Käesolev dokument on vaid dokumenteerimisvahend ja institutsioonid ei vastuta selle sisu eest

►**B**

KOMISJONI OTSUS,

29. november 2001,

millega muudetakse komisjoni kodukorda

(teatavaks tehtud numbri K(2001) 3031 all)

(2001/844/EÜ, ESTÜ, Euratom)

(EÜT L 317, 3.12.2001, lk 1)

Muudetud:

		Euroopa Liidu Teataja		
		nr	lehekülg	kuupäev
►**M1**	Komisjoni otsus 2005/94/EÜ, Euratom, 3. veebruar 2005	L 31	66	4.2.2005
►**M2**	Komisjoni otsus 2006/70/EÜ, Euratom, 31. jaanuar 2006	L 34	32	7.2.2006
►**M3**	Komisjoni otsus 2006/548/EÜ, Euratom, 2. august 2006	L 215	38	5.8.2006
►**M4**	Komisjoni määrus (EL) nr 519/2013, 21. veebruar 2013	L 158	74	10.6.2013

▼B

KOMISJONI OTSUS,

29. november 2001,

millega muudetakse komisjoni kodukorda

(teatavaks tehtud numbri K(2001) 3031 all)

(2001/844/EÜ, ESTÜ, Euratom)

EUROOPA ÜHENDUSTE KOMISJON,

võttes arvesse Euroopa Ühenduse asutamislepingut, eriti selle artikli 218 lõiget 2,

võttes arvesse Euroopa Söe- ja Teraseühenduse asutamislepingut, eriti selle artiklit 16,

võttes arvesse Euroopa Aatomienergiaühenduse asutamislepingut, eriti selle artiklit 131,

võttes arvesse Euroopa Liidu lepingut, eriti selle artiklit 28 lõiget 1 ja artikli 41 lõiget 1,

ON TEINUD JÄRGMISE OTSUSE:

Artikkel 1

Komisjoni turvasätted, mis on ära toodud käesoleva otsuse lisas, lisatakse komisjoni kodukorda.

Artikkel 2

Käesolev otsus jõustub *Euroopa Ühenduste Teatajas* avaldamise päeval.

Seda kohaldatakse alates 1. detsembrist 2001.

▼B

LISA

KOMISJONI TURVASÄTTED

Arvestades järgmist:

1) Komisjoni tegevuse arendamiseks valdkondades, mis nõuavad teatavat konfidentsiaalsust, on asjakohane luua põhjalik turvasüsteem, edaspidi „EL salajane teave”, mida kohaldatakse komisjoni, teiste institutsioonide, Euroopa Ühenduse asutamislepingu või Euroopa Liidu lepinguga või nende alusel loodud talituste, ametite ja asutuste ning liikmesriikide ja Euroopa Liidu salastatud teabe saajatele.

2) Tagamaks kõnealuse loodava turvasüsteemi tõhusust teeb komisjon Euroopa Liidu salastatud teabe kättesaadavaks ainult sellistele välisorganitele, mis tagavad kõikide vajalike meetmete kasutuselevõtu reeglite kohaldamiseks, mis vastavad rangelt käesolevatele sätetele.

3) Käesolevate sätete rakendamine ei piira 31. juuli 1958. aasta määruse nr 3, millega rakendatakse Euroopa Aatomienergiaühenduse asutamislepingu artikkel 24, ([1]) nõukogu 11. juuni 1990. aasta määruse (EMÜ) nr 1588/90 statistiliselt konfidentsiaalsete andmete Euroopa Ühenduste Statistikaametile edastamise kohta ([2]) ja komisjoni 23. novembri 1995 lõpliku otsuse K(95) 1510 informaatikasüsteemide kaitsemise kohta kohaldamist.

4) Komisjoni turvasüsteemi aluseks on nõukogu 19. märtsi 2001 aasta otsusega 2001/264/EÜ vastu võetud nõukogu julgeolekueeskirjad, ([3]) mille eesmärk on tagada liidu otsustamismenetluse sujuv toimimine.

5) Komisjon rõhutab, et vajadusel tuleb Euroopa Liidu ja tema liikmesriikide huvide kaitsmiseks vajalike konfidentsiaalsusreeglite ja -standardite kohaldamisse kaasata ka teisi institutsioone.

6) Komisjon tunnistab vajadust luua oma turvakontseptsioon, mis arvestab kõiki turvaelemente ja komisjoni kui institutsiooni eripära.

7) Käesolevate sätete rakendamine ei piira asutamislepingu artikli 255 ja Euroopa Parlamendi ja nõukogu 30. mai 2001 määruse (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele ([4]) kohaldamist.

▼M2

8) Need sätted ei kahjusta asutamislepingu artiklit 286 ega Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrust (EÜ) 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta.

▼B

Artikkel 1

Komisjoni turvaeeskirjad on esitatud lisas.

([1]) EÜT 17/58, 6.10.1958, lk 406/58.
([2]) EÜT L 151, 15.6.1990, lk 1.
([3]) EÜT L 101, 11.4.2001, lk 1.
([4]) EÜT L 145, 31.5.2001, lk 43.

▼B

Artikkel 2

1. Turvaküsimuste eest vastutav komisjoni liige võtab asjakohased meetmed, et tagada komisjoni ametnike, teiste teenistujate ning komisjonis lähetuses oleva personali poolt, samuti kõikjal komisjoni territooriumil, kaasa arvatud liidu ning komisjoni kolmandates riikides olevate delegatsioonide esindustes ja asutustes ning komisjoni välislepingupartnerite poolt Euroopa Liidu salastatud teabe käitlemisel komisjonis artiklis 1 nimetatud reeglitest kinnipidamine.

▼M3

Kui komisjoni ja välislepingupartneri või toetusesaaja vaheline leping või toetusleping sisaldab ELi salastatud teabe töötlemist välislepingupartneri või toetusesaaja tööruumides, peavad asjakohased meetmed, mida nimetatud lepingupartner või toetusesaaja peab võtma artiklis 1 osutatud eeskirjade täitmiseks ELi salastatud teabe töötlemisel, olema lepingu või toetuslepingu lahutamatu osa.

▼B

2. Liikmesriikidel, teistel asutamislepingutega või nende alusel loodud institutsioonidel, ametitel, talitustel ja asutustel võimaldatakse saada Euroopa Liidu salastatud teavet tingimusel, et nad kindlustavad oma teenistustes ja territooriumil selle, et Euroopa Liidu salastatud teabe käitlemisel peetakse kinni reeglitest, mis on ranges vastavuses artiklis 1 nimetatud reeglitega, see kehtib eriti järgnevate puhul:

a) Euroopa Liidu juures olevate liikmesriikide alaliste esinduste liikmed ja komisjon või selle organite koosolekutel või muus komisjoni tegevuses osalevate riiklike delegatsioonide liikmed;

b) liikmesriikide valitsuste muud liikmed, kes käitlevad Euroopa Liidu salastatud teavet, olenemata sellest, kas nad tegutsevad liikmesriikide territooriumil või välismaal;

c) välislepingupartnerid ja lähetuses olevad töötajad, kes käitlevad Euroopa Liidu salastatud teavet.

Artikkel 3

Kolmandatel riikidel, rahvusvahelistel organisatsioonidel ja muudel asutustel võimaldatakse saada Euroopa Liidu salastatud teavet tingimusel, et nad tagavad, et selle teabe käitlemisel peetakse kinni reeglitest, mis on ranges vastavuses artiklis 1 nimetatud reeglitega.

Artikkel 4

Turvaküsimuste eest vastutav komisjoni liige võib võtta lisa II osas esitatud meetmeid, mis on vastavuses lisa I osas esitatud turvalisuse algpõhimõtete ja miinimumstandarditega.

Artikkel 5

Käesolevate sätetega asendatakse alates kohaldamiskuupäevast järgmised õigusaktid:

a) Komisjoni 30. novembri 1994. aasta otsus K(94) 3282 Euroopa Liidu tegevusega seoses loodud või edastatud salastatud teabele kohaldatavate turvameetmete kohta;

b) Komisjoni 25. veebruari 1999. aasta otsus K(99) 423 komisjonis hoitava salastatud teabele juurdepääsu korra kohta Euroopa Komisjoni ametnike ja teiste töötajate poolt.

▼B

Artikkel 6

Alates käesolevate sätete rakendamise kuupäevast kogu antud kuupäevani komisjonis hoitav salajane teave, välja arvatud Euratomi salajane teave:

a) kui see on loodud komisjonis, liigitatakse vaikimisi ümber kui „►**M1** RESTREINT UE ◄”, kui selle autor ei soovi seda 31. jaanuariks 2002 ümber liigitada. Sellisel juhul teavitab autor kõiki asjaomase dokumendi adressaate;

b) kui selle autor on väljastpoolt komisjoni, säilitatakse selle algne liigitus ja kui autor ei ole nõus selle salastatust kaotama ega teabe salastatuse taset vähendama, käsitletakse seda vastava tasandi Euroopa Liidu salastatud teabena.

▼B

LISA

TURVAEESKIRJAD

Sisukord

I OSA:	**JULGEOLEKU ÜLDPÕHIMÕTTED JA MIINIMUMSTANDARDID**
1.	SISSEJUHATUS
2.	ÜLDPÕHIMÕTTED
3.	JULGEOLEKU ALUSED
4.	TEABETURBE PÕHIMÕTTED
4.1.	**Eesmärgid**
4.2.	**Määratlused**
4.3.	**Saladuseks tunnistamine**
4.4.	**Julgeolekumeetmete eesmärgid**
5.	JULGEOLEKUKORRALDUS
5.1.	**Ühised miinimumstandardid**
5.2.	**Korraldus**
6.	TÖÖTAJATEGA SEOTUD JULGEOLEK
6.1.	**Töötajate julgeolekukontroll**
6.2.	**Julgeolekukontrolli register**
6.3.	**Töötajatele antavad julgeolekujuhendid**
6.4.	**Juhtkonna vastutus**
6.5.	**Töötajate julgeolekustaatus**
7.	FÜÜSILINE JULGEOLEK
7.1.	**Kaitsevajadus**
7.2.	**Kontrollimine**
7.3.	**Hoonete julgeolek**
7.4.	**Situatsioonkavad**
8.	TEABETURVE
9.	SABOTAAŽ JA KURITAHTLIKU KAHJUSTAMISE MUUDE VORMIDE KONTROLL
10.	SALASTATUD TEABE AVALDAMINE KOLMANDATELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE
II OSA:	**KOMISJONI JULGEOLEKU KORRALDAMINE**
11.	TURVAKÜSIMUSTE EEST VASTUTAV KOMISJONI LIIGE
12.	KOMISJONI JULGEOLEKUPOLIITIKA NÕUANDEKOMITEE
13.	KOMISJONI JULGEOLEKUNÕUKOGU
14.	►**M2** KOMISJONI JULGEOLEKUDIREKTORAAT ◄
15.	JULGEOLEKUKONTROLL
16.	SALASTATUSE KATEGOORIAD, JULGEOLEKUTÄHISED JA -TÄHISTUSED
16.1.	**Kategooriate tasandid**

▼B

16.2. **Julgeoleku tähised**

16.3. **Tähistused**

16.4. **Kategooriate kinnitamine**

16.5. **Julgeolekutähiste kinnitamine**

17. SALASTATUSE KATEGOORIATE HALDAMINE

17.1. **Üldine**

17.2. **Kategooriate rakendamine**

17.3. **Salastatuse taseme vähendamine ja kaotamine**

18. FÜÜSILINE JULGEOLEK

18.1. **Üldine**

18.2. **Turvanõuded**

18.3. **Füüsilised julgeolekumeetmed**

18.3.1. *Turvaalad*

18.3.2. *Haldustegevuse ala*

18.3.3. *Sisse- ja väljapääsu kontrollimine*

18.3.4. *Valvepatrullid*

18.3.5. *Turvakonteinerid ja turvakambrid*

18.3.6. *Lukud*

18.3.7. *Võtmete ja koodide järelevalve*

18.3.8. *Sissetungimise avastamise seadmed*

18.3.9. *Heakskiidetud seadmed*

18.3.10. *Koopiamasinate ja faksiseadmete füüsiline kaitse*

18.4. **Salajase jälgimise ja pealtkuulamise vastane kaitse**

18.4.1. *Salajane jälgimine*

18.4.2. *Pealtkuulamine*

18.4.3. *Elektrooniliste ja salvestusseadmete kasutamine*

18.5. **Tehniliselt kaitstud alad**

19. TEADMISVAJADUSE PÕHIMÕTTE JA EUROOPA LIIDU PERSONALI JULGEOLEKUKONTROLLI KOHALDAMISE ÜLDEESKIRJAD

19.1. **Üldine**

19.2. **►M1 TRES SECRET UE/EU TOP SECRET ◄ teabele juurdepääsu erieeskirjad**

19.3. **►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ teabele juurdepääsu erieeskirjad**

19.4. **►M1 RESTREINT UE ◄ teabele juurdepääsu erieeskirjad**

19.5. **Personali üleviimine**

19.6. **Erijuhised**

▼B

20. KOMISJONI AMETNIKE JA MUUDE TÖÖTAJATE JULGEOLEKUKONTROLLI KORD

21. EUROOPA LIIDU SALASTATUD DOKUMENTIDE KOOSTAMINE, LEVITAMINE, EDASTAMINE, KULLERI ISIKLIK JULGEOLEK JA TÄIENDAVAD KOOPIAD VÕI TÕLKED NING VÄLJAVÕTTED

21.1. **Koostamine**

21.2. **Levitamine**

21.3. **Euroopa Liidu salastatud teabe edastamine**

21.3.1. *Pakendid, kättesaamistõendid*

21.3.2. *Majasisene või majade grupi sisene edastamine*

21.3.3. *Riigisisene edastamine*

21.3.4. *Edastamine ühest riigist teise*

21.3.5. ►M1 *RESTREINT UE* ◄ *dokumentide edastamine*

21.4. **Kulleri isiklik julgeolek**

21.5. **Elektroonilised ja muud tehnilised edastusvahendid**

21.6. **Euroopa Liidu salastatud teabe täiendavad koopiad ja tõlked ning väljavõtted sellistest dokumentidest**

22. EUROOPA LIIDU SALASTATUD TEABE REGISTRID, ÜLEVAATUSED, KONTROLLID, ARHIIVIS SÄILITAMINE JA HÄVITAMINE

22.1. **Euroopa Liidu salastatud teabe kohalikud registrid**

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

22.2.1. *Üldine*

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

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

22.3. **Euroopa Liidu salastatud dokumentide inventuur, ülevaatus ja kontroll**

22.4. **Euroopa Liidu salastatud teabe arhiivis hoidmine**

22.5. **Euroopa Liidu salastatud dokumentide hävitamine**

22.6. **Hädaolukorras hävitamine**

23. VÄLJASPOOL KOMISJONI TERRITOORIUMI PEETAVATE EUROOPA LIIDU SALASTATUD TEAVET SISALDAVATE ERIKOHTUMISTE TURVAMEETMED

23.1. **Üldine**

23.2. **Kohustused**

23.2.1. ►M2 *Komisjoni julgeolekudirektoraat* ◄

23.2.2. *Koosoleku julgeolekuametnik (MSO)*

23.3 **Julgeolekumeetmed**

23.3.1. *Turvaalad*

23.3.2. *Läbipääsuload*

23.3.3. *Foto- ja heliseadmete kontrollimine*

▼B

23.3.4. *Portfellide, kaasaskantavate arvutite ja pakkide kontrollimine*

23.3.5. *Tehniline julgeolek*

23.3.6. *Delegatsioonide dokumendid*

23.3.7. *Dokumentide turvaline hoidmine*

23.3.8. *Ametiruumide kontrollimine*

23.3.9. *Euroopa Liidu salastatud jäätmete kõrvaldamine*

24. JULGEOLEKU RIKKUMINE JA EUROOPA LIIDU SALASTATUD TEABE KAHJUSTAMINE

24.1. **Määratlused**

24.2. **Julgeoleku rikkumisest teatamine**

24.3. **Õiguslikud meetmed**

25. INFOTEHNOLOOGIA JA SIDESÜSTEEMIDE ABIL KÄIDELDAVA EUROOPA LIIDU SALASTATUD TEABE KAITSMINE

25.1. **Sissejuhatus**

25.1.1. *Üldine*

25.1.2. *Süsteeme ähvardavad ohud ja nende nõrgad kohad*

25.1.3. *Turvameetmete peamine eesmärk*

25.1.4. *Süsteemispetsiifiliste julgeolekunõuete loetelu (SSRS)*

25.1.5. *Turvalisuse tagamise toimimisviisid*

25.2. **Määratlused**

25.3. **Vastutus julgeolekuküsimustes**

25.3.1. *Üldine*

25.3.2. *Julgeoleku akrediteerimise ametiisik (SAA)*

25.3.3. *Teabeturbe ametiisik (IA)*

25.3.4. *Tehnilise süsteemi vastutav käitaja (TSO)*

25.3.5. *Teabeomanik (IO)*

25.3.6. *Kasutajad*

25.3.7. *Teabeturbe koolitus*

25.4. **Mittetehnilised julgeolekumeetmed**

25.4.1. *Personali julgeolek*

25.4.2. *Füüsiline julgeolek*

25.4.3. *Süsteemile juurdepääsu kontroll*

25.5. **Tehnilised julgeolekumeetmed**

25.5.1. Teabeturve

25.5.2. *Teabe kontroll ja aruandekohustus*

25.5.3. *Teisaldatavate elektrooniliste salvestusvahendite käitlemine ja kontroll*

▼B

25.5.4. *Elektrooniliste salvestusvahendite salastatuse kategooria kaotamine ja hävitamine*

25.5.5. *Teabeedastuse turve*

25.5.6. *Turvalisus installeerimisel ja radiatsiooniturvalisus*

25.6. **Julgeolek käitlemise ajal**

25.6.1. *Julgeolekuga seotud töökord (SecOPS)*

25.6.2. *Tarkvara kaitsmine/konfigureerimise juhtimine*

25.6.3. *Kahjuliku tarkvara/arvutiviiruste kontrollimine*

25.6.4. *Hooldus*

25.7. **Hanked**

25.7.1. *Üldine*

25.7.2. *Akrediteerimine*

25.7.3. *Hindamine ja sertifitseerimine*

25.7.4. *Julgeolekuomaduste jooksev kontroll pideva akrediteerimise jaoks*

25.8. **Ajutine või juhuslik kasutamine**

25.8.1. *Mikroarvutite/personaalarvutite turvalisus*

25.8.2. *Isiklike IT-seadmete kasutamine komisjoni ametlikuks tööks*

25.8.3. *Lepingupartnerite isiklike või liikmesriikide tarnitud IT-seadmete kasutamine komisjoni ametlikuks tööks*

26. EUROOPA LIIDU SALASTATUD TEABE AVALDAMINE KOLMANDATELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE

26.1.1. *Euroopa Liidu salastatud teabe avaldamist reguleerivad põhimõtted*

26.1.2. *Tasemed*

26.1.3. *Julgeolekulepped*

LIIDE 1: **Siseriiklike salastatuse tasemete võrdlus**

LIIDE 2: **Salastatuse kategooriate määramise praktiline juhend**

LIIDE 3: **Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele: 1. taseme koostöö**

LIIDE 4: **Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele: 2. taseme koostöö**

LIIDE 5: **Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele: 3. taseme koostöö**

LIIDE 6: **Lühendite loetelu**

▼B

I OSA: JULGEOLEKU ÜLDPÕHIMÕTTED JA MIINIMUMSTANDARDID

1. SISSEJUHATUS

Käesolevate sätetega kehtestatakse julgeoleku üldpõhimõtted ja miinimumstandardid, mida tuleb järgida komisjoni kõikides töökohtades asjakohasel viisil ja samuti kõigil Euroopa Liidu salastatud teabe saajatel, et tagada turvalisus ja et kõik võivad olla kindlad, et ühised kaitsestandardid on rakendatud.

2. ÜLDPÕHIMÕTTED

Komisjoni julgeolekupoliitika on komisjoni üldise sisemise halduspoliitika lahutamatu osa ja seega põhineb see komisjoni üldist poliitikat juhtivatel põhimõtetel.

Nende põhimõtete hulka kuuluvad seaduslikkus, läbipaistvus, vastutavus ja subsidiaarsus (proportsionaalsus).

Seaduslikkus tähistab vajadust püsida julgeolekufunktsioonide täitmisel rangelt õiguslikus raamistikus ning vajadust olla vastavuses õigusnormidega. Samuti tähendab see, et julgeolekualased kohustused peavad põhinema asjakohastel õigusnormidel. Personalieeskirjade sätted kehtivad täies mahus, eriti artikkel 17, mis käsitleb personali konfidentsiaalsuskohustust komisjoni teabe suhtes, ja VI jaotis distsiplinaarmeetmete kohta. Samuti tähendab see seda, et komisjoni vastutusalas toimuvate julgeoleku rikkumistega tuleb tegeleda vastavalt komisjoni distsiplinaarmeetmete poliitikale ning vastavalt komisjoni koostööpoliitikale liikmesriikidega kriminaalõiguse valdkonnas.

Läbipaistvus tähistab selguse vajadust kõikide julgeolekueeskirjade ja sätete suhtes, vajadust tasakaalu järele erinevate teenuste ja erinevate valdkondade vahel (füüsiline julgeolek *versus* teabekaitse jne) ning vajadust järjepideva ja struktureeritud teadliku julgeolekupoliitika järele. Samuti määratleb see vajaduse selgete, kirjalike juhtnööride järele julgeolekumeetmete rakendamiseks.

Vastutavus tähendab, et julgeolekualased kohustused on selgelt määratletud. Lisaks tähistab see vajadust regulaarselt kontrollida, kas neid kohustusi täidetakse korrektselt.

Subsidiaarsus või proportsionaalsus tähendab, et turvalisus organiseeritakse kõige madalamal võimalikul tasemel ning võimalikult lähedal peadirektoraatidele ja komisjoni talitustele. Samuti tähistab see seda, et julgeolekumeetmed piirduvad ainult nende elementidega, mis seda tõeliselt vajavad. Ja samuti tähendab see seda, et julgeolekumeetmed on vastavuses kaitstavate huvidega ning tegeliku või potentsiaalse ohuga nendele huvidele, võimaldades kaitset, mis põhjustab väikseima võimaliku katkestuse.

3. JULGEOLEKU ALUSED

Kindla julgeoleku aluseks on järgmised seigad:

a) igas liikmesriigis on siseriiklik julgeolekuorganisatsioon, kes vastutab järgmiste asjaolude eest:

   1. spionaaži, sabotaaži, terrorismi ja muu õõnestava tegevuse kohta luureandmete kogumine ja talletamine, ning

   2. valitsustele ja nende kaudu komisjonile teabe andmine julgeolekuohtude olemuse kohta ja nõuandmine, milliste vahenditega nende ohtude eest kaitsta;

▼B

b) igas liikmesriigis ja komisjonis on tehniline teabeturbeasutus või ametiisik (INFOSEC authority), kes vastutab koostöö eest asjaomase julgeolekuasutusega seoses teabega julgeolekuohtude tehniliste külgede kohta ja nõuannetega, milliste vahenditega nende ohtude eest kaitsta;

c) valitsusasutused ja Euroopa institutsioonide asjaomased ametid teevad regulaarselt koostööd, et vastavalt vajadusele määrata kindlaks ja soovitada:

1. milliseid isikuid, vahendeid ja millist teavet on vaja kaitsta, ning

2. ühised kaitsestandardid;

d) ►M2 komisjoni julgeolekudirektoraat ◄ teeb tihedat koostööd teiste Euroopa institutsioonide julgeolekuametitega ja NATO Julgeolekubürooga (NOS).

4. TEABETURBE PÕHIMÕTTED

4.1. **Eesmärgid**

Teabeturbe peamised eesmärgid on järgmised:

a) kaitsta Euroopa Liidu salastatud teavet spionaaži, kahjustamise ja loata avaldamise eest;

b) kaitsta side- ja teabesüsteemides ning -võrkudes käideldavat Euroopa Liidu teavet konfidentsiaalsuse, terviklikkuse ja kättesaadavuse ohtuseadmise eest;

c) kaitsta Euroopa Liidu teavet sisaldavaid komisjoni rajatisi sabotaaži ja kuritahtliku kahjustamise eest;

d) kaitse ebaõnnestumise korral hinnata tekitatud kahju, piirata selle tagajärgi ja võtta vajalikke heastamismeetmeid.

4.2. **Määratlused**

Käesolevates eeskirjades kasutatakse järgmisi mõisteid.

a) Mõiste „Euroopa Liidu salastatud teave” tähendab igasugust teavet ja materjali, mille ilma loata avaldamine võib eri määral kahjustada Euroopa Liidu huve või ühte või mitut Euroopa Liidu liikmesriiki, kui selline teave on pärit Euroopa Liidust või saadud tema liikmesriikidelt, kolmandatelt riikidelt või rahvusvahelistelt organisatsioonidelt.

b) Mõiste „dokument” tähendab igasugust kirja, märkust, protokolli, aruannet, memorandumit, signaali/sõnumit, visandit, fotot, slaidi, filmi, kaarti, skeemi, plaani, kausta, šablooni, koopiapaberit, kirjutusmasina- ja printerilinti, magnetlinti, kassetti, arvutiketast, CD-ROMi või muud füüsiliselt eksisteerivat andmekandjat.

c) Mõiste „materjal” tähendab eespool punktis b määratletud dokumente ja kõiki valmistatud või valmistamisel olevaid seadmeid.

d) Mõiste „teadmisvajadus” tähendab individuaalse töötaja vajadust pääseda ligi Euroopa Liidu salastatud teabele, et töötada või täita tööülesannet.

e) „Autoriseerimine” tähendab ►M2 komisjoni julgeolekudirektoraadi direktor ◄ otsust võimaldada isikule juurdepääs kuni teatava taseme Euroopa Liidu salastatud teabele, mis põhineb julgeolekukontrolli positiivsel tulemusel, milleni on jõudnud siseriiklik julgeolekuasutus vastavalt siseriiklikele õigusnormidele.

▼B

f) Mõiste „saladuseks tunnistamine” tähendab sobiva turvaastme määramist teabele, mille loata avaldamine võib teataval määral kahjustada komisjoni või liikmesriigi huve.

g) Mõiste „salastatuse kategooria alandamine” (*déclassement*) tähendab salastatuse taseme alandamist.

h) Mõiste „salastatuse kategooria kaotamine” (*déclassification*) tähendab igasuguse salastatuse kõrvaldamist.

i) Mõiste „koostaja” tähendab salastatud dokumendi nõuetekohaselt volitatud autorit. Komisjonis võivad osakondade juhid volitada oma personali koostama Euroopa Liidu salastatud dokumente.

j) Mõiste „komisjoni osakonnad” tähendab komisjoni osakondasid ja talitusi, muu hulgas komisjoni liikmete kabinetid, kõikides töökohtades, kaasa arvatud Teadusuuringute Ühiskeskuse esindustes ja asutustes liidus ning komisjoni delegatsioonides kolmandates riikides.

4.3. **Saladuseks tunnistamine**

a) Salastatuse puhul eeldab kaitstava teabe ja kaitstavate materjalide valik ning vajaliku kaitsetaseme hindamine hoolikust ja kogemusi. On äärmiselt oluline, et kaitse tase vastaks konkreetse kaitstava teabe või kaitstava materjali julgeoleku olulisusele. Teabe sujuva liikumise tagamiseks tuleb võtta meetmeid, mis välistaksid nii üle- kui alasalastamise.

b) Salastamissüsteem on see vahend, mille abil saab kõnealused põhimõtted ellu viia; samalaadset salastamissüsteemi tuleb järgida spionaaži, sabotaaži, terrorismi ja muude ohtude kohta vastulöökide kavandamise ja korraldamise puhul, nii et kõige rohkem kaitstaks kõige olulisemaid salastatud teavet sisaldavaid rajatisi ja kõige tundlikumaid kohti neis rajatistes.

c) Vastutus teabe salastamise eest lasub ainuisikuliselt vastava teabe koostajal.

d) Salastatuse tase võib põhineda ainult vastava teabe sisul.

e) Kui on rühmitatud mitu teabe osa, rakendatakse tervikule sellist salastatuse taset, mis on vähemalt sama kõrge kui kõige kõrgema salastatuse tasemega osa oma. Siiski võib teabe kogumikule omistada kõrgema salastatuse taseme kui selle osade oma.

f) Salastatus määratakse ainult siis, kui see on vajalik, ja nii kauaks, kui see on vajalik.

