**ÁKVÖRÐUN RÁÐSINS**

**frá 31. mars 2011**

**um öryggisreglur til að vernda trúnaðarflokkaðar upplýsingar Evrópusambandsins.**

**(2011/292/ESB)**

RÁÐ EVRÓPUSAMBANDSINS,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins, einkum 3. mgr. 240. gr.,

með hliðsjón af ákvörðun ráðsins 2009/937/ESB frá 1. desember 2009, um samþykkt starfsreglna ráðsins ([[1]](#footnote-1)), einkum 24. gr.,

að teknu tilliti til þess að:

1) Til þess að þróa starfsemi ráðsins á öllum sviðum, þar sem krafa er gerð um hvernig meðhöndla beri trúnaðarflokkaðar upplýsingar, þykir rétt að koma á víðtæku öryggiskerfi til verndar trúnaðarflokkuðum upplýsingum sem gildir fyrir ráðið, aðalskrifstofu þess og aðildarríkin.

2) Ákvörðun þessi gildir þegar ráðið, undirbúningsstofnanir þess og aðalskrifstofa ráðsins (GSC) meðhöndla trúnaðarflokkaðar upplýsingar ESB (EUCI).

3) Aðildarríkin ættu, í samræmi við innlend lög og reglugerðir og að því marki sem störf ráðsins krefjast, að virða ákvörðun þessa þegar lögbær stjórnvöld þeirra, starfsfólk eða verktakar meðhöndla trúnaðarflokkaðar upplýsingar ESB, þannig að sérhver þeirra geti verið þess fullviss að trúnaðarflokkaðar upplýsingar ESB njóti sambærilegrar verndar.

4) Ráðið og framkvæmdastjórnin skuldbinda sig til að beita sambærilegum öryggisviðmiðunum til verndar trúnaðarflokkuðum upplýsingum ESB.

5) Ráðið leggur áherslu á mikilvægi þess, þar sem það á við, að tengja Evrópuþingið og aðrar skipulagseiningar, embætti, stofnanir eða skrifstofur ESB við grundvallarsetningar, viðmiðanir og reglur um vernd trúnaðarflokkaðra upplýsinga sem eru nauðsynleg til verndar hagsmunum Sambandsins og aðildarríkja þess.

6) Embætti og stofnanir ESB, sem stofnsett eru samkvæmt ákvæðum 2. kafla í V. bálki sáttmálans um Evrópusambandið, Evrópulögreglan og Evrópska réttaraðstoðin, beita, í tengslum við innra skipulag sitt, grundvallarsetningum og lágmarksviðmiðunum, sem mælt er fyrir um í ákvörðun þessari til verndar trúnaðarflokkuðum upplýsingum ESB, í samræmi við ákvæði stofnsáttmála hvers og eins.

7) Öryggisreglum, sem ráðið samþykkir til verndar trúnaðarflokkuðum upplýsingum ESB, er beitt viðvíkjandi hættustjórnunaraðgerðum, sem ákveðnar eru samkvæmt ákvæðum 2. kafla í V. bálki sáttmálans um Evrópusambandið, og af því starfsfólki sem framkvæmir þær.

8) Sérstakir fulltrúar ESB beita, ásamt þeim sem mynda hópa þeirra, öryggisreglum sem ráðið samþykkir til verndar trúnaðarflokkuðum upplýsingum ESB.

9) Ákvörðun þessi er með fyrirvara um ákvæði 15. og 16. gr. sáttmálans um starfshætti Evrópusambandsins og gerninga þeim til framkvæmdar.

10) Ákvörðun þessi er með fyrirvara um gildandi starfsvenjur aðildarríkjanna að því er varðar upplýsingagjöf til þjóðþinga þeirra um starfsemi Sambandsins,

HEFUR SAMÞYKKT ÁKVÖRÐUN ÞESSA:

1. gr.

**Tilgangur, gildissvið og skilgreiningar.**

1. Ákvörðun þessi mælir fyrir um grundvallarsetningar og lágmarksviðmiðanir um öryggi, trúnaðarflokkuðum upplýsingum ESB til verndar.

