakirjoista kopioita, joiden numero ja jakelu on kirjattava erityisiin rekistereihin.

c) ►**M1** RESTREINT UE ◄ -tietoja on käsiteltävä tiloissa, joihin valtuuttamattomat työntekijät eivät pääse, ja ne on säilytettävä lukitussa paikassa. Asiakirjat voidaan lähettää yleisiä postipalveluja käyttäen kirjattuna lähetyksenä kahdessa sisäkkäisessä kirjekuoressa ja kiireellisissä tapauksissa operaatioiden aikana suojaamattomia yleisiä teleliikennejärjestelmiä käyttäen. Vastaanottajat voivat ottaa asiakirjoista kopioita.

▼B

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

16. Hävittäminen

Tarpeettomat asiakirjat on hävitettävä. ►M1 RESTREINT UE ◄- ja ►M1 CONFIDENTIEL UE ◄ -asiakirjojen hävittäminen kirjataan asianmukaisesti erityisiin rekistereihin. ►M1 SECRET UE ◄ -asiakirjoista annetaan hävittämistodistukset, joissa on kahden hävittämistä todistaneen henkilön allekirjoitus.

17. Turvallisuuden vaarantuminen

Jos ►M1 CONFIDENTIEL UE ◄- tai ►M1 SECRET UE ◄ -tietojen turvallisuus vaarantuu tai jos turvallisuuden epäillään vaarantuneen, vastaanottaneen valtion kansallisen turvallisuusviranomaisen tai tiedot vastaanottaneen järjestön turvallisuuspäällikön on tutkittava olosuhteet, joissa turvallisuus vaarantui. Tutkimustulokset on ilmoitettava ►M2 komission turvallisuudesta vastaavalle linjalle ◄. Jos riittämättömät menettelyt tai säilytysmenetelmät ovat olleet turvallisuuden vaarantumisen syynä, on toteutettava tarvittavat toimenpiteet kyseisten menettelyjen ja menetelmien korjaamiseksi.

▼B

Lisäys 6

LYHENNELUETTELO

ACPC	Hankintoja ja sopimuksia käsittelevä neuvoa-antava komitea
CrA	Salausasioista vastaava viranomainen
CISO	Keskustietojärjestelmien tietoturvavastaava
COMPUSEC	Tietojärjestelmäturvallisuus
COMSEC	Tietoliikenneturvallisuus
CSO	►M2 Komission turvallisuudesta vastaava linja ◄
ESDP	Euroopan turvallisuus- ja puolustuspolitiikka
EUCI	EU:n turvaluokiteltu tieto
IA	Tietoturvaviranomainen
INFOSEC	Tietoturva
IO	Sisältövastaava
ISO	Kansainvälinen standardointijärjestö
IT	Tietotekniikka
LISO	Paikallistietojärjestelmien tietoturvavastaava
LSO	Paikallinen vastaava
MSO	Kokouksen turvavastaava
NSA	Kansallinen turvallisuusviranomainen
PC	Henkilökohtainen tietokone
RCO	Rekisterin valvontavastaava
SAA	Turvallisuusjärjestelyt hyväksyvä viranomainen
SecOPS	Turvallisuusmenettelyt
SSRS	Järjestelmäkohtainen turvavaatimusilmoitus
TA	Tempest-viranomainen
TSO	Tekninen järjestelmävastaava

▼M3

DSA	Nimetty turvallisuusviranomainen
FSC	Laitoksen turvallisuusselvitys
FSO	Laitoksen turvavastaava
PSC	Henkilöstön luotettavuusselvitys
SAL	Turvallisuusnäkökohtia koskeva kirje
SCG	Turvaluokitusohjeet