4.4. **Julgeolekumeetmete eesmärgid**

Julgeolekumeetmed:

a) laienevad kõigile isikutele, kellel on juurdepääs salastatud teabele, salastatud teabe kandjatele, kõigile sellist teavet sisaldavatele ruumidele ja olulistele rajatistele;

b) peavad olema kavandatud nii, et oleks võimalik avastada isikuid, kelle positsioon võib seada ohtu salastatud teabe ja sellist teavet sisaldavate oluliste rajatiste julgeoleku, ning tagada nende kõrvaldamine või viimine teisele tööle.

▼B

c) takistavad loata isikute juurdepääsu salastatud teabele ja rajatistele, mis sisaldavad sellist teavet;

d) tagavad salastatud teabe levitamise ainult teadmisvajaduse põhimõttest lähtudes, mis on esmatähtis julgeoleku kõigi aspektide seisukohast;

e) tagavad igasuguse teabe terviklikkuse (st välditakse rikkumist, loata muutmist ja kustutamist) ja kättesaadavuse (st ei takistata nende isikute juurdepääsu, kellel on seda vaja ja kellel on selleks luba, olenemata sellest, kas teave on salastatud või salastamata, ja eriti siis, kui selline teave on salvestatud või seda töödeldakse või edastatakse elektromagnetilisel kujul.

5. JULGEOLEKUKORRALDUS

5.1. **Ühised miinimumstandardid**

Komisjon tagab, et kõik Euroopa Liidu salastatud teabe saajad nii institutsioonisiseselt kui selle võimu piires, nt kõik osakonnad ja lepingupartnerid, järgivad ühtseid julgeoleku miinimumstandardeid, et Euroopa Liidu salastatud teavet oleks võimalik edastada kindla teadmisega, et seda käideldakse samasuguse hoolega. Sellised miinimumstandardid hõlmavad töötajate julgeolekukontrolli kriteeriume ja Euroopa Liidu salastatud teabe kaitsmise korda.

Komisjon võimaldab välisorganisatsioonidel juurdepääsu Euroopa Liidu salastatud teabele ainult tingimusel, et need kindlustavad Euroopa Liidu salastatud teabe käitlemisel vähemalt selliste meetmete kasutuselevõtu, mis vastab käesolevatele miinimumstandarditele.

▼M3

Selliseid miinimumstandardeid tuleb kohaldada ka juhul, kui komisjon annab lepingu või toetuslepinguga välistele tööstus- või muudele üksustele ülesandeid, mis on seotud ELi salastatud teabega ja/või sisaldavad selle kasutamist: need ühised miinimumstandardid on esitatud II osa 27. jaos.

▼B

5.2. **Korraldus**

Komisjonis on julgeolek korraldatud kahel tasandil:

a) komisjoni kui terviku tasandil on ►M2 komisjoni julgeolekudirektoraat ◄ koos julgeoleku akrediteerimise asutuse või ametiisikuga (SAA), kes tegutseb ka salastatuse küsimuste eest vastutava ametnikuna (*Crypto Authority*, CrA) ning TEMPEST ametivõimuna, teabeturbe asutus või ametiisik (INFOSEC, IA) ja üks või enam Euroopa Liidu salastatud teabe keskregistrit, igaühes üks või mitu registri kontrollametnikku (RCO);

b) komisjoni osakondade tasandil vastutab/vastutavad julgeoleku eest üks või mitu kohalikku julgeolekuametnikku (LSO), üks või mitu keskset informaatikaturbe ametnikku (CISO), kohalikku informaatikaturbe ametnikku (LISO) ja kohalikud Euroopa Liidu salastatud teabe registrid ühe või enama registri kontrollametnikuga;

c) kesksed julgeolekuasutused annavad tegutsemisjuhised kohaliku tasandi julgeolekuasutustele.

6. TÖÖTAJATEGA SEOTUD JULGEOLEK

6.1. **Töötajate julgeolekukontroll**

Kui keegi taotleb juurdepääsu kategooriasse ►M1 CONFIDENTIEL UE ◄ või rangemasse kategooriasse kuuluvale salastatud teabele, peab ta enne sellise juurdepääsu saamist läbima julgeolekukontrolli. Samasuguse julgeolekukontrolli peavad läbima ka need isikud, kelle tööülesannete hulka kuulub salastatud teavet sisaldavate side- ja teabesüsteemide tehniline käitamine või hooldamine. Kõnealuse julgeolekukontrolliga tuleb kindlaks teha, kas asjaomane isik:

a) on vaieldamatult lojaalne;

▼B

b) on sellise iseloomu ja otsustusvõimega, et see ei sea kahtluse alla tema ausust salastatud teabe käitlemisel; või

c) võib olla vastuvõtlik välissurvele või muude allikate survele.

Julgeolekukontrolli käigus pööratakse eriti üksikasjalikku tähelepanu isikutele:

d) kellele antakse juurdepääs ►M1 TRES SECRET UE/EU TOP SECRET ◄ teabele;

e) kes töötavad ametikohal, kus on pidev juurdepääs märkimisväärsele hulgale teabele, mis kuulub kategooriasse ►M1 SECRET UE ◄;

f) kelle tööülesannetega kaasneb erijuurdepääs kaitstud side- või infosüsteemidele ja sellega ka võimalus pääseda ilma loata juurde suurele hulgale Euroopa Liidu salastatud teabele või tekitada tehnilise sabotaažiga tõsist kahju kõnealusele ülesandele.

Punktides d, e ja f kirjeldatud juhtudel kasutatakse võimalikult suures ulatuses taustauuringute tehnikat.

Kui tööle võetakse inimesed, kellel ei ole teadmisvajadust, kuid kellel võib asjaolude tõttu olla juurdepääs Euroopa Liidu salastatud teabele (nt käskjalad, turvatöötajad, hooldustöötajad ja koristajad jt), peavad nad enne läbima nõuetekohase julgeolekukontrolli.

6.2. **Julgeolekukontrolli register**

Kõik komisjoni osakonnad, mis käitlevad Euroopa Liidu salastatud teavet või mille ruumides on kaitstud side- või infosüsteemid, peavad nendega tegelevate isikute julgeolekusertifikaatide kohta registrit. Vajadusel kontrollitakse iga julgeolekusertifikaati tagamaks, et see on vastavuses asjaomase isiku käsilolevate ülesannetega; seda kontrollitakse eelisjärjekorras uuesti alati, kui saadakse uut teavet, mis näitab, et asjaomase isiku töö salastatud teabega ei ole enam kooskõlas julgeolekuhuvidega. Komisjoni osakonna kohalik julgeolekuametnik peab oma vastutuspiirkonnas väljastatud julgeolekusertifikaatide kohta registrit.

6.3. **Töötajatele antavad julgeolekujuhendid**

Kõikidele töötajatele, kellel on oma ametikoha tõttu juurdepääs salastatud teabele, antakse tööleasumisel ja regulaarsete vaheaegade järel põhjalikud juhtnöörid julgeoleku vajalikkuse ja selle saavutamise korra kohta. Nimetatud töötajad peavad kirjalikult kinnitama, et nad on käesolevad julgeolekusätted läbi lugenud ja mõistavad neid täielikult.

6.4. **Juhtkonna vastutus**

Juhtkond on kohustatud teadma, kes nende töötajatest tegelevad oma töö käigus salastatud teabega või kellel on juurdepääs kaitstud side- ja teabesüsteemidele, ning registreerima kõik vahejuhtumid ja tõenäolised nõrgad kohad, mis võivad mõjutada julgeolekut, ja neist teatama.

6.5. **Töötajate julgeolekustaatus**

Tuleb kehtestada kord tagamaks, et juhul, kui mõne isiku kohta saadakse teada teda kahjustavat teavet, tehakse kindlaks, kas see isik töötab salastatud teabega või kas tal on juurdepääs kaitstud side- või teabesüsteemidele, ja sellest teavitatakse ►M2 komisjoni julgeolekudirektoraati ◄. Kui tehakse kindlaks, et sellise isiku näol on tegemist ohuga julgeolekule, tagandatakse või kõrvaldatakse ta nende tööülesannete täitmiselt, millega seoses ta võib julgeoleku ohtu seada.

▼B

7. FÜÜSILINE JULGEOLEK

7.1. **Kaitsevajadus**

Euroopa Liidu salastatud teabe kaitsmise tagamiseks rakendatavate füüsiliste julgeolekumeetmete tase on proportsionaalne teabe ja materjali salastatuse taseme, hulga ja neile suunatud ohuga. Kõik Euroopa Liidu salastatud teabe valdajad järgivad kõnealuse teabe salastatuse taseme määramisel ühtseid tavasid ja peavad kaitset vajava teabe ja materjali säilitamisel, edastamisel ja hävitamisel kinni ühistest kaitsestandarditest.

7.2. **Kontrollimine**

Enne kui Euroopa Liidu salastatud teavet sisaldav koht jäetakse järelevalveta, peab sellise teabe eest vastutav isik tagama, et teavet säilitatakse turvaliselt ja kõik turvaseadmed (lukud, häireseadmed jms) on aktiveeritud. Pärast tööpäeva lõppu toimub täiendav sõltumatu kontroll.

7.3. **Hoonete julgeolek**

Hooned, kus on Euroopa Liidu salastatud teavet või kaitstud side- ja teabesüsteeme, peavad olema kaitstud loata juurdepääsu eest. Euroopa Liidu salastatud teabe kaitsmise viis (nt trellitatud aknad, ukselukud, uksevalve, juurdepääsu kontrollimise automaatsüsteemid, turvakontrollid ja valvepatrullid, häiresüsteemid, sissetungimise avastamise süsteemid ja valvekoerad) sõltub järgmisest:

a) kaitstava teabe ja materjali salastatuse tase, maht ja asukoht hoones;

b) sellise teabe ja materjali turvakonteinerite kvaliteet; ja

c) hoone füüsilised omadused ja asukoht.

Side- ja teabesüsteemide kaitsmise viis sõltub samuti sellest, kui väärtuslikuks asjaomast teavet peetakse ja kui suurt kahju võib tekitada julgeoleku ohtu sattumine, sellest, millised on hoone füüsilised omadused ja hoone asukoht, ning sellest, milline on süsteemi asukoht hoones.

7.4. **Situatsioonkavad**

Tuleb ette valmistada üksikasjalikud kavad salastatud teabe kaitsmiseks kohaliku või riikliku hädaolukorra puhul.

8. TEABETURVE

Teabeturve (INFOSEC) on seotud selliste julgeolekumeetmete kindlaksmääramise ja rakendamisega, millega kaitstakse side-, teabe- või muudes elektroonilistes süsteemides töödeldavat, salvestatavat või edastatavat Euroopa Liidu salastatud teavet juhuslike või tahtlike toimingute eest, mis võiksid kahjustada teabe salastatust, terviklikkust või kättesaadavust. Võetakse piisavad vastumeetmed selleks, et välistada volitamata kasutajate juurdepääs Euroopa Liidu salastatud teabele, volitatud kasutajate juurdepääsu tõkestamine Euroopa Liidu salastatud teabele ja Euroopa Liidu salastatud teabe rikkumine, loata muutmine ja loata kustutamine.

▼B

9. SABOTAAŽ JA KURITAHTLIKU KAHJUSTAMISE MUUDE VORMIDE KONTROLL

Salastatud teavet sisaldavate oluliste rajatiste kaitseks võetud füüsilised ettevaatusabinõud on parim julgeolekutagatis sabotaaži ja kuritahtliku kahjustamise muude vormide vastu ning seda ei saa asendada ainult töötajate julgeolekukontrolli läbiviimisega. Pädeval siseriiklikul ametiasutusel palutakse hankida luureandmeid spionaaži, sabotaaži, terrorismi ja muu õõnestava tegevuse kohta.

10. SALASTATUD TEABE AVALDAMINE KOLMANDATELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE

Komisjonist pärit Euroopa Liidu salastatud teabe avaldamise kolmandale riigile või rahvusvahelisele organisatsioonile otsustab komisjoni kolleegium. Kui teave, mida soovitakse avaldada, ei ole pärit komisjonist, küsib komisjon avaldamiseks kõigepealt teabe koostajate nõusolekut. Kui teabe koostajat ei ole võimalik kindlaks teha, võtab komisjon vastutuse teabe eest endale.

Kui komisjon saab kolmandatelt riikidelt, rahvusvahelistelt organisatsioonidelt või muudelt kolmandatelt isikutelt salastatud teavet, kaitstakse kõnealust teavet selle salastatuse taseme kohaselt ja pidades kinni standarditest, mis on samaväärsed käesolevate sätetega Euroopa Liidu salastatud teabe jaoks kehtestatutega, või rangematest standarditest, kui seda eeldab teabe avaldanud kolmas isik. Võib korraldada vastastikuseid kontrollimisi.

Eeltoodud põhimõtteid kohaldatakse vastavalt II osa 26. jaos ja liidetes 3, 4 ning 5 esitatud detailsetele sätetele.

II OSA: KOMISJONI JULGEOLEKU KORRALDAMINE

11. TURVAKÜSIMUSTE EEST VASTUTAV KOMISJONI LIIGE

Turvaküsimuste eest vastutav komisjoni liige:

a) viib ellu komisjoni julgeolekupoliitikat;

b) uurib julgeolekuprobleeme, mille komisjon või selle pädevad organid talle on edastanud;

c) uurib tihedas koostöös liikmesriikide julgeolekuasutustega (või muude asjakohaste asutustega) küsimusi, mis toovad kaasa muutusi komisjoni julgeolekupoliitikas.

Konkreetselt lasub turvaküsimuste eest vastutaval komisjoni liikmel vastutus:

a) koordineerida kõiki komisjoni toimingutega seotud julgeolekuküsimusi;

b) adresseerida liikmesriikide määratud asutustele liikmesriikide julgeolekuasutustele esitatud taotlused komisjonis töötavate isikute julgeolekukontrolli läbimise kohta 20. jao kohaselt;

c) uurida või tellida uurimine iga Euroopa Liidu salastatud teabe lekke kohta, mis esimesest pilgust usutava süütõendi alusel on komisjonis aset leidnud;

d) nõuda, et asjaomased julgeolekuasutused algataksid uurimise, kui ilmneb, et Euroopa Liidu salastatud teabe leke on toimunud väljaspool komisjoni, ning koordineerida uurimist, kui uurimisega on seotud mitu julgeolekuasutust;

e) vaadata regulaarselt läbi Euroopa Liidu salastatud teabe kaitsmiseks võetud julgeolekukord;

▼B

f) säilitada tihedaid sidemeid kõigi asjaomaste julgeolekuasutustega, et tagada julgeoleku üldine koordineerimine;

g) jälgida pidevalt komisjoni julgeolekupõhimõtteid ja -korda ning teha vajadusel asjakohaseid ettepanekuid. Seoses sellega esitab turvaküsimuste eest vastutav komisjoni liige komisjonile aastase uurimisplaani, mis on koostatud ►M2 komisjoni julgeolekudirektoraadis ◄.

12. KOMISJONI JULGEOLEKUPOLIITIKA NÕUANDEKOMITEE

Luuakse komisjoni julgeolekupoliitika nõuandekomitee. See koosneb turvaküsimuste eest vastutavast komisjoni liikmest või tema delegaadist, kes tegutseb esimehena, ning iga liikmesriigi julgeolekuasutuse esindajatest. Teiste Euroopa institutsioonide esindajaid võib samuti kutsuda. Kui arutatakse Euroopa ühenduste ja Euroopa Liidu detsentraliseeritud asutustega seotud küsimusi, võib komitee istungitele kutsuda ka nimetatud asutuste esindajad.

Komisjoni julgeolekupoliitika nõuandekomitee tuleb kokku komitee esimehe või mis tahes selle liikme kutsel. Komitee ülesandeks on uurida ja hinnata kõiki asjakohaseid julgeolekuküsimusi ning vajadusel teha komisjonile ettepanekuid.

▼M2

13. KOMISJONI JULGEOLEKUNÕUKOGU

Luuakse komisjoni julgeolekunõukogu. Sinna kuuluvad personali ja halduse peadirektor, kes tegutseb esimehena, julgeolekuküsimuste eest vastutava voliniku kabineti liige, presidendi kabineti liige, peasekretäri asetäitja, kes juhatab komisjoni kriisiohjeldusrühma, õigustalituse, välissuhete, õigus-, vabadus- ja turvalisusküsimuste, Teadusuuringute Ühiskeskuse, informaatika ja siseauditi talituse peadirektorid ja komisjoni julgeolekudirektoraadi direktor või nende esindajad. Kutsuda võib ka teisi komisjoni ametnikke. Julgeolekunõukogu töövaldkonda kuulub julgeolekumeetmete hindamine komisjonis ja selles valdkonnas ettepanekute tegemine julgeolekuküsimuste eest vastutavale komisjoni liikmele.

▼B

14. ►M2 KOMISJONI JULGEOLEKUDIREKTORAAT ◄

11. jaos mainitud kohustuste täitmiseks on turvaküsimuste eest vastutava komisjoni liikme käsutuses julgeolekumeetmete koordineerimiseks, kontrollimiseks ja rakendamiseks ►M2 komisjoni julgeolekudirektoraat ◄.

►M2 Komisjoni julgeolekudirektoraadi direktor ◄ on turvaküsimuste eest vastutava komisjoni liikme peamiseks nõunikuks julgeolekuküsimustes ning tegutseb julgeolekupoliitika nõuandekomitee sekretärina. Seoses sellega juhib ta julgeolekueeskirjade ajakohastamist ning koordineerib julgeolekumeetmeid liikmesriikide pädevate asutustega ja vajadusel ka rahvusvaheliste organisatsioonidega, mis on komisjoniga seotud julgeolekukokkulepete alusel. Sellisel juhul tegutseb ta kontaktametnikuna.

►M2 Komisjoni julgeolekudirektoraadi direktor ◄ vastutab infotehnoloogiasüsteemide ja -võrkude akrediteerimise eest komisjonis. ►M2 Komisjoni julgeolekudirektoraadi direktor ◄ otsustab kooskõlas asjaomase liikmesriigi julgeolekuasutusega nende infotehnoloogiasüsteemide ja -võrkude akrediteerimise, mis hõlmavad ühest küljest komisjoni ja teisest küljest mis tahes muud Euroopa Liidu salastatud teabe saajat.

▼B

15. JULGEOLEKUKONTROLL

►M2 Komisjoni julgeolekudirektoraat ◄ vaatab regulaarselt läbi Euroopa Liidu salastatud teabe kaitsmiseks võetud julgeolekukorra.

►M2 Komisjoni julgeolekudirektoraati ◄ võivad selle ülesande täitmisel abistada teiste Euroopa Liidu institutsioonide julgeolekuteenistused, kes hoiavad Euroopa Liidu salastatud teavet, või liikmesriikide julgeolekuasutused ([1]).

Liikmesriigi palvel võib Euroopa Liidu salastatud teavet komisjonis kontrollida vastava liikmesriigi julgeolekuasutus ühiselt koos ►M2 komisjoni julgeolekudirektoraadiga ◄ ja vastastikusel kokkuleppel.

16. SALASTATUSE KATEGOORIAD, JULGEOLEKUTÄHISED JA -TÄHISTUSED

16.1. **Kategooriate tasandid** ([2])

Teave on salastatud järgnevatel tasanditel (vt ka 2. liide):

►M1 TRES SECRET UE/EU TOP SECRET ◄: seda kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib väga tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve.

►M1 SECRET UE ◄: seda kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve.

►M1 CONFIDENTIEL UE ◄: seda kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve.

►M1 RESTREINT UE ◄: seda kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib negatiivselt mõjutada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi huve.

Muud kategooriad on keelatud.

16.2. **Julgeoleku tähised**

Salastatuse kategooria kehtivuse piiramiseks (salastatud teabe jaoks tähendab see automaatset salastatuse kategooria alandamist või kaotamist) võib kasutada kokkuleppelist julgeolekutähist. Selleks tähiseks võib olla kas „UNTIL… (aeg/kuupäev)” või „UNTIL… (sündmus)”.

Täiendavaid julgeolekutähiseid, näiteks tähistust CRYPTO ja muid Euroopa Liidus tunnustatud julgeolekutähiseid kasutatakse siis, kui peale salastatuse kategooria on vaja veel tähistada piiratud levikut ja erikäitlemist.

Julgeolekutähiseid kasutatakse ainult koos salastatuse kategooriaga.

16.3. **Tähistused**

Tähistust võib kasutada dokumendi valdkonna või konkreetse teadmisvajaduse põhimõttel levitamise täpsustamiseks, või (mittesalastatud teabe korral) selleks, et tähistada embargo lõppu.

Tähistus ei ole salastatuse kategooria ja seda ei tohi selle asemel kasutada.

([1]) Ilma et see piiraks 1961. aasta diplomaatiliste suhete Viini konventsiooni ja 8. aprilli 1965. aasta Euroopa ühenduste privileegide ja immuniteetide protokolli kohaldamist.

([2]) Vt Euroopa Liidu, NATO, Lääne-Euroopa Liidu ja liikmesriikide salastatuse tasemete võrdlevat tabelit liites 1.

▼B

Tähistust ESDP kasutatakse dokumentidel ja nende koopiatel, kui neis käsitletakse Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi julgeolekut ja kaitset või sõjalise või mittesõjalise kriisi ohjamist.

16.4. **Kategooriate kinnitamine**

Salastatuse kategooriad kinnitatakse järgmiselt:

a) kategooriasse ►M1 RESTREINT UE ◄ kuuluvatele dokumentidele mehaaniliste või elektrooniliste vahenditega;

b) kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvatele dokumentidele mehaaniliste vahenditega või käsitsi või trükkides eelnevalt tempiga varustatud ja registreeritud paberile;

c) kategooriatesse ►M1 SECRET UE ◄ ja ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvatele dokumentidele mehaaniliste vahenditega või käsitsi.

16.5. **Julgeolekutähiste kinnitamine**

Julgeolekutähised kinnitatakse otse salastatuse kategooria alla, kasutades samasid vahendeid, mida kasutati salastatuse kategooria kinnitamiseks.

17. SALASTATUSE KATEGOORIATE HALDAMINE

17.1. **Üldine**

Teave salastatakse ainult siis, kui see on vajalik. Salastatuse kategooria peab olema selgelt ja täpselt märgitud ning see säilib seni, kuni teavet on vaja kaitsta.

Teabe salastatuse kategooria ja selle hilisema alandamise või kaotamise eest vastutab ainult teabe looja.

Komisjoni ametnikud ja muud teenistujad määravad salastatuse kategooria, alandavad seda või kaotavad selle kas oma osakonnajuhataja juhtnööride kohaselt või kokkuleppel temaga.

Salastatud dokumentide käitlemise üksikasjalik kord on koostatud nii, et oleks tagatud selliste dokumentide kaitse neis sisalduva teabe kohaselt.

Isikute arv, kes on volitatud koostama ►M1 TRES SECRET UE/EU TOP SECRET ◄ kategooriaga dokumente, tuleb hoida võimalikult väiksena ning nende nimed on kirjas ►M2 komisjoni julgeolekudirektoraadis ◄ koostatud nimekirjas.

17.2. **Kategooriate rakendamine**

Dokumendi salastatuse kategooria määratakse dokumendi sisu delikaatsuse põhjal, võttes arvesse 16. jaos esitatud määratlust. Salastatuse kategooriaid tuleb kasutada korrektselt ja mõõdukalt. See kehtib eriti ►M1 TRES SECRET UE/EU TOP SECRET ◄ salastatuse kategooria kohta.

Salastatava dokumendi looja peab kinni eespool sätestatud eeskirjadest ega lase dokumendile anda liiga kõrget või liiga madalat salastatuse kategooriat.

Salastatuse kategooriate määramise praktiline juhend on esitatud liites 2.

Ühe dokumendi eri leheküljed, lõiked, jaotised, lisad, liited, manused ja täiendused võivad vajada eri salastatuse kategooriat ning need ka tähistatakse vastavalt. Kogu dokumendi salastatuse kategooria määratakse selle osa järgi, mille salastatuse kategooria on kõige kõrgem.

▼B

Kui dokumentidele on lisatud kiri või teade, määratakse selle salastatuse kategooria kindlaks selle dokumendi järgi, mille salastatuse kategooria on kõige rangem. Koostaja peab selgelt tähistama sellise kirja või teate salastatuse kategooria juhul, kui see lahutatakse lisatud dokumentidest.

Avalikkuse juurdepääsu reguleeritakse endiselt määrusega (EÜ) nr 1049/2001.

17.3. **Salastatuse taseme vähendamine ja kaotamine**

Euroopa Liidu salastatud dokumentide salastatuse kategooriat võib alandada või sellise kategooria kaotada ainult dokumendi koostaja loal ja vajadusel pärast arutelu muude huvitatud pooltega. Salastatuse kategooria alandamist või kaotamist tuleb kinnitada kirjalikult. Dokumendi koostaja vastutab selle eest, et dokumendi adressaate teavitatakse muudatustest, ning need adressaadid omakorda vastutavad selle eest, et muudatustest teavitatakse järgmisi adressaate, kellele nemad on saatnud kõnealuse dokumendi või selle koopia.

Võimaluse korral määravad dokumentide koostajad salastatud dokumentidele kuupäeva, ajavahemiku või sündmuse, millal võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik.

18. FÜÜSILINE JULGEOLEK

18.1. **Üldine**

Füüsilise julgeoleku meetmete peamisteks eesmärkideks on takistada volitamata isikute juurdepääsu Euroopa Liidu salastatud teabele ja/või materjalile, takistada seadmete ja muu vara vargust ning kahjustamist ja hoida ära personali, muude töötajate ja külastajate ahistamist ning mis tahes agressiooni.

18.2. **Turvanõuded**

Kõiki kohti, piirkondi, hooneid, ruume, side- ja teabesüsteeme jms, kus säilitatakse ja käideldakse Euroopa Liidu salastatud teavet, kaitstakse asjakohaste füüsiliste julgeolekumeetmetega.

Vajaliku füüsilise julgeoleku ulatuse kindlaksmääramisel võetakse arvesse asjaomased tegurid, näiteks:

a) teabe ja/või materjali salastatuse kategooria;

b) olemasoleva teabe hulk ja vorm (nt trükitud või elektrooniliselt salvestatud);

c) kohapeal antud hinnang ohule, mida näiteks sabotaaži, terrorismi ja muude õõnestavate ja/või kriminaalsete toimingute tõttu kujutavad endast luureteenistused, kelle töö on suunatud Euroopa Liidule, liikmesriikidele ja/või muudele institutsioonidele või kolmandatele isikutele, kelle valduses on Euroopa Liidu salastatud teavet.

Kohaldatavate füüsiliste julgeolekumeetmete eesmärk on:

a) välistada salajane või jõuga sissetung;

b) hoida ära, takistada ja avastada ebalojaalsete töötajate toimingud;

c) takistada nende juurdepääs Euroopa Liidu salastatud teabele, kellel ei ole teadmisvajadust.