2. Grundvallarsetningar þessar og lágmarksviðmiðanir gilda gagnvart ráðinu og aðalskrifstofu þess og skulu aðildarríkin virða þær í samræmi við innlend lög og reglugerðir hvers og eins þannig að hvert þeirra hafi fulla vissu fyrir því að trúnaðarflokkaðar upplýsingar ESB njóti sambærilegrar verndar.

3. Þær skilgreiningar sem settar eru fram í viðbæti A gilda í ákvörðun þessari.

2. gr.

**Skilgreining á trúnaðarflokkuðum upplýsingum ESB, trúnaðarflokkun og merkingum.**

1. „Trúnaðarflokkaðar upplýsingar ESB“ merkir allar upplýsingar eða efni sem auðkennt er samkvæmt trúnaðarflokkun ESB, þar sem óheimil uppljóstrun þeirra eða þess gæti skaðað hagsmuni Evrópusambandsins eða eins eða fleiri aðildarríkja í mismiklum mæli.

2. Trúnaðarflokkaðar upplýsingar ESB skulu falla undir eitt af eftirfarandi stigum:

a) ALGJÖRT LEYNDARMÁL ESB (TRÈS SECRET UE/EU TOP SECRET): upplýsingar og efni þar sem óheimil uppljóstrun þeirra gæti skaðað meginhagsmuni Evrópusambandsins eða eins eða fleiri aðildarríkja með óvenjulega háskalegum hætti,

b) LEYNDARMÁL ESB (SECRET UE/EU SECRET): upplýsingar og efni þar sem óheimil uppljóstrun þeirra gæti skaðað alvarlega meginhagsmuni Evrópusambandsins eða eins eða fleiri aðildarríkja,

c) TRÚNAÐARMÁL ESB (CONFIDENTIEL UE/EU CONFIDENTIAL): upplýsingar og efni þar sem óheimil uppljóstrun þeirra gæti skaðað meginhagsmuni Evrópusambandsins eða eins eða fleiri aðildarríkja,

d) TAKMARKAÐUR AÐGANGUR ESB (RESTREINT UE/EU RESTRICTED): upplýsingar og efni þar sem óheimil uppljóstrun upplýsinga gæti haft óhagstæð áhrif á hagsmuni Evrópusambandsins eða eins eða fleiri aðildarríkja.

3. Trúnaðarflokkaðar upplýsingar ESB skulu merktar trúnaðarflokki skv. 2. mgr. Þær geta haft viðbótarmerkingar sem auðkenna það athafnasvið sem þær varða, segja deili á útgefanda þeirra, takmarka dreifingu þeirra, takmarka notkun þeirra eða gefa til kynna heimild til birtingar.

3. gr.

**Umsjón með flokkun.**

1. Viðkomandi lögbær stjórnvöld skulu tryggja að trúnaðarflokkaðar upplýsingar ESB séu flokkaðar á viðeigandi hátt, greinilega auðkenndar trúnaðarflokkaðar upplýsingar og haldi trúnaðarflokkunarstigi sínu eins lengi og nauðsyn krefur.

2. Hvorki er heimilt er að lækka trúnaðarstig trúnaðarflokkaðra upplýsinga ESB eða aflétta trúnaðarflokkun þeirra né breyta eða fjarlægja einhverjar þær merkingar er um getur í 3. mgr. 2. gr. án skriflegs fyrirframsamþykkis útgefanda.

3. Ráðið skal samþykkja öryggisstefnu vegna tilurðar trúnaðarflokkaðra upplýsinga ESB sem skal innihalda hagnýtar flokkunarleiðbeiningar.

4. gr.

**Vernd trúnaðarflokkaðra upplýsinga.**

1. Trúnaðarflokkaðar upplýsingar ESB skal vernda samkvæmt ákvæðum ákvörðunar þessarar.

2. Handhafi trúnaðarflokkaðra upplýsinga ESB er ábyrgur fyrir því að vernda þær samkvæmt ákvæðum ákvörðunar þessarar.

3. Þegar aðildarríki fella trúnaðarflokkaðar upplýsingar, sem hafa innlenda merkingu trúnaðarflokks, inn í skipulag eða netkerfi Evrópusambandsins skal ráðið og aðalskrifstofa þess vernda upplýsingarnar eins og gerð er krafa um fyrir trúnaðarflokkaðar upplýsingar ESB og á sambærilegan hátt og kemur fram í samsvörunartöflunni fyrir trúnaðarflokkun í viðbæti B.