▼B

18.3. **Füüsilised julgeolekumeetmed**

18.3.1. *Turvaalad*

Alad, kus käideldakse ja hoitakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat teavet, tuleb korraldada ja üles ehitada nii, et need vastaksid ühele järgmistest.

a) I klassi turvaala: ala, kus käideldakse või hoitakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat teavet ja kus alale sisenemine tähendab põhimõtteliselt juurdepääsu salastatud teabele. Sellise ala puhul on nõutavad:

   i) selgelt määratletud ja kaitstud piirid, millesse sisenemist ja millest väljumist alati kontrollitakse;

   ii) sisenemise kontrollsüsteem, mis võimaldab alale siseneda ainult neil isikutel, kes on läbinud julgeolekukontrolli ja kellel on selleks eriluba;

   iii) kõnealusel alal tavaliselt hoitava teabe salastatuse kategooria täpsustamine, st täpsustatakse teave, millele saadakse juurdepääs alale sisenemisega.

b) II klassi turvaala: ala, kus käideldakse või hoitakse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat teavet nii, et seda on volitamata isikute juurdepääsu eest võimalik kaitsta sisekontrollivahendite abil, näiteks hoone, kus asuvad talitused, kus pidevalt käideldakse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat teavet. Sellise ala puhul on nõutavad:

   i) selgelt määratletud ja kaitstud piirid, millesse sisenemist ja millest väljumist alati kontrollitakse;

   ii) sisenemise kontrollsüsteem, mis võimaldab alale ilma saatjata siseneda ainult neil isikutel, kes on läbinud julgeolekukontrolli ja kellel on selleks eriluba. Kõigi teiste isikute puhul nähakse ette saatja või samaväärse kontrolli läbimine, et välistada loata juurdepääs Euroopa Liidu salastatud teabele ja kontrollimatu sissepääs aladele, kus kasutatakse tehnilist julgeolekukontrolli.

   Alasid, kus töötajad ei viibi ööpäev läbi, kontrollitakse kohe pärast tavalise tööaja lõppu, et tagada Euroopa Liidu salastatud teabe nõuetekohane kaitstus.

18.3.2. *Haldustegevuse ala*

I ja II klassi turvaalade ümber või ees võib luua madalama julgeolekuga haldustegevuse ala. Sellise ala piir peab olema visuaalselt selgelt tähistatud, et oleks võimalik töötajaid ja sõidukeid kontrollida. Sellistel aladel võib käidelda ja hoida ainult salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvat ja mittesalastatud teavet.

18.3.3. *Sisse- ja väljapääsu kontrollimine*

I ja II klassi turvaalade sisse- ja väljapääsu kontrollib läbipääsulubade või isikutuvastuse süsteem, mida rakendatakse kogu personalile, kes tavaliselt nendel aladel töötavad. Loata juurdepääsu välistamiseks Euroopa Liidu salastatud teabele tuleb luua ka külastajate kontrollimise süsteem. Läbipääsulubade süsteemi võib täiendada automaattuvastusega, mida käsitatakse valvureid täiendava, kuid mitte neid asendava vahendina. Kui ohtude hinnangus toimub muudatusi, võib sellega kaasneda sisse- ja väljapääsu kontrollimise meetmete karmistamine näiteks silmapaistvate isikute külaskäigu ajal.

▼B

18.3.4. *Valvepatrullid*

Väljaspool tavapärast tööaega patrullitakse I ja II klassi turvaaladel, et kaitsta Euroopa Liidu varasid rikkumise, kahjustamise ja hävimise eest. Patrullimissagedus määratakse kindlaks kohalike asjaolude põhjal, kuid see võiks olla vähemalt kord kahe tunni jooksul.

18.3.5. *Turvakonteinerid ja turvakambrid*

Euroopa Liidu salastatud teabe säilitamiseks kasutatakse kolme liiki konteinereid:

— A klass: konteinerid, mis on salastatuse kategooriasse ►**M1** TRES SECRET UE/EU TOP SECRET ◄ kuuluva teabe säilitamiseks I või II klassi turvaalal siseriiklikult heaks kiidetud,

— B klass: konteinerid, mis on salastatuse kategooriatesse ►**M1** SECRET UE ◄ ja ►**M1** CONFIDENTIEL UE ◄ kuuluva teabe säilitamiseks I või II klassi turvaalal siseriiklikult heaks kiidetud,

— C klass: kontorimööbel, mis sobib vaid salastatuse kategooriasse ►**M1** RESTREINT UE ◄ kuuluva teabe säilitamiseks.

Julgeoleku Akrediteerimise Asutus peab sertifitseerima I või II klassi turvaalale ehitatud turvakambrite ja kõigi selliste I klassi turvaalade, kus salastatuse kategooriasse ►**M1** CONFIDENTIEL UE ◄ või kõrgemasse salastatuse kategooriasse kuuluvat teavet säilitatakse lahtistel riiulitel või kus see on skeemidel, kaartidel vms välja pandud, seinte, põrandate ja lagede ning lukkudega uste puhul tuleb kinnitada, et need pakuvad samaväärset kaitset kui samasse salastatuse kategooriasse kuuluva teabe säilitamiseks heakskiidetud klassi turvakonteinerid.

18.3.6. *Lukud*

Euroopa Liidu salastatud teabe säilitamiseks kasutatavate turvakonteinerite ja turvakambrite lukud peavad vastama järgmistele standarditele:

— A rühm: siseriiklikult heaks kiidetud A klassi konteinerite jaoks,

— B rühm: siseriiklikult heaks kiidetud B klassi konteinerite jaoks,

— C rühm: sobib ainult C klassi kuuluva talituse mööbli jaoks.

18.3.7. *Võtmete ja koodide järelevalve*

Turvakonteinerite võtmeid ei tohi komisjoni hoonetest välja viia. Isikud, kellel on vaja teada turvakonteinerite koode, peavad need pähe õppima. Hädaolukordadeks on asjaomase komisjoni osakonna kohaliku julgeolekuametniku vastutusel varuvõtmed ja kõigi koodide kirjalik register; koode hoitakse eraldi pitseeritud läbipaistmatutes ümbrikes. Võtmeid, varuvõtmeid ja koode hoitakse eraldi turvakonteinerites. Kõnealuste võtmete ja koodide kaitse peaks olema sama range kui materjali kaitse, millele nendega on võimalik juurde pääseda.

Turvakonteinerite koode teadvate inimeste arv peab olema võimalikult väike. Koode muudetakse:

a) uue konteineri saabumisel;

b) iga personalimuutuse korral;

c) iga kord, kui on toimunud julgeoleku rikkumine või kui seda kahtlustatakse;

d) soovitatavalt iga kuue kuu järel ja vähemalt iga 12 kuu järel.

▼B

18.3.8. *Sissetungimise avastamise seadmed*

Kui Euroopa Liidu salastatud teabe kaitsmiseks kasutatakse häiresüsteeme, valvekaameraid ja muid elektrilisi seadmeid, tuleb kasutada tagavaravooluallikat, mis tagaks süsteemi töötamise ka siis, kui voolu saamine peavooluallikast katkeb. Peale selle on oluline, et selliste süsteemide riketest või nende töö segamisest antaks valvetöötajatele teada häire või muu usaldusväärse hoiatusega.

18.3.9. *Heakskiidetud seadmed*

►**M2** Komisjoni julgeolekudirektoraat ◄ haldab ajakohaseid nimekirju turvaseadmete tüüpide ja mudelite kaupa, mis on heaks kiidetud salastatud teabe kaitsmiseks erinevates kirjeldatud olukordades ja erinevatel tingimustel. ►**M2** Komisjoni julgeolekudirektoraat ◄ nimekirjad põhinevad muu hulgas liikmesriikide julgeolekuasutustelt saadud teabel.

18.3.10. *Koopiamasinate ja faksiseadmete füüsiline kaitse*

Koopiamasinaid ja faksiseadmeid kaitstakse füüsiliselt sellises ulatuses, nagu on vaja tagamaks, et neid võivad kasutada salastatud teabe töötlemiseks ainult selleks volitatud isikud ja et kõiki salastatud tooteid kontrollitakse nõuetekohaselt.

18.4. **Salajase jälgimise ja pealtkuulamise vastane kaitse**

18.4.1. *Salajane jälgimine*

Nii päeval kui ka öösel võetakse kõik vajalikud meetmed tagamaks, et selleks volitamata isikud ei näe Euroopa Liidu salastatud teavet ka mitte juhuslikult.

18.4.2. *Pealtkuulamine*

Kui esineb selline oht, tuleb talitusi ja alasid, kus regulaarselt arutletakse salastatuse kategooriasse ►**M1** SECRET UE ◄ või kõrgemasse kategooriasse kuuluva teabe üle, kaitsta nii tahtliku kui ka tahtmatu pealtkuulamise eest. Sellise pealtkuulamise ohu hindamise eest vastutab ►**M2** komisjoni julgeolekudirektoraat ◄, kes võib vajadusel enne konsulteerida liikmesriikide julgeolekuasutustega.

18.4.3. *Elektrooniliste ja salvestusseadmete kasutamine*

Keelatud on mobiiltelefonide, isiklike arvutite, salvestusseadmete, kaamerate ja teiste elektrooniliste või salvestusseadmete sissetoomine turvaaladele või tehniliselt kaitstud aladele ilma eelneva ►**M2** komisjoni julgeolekudirektoraadi direktori ◄ loata.

Tahtmatu pealtkuulamise vastu võetavate kaitsemeetmete (näiteks seinte, uste, põrandate ja lagede heliisolatsioon, paljastava kiirguse mõõtmine) ja tahtliku pealtkuulamise vastu võetavate kaitsemeetmete (näiteks mikrofonide otsimine) kindlaksmääramiseks võib ►**M2** komisjoni julgeolekudirektoraat ◄ nõuda liikmesriikide julgeolekuasutuste abi.

Samuti võivad liikmesriigi julgeolekuasutuse tehnilise julgeoleku spetsialistid ►**M2** komisjoni julgeolekudirektoraadi direktori ◄ taotluse põhjal vajadusel kontrollida kõiki sideseadmeid ja elektrilisi või elektroonilisi bürooseadmeid, mida kasutatakse salastatuse kategooriasse ►**M1** SECRET UE ◄ või kõrgemasse salastatuse kategooriasse kuuluvatel koosolekutel.

▼B

18.5. **Tehniliselt kaitstud alad**

Teatavad alad võib määrata tehniliselt kaitstud aladeks. Neile aladele sisenemisel läbitakse erikontroll. Kui sellistel aladel ei ole inimesi, on need alad heakskiidetud viisil lukustatud ning kõiki võtmeid käsitatakse turvavõtmetena. Sellistel aladel toimub regulaarselt füüsiline kontroll, mis võetakse ette ka iga loata sisenemise või sellise sisenemise kahtluse järel.

Seadmete ja mööbli üle peetakse üksikasjalikku arvestust, et jälgida nende asukoha muutust. Sellisele alale ei tohi tuua ühtegi mööblieset ega seadet enne, kui erikoolitusega julgeolekutöötaja on selle hoolikalt üle kontrollinud, et tuvastada võimalike pealtkuulamisvahendite olemasolu. Üldiselt on sideliinide paigaldamine ilma eelneva asjaomase asutuse loata tehniliselt kaitstud aladele keelatud.

19. TEADMISVAJADUSE PÕHIMÕTTE JA EUROOPA LIIDU PERSONALI JULGEOLEKUKONTROLLI KOHALDAMISE ÜLDEESKIRJAD

19.1. **Üldine**

Luba pääseda juurde Euroopa Liidu salastatud teabele antakse ainult neile isikutele, kellel on teadmisvajadus seoses oma ülesannete ja kohustuste täitmisega. Luba pääseda juurde salastatuse kategooriatesse ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvale teabele antakse ainult isikutele, kes on läbinud nõuetekohase julgeolekukontrolli.

Vastutus „teadmisvajaduse” määratlemise eest lasub sellel osakonnal, milles kõnealune isik tööle hakkab.

Töötajate julgeolekukontrolli taotlemine on iga osakonna kohustus.

Pärast julgeolekukontrolli läbimist antakse välja Euroopa Liidu isiklik julgeolekusertifikaat, millel on kirjas, millisesse salastatuse kategooriasse kuuluvale teabele on asjaomasel isikul juurdepääs, ja sertifikaadi kehtivusaeg.

Kui Euroopa Liidu isiklik julgeolekusertifikaat annab loa juurdepääsuks teatavasse salastatuse kategooriasse kuuluvale teabele, on sertifikaadi valdajal õigus juurdepääsuks ka madalamasse salastatuse kategooriasse kuuluvale teabele.

Kui isikud, kellega tuleb Euroopa Liidu salastatud teabe üle aru pidada või kellele tuleb sellist teavet näidata, ei ole ametnikud ega muud töötajad, vaid näiteks välislepingupartnerid, eksperdid või konsultandid, peavad nad läbima Euroopa Liidu isikliku julgeolekukontrolli seoses Euroopa Liidu salastatud teabega ning neile tuleb tutvustada nende julgeolekuga seotud vastutust.

Avalikkuse juurdepääsu reguleeritakse endiselt määrusega (EÜ) nr 1049/2001.

19.2. **►M1 TRES SECRET UE/EU TOP SECRET ◄ teabele juurdepääsu erieeskirjad**

Kõik isikud, kes soovivad salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvale teabele juurdepääsu, peavad sellisele teabele juurdepääsu saamiseks kõigepealt läbima julgeolekukontrolli.

Turvaküsimuste eest vastutav komisjoni liige määrab kindlaks kõik isikud, kellelt nõutakse juurdepääsu ►M1 TRES SECRET UE/EU TOP SECRET ◄ kategooriasse kuuluvale teabele ning peab nende inimeste kohta nõuetekohast ►M1 TRES SECRET UE/EU TOP SECRET ◄ registrit. See register luuakse ja seda hoitakse ►M2 komisjoni julgeolekudirektoraadis ◄.

▼B

Enne salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvale teabele juurdepääsu saamist kirjutavad kõik isikud alla tunnistusele selle kohta, et neile on tutvustatud komisjoni julgeolekukorda ning nad mõistavad täielikult oma kohustust kaitsta salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvat teavet ja tagajärgi, mis on Euroopa Liidu eeskirjade ja siseriiklike õigusaktidega ette nähtud juhuks, kui salastatud teave satub kas tahtlikult või hooletuse tõttu volitamata isikute kätte.

Kui isikutel on salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvale teabele juurdepääs koosolekutel või muudel sellistel üritustel, teavitab selle üksuse või organi pädev kontrolliametnik, kus kõnealused isikud töötavad, koosoleku korraldajat sellest, et asjaomastel isikutel on luba sellisele teabele juurdepääsuks.

Kui isiku töökohustused ei eelda enam salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvale teabele juurdepääsu, kustutatakse kõnealuse isiku nimi salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ nimekirjast. Lisaks juhitakse selliste isikute tähelepanu veel kord nende erikohustustele seoses salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluva teabe kaitsmisega. Sellised isikud kirjutavad alla deklaratsioonile selle kohta, et nad ei kasuta ega edasta nende käsutuses olnud teavet, mis kuulub salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄.

19.3. **►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ teabele juurdepääsu erieeskirjad**

Kõik isikud, kes soovivad salastatuse kategooriasse ►M1 SECRET UE ◄ või ►M1 CONFIDENTIEL UE ◄ kuuluvale teabele juurdepääsu, peavad kõigepealt läbima vastava taseme julgeolekukontrolli.

Kõigile isikutele, kellele antakse salastatuse kategooriasse ►M1 SECRET UE ◄ või ►M1 CONFIDENTIEL UE ◄ kuuluvale teabele juurdepääs, tutvustatakse asjakohaseid julgeolekusätteid ja nad peavad olema kursis nende rikkumise tagajärgedega.

Kui isikutel on salastatuse kategooriasse ►M1 SECRET UE ◄ või ►M1 CONFIDENTIEL UE ◄ kuuluvale teabele juurdepääs koosolekutel või muudel sellistel üritustel, teavitab selle organi julgeolekuametnik, kus kõnealune isik töötab, koosoleku korraldajat sellest, et asjaomastel isikutel on luba juurdepääsuks sellisele teabele.

19.4. **►M1 RESTREINT UE ◄ teabele juurdepääsu erieeskirjad**

Kõigile isikutele, kellel on salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvale teabele juurdepääs, tutvustatakse käesolevaid julgeolekueeskirju ja nende rikkumise tagajärgi.

19.5. **Personali üleviimine**

Kui töötaja lahkub töökohalt, kus tema tegevus hõlmas Euroopa Liidu salastatud teabe käitlemist, jälgib registripidaja kõnealuse materjali nõuetekohast üleandmist lahkuvalt ametnikult saabuvale ametnikule.

Kui personaliliige viiakse üle teisele töökohale, kus tema tegevus hõlmab Euroopa Liidu salastatud materjali käitlemist, instrueerib kohalik julgeolekuametnik teda vastavalt.

19.6. **Erijuhised**

Isikuid, kes peavad käitlema Euroopa Liidu salastatud teavet, tuleks kõigepealt tööülesannete täitmisele asumisel ja pärast seda regulaarselt teavitada järgmisest:

a) ebadiskreetsetest vestlustest tulenev oht julgeolekule;

b) ettevaatusabinõud, mida tuleb suhetes meediaga ja erihuvigruppide esindajatega tarvitusele võtta;

▼B

c) oht, mida kujutavad endast luureteenistuste Euroopa Liidule ja selle liikmesriikidele suunatud toimingud seoses Euroopa Liidu salastatud teabe ja toimingutega;

d) kohustus teatada viivitamata asjaomasele julgeolekuasutusele kõigist lähenemistest või teguviisidest, mis võivad anda alust kahtlustada spionaaži, ja muudest ebatavalistest julgeolekuga seotud asjaoludest.

Kui isikud puutuvad sageli kokku selliste riikide esindajatega, mille luureteenistuste tegevus võib olla suunatud Euroopa Liidu ja liikmesriikide vastu seoses Euroopa Liidu salastatud teabe ja toimingutega, tutvustatakse neile lühidalt eri luureteenistustes teadaolevalt kasutatavat tehnikat.

Komisjonil ei ole julgeolekueeskirju Euroopa Liidu salastatud teabele juurdepääsu omavate isikute erareiside kohta, olenemata sellise reisi sihtkohast. ►M2 Komisjoni julgeolekudirektoraat ◄ tutvustab oma vastutusalasse kuuluvatele ametnikele ja muudele teenistujatele siiski neid eeskirju, mida nende suhtes võidakse reisimisel kohaldada.

20. KOMISJONI AMETNIKE JA MUUDE TÖÖTAJATE JULGEOLEKUKONTROLLI KORD

a) Juurdepääs komisjoni valduses olevale salastatud teabele antakse ainult sellistele komisjoni ametnikele ja muudele töötajatele või muudele komisjonis töötavatele isikutele, kes oma ülesannete või teenistusnõuete tõttu peavad sellist teavet teadma või kasutama.

b) Juurdepääsuks salastatuse kategooriatesse ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvale teabele peavad eelpool punktis a osutatud isikud saama loa käesoleva jao punktides c ja d osutatud korra kohaselt.

c) Luba antakse ainult isikutele, kes on läbinud liikmesriigi pädeva julgeolekuasutuse julgeolekukontrolli punktides i kuni n osutatud korra kohaselt.

d) ►M2 Komisjoni julgeolekudirektoraadi direktor ◄ vastutab punktides a, b ja c osutatud lubade andmise eest.

e) Tema annab loa pärast seda, kui on saanud punktides i kuni n osutatud korra kohaselt tehtud julgeolekukontrolli põhjal liikmesriigi pädeva julgeolekuasutuse koostatud seisukoha.

f) ►M2 Komisjoni julgeolekudirektoraat ◄ haldab ajakohastatud loetelu kõikidest delikaatsetest ametikohtadest, mille on esitanud asjaomased komisjoni osakonnad, ja kõikidest isikutest, kellele on antud (ajutine) luba.

g) Luba, mille kehtivusaeg on viis aastat, ei tohi kehtida kauem kui tööülesanne, mille põhjal luba anti. Seda võib uuendada punktis e osutatud korras.

h) ►M2 Komisjoni julgeolekudirektoraadi direktor ◄ tühistab loa, kui tema arvates on selleks õigustatud alus. Loa tühistamise otsusest teatatakse asjaomasele isikule, kes võib paluda, et tema seisukohad kuulaks ära ►M2 komisjoni julgeolekudirektoraadi direktor ◄ ja pädev siseriiklik asutus.

▼B

i) Julgeolekukontroll toimub koostöös asjaomase isikuga ja ►M2 komisjoni julgeolekudirektoraadi direktori ◄ taotlusel. Pädev siseriiklik julgeolekukontrolli asutus on selle liikmesriigi vastav asutus, mille kodanik kõnealune isik on. Kui kõnealune isik ei ole ühegi Euroopa Liidu liikmesriigi kodanik, taotleb ►M2 komisjoni julgeolekudirektoraadi direktor ◄ julgeolekukontrolli sellelt Euroopa Liidu liikmesriigilt, mis on kõnealuse isiku alaliseks või tavaliseks asukohaks.

j) Julgeolekukontrolli raames peab asjaomane isik täitma isikliku infolehe.

k) ►M2 Komisjoni julgeolekudirektoraadi direktor ◄ täpsustab oma taotluses, millist liiki ja millise salastatuse tasemega teabe võib asjaomasele isikule kättesaadavaks teha, et pädev siseriiklik asutus saaks teostada julgeolekukontrolli ja esitada oma seisukoha seoses kõnealusele isikule antava loa tasemega.

l) Kogu julgeolekukontrolli protsessi suhtes, kaasa arvatud selle tulemused, kohaldatakse kõnealuses liikmesriigis kehtivaid asjaomaseid õigusnorme, sealhulgas kaebusi käsitlevaid õigusnorme.

m) Kui liikmesriigi pädevate asutuste seisukoht on positiivne, võib ►M2 komisjoni julgeolekudirektoraadi direktor ◄ anda kõnealusele isikule loa.

n) Pädeva siseriikliku asutuse negatiivsest seisukohast teatatakse asjaomasele isikule, kes võib paluda, et ►M2 komisjoni julgeolekudirektoraadi direktor ◄ kuulaks ära tema selgitused. Kui ►M2 komisjoni julgeolekudirektoraadi direktor ◄ peab seda vajalikuks, võib ta paluda, et pädevad siseriiklikud asutused annaksid oma võimete piires täiendavaid selgitusi. Kui kinnitatakse negatiivset seisukohta, siis luba ei anta.

o) Kõigile isikutele, kellele antakse punktides d ja e osutatud luba, antakse loa väljaandmisel ja pärast seda regulaarsete ajavahemike järel vajalikud juhtnöörid salastatud teabe kaitsmise ja sellise kaitse tagamise vahendite kohta. Sellised isikud kirjutavad alla deklaratsioonile, milles nad kinnitavad, et on saanud juhtnöörid ja kohustuvad neid järgima.

p) ►M2 Komisjoni julgeolekudirektoraadi direktor ◄ võtab käesoleva jao rakendamiseks kõik vajalikud meetmed, eelkõige seoses eeskirjadega, mis reguleerivad juurdepääsu loa saanud isikute nimekirjale.

q) Erandkorras, kui teenistus seda eeldab, võib ►M2 komisjoni julgeolekudirektoraadi direktor ◄ pärast pädevatele siseriiklikele asutustele teatamist ja tingimusel, et nimetatud asutused ei ole selle teatise kohta kuu aja jooksul märkusi teinud, anda enne punktis i osutatud julgeolekukontrolli tulemuste selgumist kuni kuueks kuuks ajutise loa.

r) Niiviisi antud ajutised load ei anna juurdepääsu salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvale teabele; juurdepääs nimetatud kategooriasse kuuluvale teabele antakse ainult ametnikele, kes on positiivsete tulemustega läbinud julgeolekukontrolli punkti i kohaselt. Kuni julgeolekukontrolli tulemuste selgumiseni võib ametnikele, kes peavad julgeolekukontrolli läbima salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ jaoks, anda ajutise loa juurdepääsuks teabele, mis kuulub salastatuse kategooriasse ►M1 SECRET UE ◄ või madalamatesse kategooriatesse.

▼B

21. EUROOPA LIIDU SALASTATUD DOKUMENTIDE KOOSTAMINE, LEVITAMINE, EDASTAMINE, KULLERI ISIKLIK JULGEOLEK JA TÄIENDAVAD KOOPIAD VÕI TÕLKED NING VÄLJAVÕTTED

21.1. **Koostamine**

1. Euroopa Liidu salastatuse kategooriaid kasutatakse 16. jao sätete kohaselt ja ►M1 CONFIDENTIEL UE ◄ ja sellest rangemad salastatuse kategooriad peavad olema märgitud iga lehe keskel ülemises ja alumises servas ning kõik lehed peavad olema nummerdatud. Igale Euroopa Liidu salastatud dokumendile peab olema märgitud viitenumber ja kuupäev. Kui tegemist on salastatuse kategooriatesse ►M1 TRES SECRET UE/EU TOP SECRET ◄ ja ►M1 SECRET UE ◄ kuuluvate dokumentidega, peab kõnealune viitenumber olema märgitud igale lehele. Kui dokumente levitatakse mitme koopiana, peab iga koopia esilehel olema kirjas koopia number ja dokumendi lehekülgede arv. Kui tegemist on salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või rangemasse kategooriasse kuuluva dokumendiga, peab dokumendi esimesel lehel olema nimekiri kõigi lisade ja lisatud dokumentide kohta.

2. Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvaid dokumente võivad trükkida, tõlkida, säilitada, neist koopiaid teha, neid magnetkujul paljundada või neist mikrofilme teha ainult isikud, kes on läbinud julgeolekukontrolli seoses juurdepääsuga vähemalt sellesse salastatuse kategooriasse kuuluvatele dokumentidele, kuhu kuulub asjaomane dokument.

3. Sätted, mis reguleerivad salastatud dokumentide koostamist arvutiga, on ette nähtud 25. jaos.

21.2. **Levitamine**

1. Euroopa Liidu salastatud teavet levitatakse ainult isikutele, kellel on vastav teadmisvajadus ja kes on läbinud asjakohase julgeolekukontrolli. Dokumendi koostaja määrab kindlaks esialgse levitamise.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ kategooriasse kuuluvaid dokumente levitatakse ►M1 TRES SECRET UE/EU TOP SECRET ◄ registrite kaudu (vt 22. jagu, lõige 2). Kui tegemist on salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate sõnumitega, võib pädev register volitada sidekeskuse juhatajat tegema adressaatide loetelus märgitud hulga koopiaid.

3. Esialgne adressaat võib salastatuse kategooriasse ►M1 SECRET UE ◄ ja madalamatesse salastatuse kategooriatesse kuuluvaid dokumente edastada teistele adressaatidele teadmisvajaduse põhjal. Dokumendi koostanud asutus või ametiisik annab siiski selgelt teada kõigist piirangutest, mida ta soovib kohaldada. Selliste piirangute kehtestamise korral võivad adressaadid dokumente edasi levitada ainult dokumendi koostanud asutuse või ametiisiku loal.

4. Kõik dokumendid, mis kuuluvad salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse salastatuse kategooriasse, kantakse peadirektoraati või talitusse saabumisel ja sealt lahkumisel osakonna kohalikku Euroopa Liidu salastatud teabe registrisse. Registrisse kantavad andmed (viitenumber, kuupäev ja vajadusel koopia number) peavad võimaldama dokumente kindlaks teha ning need tuleb kanda logiraamatusse või spetsiaalsele kaitstud andmekandjale (vt 22. jagu lõige 1).

21.3. **Euroopa Liidu salastatud teabe edastamine**

21.3.1. *Pakendid, kättesaamistõendid*

1. Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse salastatuse kategooriasse kuuluvaid dokumente edastatakse tugevates ja läbipaistmatutes kahekordsetes ümbrikes. Sisemisele ümbrikule märgitakse vajalik Euroopa Liidu salastatuse kategooria ning võimaluse korral saaja täielik ametinimetus ja aadress.

▼B

2. Kui ümbrik ei ole adresseeritud konkreetsele isikule, võib sisemise ümbriku avada ja selles olevate dokumentide vastuvõtmist kinnitada ainult registri kontrolliametnik (vt 22. jagu lõige 1). Sellisel juhul märgitakse asjaomases registris (vt 22. jagu lõige 1) ümbriku saabumine logiraamatusse ning sisemise ümbriku võib avada ja selles olevate dokumentide vastuvõtmist kinnitada vaid isik, kellele see on adresseeritud.

3. Sisemisse ümbrikusse tuleb panna kättesaamistõendi vorm. Kättesaamistõend ei ole salastatud ning sellele peaks olema märgitud dokumendi viitenumber, kuupäev ja koopia number, kuid sellele ei tohi kunagi kirjutada dokumendis käsitletavat teemat.

4. Sisemine ümbrik pannakse välimisse ümbrikusse, millel on kättesaamistõendi jaoks kirjas paki number. Mingil juhul ei tohi välimisele ümbrikule märkida salastatuse kategooriat.

5. Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ ja kõrgematesse kategooriatesse kuuluvate dokumentide puhul antakse kullerile või virgatsile paki numbri vastu kättesaamistõend.

21.3.2. *Majasisene või majade grupi sisene edastamine*

Ühe hoone või hoonerühma piires võib salastatud dokumente transportida pitseeritud ümbrikus, millel on kirjas ainult adressaadi nimi, kui sellist ümbrikut transpordib isik, kes on läbinud julgeolekukontrolli seoses vastava kategooria salastatud dokumentidega.

21.3.3. *Riigisisene edastamine*

1. Ühe riigi piires tuleks salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente saata ainult ametliku kullerteenuse vahendusel või isikutega, kellel on luba juurdepääsuks salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvatele dokumentidele.

2. Kui salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide edastamiseks väljapoole ühe hoone või hoonerühma piire kasutatakse kullerteenust, tuleb täita käesolevas peatükis sisalduvaid sätteid pakendamise ja kättesaamistõendite kohta. Kättetoimetamisüksustel peab olema piisavalt töötajaid tagamaks, et salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente sisaldavad pakid on kogu aeg vastutava ametniku otsese järelevalve all.

3. Erandkorras võivad ametnikud, kes ei ole kullerid, viia salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente hoonest või hoonerühmast välja, et neid kasutada kohalikul koosolekul või arutelul, kui:

   a) dokumentide kandjal on luba juurdepääsuks kõnealustele salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvatele dokumentidele;

   b) transpordiliik vastab eeskirjadele, mis reguleerivad ►M1 TRES SECRET UE/EU TOP SECRET ◄ kategooriasse kuuluvate dokumentide edastamist;

   c) ametnik ei jäta salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente mingil juhul järelevalveta;

   d) nähakse ette kord sel viisil edastatavate dokumentide loetelu andmiseks salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registrisse, kus nimetatud dokumente hoitakse, ja nende dokumentide kontrollimiseks nimetatud loetelu alusel pärast tagasitoomist.

4. Ühe riigi piires võib salastatuse kategooriatesse ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvaid dokumente saata kas postiga, kui selline edastamisviis on siseriiklike õigusnormidega lubatud ja vastab nende õigusnormide sätetele, või selliste kullerteenistuste või isikute kaudu, kes on läbinud julgeolekukontrolli seoses juurdepääsuga Euroopa Liidu salastatud teabele.

▼B

5. ►M2 Komisjoni julgeolekudirektoraat ◄ koostab juhised Euroopa Liidu salastatud dokumentide kaasaskandmise kohta põhinedes nendele eeskirjadele. Dokumentide transportijad peavad sellised juhtnöörid läbi lugema ja neile alla kirjutama. Eelkõige tuleb sellistes juhtnöörides sätestada, et mingil juhul ei või:

   a) dokumendid lahkuda nende vedaja valdusest, kui nad ei ole turvaliselt hoiule antud 18. jao sätete kohaselt;

   b) jätta dokumente järelevalveta ühissõidukis või eraautos või sellistes kohtades nagu restoranid ja hotellid. Selliseid dokumente ei tohi hoida hotelli seifis ega jätta järelevalveta hotellituppa;

   c) lugeda avalikus kohas, näiteks õhusõidukis või rongis.

21.3.4. *Edastamine ühest riigist teise*

1. Salastatuse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat materjali toimetatakse edasi Euroopa Liidu diplomaatilisi või sõjaväe kullerteenuseid kasutades.

2. Salastatuse kategooriatesse ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluva materjali isiklikku transportimist võib lubada, kui transporditingimused tagavad, et selline materjal ei või sattuda volitamata isikute kätte.

3. Turvaküsimuste eest vastutav komisjoni liige võib lubada isikutel materjali transportida, kui diplomaatilise või sõjaväe kullerteenistuse abi ei ole võimalik kasutada või kui selliste kullerteenistuste kasutamine tooks kaasa viivituse, mis kahjustaks Euroopa Liidu toiminguid, ning kui kavandatud adressaadil on kõnealust materjali kiiresti vaja. ►M2 Komisjoni julgeolekudirektoraat ◄ koostab juhtnöörid, mis käsitlevad salastatuse kategooriasse ►M1 SECRET UE ◄ või madalamasse kategooriasse kuuluva materjali rahvusvahelist transportimist isikute poolt, kes ei tööta diplomaatilises ega sõjaväe kullerteenistuses. Sellistes juhtnöörides tuleb sätestada järgmised nõuded:

   a) dokumentide transportija on läbinud nõuetekohase julgeolekukontrolli;

   b) kõigi sel viisil transporditavate materjalide kohta peetakse arvet asjaomases osakonnas või registris;

   c) Euroopa Liidu materjale sisaldavad pakid või kotid peavad olema varustatud ametliku pitseriga, et välistada või piirata nende läbivaatamist tollis, ning tunnussiltide ja juhtnööridega paki või koti leidjale;

   d) materjali transportijal on kõigis Euroopa Liidu liikmesriikides tunnustatud kulleritunnistus ja/või töökäsk, mis lubavad tal nõuetekohaselt tähistatud pakki transportida;

   e) maismaal reisides ei tohi läbida kolmandaid riike ega ületada nende riikide piire, kui materjali saatev riik ei ole saanud asjaomaselt kolmandalt riigilt konkreetset garantiid;

   f) materjali transportija reis peab sihtkoha, läbitava marsruudi ja kasutatavate transpordivahendite poolest vastama Euroopa Liidu eeskirjadele või kui siseriiklikud õigusnormid on sellises küsimuses rangemad, siis neile õigusnormidele;

   g) materjal peab olema kogu aeg selle transportija valduses, kuni see antakse hoiule 18. jao turvalist säilitamist käsitlevate sätete kohaselt;

   h) materjali ei tohi jätta järelevalveta ühissõidukis või eraautos või sellistes kohtades nagu restoranid ja hotellid. Sellist materjali ei tohi hoida hotelli seifis ega jätta järelevalveta hotellituppa;

   i) kui transporditava materjali hulka kuuluvad ka dokumendid, ei tohi neid lugeda avalikus kohas (nt lennukis, rongis jms kohas).

▼B

4. Salastatud materjali transportiv isik peab läbi lugema ja allkirjastama julgeolekujuhendid, mis sisaldavad vähemalt eespool loetletud juhtnööre ja korda, mida tuleb järgida hädaolukorras või juhul, kui toll või lennujaama julgeolekuametnikud soovivad kontrollida salastatud materjali sisaldavat pakki.

21.3.5. ►M1 *RESTREINT UE* ◄ *dokumentide edastamine*

Salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvate dokumentide edasitoimetamiseks ei nähta ette erisätteid, kuid nende dokumentide edasitoimetamisel tuleks tagada, et nad ei satu volitamata isikute kätte.

21.4. **Kulleri isiklik julgeolek**

Kui virgatsit või kullerit kavatsetakse kasutada salastatuse kategooriatesse ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvate dokumentide vedamiseks, peab ta läbima nõuetekohase julgeolekukontrolli.

21.5. **Elektroonilised ja muud tehnilised edastusvahendid**

1. Sideturbe julgeolekumeetmete eesmärk on tagada Euroopa Liidu salastatud teabe turvaline edastamine. Sellise Euroopa Liidu salastatud teabe edastamise üksikasjalikke eeskirju käsitletakse 25. jaos.

2. Salastatuse kategooriatesse ►M1 CONFIDENTIEL UE ◄ ja ►M1 SECRET UE ◄ kuuluvat teavet võib edastada ainult akrediteeritud sidekeskuste, -võrkude ja/või -terminalide ja -süsteemide kaudu.

21.6. **Euroopa Liidu salastatud teabe täiendavad koopiad ja tõlked ning väljavõtted sellistest dokumentidest**

1. Salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvatest dokumentidest võib teha koopiaid või selliseid dokumente tõlkida ainult dokumendi koostaja loal.

2. Kui isik, kes ei ole läbinud julgeolekukontrolli salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluva teabe jaoks, vajab teavet, mis sisaldub salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvas dokumendis, kuid ei kuulu nimetatud salastatuse kategooriasse, võib salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registri juhataja (vt 22. jagu lõige 2) anda loa teha kõnealusest dokumendist vajaliku hulga väljavõtteid. Samal ajal võtab asjaomase registri juhataja vajalikud meetmed tagamaks, et nimetatud väljavõtetele antakse asjakohane salastatuse tase.

3. Adressaat võib salastatuse kategooriasse ►M1 SECRET UE ◄ või madalamasse kategooriasse kuuluvaid dokumente paljundada või tõlkida käesolevate julgeolekusätete kohaselt ja tingimusel, et selline tegevus on rangelt kooskõlas teadmisvajaduse põhimõttega. Esialgse dokumendi suhtes rakendatavaid julgeolekumeetmeid rakendatakse ka selle dokumendi paljunduste ja/või tõlgete suhtes.

22. EUROOPA LIIDU SALASTATUD TEABE REGISTRID, ÜLEVAATUSED, KONTROLLID, ARHIIVIS SÄILITAMINE JA HÄVITAMINE

22.1. **Euroopa Liidu salastatud teabe kohalikud registrid**

1. Komisjonis, vajadusel igas osakonnas, vastutab üks või mitu kohalikku Euroopa Liidu salastatud teabe registrit salastatuse kategooriatesse ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvate dokumentide registreerimise, kopeerimise, lähetamise, arhiveerimise ja hävitamise eest.

2. Kui osakonnal puudub oma kohalik Euroopa Liidu salastatud teabe register, toimib peasekretariaadi kohalik Euroopa Liidu salastatud teabe register osakonna Euroopa Liidu salastatud teabe registrina.

3. Kohalikud Euroopa Liidu salastatud teabe registrid alluvad osakonna juhile, kellelt nad saavad oma korraldused. Nende registrite juht on registri kontrollametnik (RCO).

▼B

4. Kohalik julgeolekuametnik teostab nende üle järelevalvet Euroopa Liidu salastatud dokumentide käitlemise kohta käivate sätete rakendamise ja vastavatest julgeolekumeetmetest kinnipidamise osas.

5. Kohalikele Euroopa Liidu salastatud teabe registritele määratud ametnikel on juurdepääs Euroopa Liidu salastatud teabele vastavalt 20. jaole.

6. Kohalikud Euroopa Liidu salastatud teabe registrid teostavad asjaomase osakonna juhataja juhtimisel järgmisi toiminguid:

   a) juhivad toiminguid, mis on seotud sellise teabe registreerimise, kopeerimise, tõlkimise, edastamise, lähetamise ja hävitamisega;

   b) ajakohastavad salastatud teabe andmete loetelu;

   c) küsitlevad korrapäraselt teabe väljaandjaid seoses teabe salastatuse säilitamise vajalikkusega.

7. Kohalikud Euroopa Liidu salastatud teabe registrid peavad registrit järgmiste andmete kohta:

   a) salastatud teabe koostamise kuupäev;

   b) salastatuse tase;

   c) salastatuse tähtaeg;

   d) väljaandja nimi ja üksus;

   e) vastuvõtja või vastuvõtjad, järjekorranumber;

   f) teema;

   g) number;

   h) tehtud koopiate arv;

   i) osakonnale esitatud salastatud teabe kohta koostatud inventuurid;

   j) salastatud teabe salastatuse kaotamise ja alandamise register.

8. 21. jaos esitatud üldised eeskirjad kehtivad komisjoni kohalikele Euroopa Liidu salastatud teabe registritele, kui neid ei ole muudetud käesolevas jaos sätestatud erisätetega.

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

22.2.1. *Üldine*

1. ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentide keskregister kindlustab ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentide salvestamine, käitlemine ja levitamise vastavalt käesolevatele turvasätetele. ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentide registri juhataja on ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentide registri kontrolliametnik.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentide keskregister toimib komisjonis peamise vastuvõtva ja lähetava ametivõimuna teiste Euroopa Liidu institutsioonide, liikmesriikide, rahvusvaheliste organisatsioonide ja kolmandate riikide suhtes, kellega komisjon on sõlminud salastatud teabe vahetamise kohta julgeolekualased kokkulepped.

3. Vajadusel luuakse alamregistrid, mis vastutavad salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide sisemise haldamise eest; sellistes alamregistrites peetakse ajakohastatud andmeid iga alamregistri vastutusel oleva dokumendi liikumise kohta.

▼B

4. Salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ alamregistrid luuakse 22. jao lõike 2 punkti 3 kohaselt, et rahuldada pikaajaline vajadus, ning sellised alamregistrid on seotud salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ keskregistriga. Kui salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente on vaja kasutada üksnes ajutiselt ja juhuti, võib neid dokumente välja anda ilma, et selleks loodaks salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ alamregister, kui ette on nähtud eeskirjad, millega tagatakse, et sellised dokumendid jäävad salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ asjaomase registri kontrolli alla ning et järgitakse kõiki füüsilisi ja personaliga seotud julgeolekumeetmeid.

5. Alamregistrid ei tohi edastada salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumente otse teistele sama ►M1 TRES SECRET UE/EU TOP SECRET ◄ keskregistri alamregistritele ilma nimetatud keskregistri selgesõnalise nõusolekuta.

6. Eri keskregistrite juurde kuuluvad alamregistrid vahetavad salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ keskregistrite vahendusel.

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

Kontrolliametnikuna vastutab salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ keskregistri juhataja järgmise eest:

a) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide edastamine kooskõlas 21. jao lõikes 3 määratletud sätetega;

b) kõigi keskregistriga seotud salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ alamregistrite loetelu pidamine koos ametissenimetatud kontrolliametnike ja nende volitatud asetäitjate nimede ja allkirjadega;

c) registrite kättesaamistõendite säilitamine kõigi salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate ja keskregistri kaudu levitatud dokumentide kohta;

d) registri pidamine hallatavate ja levitatavate salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide kohta;

e) ajakohastatud loetelu pidamine kõigi salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ keskregistrite kohta, millega ta tavapäraselt suhtleb, koos nende ametissenimetatud kontrolliametnike ja nende volitatud asetäitjate nimede ja allkirjadega;

f) kõigi registris olevate salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide füüsiline kaitsmine 18. jaos sätestatud eeskirjade kohaselt.

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

Kontrolliametnikuna vastutab salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ alamregistri juhataja järgmise eest:

a) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide edastamine kooskõlas 21. jao lõikes 3 esitatud sätetega;

b) ajakohastatud loetelu pidamine kõigi isikute kohta, kellel on luba juurdepääsuks tema kontrolli all olevale salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvale teabele;

c) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide levitamine kooskõlas nende koostaja juhtnööridega või teadmisvajaduse põhimõttel, olles kõigepealt kontrollinud, et adressaat on läbinud julgeolekukontrolli nõutaval tasemel;

d) ajakohastatud registri pidamine kõigi salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide kohta, mida hoitakse või mis ringlevad tema kontrolli all või mis on antud edasi teistele salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registritele, ja kõigi asjaomaste kättesaamistõendite säilitamine;

▼B

e) ajakohastatud loetelu pidamine salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registrite kohta, millega tal on lubatud vahetada salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente, koos nende kontrolliametnike ja nende volitatud asetäitjate nimede ja allkirjadega;

f) kõigi alamregistris olevate salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide füüsiline kaitsmine 18. jaos sätestatud eeskirjade kohaselt.

22.3. **Euroopa Liidu salastatud dokumentide inventuur, ülevaatus ja kontroll**

1. Iga käesolevas jaos osutatud ►M1 TRES SECRET UE/EU TOP SECRET ◄ register teostab igal aastal detailse salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ dokumentide inventuuri. Dokument loetakse arvelevõetuks, kui ta on registris füüsiliselt inventeeritud või kui registris on kättesaamistõend salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registrilt, kuhu dokument on edasi antud, dokumendi hävitamisakt või juhend asjaomase dokumendi salastatuse taseme vähendamiseks või kaotamiseks. Iga-aastaste inventuuride tulemused edastatakse turvaküsimuste eest vastutavale komisjoni liikmele igal aastal hiljemalt 1. aprilliks.

2. ►M1 TRES SECRET UE/EU TOP SECRET ◄ alamregistrid edastavad oma iga-aastase inventuuri tulemused keskregistrisse, mille ees nad vastutavad, asjaomase keskregistri määratud kuupäevaks.

3. Euroopa Liidu salastatud dokumentide kohta, millel on madalam salastatuse kategooria kui ►M1 TRES SECRET UE/EU TOP SECRET ◄, teostatakse sisekontrolle vastavalt turvaküsimuste eest vastutava komisjoni liikmelt saadud juhtnööridele.

4. Selliste toimingute käigus võivad salastatud teabe valdajad võtta seisukoha:

   a) teatavate dokumentide salastatuse kategooria alandamise või kaotamise kohta;

   b) dokumentide hävitamise kohta.

22.4. **Euroopa Liidu salastatud teabe arhiivis hoidmine**

1. Euroopa Liidu salastatud teabe talletatakse tingimustel, mis vastavad kõikidele 18. jaos loetletud asjaomastele nõuetele.

2. Säilitamisega seotud probleemide minimeerimiseks on kõigi registrite kontrolliametnikel luba kanda salastatuse kategooriatesse ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvad dokumendid mikrofilmile või säilitada neid arhiveerimiseks muul magnet- või optilisel andmekandjal, kui:

   a) mikrofilmile kandmise/salvestamisega tegelevad töötajad, kes on läbinud julgeolekukontrolli, mis vastab asjaomasele salastatuse tasemele;

   b) mikrofilmile/andmekandjale tagatakse samasugune julgeolek nagu esialgsetele dokumentidele;

   c) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluva dokumendi mikrofilmile kandmisest/salvestamisest teatatakse dokumendi koostajale;

   d) filmirullid või muud salvestusvahendid sisaldavad ainult samasse salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ või ►M1 CONFIDENTIEL UE ◄ kuuluvaid dokumente;

▼B

e) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ või ►M1 SECRET UE ◄ kuuluva dokumendi kandmisest/salvestamisest mikrofilmile tehakse selge märkus iga-aastaseks inventuuriks kasutatavasse registrisse;

f) originaaldokumendid, mis on kantud mikrofilmile või muul viisil salvestatud, hävitatakse 22. jao punktis 5 sätestatud korra kohaselt.

3. Neid eeskirju kohaldatakse ka muude lubatud salvestusvahendite suhtes, näiteks elektromagnetiliste andmekandjate ja optiliste ketaste suhtes.

22.5. **Euroopa Liidu salastatud dokumentide hävitamine**

1. Euroopa Liidu salastatud dokumentide asjatu kuhjumise vältimiseks hävitatakse need dokumendid, mis dokumente valdava asutuse juhataja arvates on aegunud või üleliigsed, nii ruttu kui võimalik järgmisel viisil:

a) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente võib hävitada ainult nende dokumentide eest vastutav keskregister. Iga hävitatud dokumendi kohta koostatakse hävitamisakt, millele kirjutavad alla salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ kontrolliametnik ja hävitamist tunnistama kutsutud ametnik, kes peab olema läbinud julgeolekukontrolli salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ jaoks. Logiraamatusse tehakse vastav märkus;

b) register säilitab hävitamisakte koos ringkäigulehtedega kümme aastat. Koopiad edastatakse esialgse dokumendi koostajale või asjaomasele keskregistrile ainult selgesõnalise taotluse korral;

c) salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvad dokumendid, kaasa arvatud salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja disketid) hävitatakse salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registri kontrolliametniku järelevalve all kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul viisil loetamatuks nii, et neid ei ole võimalik enam kokku panna.

2. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvad dokumendid hävitab nende dokumentide eest vastutav register, kasutades üht punkti 1 alapunktis c osutatud meetoditest sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuulunud hävitatud dokumendid loetletakse allakirjutatud hävitamisaktis, mida register säilitab koos ringkäigulehtedega vähemalt kolm aastat.

3. Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvad dokumendid hävitab nende dokumentide eest vastutav register, kasutades ühte punkti 1 alapunktis c osutatud meetoditest sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Nende hävitamine registreeritakse vastavalt turvaküsimuste eest vastutavalt komisjoni liikmelt saadud juhistele.

4. Salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvad dokumendid hävitab nende dokumentide eest vastutav register, või kasutaja vastavalt turvaküsimuste eest vastutava komisjoni liikme käest saadud juhistele.

22.6. **Hädaolukorras hävitamine**

1. Komisjoni osakonnad koostavad kohalikel tingimustel põhinevaid plaane Euroopa Liidu salastatud materjali kaitsmiseks kriisiolukorras, hõlmates vajadusel hädaolukorras hävitamise ja evakueerimise plaanid. Nad teevad teatavaks juhtnöörid, mida peetakse vajalikuks, et välistada Euroopa Liidu salastatud teabe langemine volitamata isikute kätte.

▼B

2. Salastatuse kategooriatesse ►M1 SECRET UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluva materjali kaitsmiseks ja/või hävitamiseks kriisiolukorras võetavad meetmed ei tohi mingil juhul kahjustada salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluva materjali, sealhulgas šifreerimisvahendite kaitsmist või hävitamist, mis on olulisemad kui kõik muud ülesanded.

3. Hädaolukorras šifreerimisvahendite kaitsmiseks või hävitamiseks võetavate meetmete puhul kohaldatakse erijuhtnööre.

4. Juhtnöörid peavad olema kohapeal pitseeritud ümbrikus kättesaadavad. Hävitamise vahendid/riistad peavad olema kättesaadavad.

23. VÄLJASPOOL KOMISJONI TERRITOORIUMI PEETAVATE EUROOPA LIIDU SALASTATUD TEAVET SISALDAVATE ERIKOHTUMISTE TURVAMEETMED

23.1. **Üldine**

Kui komisjoni või muid olulisi koosolekuid peetakse väljaspool komisjoni ruume ja kui see on põhjendatud konkreetsete julgeolekueeskirjadega, mis on seotud käsitletavate teemade või teabe delikaatsusega, tuleb võtta allpool kirjeldatud julgeolekumeetmed. Kõnealused meetmed on seotud ainult Euroopa Liidu salastatud teabe kaitsega; kavandada võib ka muid julgeolekumeetmeid.

23.2. **Kohustused**

23.2.1. ►M2 *Komisjoni julgeolekudirektoraat* ◄

►M2 Komisjoni julgeolekudirektoraat ◄ teeb koostööd selle liikmesriigi pädevate ametiasutustega, kelle territooriumil kohtumine aset leiab (vastuvõttev liikmesriik), et tagada komisjoni või muude oluliste kohtumiste julgeolek ning saadikute ning nende personali turvalisus. Seoses julgeoleku kaitsmisega peaks kõnealune liikmesriik eelkõige tagama, et:

a) koostatakse kavad selle kohta, kuidas reageerida julgeolekut ähvardavatele ohtudele ja julgeolekuga seotud vahejuhtumitele; kõnealused meetmed peavad eelkõige hõlmama Euroopa Liidu salastatud dokumentide turvalist säilitamist büroodes;

b) võetakse meetmeid, et võimaldada juurdepääs komisjoni sidesüsteemidele, et nende kaudu võtta vastu ja edastada Euroopa Liidu salastatud sõnumeid. Vajadusel palutakse vastuvõtval liikmesriigil võimaldada juurdepääsu ka turvalistele telefonisüsteemidele.

►M2 Komisjoni julgeolekudirektoraat ◄ tegutseb koosoleku ettevalmistamise julgeolekunõuandjana; kõnealune büroo peaks olema koosolekul esindatud ja vajadusel nõustama koosoleku julgeolekuametnikku (MSO) ja osalejaid.

Igal koosolekul osaleval delegatsioonil palutakse määrata julgeolekuametnik, kes vastutab julgeolekuküsimuste eest oma delegatsioonis ja peab sidet koosoleku julgeolekuametnikuga ning vajadusel ka ►M2 komisjoni julgeolekudirektoraadi ◄ esindajaga.

23.2.2. *Koosoleku julgeolekuametnik (MSO)*

Ametisse määratakse koosoleku julgeolekuametnik, kes vastutab üldise ettevalmistamise ja üldiste sisemiste julgeolekumeetmete kontrollimise eest ning kooskõlastamise eest muude asjaomaste julgeolekuasutustega. Koosoleku julgeolekuametniku võetavad meetmed on üldiselt seotud järgmisega:

a) kaitsemeetmed koosoleku toimumiskohas tagamaks, et koosolek toimub vahejuhtumiteta, mis võiksid kahjustada koosolekul kasutatava Euroopa Liidu salastatud teabe julgeolekut;

▼B

b) nende töötajate kontrollimine, kellele on lubatud juurdepääs koosoleku toimumiskohta, osalejate ruumidesse ja konverentsiruumidesse, ja seadmete kontrollimine;

c) pidev koordineerimine vastuvõtva liikmesriigi pädevate asutustega ja ►M2 komisjoni julgeolekudirektoraadiga ◄;

d) julgeolekujuhendite lisamine koosoleku kausta, võttes nõuetekohaselt arvesse käesolevates julgeolekueeskirjades sätestatud nõudeid ja muid vajalikuks peetavaid julgeolekujuhendeid.

23.3. **Julgeolekumeetmed**

23.3.1. *Turvaalad*

Järgmised turvaalad määratakse kindlaks:

a) II klassi turvaala, mis hõlmab dokumentide ettevalmistamise ruumi, komisjoni ametiruume ja paljundusseadmeid ning vajadusel delegatsioonide ametiruume;

b) I klassi turvaala, mis hõlmab konverentsiruumi, tõlkekabiine ja helitehnikute kabiine;

c) haldustegevuse alad, mis hõlmavad pressiruume ja koosolekukoha neid osi, mida kasutatakse haldustegevuseks, toitlustamiseks ja majutamiseks, ning vahetult pressikeskuse ja koosoleku toimumiskoha ümbruses paiknev ala.

23.3.2. *Läbipääsuload*

Koosoleku julgeolekuametnik annab välja vajalikud nimesildid delegatsioonide teatatud vajaduste kohaselt. Vajadusel võib eristada juurdepääsu eri turvaaladele.

Koosoleku julgeolekujuhendid kohustavad kõiki asjaomaseid isikuid kandma oma nimesilti koosolekukohas viibides alati nähtaval kohal, et julgeolekutöötajad saaksid neid vajadusel kontrollida.

Peale nimesilti kandvate osalejate lubatakse koosoleku toimumiskohta võimalikult vähe inimesi. Koosoleku julgeolekuametnik lubab riikide delegatsioonidel vastu võtta külalisi koosoleku jooksul ainult nende palvel. Külalistele tuleb anda külalise nimesilt. Sellega seoses täidetakse külastaja läbipääsuloa vorm, millele märgitakse külastaja nimi ja külastatava isiku nimi. Külastajaid saadetakse kogu aeg turvatöötaja või külastatava isiku poolt. Külalise läbipääsuloa vorm on külalise saatja käes, kes tagastab selle koos külalise nimesildiga julgeolekutöötajale, kui külaline lahkub koosoleku toimumiskohast.

23.3.3. *Foto- ja heliseadmete kontrollimine*

I klassi turvaalale ei tohi tuua fotoaparaate ega salvestusseadmeid, kui tegemist ei ole seadmetega, mille toovad sinna fotograafid või helitehnikud, kellel on selleks koosoleku julgeolekuametniku nõuetekohane luba.

23.3.4. *Portfellide, kaasaskantavate arvutite ja pakkide kontrollimine*

Läbipääsuloa omanikud, kellel on lubatud pääs turvaaladele, võivad tavaliselt võtta kaasa oma portfellid ja kaasaskantavad arvutid (ainult autonoomse vooluallikaga), ilma et neid kontrollitaks. Delegatsioonidele mõeldud pakkide puhul võivad delegatsioonid võtta vastu neile toodud pakid, mida kontrollib kas delegatsiooni julgeolekuametnik, mis vaadatakse läbi spetsiaalsete seadmetega või mille julgeolekutöötajad avavad kontrollimiseks. Kui koosoleku julgeolekuametnik peab seda vajalikuks, võib portfellide ja pakkide kontrollimiseks kehtestada rangemad meetmed.