4. Mikið magn trúnaðarflokkaðra upplýsinga ESB eða uppsöfnun slíkra upplýsinga getur gefið tilefni til ákvörðunar verndarstigs sem samsvarar hærri trúnaðarflokkun.

5. gr.

**Öryggisáhættustjórnun.**

1. Fást skal við hættu sem steðjar að trúnaðarflokkuðum upplýsingum ESB sem ferli. Þetta ferli skal miða að því að ákvarða þekkta öryggisáhættu, skilgreina öryggisráðstafanir til að minnka slíka áhættu að því marki sem er ásættanlegt í samræmi við þær grundvallarsetningar og þá lágmarksviðmiðanir sem settar eru fram í ákvörðun þessari og að því að beita þessum ráðstöfunum í samræmi við hugtakið lagskiptar varnir, eins og það er skilgreint í viðbæti A. Árangur slíkra ráðstafana skal meta stöðugt.

2. Öryggisráðstafanir til verndar trúnaðarflokkuðum upplýsingum ESB á líftíma þeirra skulu einkum svara til trúnaðarflokkunar þeirra, forms og magns upplýsinganna eða efnisins, staðsetningar og byggingar þeirrar aðstöðu þar sem hinar trúnaðarflokkuðu upplýsingar ESB eru hýstar og þess áhættumats, sem er framkvæmt á staðnum, vegna illvirkja og/eða glæpastarfsemi, þ.m.t. njósnir, skemmdarverk og hryðjuverk.

3. Viðbragðsáætlanir skulu miðast við nauðsyn þess að vernda trúnaðarflokkaðar upplýsingar ESB meðan neyðarástand ríkir, til þess að koma í veg fyrir óheimilan aðgang að þeim, óheimila uppljóstrun þeirra eða það að heilleiki þeirra eða aðgengi að þeim fari forgörðum.

4. Fyrirbyggjandi ráðstafanir og ráðstafanir um endurheimt, sem miða að því að lágmarka áhrif alvarlegra mistaka eða atvika á meðhöndlun og geymslu trúnaðarflokkaðra upplýsinga ESB, skal fella inn í áætlanir um framhald aðgerða.

6. gr.

**Framkvæmd ákvörðunar þessarar.**

1. Ráðið skal, að tilmælum öryggisnefndarinnar og ef nauðsyn krefur, samþykkja öryggisstefnu þar sem greint er frá ráðstöfunum vegna framkvæmdar ákvörðunar þessarar.

2. Öryggisnefndin getur, á vettvangi sínum, samþykkt öryggisleiðbeiningar sem viðbót eða stuðning við ákvörðun þessa og öryggisstefnu sem ráðið samþykkir.

7. gr.

**Öryggi með tilliti til starfsfólks.**

1. Öryggi með tilliti til starfsfólks eru ráðstafanir sem eru gerðar til að tryggja að aðgangur að trúnaðarflokkuðum upplýsingum ESB sé aðeins heimilaður einstaklingum sem hafa:

— vitneskjuþörf,

— hlotið öryggisvottun á viðeigandi stigi, þar sem það á við, og verið leiðbeint um ábyrgð sína.

2. Verklag við öryggisvottun starfsfólks skal miða að því að ákvarða hvort heimila megi einstaklingi aðgang að trúnaðarflokkuðum upplýsingum ESB, að teknu tilliti til hollustu hans, trúverðugleika og áreiðanleika.

3. Allir einstaklingar, sem starfa á aðalskrifstofu ráðsins og þurfa skyldu sinnar vegna að hafa aðgang að trúnaðarflokkuðum upplýsingum ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar, skulu hafa öryggisvottun á viðeigandi stigi áður en þeim er veittur aðgangur að slíkum trúnaðarflokkuðum upplýsingum ESB. Verklag við öryggisvottun starfsfólks aðalskrifstofu ráðsins og annarra starfsmanna er sett fram í I. viðauka.