▼B

23.3.5. *Tehniline julgeolek*

Tehnilise julgeoleku meeskond võib tagada tehniliselt koosolekuruumi julgeoleku ja jälgida seda koosoleku ajal ka elektrooniliselt.

23.3.6. *Delegatsioonide dokumendid*

Delegatsioonid on vastutavad Euroopa Liidu salastatud dokumentide viimise eest koosolekule ja sealt ära. Nad vastutavad ka nende dokumentide kontrollimise ja julgeoleku eest dokumentide kasutamise ajal neile määratud ruumides. Vastuvõtvatelt liikmesriikidelt võib paluda, et nad aitaksid vedada salastatud dokumente koosolekukohta ja sealt tagasi.

23.3.7. *Dokumentide turvaline hoidmine*

Kui komisjon või delegatsioonid ei suuda oma salastatud dokumente säilitada kooskõlas vastuvõetud standarditega, võivad nad jätta sellised dokumendid pitseeritud ümbrikus kättesaamistõendi vastu koosoleku julgeolekuametniku kätte, kes säilitab dokumente kooskõlas vastuvõetud standarditega.

23.3.8. *Ametiruumide kontrollimine*

Koosoleku julgeolekuametnik korraldab komisjoni ja delegatsioonide ametiruumide kontrollimise iga tööpäeva lõpus, et tagada kõigi Euroopa Liidu salastatud dokumentide säilitamine turvalises kohas. Teistsuguste asjaolude korral võtab ta vajalikud meetmed.

23.3.9. *Euroopa Liidu salastatud jäätmete kõrvaldamine*

Kõiki jäätmeid peetakse Euroopa Liidu seisukohast salastatuks ning prügikorvid ja -kotid tuleks anda komisjonile või delegatsioonidele nende kõrvaldamiseks. Enne kui komisjon ja delegatsioonid lahkuvad neile määratud ruumidest, peavad nad viima oma jäätmed koosoleku julgeolekuametnikule, kes korraldab jäätmete hävitamise korra kohaselt.

Koosoleku lõpus käsitletakse jäätmetena kõiki komisjonis või delegatsioonides olevaid dokumente, mida enam vaja pole. Enne koosoleku jaoks võetud julgeolekumeetmete lõpetamist tuleb komisjoni ja delegatsioonide ruumides teha põhjalik läbiotsmine. Dokumendid, mille kohta on kättesaamistõendile alla kirjutatud, hävitatakse võimaluse korral nii, nagu on sätestatud 22. jao punktis 5.

24. JULGEOLEKU RIKKUMINE JA EUROOPA LIIDU SALASTATUD TEABE KAHJUSTAMINE

24.1. **Määratlused**

Julgeoleku rikkumine toimub sellise tegevuse või tegematajätmise tagajärjel, mis on vastuolus komisjoni mingi julgeolekusättega ja mis võib seada ohtu Euroopa Liidu salastatud teabe või kahjustada seda.

Euroopa Liidu salastatud teabe kahjustamine toimub siis, kui kõnealune teave on tervikuna või osaliselt sattunud volitamata isikute kätte, st isikute kätte, kes ei ole läbinud julgeolekukontrolli vastaval tasemel või kellel puudub asjaomaste dokumentide kohta teadmisvajadus, või kui on tõenäoline, et teave on sattunud selliste isikute kätte.

Euroopa Liidu salastatud teavet võidakse kahjustada hooletuse, ettevaatamatuse või mõtlematuse tagajärjel või seda võivad teha Euroopa Liidu või tema liikmesriikide vastu suunatud teenistused, kes huvituvad Euroopa Liidu salastatud teabest ja tema tegevusest, või õõnestusorganisatsioonid.

24.2. **Julgeoleku rikkumisest teatamine**

Kõiki isikuid, kellelt nõutakse Euroopa Liidu salastatud teabe käitlemist, instrueeritakse põhjalikult nende kohustustest selles valdkonnas. Nad teatavad kohe mis tahes avastatud julgeoleku rikkumisest.

▼B

Kui kohalik julgeolekuametnik või koosoleku julgeolekuametnik avastab Euroopa Liidu salastatud teabega seotud julgeoleku rikkumise või Euroopa Liidu salastatud materjali kaotamise või kadumise või kui talle teatatakse sellest, võtab ta viivitamata meetmeid, et:

a) kaitsta tõendusmaterjali;

b) teha kindlaks asjaolud;

c) hinnata kahju ja minimeerida selle mõju;

d) välistada sellise juhtumi kordumine;

e) teavitada asjaomaseid asutusi julgeoleku rikkumise tagajärgedest.

Seoses sellega esitatakse järgmine teave:

i) asjaomase teabe kirjeldus, sealhulgas selle salastatuse tase, viitenumber, koopia number, kuupäev, koostaja, teema ja reguleerimisala;

ii) lühike ülevaade julgeoleku rikkumise asjaoludest, sealhulgas kuupäev ja ajavahemik, mille jooksul teavet kahjustati;

iii) teatis selle kohta, kas juhtunust on teatatud dokumendi koostajale.

Pärast seda, kui neile on teatatud sellise julgeoleku rikkumise võimalikkusest, on kõik julgeolekuasutused kohustatud sellest viivitamata teatama ►**M2** komisjoni julgeolekudirektoraadile ◄.

Salastatuse kategooriasse ►**M1** RESTREINT UE ◄ kuuluva teabega seotud juhtumitest tuleb teatada ainult siis, kui tegemist on ebatavaliste asjaoludega.

Turvaküsimuste eest vastutav komisjoni liige, kui teda on teavitatud esinenud julgeoleku rikkumisest:

a) teatab sellest asutusele või ametiisikule, kes koostas kõnealuse salastatud teabe;

b) palub asjaomasel julgeolekuasutusel alustada uurimist;

c) koordineerib uurimist, kui juhtum puudutab mitut julgeolekuasutust;

d) palub esitada aruande rikkumise asjaolude, toimumise tõenäolise kuupäeva ja ajavahemiku ning avastamise kuupäeva ja aja kohta koos asjaomase materjali sisu ja salastatuse taseme üksikasjaliku kirjeldusega. Aruanne tuleb esitada ka Euroopa Liidu või ühe või mitme tema liikmesriigi huvidele tekitatud kahju ja sellise juhtumi kordumise välistamiseks võetud meetmete kohta.

Dokumendi koostaja teatab juhtunust dokumendi adressaatidele ja annab neile vajalikud juhtnöörid.

24.3. **Õiguslikud meetmed**

Kõik isikud, kes vastutavad Euroopa Liidu salastatud teabe kahjustamise eest, kannavad distsiplinaarvastutust asjakohaste reeglite ja eeskirjade kohaselt, eriti vastavalt personalieeskirjade VI jaotisele. Distsiplinaarvastutus ei piira edasiste õiguslike meetmete võtmist.

Asjakohastel juhtudel ja 24. jao lõikes 2 mainitud aruande alusel võtab turvaküsimuste eest vastutav komisjoni liige vajalikud meetmed, võimaldamaks pädevatel siseriiklikel ametivõimudel algatada kriminaalõiguslikke menetlusi.

▼B

25. INFOTEHNOLOOGIA JA SIDESÜSTEEMIDE ABIL KÄIDELDAVA EUROOPA LIIDU SALASTATUD TEABE KAITSMINE

25.1. **Sissejuhatus**

25.1.1. *Üldine*

Julgeolekupoliitikat ja -eeskirju kohaldatakse kõigi side- ja infosüsteemide ja -võrkude (edaspidi süsteemid) suhtes, mille abil käideldakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ ja kõrgemasse salastatuse kategooriasse kuuluvat teavet. Neid kohaldatakse komisjoni 23. novembri 1995 lõpliku otsuse K(95) 1510 lisana informaatikasüsteemide kaitsmise kohta.

Ka süsteemide puhul, mille abil käideldakse salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvat teavet, tuleb võtta julgeolekumeetmeid sellise teabe kaitsmiseks. Kõigi süsteemide puhul tuleb võtta julgeolekumeetmed, et kaitsta nende süsteemide ja neis sisalduva teabe terviklikkust ja kättesaadavust.

Komisjoni poolt rakendatav infotehnoloogiaalane julgeolekupoliitika koosneb järgnevast:

— see on lahutamatu osa üldisest julgeolekust ja täiendab kõiki teabeturbe, töötajate julgeoleku ja füüsilise julgeoleku elemente,

— kohustuste jagunemine tehniliste süsteemide omanike, tehnilistes süsteemides salvestatud või käideldud Euroopa Liidu salastatud teabe omanike, infotehnoloogia turvaspetsialistide ja kasutajate vahel,

— iga infotehnoloogiasüsteemi turvapõhimõtete ja -nõuete kirjeldus,

— kõnealuste põhimõtete ja nõuete kooskõlastus määratud ametiasutusega,

— arvestamine infotehnoloogia valdkonna eriohtude ja -nõrkustega.

25.1.2. *Süsteeme ähvardavad ohud ja nende nõrgad kohad*

Ohtu võib määratleda kui võimalust, et juhuslikult või tahtlikult kahjustatakse julgeolekut. Süsteemide puhul kaasneb sellise kahjustamisega ühe või mitme salastatuse, terviklikkuse või kättesaadavuse atribuudi kaotus. Nõrka kohta võib määratleda kui nõrkust või kontrolli puudumist, mis soodustab konkreetse vahendi või sihtmärgi vastu suunatud ohu realiseerumist või võimaldab sellel realiseeruda.

Kiirotsinguteks, edastamiseks ja kasutamiseks mõeldud süsteemides kontsentreeritud kujul käideldavat Euroopa Liidu salastatud ja salastamata teavet võivad ohustada mitmed ohud. Selliste riskide hulka kuuluvad volitamata kasutajate juurdepääs teabele ja juurdepääsu keelamine volitatud kasutajatele. Samuti on olemas teabe volitamata avaldamise, kahjustamise, muutmise või kustutamise risk. Lisaks sellele on keerukad ja vahel ka haprad seadmed sageli kallid ning neid on raske parandada või kiiresti asendada.

25.1.3. *Turvameetmete peamine eesmärk*

Käesolevas jaos sätestatud julgeolekumeetmete põhieesmärk on kaitsta Euroopa Liidu salastatud teavet volitamata avaldamise (salastatuse kadumise) ning teabe terviklikkuse ja kättesaadavuse kadumise vastu. Euroopa Liidu salastatud teabe käitlemiseks kasutatava süsteemi julgeoleku piisavaks kaitsmiseks määratleb ►M2 komisjoni julgeolekudirektoraat ◄ tavapärase julgeoleku asjakohased standardid koos iga süsteemi jaoks kavandatud spetsiaalsete julgeolekumenetluste ja -tehnikaga.

▼B

25.1.4. *Süsteemispetsiifiliste julgeolekunõuete loetelu (SSRS)*

Kõikide süsteemide kohta, mis käitlevad ►M1 CONFIDENTIEL UE ◄ ja kõrgema salastatuse kategooriaga teavet, tuleb koostada süsteemispetsiifiliste julgeolekunõuete loetelu (SSRS) tehnilise süsteemi vastutava käitaja (TSO, vt 25. jao lõike 3 punkt 4) ja teabeomaniku (vt 25. jao lõike 3 punkt 5) poolt, kes teevad koostööd ning viivad vajadusel sisse projektipersonali ja ►M2 komisjoni julgeolekudirektoraat ◄ (mis on teabeturbe asutus — IA, vt 25. jao lõike 3 punkt 3) ettepanekud ja arvestavad nende abiga; kõnealune loetelu tuleb kooskõlastada julgeoleku akrediteerimise ametiisikuga (SAA, vt 25. jao lõike 3 punkt 2).

Süsteemispetsiifiliste julgeolekunõuete loetelu nõutakse ka siis, kui julgeoleku akrediteerimise ametiisik (SAA) peab salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluva teabe või salastamata teabe kättesaadavust ja terviklikkust üliolulisteks.

Süsteemispetsiifiliste julgeolekunõuete loetelu koostatakse võimalikult varases projekti käivitamise järgus ning projekti jätkumise käigus arendatakse seda edasi ja täiustatakse; projekti eri etappidel ja süsteemi elutsükli jooksul täidab süsteemispetsiifiliste julgeolekunõuete loetelu eri funktsioone.

25.1.5. *Turvalisuse tagamise toimimisviisid*

Kõik süsteemid, mille abil käideldakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat teavet, akrediteeritakse tööks ühes või kui eri ajavahemike nõuded seda eeldavad, mitmes turvarežiimis või selle siseriiklikus ekvivalendis:

a) ühtlane ülaturve;

b) diferentsiaalne ülaturve ja

c) mitmetasemeline turve.

25.2. **Määratlused**

„Akrediteerimine” tähendab süsteemile loa andmist ja heakskiitu töödelda Euroopa Liidu salastatud teavet süsteemi töökeskkonnas.

Märkus:

Selline akrediteerimine peaks toimuma pärast kõigi asjakohaste julgeolekumenetluste rakendamist ja süsteemi vahendite piisava julgeolekutaseme saavutamist. Akrediteerimine peaks tavaliselt toimuma süsteemispetsiifiliste julgeolekunõuete loetelu põhjal ja sisaldama järgmist:

a) süsteemi akrediteerimise eesmärk; eelkõige see, millisesse salastatuse kategooriasse kuuluvat teavet kavatsetakse käitlema hakata ja milliseid süsteemi või võrgu turvarežiime kavatsetakse kasutada;

b) riskijuhtimise ülevaade, et teha kindlaks ohud ja nõrgad kohad ning nende vastu võetavad meetmed;

c) julgeolekuga seotud töökord koos kavandatud toimingute üksikasjalise kirjeldusega (näiteks pakutavad režiimid, teenused), kaasa arvatud süsteemi turvaelementide kirjeldus, mis on akrediteerimise aluseks;

d) turvaelementide rakendamise ja ülalpidamise kava;

e) süsteemi turvalisuse või võrgu turvalisuse esialgse ja edaspidise katsetamise, hindamise ja sertifitseerimise kava; ja

f) vajadusel tõend koos muude akrediteerimisdokumentidega.

▼B

„Keskne teabeturbe ametnik” (CISO) tähendab keskse infotehnoloogiateenuse ametnikku, kes koordineerib turvameetmeid ja teostab nende järelevalvet keskselt organiseeritud süsteemides.

„Sertifitseerimine” tähendab sellise ametliku teatise väljaandmist, mida toetab sõltumatu ülevaade hindamise käigu ja tulemuste kohta ning selle kohta, kuivõrd süsteem vastab julgeolekunõuetele või arvutiturbetoode eelnevalt kindlaksmääratud turvanõuetele.

„Sideturve” (COMSEC) tähendab turvameetmete rakendamist sides, et keelata volitamata isikutele juurdepääs väärtuslikule teabele, mida nad võiksid saada sellise side valdamise ja uurimise käigus, ning tagada sellise side autentsus.

Märkus:

Need meetmed hõlmavad krüptograafia, edastuse ja lähetuse turvalisust; ja samuti toimimise, füüsilist, töötajate julgeolekut ning dokumentide ja arvutiturvet.

„Arvutiturve” (COMPUSEC) tähendab riistvara, püsivara ja tarkvara turvaelementide rakendamist arvutisüsteemis, et kaitsta teabe volitamata avaldamise, manipuleerimise, muutmise/kustutamise ja teenuste keelamise eest või neid takistada.

„Arvutiturbetoode” tähendab üldist arvutiturbeeset, mis sisestatakse infotehnoloogiasüsteemi, et see tõhustaks või tagaks käideldava teabe salastatuse, terviklikkuse ja kättesaadavuse.

„Ühtlase ülaturbe režiim” tähendab süsteemi turvarežiimi, mille puhul KÕIK isikud, kellel on süsteemile juurdepääs, peavad läbima süsteemis käideldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli ja neil on ühine teadmisvajadus KOGU süsteemis käideldava teabe järele.

Märkused:

1) Ühine teadmisvajadus tähendab seda, et arvutiturvaelementidega ei pea kohustuslikus korras eristama teavet süsteemi sees.

2) Muud turvaelemendid (näiteks füüsilised, personaliga seotud ja menetluslikud) vastavad süsteemis käideldava teabe kõrgeima salastatuse taseme nõudmistele ja kõigi kategooriate tähistele.

„Hindamine” tähendab seda, et asjaomane asutus teeb üksikasjaliku tehnilise uuringu süsteemi julgeolekuaspektide või krüpteerimis- või arvutiturbetoote kohta.

Märkused:

1) Hindamise käigus uuritakse nõutavate turbefunktsioonide olemasolu ja selliste funktsioonide kahjulike kõrvalmõjude puudumist ning antakse hinnang sellele, kas kõnealuseid funktsioone on võimalik rikkuda.

2) Hindamise käigus tehakse kindlaks, kui suures ulatuses on täidetud süsteemi või arvutiturbetoote turvanõuded, ja kehtestatakse süsteemi või krüpteerimisseadme või arvutiturbetootele usaldatud funktsiooni kindluse tase.

„Teabeomanik” (IO) tähendab ametiisikut (osakonna juhataja), kes vastutab teabe koostamise, töötlemise ja kasutamise eest, kaasa arvatud otsustamine selle üle, kellele lubatakse kõnealusele teabele juurdepääs.

▼B

„Teabeturve” (INFOSEC) tähendab turvameetmete rakendamist selleks, et kaitsta side-, teabe- ja muudes elektroonilistes süsteemides töödeldavat, säilitatavat ja edastatavat teavet salastatuse, terviklikkuse või kättesaadavuse juhusliku ja tahtliku rikkumise eest ning välistada süsteemide terviklikkuse ja kättesaadavuse rikkumine.

„Teabeturbe meetmete” hulka kuuluvad arvutite, edastuse, lähetuste ja krüptograafia turvalisus ning teabe ja süsteemide vastu suunatud ohtude avastamine, dokumenteerimine ja nende suhtes vastumeetmete võtmine.

„Infotehnoloogiaala” tähendab ala, millel on üks või mitu arvutit, nende kohalikud välis- ja salvestusseadmed, juhtimisseadmed ning erivõrgu- ja -sideseadmed.

Märkus:

Kõnealune ala ei hõlma eraldi ala, millel asuvad kaugvälisseadmed või -terminalid/tööjaamad, isegi siis, kui need seadmed on ühendatud infotehnoloogiaalal asuvate seadmetega.

„Infotehnoloogiavõrk” tähendab teabe vahetamiseks omavahel seotud infotehnoloogiasüsteemide geograafiliselt jaotatud organisatsiooni, mis hõlmab omavahel seotud infotehnoloogiasüsteemide komponente ja nende liideseid koos toetava teabe ja sidevõrkudega.

Märkused:

1) Infotehnoloogiavõrk võib teabe vahetamiseks kasutada üht või mitut omavahel seotud sidevõrku; mitu infotehnoloogiavõrku võivad kasutada ühise sidevõrgu teenuseid.

2) Infotehnoloogiavõrku nimetatakse „kohalikuks”, kui see ühendab mitu samas kohas asuvat arvutit.

„Infotehnoloogiavõrgu turvaelemendid” hõlmavad üksikute infotehnoloogiasüsteemide turvaelemente, koosnedes võrgust koos võrgu kui sellisega seotud lisakomponentide ja -omadustega (näiteks võrguside, turvatunnus, märgistusmehhanismid ja -menetlused, juurdepääsukontroll, programmid ja kontrolljäljed), mis on vajalikud salastatud teabe vastuvõetava kaitsetaseme pakkumiseks.

„Infotehnoloogiasüsteem” tähendab seadmete, meetodite ja menetluste ja vajadusel töötajate kogumit, mis täidab teabe töötlemisega seotud funktsioone.

Märkused:

1) Seda käsitatakse kui vahendite kogumit, mis on konfigureeritud teabe käitlemiseks süsteemis.

2) Sellised süsteemid võivad toetada konsulteerimist, juhtimist, sidet, teadus- ja haldusrakendusi, kaasa arvatud tekstitöötlus.

3) Süsteemi piirid määratakse üldiselt kindlaks kui elemendid, mis on ühe tehnilise süsteemi vastutava käitaja kontrolli all.

4) Infotehnoloogiasüsteem võib hõlmata alamsüsteeme, millest mõned on ise infotehnoloogiasüsteemid.

▼B

„Infotehnoloogiasüsteemi turvaelementide” hulka kuuluvad kõik riistvara/püsivara/tarkvara funktsioonid, omadused ja elemendid; operatsioonisüsteemid, arvestussüsteemid ja juurdepääsukontroll, infotehnoloogiaala, terminali- või tööjaamaala ja juhtimispiirangud, füüsiline struktuur ja seadmed, töötajad ja sidekontroll, mis on vajalikud, et pakkuda infotehnoloogiasüsteemis käideldavale salastatud teabele vastuvõetaval tasemel kaitse.

„Kohalik teabeturve ametnik” (LISO) tähendab komisjoni osakonna ametnikku, kes vastutab turvameetmete koordineerimise eest ning järelevalve teostamise eest oma valdkonnas.

„Mitmetasemelise turbe režiim” tähendab süsteemi turvarežiimi, mille puhul KÕIK isikud, kellel on juurdepääs süsteemile, EI pea läbima süsteemis käideldava teabe kõrgeimale salastatuse tasemele vastavat julgeolekukontrolli ning KÕIGIL isikutel EI ole ühist teadmisvajadust kogu süsteemis käideldava teabe järele.

Märkused:

1) Kõnealune süsteemi turvarežiim võimaldab praegu käidelda eri salastatuse tasemetele ja eri teabekategooriatesse kuuluvat teavet.

2) Asjaolu, et kõiki isikud ei pea läbima kõige kõrgemale salastatuse tasemele vastavat julgeolekukontrolli koos ühise teadmisvajaduse puudumisega, tähendab seda, et arvutiturvaelementidega tuleb tagada valikuline juurdepääs süsteemis sisalduvale teabele ja selle teabe eristamine süsteemi sees.

„Terminali- või tööjaamaala” tähendab ala, kus on mõned arvutiseadmed, nende kohalikud välisseadmed või terminalid/tööjaamad ja nendega seotud sideseadmed, mis paiknevad väljaspool infotehnoloogiaala.

„Julgeolekuga seotud töökord” tähendab tehnilise süsteemi vastutava käitaja poolt koostatud töökorda, mis määrab kindlaks julgeolekuküsimustes vastuvõetavad põhimõtted, järgitava töökorra ning töötajate kohustused.

„Diferentsiaalse ülaturbe režiim” tähendab süsteemi turvarežiimi, mille puhul KÕIK isikud, kellel on juurdepääs süsteemile, peavad läbima süsteemis käideldava teabe kõrgeimale salastatuse tasemele vastava julgeolekukontrolli, kuid KÕIGIL isikutel EI ole ühist teadmisvajadust kogu süsteemis käideldava teabe järele.

Märkused:

1) Ühise teadmisvajaduse puudumine tähendab seda, et arvutiturvaelementidega tuleb tagada valikuline juurdepääs süsteemis sisalduvale teabele ja selle teabe eristamine süsteemi sees.

2) Muud turvaelemendid (näiteks füüsilised, personaliga seotud ja menetluslikud) vastavad süsteemis käideldava teabe kõrgeima salastatuse taseme nõudmistele ja kõigi kategooriate tähistele.

3) Kõnealuses turvarežiimis süsteemis käideldavat või olemasolevat teavet koos genereeritava väljundiga kaitstakse nii, nagu kuuluks see vastavasse teabekategooriasse ja nõuaks kõrgeimat salastatuse taset, kuni vastupidise otsuse tegemiseni, kui puudub piisavalt usaldusväärne kasutatav märgistamissüsteem.

▼B

„Süsteemispetsiifiliste julgeolekunõuete loetelus” (SSRS) väljendatakse lõplikult ja selgelt, milliseid julgeolekupõhimõtteid tuleb järgida ja milliseid üksikasjalikke julgeolekunõudeid täita. See põhineb komisjoni julgeolekupoliitikal ja riski hindamisel või see määratakse kindlaks selliste parameetritega nagu töökeskkond, töötajate julgeolekukontrolli miinimumtase, käideldava teabe salastatuse kõrgeim tase, süsteemi turvarežiim või kasutajate nõudmised. Süsteemispetsiifiliste julgeolekunõuete loetelu on projekti dokumentatsiooni lahutamatu osa, mis esitatakse pädevatele asutustele tehniliseks, eelarveliseks ja julgeolekualaseks heakskiitmiseks. Lõplikul kujul moodustab süsteemispetsiifiliste julgeolekunõuete loetelu täieliku selgituse selle kohta, mida tähendab süsteemi turvalisus.

„Tehnilise süsteemi vastutav käitaja” (TSO) tähendab ametiisikut, kes vastutab süsteemi loomise, administreerimise, tegevuse ja sulgemise eest.

„Tempest-vastumeetmed” on julgeolekumeetmed, mille eesmärk on kaitsta seadmeid ja side infrastruktuure tahtmatu elektromagnetkiirguse ja juhtivusest põhjustatud salastatud teabe kahjustamise eest.

25.3. **Vastutus julgeolekuküsimustes**

25.3.1. *Üldine*

Komisjoni julgeolekupoliitika nõuandekomitee 12. jaos määratletud nõuandealased kohustused hõlmavad teabeturbe küsimusi. Nõuandekomitee korraldab oma töö nii, et ta suudab anda eksperdiabi eespool kirjeldatud küsimustes.

►M2 Komisjoni julgeolekudirektoraat ◄ vastutab üksikasjalike teabeturbe sätete, mis põhinevad käesoleva peatüki sätetele, väljaandmise eest.

Julgeolekuga seotud probleemide puhul (vahejuhtumid, rikkumised jms) võtab ►M2 komisjoni julgeolekudirektoraat ◄ viivitamata meetmeid.

►M2 Komisjoni julgeolekudirektoraadil ◄ on oma teabeturbe üksus.

25.3.2. *Julgeoleku akrediteerimise ametiisik (SAA)*

►M2 Komisjoni julgeolekudirektoraadi direktor ◄ on komisjoni julgeoleku akrediteerimise ametiisik (SAA). Julgeoleku akrediteerimise ametiisik vastutab üldise julgeoleku valdkonna eest ning samuti teabeturbe, sideturbe, CRYPTO-turbe ja Tempest-turbe erivaldkondade eest.

Julgeoleku akrediteerimise ametiisik vastutab selle eest, et süsteemid oleksid kooskõlas komisjoni julgeolekupõhimõtetega. Üks sellise asutuse ülesannetest on süsteemide tunnustamine seoses Euroopa Liidu salastatud teabe käitlemisega määratud salastatuse tasemel tema töökeskkonnas.

Komisjoni julgeoleku akrediteerimise ametiisiku pädevus hõlmab kõiki komisjoni ruumides toimivaid süsteeme. Kui süsteemi eri komponendid kuuluvad komisjoni julgeoleku akrediteerimisasutuse ja muude julgeoleku akrediteerimisasutuste jurisdiktsiooni alla, määravad kõik asjaomased osapooled komisjoni julgeoleku akrediteerimisasutuse koordineerimisel ühise akrediteerimisameti.

25.3.3. *Teabeturbe ametiisik (IA)*

►M2 Komisjoni julgeolekudirektoraadi ◄ teabeturbe üksuse juhataja on komisjoni teabeturbe ametiisik. Teabeturbe ametiisiku vastutusalasse kuuluvad:

— tehniliste nõuannete ja abi andmine julgeoleku akrediteerimisasutusele;

— süsteemispetsiifiliste julgeolekunõuete loetelu väljatöötamisele kaasaaitamine;

▼B

— süsteemispetsiifiliste julgeolekunõuete loetelu läbivaatamine, et tagada nende vastavus käesolevatele julgeolekueeskirjadele, teabeturbe põhimõtetele ja arhitektuuri käsitlevatele dokumentidele;

— osalemine akrediteerimisrühmades/-kogudes vastavalt vajadusele ja akrediteerimisega seotud teabeturbesoovituste andmine julgeoleku akrediteerimisasutusele;

— teabeturbe koolitus- ja haridustegevuse toetamine;

— tehniliste nõuannete jagamine teabeturbega seotud vahejuhtumite uurimiseks;

— tehniliste suuniste koostamine selleks, et tagada ainult lubatud tarkvara kasutamine.

25.3.4. *Tehnilise süsteemi vastutav käitaja (TSO)*

Vastutus süsteemi juhtelementide ja eriturvaelementide teostamise ja töö eest lasub vastava süsteemi vastutaval käitajal, tehnilise süsteemi vastutaval käitajal (TSO). Keskselt juhitavatele süsteemidele määratakse keskne informaatikaturbe ametnik (CISO). Iga osakond määrab vajadusel kohaliku informaatikaturbe ametniku (LISO). Tehnilise süsteemi vastutava käitaja kohustuste hulka kuulub julgeolekuga seotud töökorra (SecOP) loomine ja need ulatuvad läbi kogu süsteemi eluea alates projekti kontseptsiooni etapist kuni selle lõpliku lahenduseni.

Tehnilise süsteemi vastutav käitaja täpsustab julgeolekustandardid ja -tavad, mida süsteemi tarnijad peavad järgima.

Tehnilise süsteemi vastutav käitaja võib vajadusel delegeerida osa oma kohustustest kohalikule informaatikaturbe ametnikule. Üks isik võib täita erinevaid teabeturve funktsioone.

25.3.5. *Teabeomanik (IO)*

Teabeomanik (IO) vastutab Euroopa Liidu salastatud (ja muu) teabe eest, mida hoitakse, töödeldakse ja toodetakse tehnilistes süsteemides. Tema määratleb nõuded juurdepääsuks süsteemis olevale teabele. Ta võib delegeerida selle kohustuse tema vastutusalas tegutsevale teabejuhile või andmebaasi haldurile.

25.3.6. *Kasutajad*

Kõik kasutajad vastutavad selle eest, et nende toimingud ei kahjustaks nende kasutatava süsteemi julgeolekut.

25.3.7. *Teabeturbe koolitus*

Teabeturbe haridus ja koolitus on kättesaadav kogu personalile, kes seda vajab.

25.4. **Mittetehnilised julgeolekumeetmed**

25.4.1. *Personali julgeolek*

Süsteemi kasutajad peavad läbima julgeolekukontrolli ning neil peab olema teadmisvajadus, mis vastab nende konkreetses süsteemis käideldava teabe salastatuse tasemele ja sisule. Juurdepääs teatavatele seadmetele või teabele, mis iseloomustavad süsteemide julgeolekut, eeldab seda, et asjaomane isik on komisjoni korra kohaselt läbinud julgeolekukontrolli.

Julgeoleku akrediteerimisasutus määrab kindlaks kõik tundlikud ametikohad ja täpsustab neile ametikohtadele asuvate isikute julgeolekukontrolli ja järelevalve taseme.

Süsteemid täpsustatakse ja määratakse kindlaks viisil, mis soodustab ülesannete ja vastutuse jagamist töötajate vahel, et välistada olukord, kus kõiki süsteemi julgeoleku võtmeaspekte teaks või kontrolliks täielikult üks isik.

▼B

Infotehnoloogiaaladel ning terminali- või tööjaamaaladel, kus on võimalik süsteemi turvalisust muuta, ei tohi viibida ainult üks volitatud ametnik/muu töötaja.

Süsteemi turvasätteid muudetakse ainult vähemalt kahe volitatud töötaja poolt, kes teevad koostööd.

25.4.2. *Füüsiline julgeolek*

Infotehnoloogiaalad ja terminali- või tööjaamaalad (mis on määratletud 25. jao lõigus 2), kus infotehnoloogiavahendite abil käideldakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluvat teavet või kus on võimalik sellisele teabele juurde pääseda, kinnitatakse vastavalt vajadusele Euroopa Liidu I või II klassi turvaaladeks.

25.4.3. *Süsteemile juurdepääsu kontroll*

Kogu teavet ja materjali, mis võimaldavad kontrollida süsteemile juurdepääsu, kaitstakse abinõudega, mis vastavad kõrgeimale salastatuse tasemele ja salastatuse teabe kategooriale, millele süsteem juurdepääsu võimaldab.

Kui juurdepääsu kontrollimise teavet ja materjali sel otstarbel enam ei kasutata, hävitatakse need 25. jao lõike 5 punkti 4 kohaselt.

25.5. **Tehnilised julgeolekumeetmed**

25.5.1. *Teabeturve*

Teabe koostaja on kohustatud kindlaks tegema ja salastama kõik teavet sisaldavad dokumendid olenemata sellest, kas need on paberkoopiad või elektrooniliselt salvestatud. Paberkoopiate kõigi lehekülgede ülemisse ja alumisse serva märgitakse salastatuse kategooria. Olenemata sellest, kas väljund on paberkoopia või elektrooniliselt salvestatud, on selle salastatuse kategooria sama nagu kõrgeima salastatuse kategooriaga teabel, mida dokumendi koostamisel kasutati. Ka süsteemi kasutamisviis võib mõjutada kõnealuse süsteemi väljundite salastatuse kategooriat.

Komisjoni osakonnad ja nende teabe valdajad on kohustatud arvesse võtma üksikute teabeelementide koondumisega seotud probleeme ja järeldusi, mida võib teha omavahel seotud elementide põhjal, ning otsustama, kas kogu teabekogumi salastatuse kategooriat tuleks tõsta või ei.

Asjaolu, et teave võib olla lühikood, edastuskood või esitatud kahendkujul, ei taga julgeoleku kaitstust ja seega ei tohiks see mõjutada teabe salastatuse kategooriat.

Kui teave edastatakse ühest süsteemist teise, tuleb teavet edastamise ajal ja vastuvõtvas süsteemis kaitsta viisil, mis oleks vastavuses esialgse salastatuse taseme ja teabe salastatuse kategooriaga.

Kõiki elektroonilisi salvestusvahendeid tuleb käsitleda viisil, mis on vastavuses salvestatud teabe kõrgeima salastatuse kategooria või vahendi liigiga, ja alati vastavalt kaitsta.

Korduvkasutusega elektroonilistel salvestusvahenditel, mida on kasutatud Euroopa Liidu salastatud teabe salvestamiseks, säilib kõrgeim salastatuse tase, mille jaoks neid on kasutatud, kuni asjaomase teabe salastatuse kategooriat on vajalikul määral alandatud või see on kaotatud ja elektroonilise salvestusvahendi salastatuse taset on vastavalt muudetud, selle salastatuse tase kaotatud või vahend hävitatud korras, mille on heaks kiitnud julgeoleku akrediteerimisasutus (vt 25.5.4).

▼B

25.5.2. *Teabe kontroll ja aruandekohustus*

Salastatuse kategooriasse ►M1 SECRET UE ◄ ja kõrgemasse kategooriasse kuuluva teabe kasutamise üle peetakse registrit automaatsete (kontrolljälg) või manuaalsete logiraamatute abil. Kõnealuseid registreid säilitatakse käesolevate julgeolekueeskirjade kohaselt.

Infotehnoloogiaaladel asuvaid Euroopa Liidu salastatud teabe väljundeid võib käidelda ühe salastatud ühikuna ning neid ei pea registreerima, kui materjal on identifitseeritud, salastatuse kategooriaga tähistatud ja nõuetekohaselt kontrollitud.

Kui väljund luuakse Euroopa Liidu salastatud teavet käitlevas süsteemis ja edastatakse infotehnoloogiaalalt terminali- või tööjaamaalale, kehtestatakse julgeoleku akrediteerimisasutuse nõusolekul kaugväljundi kontrollimise ja logimise kord. Salastatuse kategooriasse ►M1 SECRET UE ◄ ja kõrgemasse salastatuse kategooriasse kuuluva teabe korral hõlmab selline kord konkreetseid juhtnööre teabe üle arvestuse pidamiseks.

25.5.3. *Teisaldatavate elektrooniliste salvestusvahendite käsitlemine ja kontroll*

Kõiki teisaldatavaid elektroonilisi salvestusvahendeid, mis kuuluvad salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või rangemasse kategooriasse, käsitatakse materjalina ja nende suhtes kohaldatakse üldisi eeskirju. Vajalikke tunnuseid ja salastatuse kategooriate tähiseid tuleb kohandada konkreetsete salvestusvahendite välimusega, et neid oleks võimalik selgelt ära tunda.

Kasutajad vastutavad selle eest, et Euroopa Liidu salastatud teavet säilitatakse vahendite abil, millel on nõuetekohane salastatuse kategooria ja kaitstus. Kehtestatakse kord tagamaks, et kõigisse salastatuse kategooriatesse kuuluvat Euroopa Liidu salastatud teavet säilitatakse elektroonilistel salvestusvahenditel käesolevate julgeolekueeskirjade kohaselt.

25.5.4. *Elektrooniliste salvestusvahendite salastatuse kategooria kaotamine ja hävitamine*

Euroopa Liidu salastatud teabe salvestamiseks kasutatud elektrooniliste salvestusvahendite salastatuse kategooria võib ära kaotada või seda võib vähendada vastavalt julgeoleku akrediteerimisasutuse poolt heakskiidetud korrale.

Kui salvestusvahendeid on kasutatud salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ või erikategooriasse kuuluva teabe säilitamiseks, ei tohi sellise vahendi salastatuse kategooriat kaotada ega vahendit uuesti kasutada.

Kui elektroonilise salvestusvahendi salastatuse kategooriat ei saa kaotada või vahendit uuesti kasutada, tuleb vahend hävitada eeltoodud korra kohaselt.

25.5.5. *Teabeedastuse turve*

►M2 Komisjoni julgeolekudirektoraadi direktor ◄ on salastatuse küsimuste eest vastutav ametnik.

Kui Euroopa Liidu teavet edastatakse elektromagnetiliselt, tuleb sellise edastuse salastatuse, terviklikkuse ja kättesaadavuse kaitsmiseks rakendada erimeetmeid. Julgeoleku akrediteerimisasutus määrab kindlaks nõuded, mille kohaselt kaitstakse edastust avastamise ja pealtkuulamise eest. Sidesüsteemi abil edastatavat teavet kaitstakse salastatuse, terviklikkuse ja kättesaadavuse nõuete kohaselt.

Kui salastatus, terviklikkus ja kättesaadavus eeldavad krüptograafiameetodite kasutamist, peab julgeoleku akrediteerimisasutus salastatuse küsimuste eest vastutava ametnikuna sellised meetodid ja seotud tooted selleks otstarbeks eraldi heaks kiitma.

▼B

Edastamise jooksul kaitstakse ►M1 SECRET UE ◄ ja kõrgema salastatuse kategooria teabe salastatust turvaküsimuste eest vastutava komisjoni liikme poolt heakskiidetud krüptograafiliste meetodite või toodetega, kes on eelnevalt konsulteerinud komisjoni julgeolekupoliitika nõuandekomiteega. Edastamise jooksul kaitstakse ►M1 CONFIDENTIEL UE ◄ või ►M1 RESTREINT UE ◄ salastatuse kategooria teabe salastatust komisjoni salastatuse küsimuste eest vastutava ametniku poolt heakskiidetud krüptograafiliste meetodite või toodetega, kes on eelnevalt konsulteerinud komisjoni julgeolekupoliitika nõuandekomiteega.

Euroopa Liidu salastatud teabe edastamise suhtes kohaldatavad üksikasjalikud eeskirjad sätestatakse julgeoleku erijuhendites, mille ►M2 komisjoni julgeolekudirektoraat ◄ kiidab heaks, olles eelnevalt konsulteerinud komisjoni julgeolekupoliitika nõuandekomiteega.

Erandolukorras võib salastatuse kategooriatesse ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ ja ►M1 SECRET UE ◄ kuuluvat teavet edastada tavalise tekstina, kuid iga selline juhtum eeldab selgesõnalise loa andmist ja nõuetekohast registreerimist teabeomaniku poolt. Sellised erandolukorrad on järgmised:

a) ähvardav või reaalne kriisi-, konflikti- või sõjaolukord; ja

b) kui kohaletoimetamise kiirus on esmatähtis ja krüpteerimisvahendid ei ole kättesaadavad ning leitakse, et edastatavat teavet ei saa kasutada nii ruttu, et see kahjustaks toiminguid.

Süsteem peab olema suuteline keelama vajadusel juurdepääsu Euroopa Liidu salastatud teabele kõigis tööjaamades ja terminalides kas ühenduse füüsilise katkestamise teel või spetsiaalsete tarkvaravõimaluste abil, mille julgeoleku akrediteerimisasutus on heaks kiitnud.

25.5.6. *Turvalisus installeerimisel ja radiatsiooniturvalisus*

Süsteemi esialgse installeerimise ja edaspidise olulise muutmise sätetes peab olema ette nähtud, et süsteemi installeerivad julgeolekukontrolli läbinud isikud tehniliselt pädevate töötajate pideva järelevalve all, kes on läbinud julgeolekukontrolli juurdepääsuks sellisele Euroopa Liidu salastatud teabele, mille salastatuse kategooria on samaväärne kõrgeima salastatuse kategooriaga, millesse kuuluvat teavet kavatsetakse süsteemis säilitada ja käidelda.

Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse kategooriasse kuuluva teabe käitlemiseks kasutatavaid süsteeme tuleb kaitsta nii, et nende julgeolekut ei seaks ohtu paljastav kiirgus ja/või elektrijuhtivus, mille uurimise ja kontrollimise kohta kasutatakse tähistust „Tempest”.

Tempest-vastumeetmed vaatab läbi ja kiidab heaks *Tempest*-ametiisik (vt 25.3.2).

25.6. **Julgeolek käitlemise ajal**

25.6.1. *Julgeolekuga seotud töökord (SecOPs)*

Julgeolekuga seotud töökord määrab kindlaks julgeolekuküsimustes vastuvõetavad põhimõtted, järgitava töökorra ja töötajate vastutuse. Julgeolekuga seotud töökorra ettevalmistamise eest vastutab tehnilise süsteemi vastutav käitaja (TSO).

25.6.2. *Tarkvara kaitsmine/konfigureerimise juhtimine*

Rakendusprogrammide julgeoleku kaitset ei määrata kindlaks mitte programmi abil töödeldava teabe, vaid programmi enda salastatuse kategooria hindamise põhjal. Kasutatavaid tarkvaraversioone kontrollitakse regulaarselt, et tagada nende terviklikkus ja korrektne funktsioneerimine.

▼B

Tarkvara uusi või muudetud versioone ei tohi hakata Euroopa Liidu salastatud teabe käitlemiseks kasutama enne, kui tehnilise süsteemi vastutav käitaja on need üle kontrollinud.

25.6.3. *Kahjuliku tarkvara/arvutiviiruste kontrollimine*

Kahjulikku tarkvara/arvutiviiruseid kontrollitakse regulaarselt julgeoleku akrediteerimisasutuse nõuete kohaselt.

Kõik komisjoni saabuvad elektroonilised salvestusvahendid kontrollitakse üle kahjuliku tarkvara või arvutiviiruste suhtes enne nende mis tahes süsteemiga ühendamist.

25.6.4. *Hooldus*

Selliste süsteemide korralise ja erakorralise hoolduse lepingutes ja korras, mille kohta on koostatud süsteemispetsiifiliste julgeolekunõuete loetelu, täpsustatakse infotehnoloogiaalale sisenevatele hooldetöötajatele ja nende seadmetele kehtestatud nõuded ja kord.

Nõuded sätestatakse selgelt süsteemispetsiifiliste julgeolekunõuete loetelus ja kord julgeolekuga seotud töökorras. Kaugjuurdepääsu diagnostikameetodeid eeldav lepinguline hooldus on lubatud ainult erandolukorras range julgeolekukontrolli all ja julgeoleku akrediteerimisasutuse nõusolekul.

25.7. **Hanked**

25.7.1. *Üldine*

Kõik süsteemis kasutatavad turbetooted, mida kavatsetakse hankida, peavad olema kas hinnatud ja sertifitseeritud või nende hindamine ja sertifitseerimine mõnes Euroopa Liidu liikmesriigi hindamis- ja sertifitseerimisasutuses rahvusvaheliselt tunnustatud kriteeriumide kohaselt (näiteks infotehnoloogia turvalisuse hindamise ühised kriteeriumid, vt ISO 15408) peab olema pooleli. Hangete ja lepingute nõuandekomitee heakskiidu saamiseks on vajalikud eritoimingud.

Otsustades, kas seadmeid, eriti elektroonilisi salvestusvahendeid, võiks ostmise asemel pigem üürida, tuleb meeles pidada, et pärast seda, kui selliseid seadmeid on kasutatud Euroopa Liidu salastatud teabe käitlemiseks, ei tohi neid lubada nõuetekohase julgeolekuga alast välja, ilma et nende salastatuse kategooria kaotataks julgeoleku akrediteerimisasutuse nõusolekul, ning et sellise nõusoleku saamine ei pruugi alati võimalik olla.

25.7.2. *Akrediteerimine*

Julgeoleku akrediteerimisasutus akrediteerib süsteemispetsiifiliste julgeolekunõuete loetelus, julgeolekuga seotud töökorras ja muudes asjaomastes dokumentides esitatud teabe põhjal kõik süsteemid, mille jaoks tuleb enne Euroopa Liidu salastatud teabe käitlemist koostada süsteemispetsiifiliste julgeolekunõuete loetelu. Alamsüsteemid ja terminalid/tööjaamad akrediteeritakse selle süsteemi osana, millega nad on ühendatud. Kui süsteemi kasutavad peale komisjoni ka muud organisatsioonid, siis lepivad komisjon ja asjaomased julgeolekuasutused akrediteerimises vastastikku kokku.

Akrediteerimise protsess võib toimuda akrediteerimisstrateegia kohaselt, mis iseloomustab konkreetset süsteemi ja mille on määratlenud julgeoleku akrediteerimisasutus.

25.7.3. *Hindamine ja sertifitseerimine*

Teatavatel juhtudel hinnatakse enne akrediteerimist süsteemi riistvara, püsivara ja tarkvara turvaelemente ning need sertifitseeritakse, kui nad on suutelised tagama teabe julgeoleku kavandatud salastatuse tasemel.

Hindamis- ja sertifitseerimisnõuded peavad sisalduma süsteemi planeerimises ning need peavad olema täpselt sätestatud süsteemispetsiifiliste julgeolekunõuete loetelus.

▼B

Hindamine ja sertifitseerimine toimub heakskiidetud suuniste kohaselt ning seda teostavad tehnilise kvalifikatsiooniga ja vajalikul tasemel julgeolekukontrolli läbinud töötajad, kes tegutsevad tehnilise süsteemi vastutava käitaja nimel.

Töörühmad võib moodustada nimetatud liikmesriigi hindamis- ja sertifitseerimisasutusest või selle nimetatud esindajatest, näiteks pädevast tööettevõtjast, kes on läbinud julgeolekukontrolli.

Asjaomase hindamise ja sertifitseerimise ulatust võib vähendada (näiteks nii, et hõlmatakse ainult integreerimisega seotud aspektid), kui süsteemid põhinevad olemasolevatel siseriiklikult hinnatud ja sertifitseeritud arvutiturbetoodetel.

25.7.4. *Julgeolekuomaduste jooksev kontroll pideva akrediteerimise jaoks*

Tehnilise süsteemi vastutav käitaja kehtestab korralise kontrollimise korra, mis tagab, et kõik süsteemi turvaelemendid on endiselt kehtivad.

Süsteemispetsiifiliste julgeolekunõuete loetelus tuleb selgelt kindlaks teha ja sätestada sellised muudatused, mis eeldavad uut akrediteerimist või julgeoleku akrediteerimisasutuse eelnevat nõusolekut. Pärast igasugust muutmist, parandamist või riket, mis võis mõjutada süsteemi turvaelemente, tagab tehnilise süsteemi vastutav käitaja turvaelementide nõuetekohase toimimise kontrollimise. Süsteemi akrediteeringu pikendamine sõltub tavaliselt sellest, kas kontrolli tulemused on rahuldavad.

Julgeoleku akrediteerimisasutus kontrollib või vaatab regulaarselt üle kõik süsteemid, mille puhul on rakendatud turvaelemente. Süsteemid, mis käitlevad ►M1 TRES SECRET UE/EU TOP SECRET ◄ salastatuse kategooriasse kuuluvat teavet, vaadatakse üle vähemalt kord aastas.

25.8. **Ajutine või juhuslik kasutamine**

25.8.1. *Mikroarvutite/personaalarvutite turvalisus*

Püsikettaga (või muude alaliste salvestusseadmetega) mikroarvuteid/personaalarvuteid, mis töötavad kas autonoomselt või võrku ühendatuna, ja kaasaskantavaid, püsikõvakettaga arvutiseadmeid (näiteks kaasaskantavad personaalarvutid ja sülearvutid) peetakse samasugusteks teabesalvestusvahenditeks nagu diskette ja muid teisaldatavaid elektroonilisi salvestusvahendeid.

Sellistele seadmetele tagatakse seoses nende kasutamise, käitlemise, säilitamise ja transportimisega kaitse, mis vastab nende abil aegade jooksul salvestatud või töödeldud teabe kõrgeimale salastatuse tasemele (kuni salastatuse kategooria vähendamise või kaotamiseni asjaomase korra kohaselt).

25.8.2. *Isiklike IT-seadmete kasutamine komisjoni ametlikuks tööks*

Salvestusvõimeliste isiklike teisaldatavate elektrooniliste salvestusvahendite, tarkvara ja infotehnoloogilise riistvara (näiteks personaalarvutite ja kaasaskantavate arvutite) kasutamine Euroopa Liidu salastatud teabe käitlemiseks on keelatud.

Isiklikku riistvara, tarkvara ning isiklikke salvestusvahendeid ei tohi ilma ►M2 komisjoni julgeolekudirektoraadi direktor ◄ kirjaliku nõusolekuta tuua I või II klassi turvaalale, kus käideldakse Euroopa Liidu salastatud teavet. Sellist luba võib anda ainult tehnilistel põhjustel erandkorras.

▼B

25.8.3. *Lepingupartnerite isiklike või liikmesriikide tarnitud IT-seadmete kasutamine komisjoni ametlikuks tööks*

►M2 Komisjoni julgeolekudirektoraadi direktor ◄ võib lubada lepingupartnerite isiklike infotehnoloogiaseadmete ja isikliku tarkvara kasutamist organisatsioonides, mis toetavad komisjoni ametlikku tööd. Samuti võib lubada liikmesriikide tarnitud infotehnoloogiaseadmete ja tarkvara kasutamist; sellisel juhul kuuluvad infotehnoloogiaseadmed komisjoni kontrolli alla. Kui infotehnoloogiaseadmeid kasutatakse Euroopa Liidu salastatud teabe käitlemiseks, konsulteeritakse julgeoleku akrediteerimisasutusega, et kõnealuste seadmete kasutamisel kohaldatavaid teabeturbeelemente võetaks arvesse ja rakendataks nõuetekohaselt.

26. EUROOPA LIIDU SALASTATUD TEABE AVALDAMINE KOLMANDATELE RIIKIDELE JA RAHVUSVAHELISTELE ORGANISATSIOONIDELE

26.1.1. *Euroopa Liidu salastatud teabe avaldamist reguleerivad põhimõtted*

Komisjoni kolleegium otsustab Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele järgneva alusel:

— sellise teabe laad ja sisu,

— vastuvõtjate teadmisvajadus,

— Euroopa Liidule toodava kasu ulatus.

Euroopa Liidu salastatud teabe avaldamiseks küsitakse teabe koostaja nõusolekut.

Sellised otsused tehakse igal üksikjuhul eraldi, võttes arvesse:

— koostöö soovitavat ulatust asjaomaste kolmandate riikide või rahvusvaheliste organisatsioonidega,

— nende usaldatavust, mis tuleneb kõnealustele riikidele või organisatsioonidele usaldatava Euroopa Liidu salastatud teabe salastatuse tasemest ja kõnealustes riikides või organisatsioonides kohaldatavate julgeolekueeskirjade vastavusest Euroopa Liidus kohaldatavatele eeskirjadele. Komisjoni julgeolekupoliitika nõuandekomitee annab komisjonile oma tehnilise arvamuse selle küsimuse kohta.

Võttes vastu Euroopa Liidu salastatud teabe, kinnitavad kolmandad riigid või rahvusvahelised organisatsioonid, et teavet ei kasutata ühelgi muul eesmärgil kui see, milleks teave avaldati või teavet vahetati, ja et nad tagavad teabe kaitsmise komisjoni nõutaval tasemel.

26.1.2. *Tasemed*

Kui komisjon on otsustanud, et salastatud teavet võib konkreetsele riigile või organisatsioonile avaldada või seda nendega vahetada, määrab ta kindlaks võimaliku koostöö taseme. Kõnealune tase sõltub eelkõige asjaomase riigi või organisatsiooni rakendatavatest julgeolekupõhimõtetest ja -eeskirjadest.

On olemas kolm koostöö taset:

1. tase

Koostöö kolmandate riikide või rahvusvaheliste organisatsioonidega, kelle julgeolekupõhimõtted ja -eeskirjad on väga sarnased Euroopa Liidu omadega.

2. tase

Koostöö kolmandate riikide või rahvusvaheliste organisatsioonidega, kelle julgeolekupõhimõtted ja -eeskirjad erinevad Euroopa Liidu omadest märkimisväärselt.

▼B

3. tase

Episoodiline koostöö kolmandate riikide ja rahvusvaheliste organisatsioonidega, kelle põhimõtteid ja julgeolekueeskirju ei ole võimalik hinnata.

Iga koostöötase määrab kindlaks menetlused ja turvasätted, mis on üksikasjaliselt esitatud liidetes 3, 4 ja 5.

26.1.3. *Julgeolekulepped*

Kui komisjon on otsustanud, et vajadus vahetada salastatud teavet komisjoni ja kolmandate riikide või rahvusvaheliste organisatsioonide vahel on alaline või pikaajaline, koostab ta koos kõnealuste riikide või organisatsioonidega „salastatud teabe vahetamise julgeolekukorra kokkuleppe" ja määratleb selles koostöö eesmärgi ja vahetatava teabe kaitsmise vastastikused eeskirjad.

3. taseme episoodilise koostöö puhul, mis on oma kestuselt ja eesmärgilt piiratud, võib „salastatud teabe vahetamise julgeolekukorra kokkuleppe" asendada vastastikuse mõistmise memorandumiga, milles määratletakse vahetatava salastatud teabe laad ja vastastikused kohustused seoses kõnealuse teabega, kui kõnealune teave kuulub salastatuse kategooriasse ►M1 RESTREINT UE ◄ või madalamasse kategooriasse.

Enne kui julgeolekukorra koguleppe või vastastikuse mõistmise memorandumi eelnõu esitatakse seisukoha saamiseks komisjonile, arutatakse neid komisjoni julgeolekupoliitika nõuandekomitees.

Turvaküsimuste eest vastutav komisjoni liige taotleb kogu vajalikku abi liikmesriigi julgeolekuasutustelt, et tagada avaldatava teabe kasutamine ja kaitsmine vastavalt julgeolekukorra kokkulepete või vastastikuse mõistmise memorandumite sätetele.

▼M3

27. TÖÖSTUSJULGEOLEKU ÜHISED MIINIMUMSTANDARDID

27.1 **Sissejuhatus**

Käesolevas jaos käsitletakse tööstustegevuse julgeolekuaspekte, mis on iseloomulikud selliste läbirääkimiste pidamisele ja lepingute või toetuslepingute sõlmimisele, millega antakse tööstus- või muudele üksustele täitmiseks ülesandeid, mis on seotud ELi salastatud teabega ja/või sisaldavad selle kasutamist, sealhulgas ELi salastatud teabe edastamine või sellele juurdepääs riigihankemenetluse ja konkursikutsemenetluse käigus (pakkumisperiood ja lepingueelsed läbirääkimised).

27.2 **Mõisted**

Käesolevates ühistes miinimumstandardites kasutatakse järgmisi mõisted:

a) salastatud leping – mis tahes toodete tarnimise, tööde tegemise, hoonete kasutuseleandmise või teenuste osutamise leping või toetusleping, mille täitmise eelduseks on või millega kaasneb juurdepääs ELi salastatud teabele või sellise teabe loomine,

b) salastatud alltöövõtuleping – leping, mille lepingupartner või toetusesaaja on sõlminud teise partneriga (st alltöövõtjaga) kaupade tarnimise, tööde tegemise, hoonete kasutuseleandmise või teenuste osutamise eesmärgil, mille täitmise eelduseks on või millega kaasneb juurdepääs ELi salastatud teabele või sellise teabe loomine,

c) lepingupartner – ettevõtja või juriidiline isik, kellel on lepinguliste kohustuste võtmiseks või toetusesaajaks olemiseks vajalik õigus- ja teovõime,

▼M3

d) määratud julgeolekuasutus (DSA) – asutus, mis vastutab ELi liikmesriigi julgeolekuasutuse (NSA) ees tööstus- või muudele üksustele riigi kõigi tööstusjulgeolekuga seotud poliitikaküsimuste edastamise eest ning kõnealuse poliitika suunamise ja selle rakendamisel abi andmise eest. Riigisisene julgeolekuasutus võib täita määratud julgeolekuasutuse ülesandeid,

e) ettevõtte julgeolekukontroll (FSC) – riigisisese julgeolekuasutuse/määratud julgeolekuasutuse haldusotsus selle kohta, et julgeoleku seisukohast suudab ettevõte tagada teatava salastatuse tasemega ELi salastatud teabele piisava kaitse ning et ettevõtte töötajad, kes peavad pääsema juurde ELi salastatud teabele, on läbinud nõuetekohase julgeolekukontrolli ja neid on teavitatud julgeolekunõuetest, mis on vajalikud juurdepääsuks ELi salastatud teabele ja selle kaitsmiseks,

f) tööstus- või muu üksus – lepingupartner või tema alltöövõtja, kes on kaasatud kaupade tarnimisse, tööde tegemisse või teenuste osutamisse; siia võivad kuuluda tööstus-, kaubandus-, teenindus-, teadus-, uurimis-, haridus- või arendusüksused,

g) tööstusjulgeolek – kaitsemeetmete ja -menetluste kohaldamine, et vältida, avastada ja korvata lepingupartneri või alltöövõtja poolt lepingu(eelsetel) läbirääkimistel ja salastatud lepingute täitmisel käideldud ELi salastatud teabe kaotust ja kahjustamist,

h) riigisisene julgeolekuasutus – ELi liikmesriigi valitsusasutus, mis vastutab lõplikult ELi salastatud teabe kaitsmise eest kõnealuses liikmesriigis,

i) lepingu üldine salastatuse tase – kogu lepingu või toetuslepingu salastatuse kategooria määramine, mis põhineb sellise teabe ja/või materjali salastatuse kategoorial, mida luuakse, edastatakse või millele saadakse juurdepääs või mida võidakse luua või edastada või millele võidakse saada juurdepääs üldise lepingu või toetuslepingu mis tahes osa alusel. Lepingu üldine salastatuse tase ei või olla madalam kui selle mis tahes osa kõige kõrgem salastatuse tase, kuid tulenevalt tasemete kogumõjust võib olla sellest kõrgem,

j) julgeolekuaspekte käsitlev dokument (SAL) – lepingu sõlminud ametiasutuse poolt esitatud konkreetsete lepinguliste tingimuste kogum, mis moodustab sellise salastatud lepingu lahutamatu osa, millega kaasneb juurdepääs ELi salastatud teabele või millega kaasneb sellise teabe loomine, ning millega määratakse kindlaks lepingu julgeolekunõuded või need lepingu osad, mida tuleb julgeoleku kaalutlustel kaitsta,

k) salastatuse kategooriate määramise juhend (SCG) – dokument, milles kirjeldatakse programmi, lepingu või toetuslepingu salastatud osasid, määrates kindlaks neile kohaldatavad salastatuse kategooriad. Salastatuse kategooriate määramise juhendit võib kogu programmi, lepingu või toetuslepingu kehtivuse aja jooksul täiendada ja nende teabeelementide salastatuse kategooriat võib ümber klassifitseerida või alandada. Salastatuse kategooria määramise juhend peab olema julgeolekuaspekte käsitleva dokumendi osa.

27.3 **Korraldus**

a) Komisjon võib anda liikmesriikides registreeritud tööstus- või muudele üksustele salastatud lepinguga selliseid ülesandeid, mis on seotud ELi salastatud teabega ja/või sisaldavad selle kasutamist.

b) Komisjon tagab, et salastatud lepingute sõlmimisel järgitakse kõiki kõnealustest miinimumstandarditest tulenevaid nõudeid.

c) Komisjon kaasab kõnealuste tööstusjulgeoleku miinimumstandardite kohaldamiseks asjakohase riigisisese julgeolekuasutuse või riigisisesed julgeolekuasutused. Riigisisesed julgeolekuasutused võivad kõnealused ülesanded anda täitmiseks ühele või mitmele määratud julgeolekuasutusele.

▼M3

d) Nimetatud julgeolekuasutuste juhtkond vastutab lõplikult tööstus- või muudes üksustes ELi salastatud teabe kaitsmise eest.

e) Kui sõlmitakse kõnealuste miinimumstandardite kohaldamisalasse kuuluv salastatud leping või alltöövõtuleping, teatab komisjon ja/või vajaduse korral riigisisene julgeolekuasutus/määratud julgeolekuasutus sellest viivitamata selle liikmesriigi riigisisesele julgeolekuasutusele/määratud julgeolekuasutusele, kus lepingupartner või alltöövõtja on registreeritud.

27.4 **Salastatud lepingud ja toetuse andmise otsused**

a) Salastatud lepingute või toetuslepingute salastatuse kategooria määramisel tuleb arvesse võtta järgmisi põhimõtteid:

— komisjon määrab vajaduse korral kindlaks kaitset vajava salastatud lepingu aspektid ja vastava salastatuse kategooria, sealjuures peab ta arvesse võtma enne salastatud lepingu sõlmimist loodud teabele selle koostaja poolt esialgselt määratud salastatuse kategooriat,

— lepingu üldine salastatuse kategooria ei või olla madalam kui selle mis tahes osa kõrgeim salastatuse kategooria,

— lepingujärgselt loodud ELi salastatud teabe kategooria määratakse vastavalt salastatuse kategooriate määramise juhendile,

— vajaduse korral vastutab komisjon lepingu üldise salastatuse kategooria või lepingu mis tahes osa salastatuse kategooria muutmise eest, konsulteerides selle koostajaga, ning kõikide huvitatud osapoolte teavitamise eest,

— salastatud teavet, mis on avaldatud lepingupartnerile või alltöövõtjale või on lepingujärgselt loodud, ei tohi kasutada muudel kui salastatud lepingus määratletud eesmärkidel ning seda ei tohi ilma selle koostaja kirjaliku nõusolekuta edastada kolmandatele isikutele.

b) Asjaomaste liikmesriikide riigisisesed julgeolekuasutused/määratud julgeolekuasutused vastutavad selle eest, et lepingupartnerid ja alltöövõtjad, kellega on sõlmitud salastatud lepingud, mis sisaldavad kategooriasse CONFIDENTIEL UE või sellest kõrgemasse salastatuse kategooriasse kuuluvat teavet, võtavad kõik vajalikud meetmed salastatud lepingu täitmisel neile avaldatud või nende poolt lepingujärgselt loodud ELi salastatud teabe kaitsmiseks kooskõlas riigisiseste õigusnormidega. Julgeolekunõuete täitmata jätmine võib tuua kaasa lepingu lõpetamise.

c) Kõik tööstus- või muud üksused, kes osalevad selliste salastatud lepingute täitmises, millega kaasneb juurdepääs kategooria CONFIDENTIEL UE või sellest kõrgema salastatuse kategooria teabele, peavad olema läbinud ettevõtte julgeolekukontrolli. Liikmesriigi riigisisese julgeolekuasutuse/määratud julgeolekuasutuse väljastatud tõend kinnitab, et ettevõte suudab julgeoleku seisukohast pakkuda ja tagada ELi salastatud teabele kaitse, mis on vastavuses selle salastatuse tasemega.

d) Pärast salastatud lepingu sõlmimist vastutab lepingupartneri või alltöövõtja juhtkonna määratud julgeolekuülem selle eest, et kõik need konkreetses liikmesriigis registreeritud tööstus- või muude üksuste töötajad, kes oma ülesannete tõttu vajavad juurdepääsu kategooria CONFIDENTIEL UE või kõrgema salastatuse kategooria ELi salastatud teabele, läbiksid julgeolekukontrolli. Seda kontrolli viib läbi riigisisene julgeolekuasutus/määratud julgeolekuasutus vastavalt oma riigisisestele eeskirjadele.

▼**M3**

e) Salastatud lepingutes peab sisalduma 27. jao 2. punkti alapunktis j määratletud julgeolekuaspekte käsitlev dokument. Julgeolekuaspekte käsitlev dokument peab sisaldama salastatuse kategooriate määramise juhendit.

f) Enne läbirääkimismenetluse alustamist salastatud lepingu sõlmimiseks võtab komisjon ühendust selle liikmesriigi riigisisese julgeolekuasutusega/määratud julgeolekuasutusega, kus asjaomased tööstus- või muud üksused on registreeritud, et saada kinnitust selle kohta, et neil on kehtiv ja lepingu salastatuse kategooriale vastav ettevõtte julgeolekukontrolli tõendav dokument.

g) Lepingut sõlmiv ametiasutus ei tohi anda väljavalitud ettevõttele salastatud lepingut täitmiseks enne julgeolekukontrolli läbimist kinnitava tõendi saamist.

h) Julgeolekukontrolli ei nõuta lepingute puhul, mis sisaldavad kategooriasse RESTREINT UE kuuluvat teavet, kui liikmesriikide riigisisestes õigusnormides ei ole sätestatud teisiti.

i) Salastatud lepingute korral peavad pakkumiskutsed sisaldama sätet selle kohta, et ettevõte, kes pakkumist ei esita või keda ei valita lepingupartneriks, peab tagastama kõik dokumendid kindlaksmääratud tähtaja jooksul.

j) Lepingupartneril võib olla vajalik pidada läbirääkimisi salastatud alltöövõtulepingute sõlmimiseks alltöövõtjatega eri tasanditel. Lepingupartner vastutab selle eest, et kõigi alltöövõtuga seotud ülesannete täitmine toimub kooskõlas käesolevas jaos sisalduvate ühiste miinimumstandarditega. Lepingupartner ei või siiski edastada ELi salastatud teavet või materjali alltöövõtjale ilma selle koostaja eelneva kirjaliku nõusolekuta.

k) Tingimused, mille alusel lepingupartner võib alltöövõtulepinguid sõlmida, peavad olema määratletud nii pakkumises või konkursikutses kui ka salastatud lepingus. Euroopa Liitu mittekuuluvates riikides registreeritud üksustega ei tohi sõlmida alltöövõtulepinguid ilma komisjoni selgesõnalise kirjaliku loata.

l) Kogu salastatud lepingu kehtivusaja jooksul jälgib komisjon koostöös asjaomase riigisisese julgeolekuasutuse/määratud julgeolekuasutusega lepingu julgeolekusätete täitmist. Salastatud teabega seotud juhtumitest teatatakse vastavalt käesolevate julgeolekueeskirjade II osa 24. jaole. Ettevõtte julgeolekukontrolli otsuse muutmisest või selle tühistamisest teatatakse viivitamata komisjonile ja muule riigisisesele julgeolekuasutusele/määratud julgeolekuasutusele, keda oli julgeolekukontrollist teavitatud.

m) Kui salastatud leping või salastatud alltöövõtuleping lõpetatakse, teatavad komisjon ja/või vajaduse korral riigisisene julgeolekuasutus/määratud julgeolekuasutus sellest viivitamata selle liikmesriigi riigisisesele julgeolekuasutusele/määratud julgeolekuasutusele, kus lepingupartner või alltöövõtja on registreeritud.

n) Pärast salastatud lepingu või alltöövõtulepingu lõpetamist või sõlmimist järgivad lepingupartnerid ja alltöövõtjad jätkuvalt käesolevas jaos sisalduvaid ühiseid miinimumstandardeid ning säilitavad salastatud teabe konfidentsiaalsuse.

o) Erisätted salastatud teabe hävitamise kohta lepingu lõppemisel nähakse ette julgeolekuaspekte käsitlevas dokumendis või muudes asjakohastes julgeolekunõudeid kehtestavates sätetes.

p) Käesolevas jaos nimetatud kohustusi ja tingimusi kohaldatakse *mutatis mutandis* menetluste suhtes, mille raames antakse toetusi otsuse alusel, eriti selliste toetuste saajate suhtes. Kohustused ja tingimused sätestatakse toetuse andmise otsustes.

▼M3

27.5 **Külastused**

Salastatud lepingute raames toimuvad komisjoni töötajate külastused ELi salastatud lepinguid täitvatesse liikmesriikide tööstus- või muudesse üksustesse peavad olema korraldatud asjaomase riigisisese julgeolekuasutuse/määratud julgeolekuasutuse kaudu. ELi salastatud lepingute raames toimuvad tööstus- või muude üksuste töötajate külastused peavad olema korraldatud asjaomaste julgeolekuasutuste/määratud julgeolekuasutuste kaudu. ELi salastatud lepinguga seotud riigisisesed julgeolekuasutused/määratud julgeolekuasutused võivad siiski leppida kokku korras, mille kohaselt tööstus- või muude üksuste töötajate külastusi võib korraldada otse.

27.6 **ELi salastatud dokumentide edastamine ja vedu**

a) ELi salastatud teabe edastamisel kohaldatakse käesolevate julgeolekueeskirjade II osa 21. jagu. Täiendavalt nimetatud sätetele kohaldatakse kõiki kehtivaid liikmesriikidevahelisi menetlusi.

b) Salastatud lepingutega seotud ELi salastatud materjali rahvusvaheline vedu toimub vastavalt liikmesriikide riigisisesele korrale. Rahvusvaheliseks veoks kohaldatavate julgeolekukorralduste käsitlemisel kohaldatakse järgmisi põhimõtteid:

   — julgeolek kindlustatakse veo kõigil etappidel ja igas olukorras saatekohast kuni lõppsihtkohani,

   — saadetisele kohaldatava kaitse tase määratakse selles sisalduva materjali kõrgeima salastatuse kategooria järgi,

   — vajaduse korral viiakse veoteenuseid pakkuvates äriühingutes läbi ettevõtte julgeolekukontroll. Sellistel juhtudel tehakse saadetist käitlevale personalile julgeolekukontroll vastavalt käesolevas jaos sisalduvatele ühistele miinimumstandarditele,

   — vedu toimub võimalikult täpselt punktist punkti ja see lõpetatakse nii kiiresti kui võimalik,

   — võimaluse korral peaks teekond kulgema üksnes läbi ELi liikmesriikide. Teekond läbi Euroopa Liitu mittekuuluvate riikide tuleks ette võtta üksnes siis, kui selleks on andnud loa nii lähteriigi kui ka vastuvõtjariigi riigisisene julgeolekuasutus/määratud julgeolekuasutus,

   — enne ELi salastatud materjali edastamist koostab saatja veoplaani, mille kinnitab asjaomane riigisisene julgeolekuasutus/määratud julgeolekuasutus.

▼M1

1. liide

SISERIIKLIKE SALASTATUSE TASEMETE VÕRDLUS

Euroopa Liidu salastatuse tase	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Lääne-Euroopa Liidu salastatuse tase	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Euratomi salastatuse tase	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
NATO salastatuse tase	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgia	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Küpros	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Tšehhi Vabariik	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Taani	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Eesti	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Saksamaa	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Kreeka	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Soome	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Prantsusmaa	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	

▼M4

Horvaatia	Vrlo tajno	Tajno	Povjerljivo	Ograničeno

▼M1

Iirimaa	Top Secret	Secret	Confidential	Restricted
Itaalia	Segretissimo	Segreto	Riservatissimo	Riservato
Läti	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Leedu	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luksemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼M1

Ungari	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Madalmaad	Stg. ([3]) Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Poola	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Sloveenia	Strogo tajno	Tajno	Zaupno	SVN Interno
Slovakkia	Prísne tajné	Tajné	Dôverné	Vyhradené
Hispaania	Secreto	Reservado	Confidencial	Difusión Limitada
Rootsi	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Ühendkuningriik	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) Salastatuse taset „Très Secret Défense”, mis hõlmab valitsuse prioriteetseid küsimusi, võib muuta ainult peaministri loal.
([3]) Stg = staatsgeheim.

2. liide

SALASTATUSE KATEGOORIATE MÄÄRAMISE PRAKTILINE JUHEND

Käesolev juhend on soovituslik ja selle tõlgendamisega ei tohi muuta 16., 17., 20. ja 21. jaos ettenähtud olulisi sätteid.

Salastatuse kategooria	Millal	Kes	Tähistamine	Kategooria alandamine/kaotamine/hävitamine	
				Kes	Millal
►M1 TRES SECRET UE/EU TOP SECRET ◄: Sellist kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib väga tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve [16.1].	Kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate varade kahjustamine võib: — seada otsesesse ohtu Euroopa Liidu või ühe selle liikmesriigi või sõbralike riikide sisemise stabiilsuse — tekitada erakordselt tõsist kahju suhetele sõbralike valitsustega — põhjustada otseselt hulgaliselt surmajuhtumeid — tekitada erakordselt tõsist kahju liikmesriikide töö tulemuslikkusele või julgeolekule või muude osalistele jõududele või eriti väärtuslike julgeoleku- või luureoperatsioonide jätkuvale tõhususele — tekitada tõsist pikaajalist kahju Euroopa Liidu või selle liikmesriikide majandusele.	Nõuetekohaselt volitatud isikud (dokumentide koostajad), peadirektorid, talituste juhid [17.1]. Dokumentide koostajad määravad kuupäeva, ajavahemiku või sündmuse, millal võib salastatuse kategooriat alandada või selle kaotada [16.2]. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [17.3].	Salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ kantakse salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvatele dokumentidele ja vajadusel kantakse neile mehaaniliselt ja käsitsi julgeoleku tähis ja/või kaitsetähistus ESDP [16.4, 16.5, 16.3]. Euroopa Liidu salastatuse kategooria nimetus ja julgeoleku tähis märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev; viitenumber tuleb märkida igale lehele. Kui dokumente levitatakse mitme koopiana, peab iga koopia esilehel olema kirjas koopia number ja dokumendi lehekülgede arv. Esimesel leheküljel tuleb loetleda kõik lisad ja manustatud materjalid [21.1].	Salastatuse taset võib vähendada või selle kaotada ainult koostaja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia on saadetud [17.3]. Salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvaid dokumente hävitab nende dokumentide eest vastutav keskregister või alamregister. Iga hävitatud dokumendi kohta koostatakse hävitamisakt, millele kirjutavad alla salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ kontrolliametnik ja hävitamist tunnistama kutsutud ametnik, kes peab olema läbinud julgeolekukontrolli salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ jaoks. Logiraamatusse tehakse vastav märkus. Register säilitab hävitamisakte koos ringkäigulehega kümme aastat [22.5].	Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [22.5]. Salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvad dokumendid, kaasa arvatud salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse salastatuse kategooria ►M1 TRES SECRET UE/EU TOP SECRET ◄ registri kontrolliametniku järelevalve all kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul viisil loetamatuks nii, et neid ei ole võimalik enam kokku panna [22.5].

▼B

Salastatuse kategooria	Millal	Kes	Tähistamine	Kategooria alandamine/kaotamine/hävitamine	
				Kes	Millal
►M1 SECRET UE ◄: seda kategooriat kasutatakse ainult sellise teabe ja materjali puhul, mille loata avaldamine võib tõsiselt kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve [16.1].	Kategooriasse ►M1 SECRET UE ◄ kuuluvate varade kahjustamine võib: — suurendada rahvusvahelisi pingeid — halvendada tõsiselt suhteid sõbralike valitsustega — seada otseselt ohtu elu või kahjustada tõsiselt avalikku korda või üksikisikute julgeolekut või vabadust — tekitada tõsist kahju liikmesriikide töö tulemuslikkusele või julgeolekule või muude osalistele jõududele või väga väärtuslike julgeoleku- või luureoperatsioonide jätkuvale tõhususele — tekitada märkimisväärset materiaalset kahju Euroopa Liidu või ühe tema liikmesriigi finants-, monetaar-, majandus- ja kaubandushuvidele.	Volitatud isikud (dokumentide koostajad), peadirektorid, talituste juhid [17.1]. Dokumentide koostajad määravad kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada [16.2]. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [17.3].	Salastatuse kategooria ►M1 SECRET UE ◄ kantakse salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvatele dokumentidele ja vajadusel kantakse neile mehaaniliselt ja käsitsi julgeoleku tähis ja/või kaitsetähistus ESDP [16.4, 16.5, 16.3]. Euroopa Liidu salastatuse kategooria nimetus ja julgeoleku tähis märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev; viitenumber tuleb märkida igale lehele. Kui dokumente levitatakse mitme koopiana, peab iga koopia esilehel olema kirjas koopia number ja dokumendi lehekülgede arv. Esimesel leheküljel tuleb loetleda kõik lisad ja manustatud materjalid [21.1].	Salastatuse taset võib vähendada ja selle kaotada ainult koostaja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia on saadetud [17.3]. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvaid dokumente hävitab nende dokumentide eest vastutav register sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvate hävitatud dokumentide loetelu kantakse allakirjutatud hävitamisaktile, mida register säilitab koos hävitamislehtedega vähemalt kolm aastat [22.5].	Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [22.5]. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvad dokumendid, kaasa arvatud kõik salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul moel loetamatuks selliselt, et neid ei ole võimalik enam kokku panna [22.5].
►M1 CONFIDENTIEL UE ◄:	Kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvate varade kahjustamine võib: — kahjustada oluliselt diplomaatilisi suhteid, s.t anda alust ametlikuks protestiks või muudeks sanktsioonideks;	Volitatud isikud (dokumentide koostajad), peadirektorid ja talituste juhid [17.1].	Salastatuse kategooria ►M1 CONFIDENTIEL UE ◄ kantakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvatele dokumentidele ja vajadusel kantakse neile julgeoleku tähis ja/või kaitsetähistus ESDP mehaaniliselt ja käsitsi või trükituna eelnevalt templiga varustatud ja registreeritud paberile [16.4, 16.5, 16.3].	Salastatuse taset võib vähendada ja selle kaotada ainult koostaja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia on saadetud [17.3].	Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [22.5].

Salastatuse kategooria	Millal	Kes	Tähistamine	Kategooria alandamine/kaotamine/hävitamine	
				Kes	Millal
Seda kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib kahjustada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi olulisi huve [16.1].	— piirata üksikisikute julgeolekut või vabadust; — tekitada kahju liikmesriikide töö tulemuslikkusele või julgeolekule või muude osalistele jõududele või väärtuslike julgeoleku- või luureoperatsioonide tõhususele; — õõnestada märkimisväärselt suurorganisatsioonide rahalist elujõudu; — takistada raskete kuritegude uurimist või soodustada nende toimepanekut; — olla märkimisväärses vastuolus Euroopa Liidu või selle liikmesriikide finants-, monetaar-, majandus- ja kaubandushuvidega; — takistada tõsiselt Euroopa Liidu oluliste põhimõtete väljatöötamist või toimimist; — peatada või muul viisil märkimisväärselt häirida olulisi Euroopa Liidu toiminguid.	Dokumentide koostajad määravad kuupäeva või ajavahemiku, mille jooksul võib salastatuse kategooriat alandada või selle kaotada. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [17.3].	Euroopa Liidu salastatuse kategooria nimetus märgitakse iga lehekülje ülemisse ja alumise serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev. Esimesel leheküljel tuleb loetleda kõik lisad ja manustatud materjalid [21.1].	Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvaid dokumente hävitab nende dokumentide eest vastutav register sellise isiku järelevalve all, kes on läbinud julgeolekukontrolli. Nende hävitamine dokumenteeritakse siseriiklike õigusnormide kohaselt ning komisjoni või Euroopa Liidu detsentraliseeritud asutuste puhul ►M2 julgeolekuküsimuste eest vastutava komisjoni liikme ◄ juhtnööride kohaselt [22.5].	Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvad dokumendid, kaasa arvatud kõik salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvate dokumentide koostamise käigus tekkinud salastatud jäätmed (näiteks vigased koopiad, mustandid, trükitud märkmed ja koopiapaber) hävitatakse kas põletamise, paberimassiks muutmise või narmastamise teel või muutes need muul moel loetamatuks selliselt, et neid ei ole võimalik enam kokku panna [22.5].

Salastatuse kategooria	Millal	Kes	Tähistamine	Kategooria alandamine/kaotamine/hävitamine	
				Kes	Millal
►M1 RESTREINT UE ◄: Sellist kategooriat kasutatakse sellise teabe ja materjali puhul, mille loata avaldamine võib negatiivselt mõjutada Euroopa Liidu või ühe või mitme Euroopa Liidu liikmesriigi huve [16.1].	Kategooriasse ►M1 RESTREINT UE ◄ kuuluvate varade kahjustamine võib: — kahjustada diplomaatilisi suhteid — tekitada üksikisikutele märkimisväärseid ebameeldivusi — raskendada liikmesriikide või muude osaliste jõudude töö tulemuslikkuse või julgeoleku säilitamist — üksikisikutele või ettevõtetele finantskahju või soodustada sobimatu kasu või edu saamist — rikkuda nõuetekohaseid kohustusi säilitada kolmandate isikute avaldatud teabe salajasus — rikkuda õiguspäraseid piiranguid teabe avaldamise kohta — piirata kuritegude uurimist või soodustada nende toimepanekut — seada Euroopa Liidu või selle liikmesriigid ebasoodsasse olukorda kolmandate isikutega toimuvatel kaubanduslikel või poliitilistel läbirääkimistel — takistada Euroopa Liidu oluliste põhimõtete tulemuslikku väljatöötamist või toimimist — õõnestada Euroopa Liidu ja selle toimingute nõuetekohast juhtimist.	Volitatud isikud (dokumentide koostajad), peadirektorid, talituste juhid [17.1]. Dokumentide koostajad määravad ajavahemiku või sündmuse, millal võib salastatuse kategooriat alandada või selle kaotada [16.2]. Kui see ei ole võimalik, vaatavad nad dokumendid hiljemalt iga viie aasta järel läbi, et teha kindlaks, kas esialgne salastatuse kategooria on endiselt vajalik [17.3].	Salastatuse kategooria ►M1 RESTREINT UE ◄ kantakse salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvatele dokumentidele ja vajadusel kantakse neile mehaaniliselt ja käsitsi julgeoleku tähis ja/või kaitsetähistus ESDP [16.4, 16.5, 16.3]. Euroopa Liidu salastatuse kategooria nimetus ja julgeoleku tähis märgitakse esimese leheküljе ülemisse serva ning kõik lehed nummerdatakse. Igal dokumendil peab olema kirjas viitenumber ja kuupäev [21.1].	Salastatuse taset võib vähendada ainult koostaja, kes teatab muudatusest kõigile adressaatidele, kellele dokument või selle koopia on saadetud [17.3]. Salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvad dokumendid hävitab nende dokumentide eest vastutav register või kasutaja vastavalt ►M2 julgeolekuküsimuste eest vastutava komisjoni liikme ◄ juhistele [22.5].	Ülejäänud koopiad ja dokumendid, mida enam ei vajata, tuleb hävitada [22.5].

▼B

3. liide

Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele: 1. taseme koostöö

MENETLUSED

1. Komisjoni kolleegium on volitatud avaldama Euroopa Liidu salastatud teavet riikidele, kes ei ole Euroopa Liidu liikmed, ja muudele rahvusvahelistele organisatsioonidele, mille julgeolekupõhimõtted ja -eeskirjad on võrreldavad Euroopa Liidu omadega.

2. Kuni julgeolekukokkuleppe sõlmimiseni on turvaküsimuste eest vastutaval komisjoni liikmel pädevus vaadata läbi Euroopa Liidu salastatud teabe avaldamise taotlusi.

3. Seda tehes ta:

   — taotleb avaldatava Euroopa Liidu salastatud teabe koostajate arvamust,

   — loob vajalikud sidemed julgeolekuorganitega taotluse esitanud riikides või rahvusvahelistes organisatsioonides, et kontrollida, kas nende julgeolekupõhimõtted ja -sätted on sellised, mis tagaksid avaldatava salastatud teabe kaitsmise käesolevate julgeolekusätete kohaselt,

   — küsib komisjoni julgeolekupoliitika nõuandekomitee seisukohta selle kohta, kui usaldusväärsed on teavet kasutada soovivad riigid või rahvusvahelised organisatsioonid.

4. Turvaküsimuste eest vastutav komisjoni liige saadab taotluse koos komisjoni julgeolekupoliitika nõuandekomitee arvamusega komisjonile otsuse tegemiseks.

JULGEOLEKUSÄTTED, MIDA PEAVAD KOHALDAMA TEABESAAJAD

5. Turvaküsimuste eest vastutav komisjoni liige teatab teabesaajatele riikidele või rahvusvahelistele organisatsioonidele komisjoni otsusest volitada Euroopa Liidu salastatud teabe avaldamine.

6. Avaldamise otsus jõustub ainult juhul, kui teabesaajad on kinnitanud kirjalikult, et nad:

   — kasutavad teavet ainult kokkulepitud eesmärgil,

   — kaitsevad teavet käesolevate julgeolekusätete ja eelkõige allpool esitatud erireeglite kohaselt.

7. Personal

   a) Euroopa Liidu salastatud teabele juurdepääsu omavate ametnike hulk peab teadmisvajaduse põhimõttest lähtuvalt olema rangelt piiratud nende isikutega, kelle tööülesanded eeldavad sellist juurdepääsu.

   b) Kõigil ametnikel ja kodanikel, kellel on luba juurdepääsuks salastatuse kategooriasse ►**M1** CONFIDENTIEL UE ◄ või rangemasse salastatuse kategooriasse kuuluvale teabele, peab olema kas vastava taseme julgeolekusertifikaat või nad peavad olema läbinud vastava taseme julgeolekukontrolli, kusjuures mõlemaga tegeleb asjaomase isiku oma riigi valitsus.

8. Dokumentide edastamine

   a) Praktiline dokumentide edastamise kord otsustatakse kokkuleppe teel. Sellise kokkuleppe sõlmimiseni kohaldatakse 21. jao sätteid. Eelkõige määratakse selles kokkuleppes kindlaks registrid, millesse Euroopa Liidu salastatud teave tuleb edastada.

▼B

b) Kui teabe hulka, mille avaldamiseks komisjon on loa andnud, kuulub ka salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvat teavet, loob teabesaaja riik või rahvusvaheline organisatsioon keskregistri Euroopa Liidu küsimuste jaoks ja vajadusel ka alamregistrid. Nendes registrites kohaldatakse meetmeid, mis on ranges vastavuses käesoleva eeskirja 22. jaos esitatutega.

9. Registreerimine

Niipea, kui register saab Euroopa Liidu dokumendi, mis kuulub salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või kõrgemasse salastatuse kategooriasse, teeb ta selle dokumendi kohta kande organisatsiooni peetavasse eriregistrisse, milles on eraldi veerud kättesaamiskuupäeva, dokumenti iseloomustavate andmete (kuupäev, viitenumber ja koopia number), salastatuse kategooria, pealkirja, saaja nime või ametinimetuse ja vastuvõtmistõendi tagastamiskuupäeva jaoks ning kuupäeva jaoks, mil dokument tagastatakse Euroopa Liiduga seotud koostajale või hävitatakse.

10. Hävitamine

a) Euroopa Liidu salastatud dokumendid hävitatakse käesolevate julgeolekusätete 22. jaos sätestatud juhtnööride kohaselt. Salastatuse kategooriatesse ►M1 SECRET UE ◄ ja ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide hävitamisaktide koopiad saadetakse sellele Euroopa Liidu registrile, kes dokumendid edastas.

b) Euroopa Liidu salastatud dokumendid hõlmatakse teabesaaja enda salastatud dokumentide hädaolukorras hävitamise kavasse.

11. Dokumentide kaitsmine

Võetakse kõik meetmed, et välistada volitamata isikute juurdepääs Euroopa Liidu salastatud teabele.

12. Koopiad, tõlked ja väljavõtted

Salastatuse kategooriatesse ►M1 CONFIDENTIEL UE ◄ ja ►M1 SECRET UE ◄ kuuluvatest dokumentidest ei tehta koopiaid, neid ei tõlgita ning neist ei tehta väljavõtteid ilma asjaomase julgeolekuorganisatsiooni juhi loata; kõnealune juht registreerib need koopiad, tõlked või väljavõtted, kontrollib need ja lööb neile vajadusel templi.

Salastatuse kategooriasse ►M1 TRES SECRET UE/EU TOP SECRET ◄ kuuluvate dokumentide paljundamine ja tõlkimine on lubatud ainult juhul, kui selleks on andnud loa dokumendi koostaja, kes täpsustab lubatud koopiate arvu; kui dokumendi koostanud asutust või ametiisikut ei ole võimalik kindlaks teha, saadetakse taotlus edasi ►M2 komisjoni julgeolekudirektoraati ◄.

13. Julgeoleku rikkumine

Kui julgeolekut on rikutud või kui kahtlustatakse sellist rikkumist seoses Euroopa Liidu salastatud dokumendiga, tuleb julgeolekukokkuleppe sõlmimist arvestades võtta viivitamata järgmised meetmed:

a) korraldada uurimine, et teha kindlaks julgeoleku rikkumise asjaolud;

b) teatada sellest ►M2 komisjoni julgeolekudirektoraadile ◄, asjaomasele siseriiklikule julgeolekuasutusele ja dokumendi koostanud asutusele või ametiisikule, või kui viimasena nimetatut ei ole teavitatud, siis selgelt teatada, et seda ei ole tehtud;

c) võtta meetmeid julgeoleku rikkumise tagajärgede minimeerimiseks;

d) vaadata läbi ja rakendada meetmed, et välistada samasuguse sündmuse kordumine;

e) rakendada ►M2 komisjoni julgeolekudirektoraat ◄ soovitatud meetmeid, et välistada samasuguse sündmuse kordumine.

▼B

14. Inspekteerimised

Kokkuleppel asjaomaste riikide või rahvusvaheliste organisatsioonidega on ►M2 komisjoni julgeolekudirektoraadil ◄ lubatud hinnata avaldatud Euroopa Liidu salastatud teabe kaitsmise meetmete tõhusust.

15. Aruandlus

Julgeolekukokkuleppe sõlmimist arvestades peab riik või rahvusvaheline organisatsioon, kelle valduses on Euroopa Liidu salastatud teave, esitama kord aastas kuupäevaks, mis sätestatakse siis, kui antakse luba teabe avaldamiseks, aruande käesolevate julgeolekusätete täitmise kohta.

▼B

4. liide

Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele: 2. taseme koostöö

MENETLUSED

1. Dokumendi koostaja on volitatud avaldama Euroopa Liidu salastatud teavet kolmandatele riikidele ja rahvusvahelistele organisatsioonidele, mille julgeolekupõhimõtted ja -eeskirjad erinevad märkimisväärselt Euroopa Liidu omadest. Komisjoni kolleegium on volitatud avaldama Euroopa Liidu salastatud teavet, mis on koostatud komisjonis.

2. Põhimõtteliselt on tegemist teabega, mis kuulub salastatuse kategooriasse ►M1 SECRET UE ◄ või madalamasse salastatuse kategooriasse; siia ei kuulu salastatud teave, mida kaitstakse erijulgeoleku tähiste või tähistustega.

3. Kuni julgeolekukokkuleppe sõlmimiseni on turvaküsimuste eest vastutaval komisjoni liikmel pädevus vaadata läbi Euroopa Liidu salastatud teabe avaldamise taotlusi.

4. Seda tehes ta:

   — taotleb avaldatava Euroopa Liidu salastatud teabe koostajate arvamust,

   — loob vajalikud sidemed teabesaajate riikide või rahvusvaheliste organisatsioonide julgeolekuasutustega, et saada teavet nende julgeolekupõhimõtete ja -sätete kohta, ja eelkõige selleks, et koostada tabel, võrdlemaks Euroopa Liidus kasutatavaid salastatuse kategooriaid asjaomases riigis või rahvusvahelises organisatsioonis kasutatavatega,

   — korraldab komisjoni julgeolekupoliitika nõuandekomitee koosoleku või küsitleb, vajadusel vaikiva menetluse alusel, liikmesriikide siseriiklikke julgeolekuasutusi, et koostada komisjoni julgeolekupoliitika nõuandekomitee seisukoht.

5. Komisjoni julgeolekupoliitika nõuandekomitee seisukoht on järgneva kohta:

   — teabesaajate riikide või rahvusvaheliste organisatsioonide usaldatavus, et hinnata Euroopa Liidule või selle liikmesriikidele tulenevaid julgeolekuriske,

   — hinnang selle kohta, kuivõrd teabesaajad suudavad kaitsta Euroopa Liidu avaldatud salastatud teavet,

   — ettepanekud Euroopa Liidu salastatud teabe käitlemise (näiteks selliste versioonide koostamine, millest on teatavad osad välja jäetud) ja dokumentide edastamise (Euroopa Liidu salastatuse kategooria märgete säilitamine või kustutamine, eritähised jne) praktilise korra kohta,

   — salastatuse kategooria alandamine või kaotamine enne teabe avaldamist teabesaaja riikidele või rahvusvahelistele organisatsioonidele.

6. Turvaküsimuste eest vastutav komisjoni liige saadab taotluse koos komisjoni julgeolekupoliitika nõuandekomitee arvamusega komisjonile otsuse tegemiseks.

JULGEOLEKUREEGLID, MIDA PEAVAD KOHALDAMA TEABESAAJAD

7. Turvaküsimuste eest vastutav komisjoni liige teatab teabesaajatele riikidele või rahvusvahelistele organisatsioonidele komisjoni otsusest volitada Euroopa Liidu salastatud teabe avaldamine ja selle piirangutest.

▼B

8. Avaldamise otsus jõustub ainult juhul, kui teabesaajad on kinnitanud kirjalikult, et nad:

— kasutavad teavet ainult kokkulepitud eesmärgil,

— kaitsevad teavet komisjoni kehtestatud sätete kohaselt.

9. Kui komisjon ei otsusta pärast komisjoni julgeolekupoliitika nõuandekomitee tehnilise seisukoha saamist kehtestada Euroopa Liidu salastatud dokumentide käitlemiseks (Euroopa Liidu salastatuse kategooria märke kustutamine, eritähised jne) erikorda, kehtestatakse kaitse kohta järgmised eeskirjad.

10. Personal

a) Euroopa Liidu salastatud teabele juurdepääsu omavate ametnike hulk on teadmisvajaduse põhimõttest lähtuvalt rangelt piiratud nende isikutega, kelle tööülesanded eeldavad sellist juurdepääsu;

b) kõik ametnikud ja kodanikud, kellel on luba juurdepääsuks komisjoni avaldatud salastatud teabele, peavad olema läbinud siseriikliku julgeolekukontrolli või neil peab olema luba juurdepääsuks sellisese salastatuse kategooriasse kuuluvale teabele, mis on vastavalt võrdlustabelile samaväärne asjaomase Euroopa Liidu omaga;

c) kõnealused siseriiklikud julgeolekusertifikaadid või load edastatakse teadmiseks ►**M2** komisjoni julgeolekudirektoraadi direktorile. ◄

11. Dokumentide edastamine

Praktiline dokumentide edastamise kord otsustatakse kokkuleppe teel. Sellise kokkuleppe sõlmimiseni kohaldatakse 21. jao sätteid. Eelkõige määratakse selles kokkuleppes kindlaks registrid, millesse Euroopa Liidu salastatud teave tuleb edastada koos täpsete aadressidega, kuhu dokumendid edastatakse, ning samuti kuller- või postiteenused, mida kasutatakse Euroopa Liidu salastatud teabe edastamisel.

12. Registreerimine saabumisel

Adressaatriigi julgeolekuasutus või sellega samaväärne asutus riigis, mis võtab komisjoni edastatud salastatud teabe vastu oma valitsuse nimel, või vastuvõtva rahvusvahelise organisatsiooni julgeolekubüroo avab eraldi registri, et registreerida Euroopa Liidu salastatud teave selle saabumisel. Registris on veerud saabumiskuupäeva, dokumendi andmete (kuupäev, viitenumber ja koopia number), salastatuse kategooria, pealkirja, adressaadi nime või ametinimetuse ja vastuvõtmistõendi tagastamiskuupäeva jaoks ning kuupäeva jaoks, mil dokument tagastatakse Euroopa Liidule või hävitatakse.

13. Dokumentide tagastamine

Kui saaja tagastab salastatud dokumendi komisjonile, tegutseb ta eelpool lõigus „Dokumentide edastamine” kirjeldatud viisil.

14. Kaitse

a) Kui dokumente ei kasutata, hoitakse neid turvakonteineris, mis on heaks kiidetud sama kategooria siseriiklike salastatud materjalide säilitamiseks. Turvakonteineril ei ole mingit märget selle kohta, mida ta sisaldab, ning konteineri sisule pääsevad juurde ainult isikud, kellel on Euroopa Liidu salastatud teabe käitlemise luba. Kui kasutatakse kombinatsioonlukke, võivad luku kombinatsiooni teada ainult need riigi või organisatsiooni ametnikud, kellel on luba juurdepääsuks Euroopa Liidu salastatud teabele, mida konteineris säilitatakse, ning kombinatsioone muudetakse kord kuue kuu jooksul või sagedamini, kui ametnik viiakse üle teisele ametikohale, kui tühistatakse ühe kombinatsiooni teadva ametniku julgeolekusertifikaat või kui on julgeoleku ohustamise risk.

▼B

b) Euroopa Liidu salastatud dokumente võivad turvakonteinerist võtta ainult need ametnikud, kes on läbinud julgeolekukontrolli Euroopa Liidu salastatud dokumentide jaoks ja kellel on teadmisvajadus. Kuni dokumendid on nende valduses, vastutavad need isikud kõnealuste dokumentide turvalise säilitamise eest ja eelkõige selle eest, et dokumentidele ei pääseks ligi selleks volitamata isikud. Need isikud tagavad ka, et dokumente hoitakse turvakonteineris, kui nad on lõpetanud töö dokumentidega, samuti väljaspool tööaega.

c) Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ ja kõrgemasse kategooriasse kuuluvatest dokumentidest võib teha koopiaid ja väljavõtteid ainult ►M2 komisjoni julgeolekudirektoraadi ◄ loal.

d) Tuleb määratleda dokumentide kiire ja täieliku hävitamise kord hädaolukorras ning selle korra peab kinnitama ►M2 komisjoni julgeolekudirektoraat ◄.

15. Füüsiline julgeolek

a) Kui Euroopa Liidu salastatud dokumentide säilitamiseks kasutatavaid turvakonteinereid ei kasutata, peavad need olema alati lukustatud;

b) kui hooldus personal või koristajad peavad sisenema ruumi, kus on sellised turvakonteinerid, või töötama sellises ruumis, saadab neid alati riigi või organisatsiooni julgeolekuteenistuse liige või selle ruumi julgeoleku eest vastutav ametnik;

c) väljaspool tavapärast tööaega (öösiti, nädalavahetustel ja riigipühadel) kaitseb Euroopa Liidu salastatud dokumente sisaldavaid turvakonteinereid kas valvur või automaatne häiresüsteem.

16. Julgeoleku rikkumine

Kui on rikutud julgeolekut või kui kahtlustatakse sellist rikkumist seoses Euroopa Liidu salastatud dokumendiga, tuleb viivitamata võtta järgmised meetmed:

a) edastada viivitamata aruanne ►M2 komisjoni julgeolekudirektoraadile ◄ või liikmesriigi siseriiklikule julgeolekuasutusele, kes tegeleb dokumentide edastamisega (koos koopiaga ►M2 komisjoni julgeolekudirektoraadile ◄);

b) viia läbi uurimine ja edastada selle lõpetamisel täiemahuline aruanne julgeolekuorganile (vt punkt a eespool). Seejärel tuleb võtta vajalikud meetmed olukorra heastamiseks.

17. Inspekteerimised

Kokkuleppel asjaomaste riikide või rahvusvaheliste organisatsioonidega on ►M2 komisjoni julgeolekudirektoraadil ◄ lubatud hinnata avaldatud Euroopa Liidu salastatud teabe kaitsmise meetmete tõhusust.

18. Aruandlus

Julgeolekukokkuleppe sõlmimist arvestades peab riik või rahvusvaheline organisatsioon, kelle valduses on Euroopa Liidu salastatud teave, esitama kord aastas kuupäevaks, mis sätestatakse siis, kui antakse luba teabe avaldamiseks, aruande käesolevate julgeolekusätete täitmise kohta.

▼B

5. liide

Juhtnöörid Euroopa Liidu salastatud teabe avaldamiseks kolmandatele riikidele või rahvusvahelistele organisatsioonidele: 3. taseme koostöö

MENETLUSED

1. Aeg-ajalt võib komisjon teatavate eriliste asjaolude korral soovida teha koostööd riikide või organisatsioonidega, kes ei saa tagada käesolevate julgeolekusätetega nõutavat turvalisust, kuid kõnealune koostöö võib siiski eeldada Euroopa Liidu salastatud teabe avaldamist.

2. Dokumendi koostaja on volitatud avaldama Euroopa Liidu salastatud teavet kolmandatele riikidele ja rahvusvahelistele organisatsioonidele, mille julgeolekupõhimõtted ja -eeskirjad erinevad märkimisväärselt Euroopa Liidu omadest. Komisjoni kolleegium on volitatud avaldama Euroopa Liidu salastatud teavet, mis on koostatud komisjonis.

   Põhimõtteliselt on tegemist teabega, mis kuulub salastatuse kategooriasse ►M1 SECRET UE ◄ või madalamasse salastatuse kategooriasse; siia ei kuulu salastatud teave, mida kaitstakse erijulgeoleku tähiste või tähistustega.

3. Komisjon kaalub, kuivõrd põhjendatud on salastatud teabe avaldamine, hindab teabetaotlejate teadmisvajadust ja otsustab selle salastatud teabe laadi, mida võib edastada.

4. Kui komisjon on nõus, siis turvaküsimuste eest vastutav komisjoni liige:

   — taotleb avaldatava Euroopa Liidu salastatud teabe koostajate arvamust,

   — korraldab komisjoni julgeolekupoliitika nõuandekomitee koosoleku või küsitleb, vajadusel vaikiva menetluse alusel, liikmesriikide siseriiklikke julgeolekuasutusi, et koostada komisjoni julgeolekupoliitika nõuandekomitee seisukoht.

5. Komisjoni julgeolekupoliitika nõuandekomitee seisukoht on järgneva kohta:

   a) Euroopa Liidule või selle liikmesriikidele tulenevate julgeolekuriskide hinnang;

   b) avaldamisele kuuluda võiva teabe salastatuse tase;

   c) salastatuse kategooria alandamine või kaotamine enne teabe avaldamist;

   d) avaldatavate dokumentide käitlemise kord (vt järgmine lõik);

   e) võimalikud edastusviisid (avaliku postiteenistuse, üldkasutatavate või turvaliste sidesüsteemide, diplomaatilise posti, julgeolekukontrolli läbinud kullerite jms kasutamine).

6. Käesolevas liites käsitletavatele riikidele või organisatsioonidele avaldatavad dokumendid ei sisalda põhimõtteliselt viiteid dokumendi allikale ega Euroopa Liidu salastatuse tasemele. Komisjoni julgeolekupoliitika nõuandekomitee võib soovitada:

   — kasutada spetsiifilist märgistust või koodnimetust,

   — kasutada spetsiifilist salastamissüsteemi, mille puhul oleks teabe tundlikkus seotud kontrollimeetmetega, mida eeldatakse vastuvõtja kasutatavatelt edastusviisidelt.

▼B

7. ►M2 Julgeolekuküsimuste eest vastutav komisjoni liige ◄ edastab komisjoni julgeolekupoliitika nõuandekomitee seisukoha komisjonile otsuse tegemiseks.

8. Kui komisjon on heaks kiitnud Euroopa Liidu salastatud teabe avaldamise ja praktilise rakenduskorra, loob ►M2 komisjoni julgeolekudirektoraat ◄ vajalikud sidemed asjaomase riigi või organisatsiooni julgeolekuorganiga, et soodustada kavandatud julgeolekumeetmete rakendamist.

9. Turvaküsimuste eest vastutav komisjoni liige teavitab liikmesriike teabe iseloomust ja salastatuse kategooriast ning esitab loetelu organisatsioonidest ja riikidest, kellele seda võib avaldada vastavalt komisjoni otsusele.

10. ►M2 Komisjoni julgeolekudirektoraat ◄ võtab kõik vajalikud meetmed, et aidata kaasa mis tahes järgnevale kahju hindamisele ja menetluste läbivaatamistele.

Iga kord, kui koostöötingimused muutuvad, vaatab komisjon selle küsimuse uuesti läbi.

JULGEOLEKUSÄTTED, MIDA PEAVAD KOHALDAMA TEABESAAJAD

11. Turvaküsimuste eest vastutav komisjoni liige teatab teabesaajatele riikidele või rahvusvahelistele organisatsioonidele komisjoni otsusest volitada Euroopa Liidu salastatud teabe avaldamine koos üksikasjaliste kaitse-eeskirjadega, mis on esitatud komisjoni julgeolekupoliitika nõuandekomitee poolt ja heaks kiidetud komisjoni poolt.

12. Otsus jõustub ainult juhul, kui teabesaajad on kinnitanud kirjalikult, et nad:

— kasutavad teavet ainult komisjoni otsuse kohase koostöö eesmärgil,

— tagavad teabele komisjoni nõutava kaitse.

13. Dokumentide edastamine

a) Dokumentide edastamise praktilises korras lepivad kokku ►M2 komisjoni julgeolekudirektoraat ◄ ja teabesaajate riikide või rahvusvaheliste organisatsioonide julgeolekuasutused. Eelkõige nimetatakse täpsed aadressid, kuhu dokumendid tuleb saata.

b) Salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ ja kõrgemasse salastatuse kategooriasse kuuluvad dokumendid edastatakse kahekordses ümbrikus. Sisemisel ümbrikul on kokkulepitud eritempel või koodnimetus ja märge dokumendi jaoks vastuvõetud salastatuse erikategooria kohta. Iga salastatud dokumendi kohta lisatakse kättesaamistõendi vorm. Kättesaamistõendi vormil, mis ei ole salastatud, märgitakse dokumendi kohta ainult teatavad andmed (viitenumber, kuupäev, koopia number) ja keel, milles dokument on koostatud, mitte aga dokumendi pealkirja.

c) Seejärel pannakse sisemine ümbrik välimisse ümbrikku, millel on arvepidamiseks kirjas paki number. Välimisele ümbrikule salastatuse kategooriat ei märgita.

d) Kullerile antakse alati kättesaamiskinnitus, millel on kirjas paki number.

▼B

14. Registreerimine saabumisel

Adressaatriigi julgeolekuasutus või sellega samaväärne asutus riigis, mis võtab Euroopa Liidu edastatud salastatud teabe vastu oma valitsuse nimel, või vastuvõtva rahvusvahelise organisatsiooni julgeolekubüroo avab eraldi registri, et registreerida Euroopa Liidu salastatud teave selle saabumisel. Registris on veerud saabumiskuupäeva, dokumendi andmete (kuupäev, viitenumber ja koopia number), salastatuse kategooria, pealkirja, adressaadi nime või ametinimetuse ja vastuvõtmistõendi tagastamiskuupäeva jaoks ning kuupäeva jaoks, mil vastuvõtmistõend tagastatakse Euroopa Liidule või hävitatakse.

15. Vahetatud salastatud teabe kasutamine ja kaitsmine

a) Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvat teavet käitlevad spetsiaalselt määratud ametnikud, kellel on luba juurdepääsuks sellise salastatuse tasemega teabele. Sellist teavet säilitatakse kvaliteetsetes turvakappides, mida saavad avada ainult isikud, kellel on luba juurdepääsuks neis sisalduvale teabele. Aladel, kus sellised kapid asuvad, peab olema alaline valve ning tuleb luua kontrollsüsteem tagamaks, et sinna lubatakse siseneda ainult nõuetekohaselt volitatud isikutel. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvat teavet võib edastada diplomaatilise posti, turvalise postiteenuse või turvaliste sideteenuste abil. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvatest dokumentidest võib koopiaid teha ainult nende koostaja kirjalikul loal. Kõik koopiad registreeritakse ja neid jälgitakse. Kõigi salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvate dokumentidega seotud toimingute kohta väljastatakse tõendid;

b) salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvat teavet käitlevad nõuetekohaselt määratud ametnikud, kellel on luba saada teavet asjaomase teema kohta. Dokumente säilitatakse kontrollitud alal asuvates lukustatud turvakappides;

salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ kuuluvat teavet edastatakse diplomaatilise posti, sõjaväelise postiteenuse ja turvaliste sideteenuste abil. Vastuvõtja või teha teabest koopiaid ning nende arv ja andmed nende levitamise kohta tuleb registreerida eriregistris;

c) salastatuse kategooriasse ►M1 RESTREINT UE ◄ kuuluvat teavet käideldakse ruumides, kuhu ei pääse volitamata isikud, ja säilitatakse lukustatud konteinerites. Dokumente võib edastada üldkasutatava postiteenistuse kaudu kahekordses ümbrikus tähitud kirjana ja hädaolukorras turvamata üldkasutatavate sidesüsteemide kaudu. Vastuvõtjad võivad teha koopiaid;

d) Salastamata teabe puhul ei ole spetsiaalsed kaitsemeetmed vajalikud ning sellist teavet võib edastada posti teel ja üldkasutatavate sidesüsteemide kaudu. Adressaadid võivad teha koopiaid.

16. Hävitamine

Dokumendid, mida enam ei vajata, hävitakse. Salastatuse kategooriatesse ►M1 RESTREINT UE ◄ ja ►M1 CONFIDENTIEL UE ◄ kuuluvate dokumentide puhul tehakse vajalik märge eriregistritesse. Salastatuse kategooriasse ►M1 SECRET UE ◄ kuuluvate dokumentide puhul antakse välja hävitamisakt, millele kirjutavad alla kaks hävitamise tunnistajaks olnud isikut.

17. Julgeoleku rikkumine

Kui kahjustatakse salastatuse kategooriasse ►M1 CONFIDENTIEL UE ◄ või ►M1 SECRET UE ◄ kuuluvat teavet või kui kahtlustatakse sellist kahjustamist, teostab riigi siseriiklik julgeolekuasutus või organisatsiooni julgeolekujuht kahjustamise asjaolude uurimise. Selle tulemustest teavitatakse ►M2 komisjoni julgeolekudirektoraati ◄. Kui kahjustamise on põhjustanud mitterahuldavad menetlused või säilitamismeetodid, võetakse vajalikud meetmed nende parandamiseks.

▼B

6. liide

LÜHENDITE LOETELU

ACPC	Hangete ja lepingute nõuandekomitee
CrA	Salastatuse küsimuste eest vastutav ametnik
CISO	Keskse informaatikaturbe ametnik
COMPUSEC	Arvutiturve
COMSEC	Sideturve
CSO	►M2 Komisjoni julgeolekudirektoraat ◄
ESDP	Euroopa julgeoleku- ja kaitsepoliitika
EUCI	Euroopa Liidu salastatud teave
IA	Teabeturbe asutus või ametiisik
INFOSEC	Teabeturve
IO	Teabeomanik
ISO	Rahvusvaheline Standardiorganisatsioon
IT	Infotehnoloogia
LISO	Kohaliku informaatikaturbe ametnik
LSO	Kohalik julgeolekuametnik
MSO	Koosoleku julgeolekuametnik
NSA	Siseriiklik julgeolekuasutus
PC	Personaalarvuti
RCO	Registri kontrolliametnik
SAA	Julgeoleku akrediteerimise asutus või ametiisik
SecOPS	Julgeolekuga seotud töökord
SSRS	Süsteemispetsiifiliste julgeolekunõuete loetelu
TA	*Tempest*-ametiisik
TSO	Tehnilise süsteemi vastutav käitaja

▼M3

DSA	määratud julgeolekuasutus
FSC	ettevõtte julgeolekukontroll
FSO	ettevõtte julgeolekuülem
PSC	töötajate julgeolekukontroll
SAL	julgeolekuaspekte käsitlev dokument
SCG	salastatuse kategooriate määramise juhend