4. Starfsfólk aðildarríkjanna, sem um getur í 3. mgr. 14. gr. og kann skyldu sinnar vegna að þurfa aðgang að trúnaðarflokkuðum upplýsingum ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar, skal hafa öryggisvottun á viðeigandi stigi eða fá, með öðrum hætti, fullar heimildir með skírskotun til þess hlutverks sem það gegnir, í samræmi við innlend lög og reglugerðir, áður en því er veittur aðgangur að slíkum trúnaðarflokkuðum upplýsingum ESB.

5. Allir einstaklingar skulu, áður en þeim er veittur aðgangur að trúnaðarflokkuðum upplýsingum ESB og með reglulegu millibili eftir það, fá leiðbeiningar um þá ábyrgð sem þeir bera í því tilliti að vernda trúnaðarflokkaðar upplýsingar ESB í samræmi við ákvörðun þessa og gangast við þeirri ábyrgð.

6. Í I. viðauka er kveðið á um framkvæmd efnisatriða þessarar greinar.

8. gr.

**Hlutkennt öryggi.**

1. Hlutkennt öryggi er beiting hlutkenndra og tæknilegra verndarráðstafana til að fyrirbyggja óheimilan aðgang að trúnaðarflokkuðum upplýsingum ESB.

2. Hlutkenndar öryggisráðstafanir skulu miða að því að meina óviðkomandi aðila aðgang í laumi eða með innbroti, að fyrirbyggja, koma í veg fyrir og koma upp um óheimilar aðgerðir og að gera kleift að aðgreina starfsfólk, á grundvelli vitneskjuþarfar, með tilliti til aðgangs þess að trúnaðarflokkuðum upplýsingum ESB. Ákvarða skal þess konar ráðstafanir á grundvelli áhættustjórnunarferlis.

3. Hlutkenndum öryggisráðstöfunum skal komið á í öllu húsnæði, byggingum, skrifstofum, rýmum og á öðrum svæðum þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar eða geymdar, þ.m.t. svæði sem hýsa samskipta- og upplýsingakerfi, sbr. skilgreiningu í 2. mgr. 10. gr.

4. Svæði, þar sem trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar eru geymdar, skulu stofnsett sem öryggissvæði í samræmi við ákvæði II. viðauka og hljóta samþykki viðkomandi bærs öryggisyfirvalds.

5. Aðeins skal nota samþykktan búnað eða tæki til verndar trúnaðarflokkuðum upplýsingum ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar.

6. Í II. viðauka er kveðið á um framkvæmd efnisatriða þessarar greinar.

9. gr.

**Umsjón með trúnaðarflokkuðum upplýsingum.**

1. Umsjón með trúnaðarflokkuðum upplýsingum felst í því að beita stjórnsýsluráðstöfunum til þess að geta haft stjórn á trúnaðarflokkuðum upplýsingum ESB á líftíma þeirra, í því skyni að auka við þær ráðstafanir sem kveðið er á um í 7., 8. og 10. gr. og þannig að aðstoða við að fyrirbyggja, koma upp um og bæta skaða sem orsakast af því að fyrrnefndum upplýsingum er stofnað í hættu eða tapast af ásetningi eða fyrir slysni. Slíkar ráðstafanir eiga einkum skylt við tilurð, skráningu, afritun, þýðingu, flutning og eyðingu trúnaðarflokkaðra upplýsinga ESB.

2. Upplýsingar á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar skulu skráðar af öryggisástæðum við móttöku og áður en þeim er dreift. Bær stjórnvöld innan aðalskrifstofu ráðsins og í aðildarríkjunum skulu koma á fót skráningarkerfi í þessum tilgangi. Upplýsingar á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB, skal skrá í tilnefndum skráningarstofum.

3. Bært öryggisyfirvald skal hafa reglulegt eftirlit með þjónustustofnunum og húsnæði þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar eða geymdar.

4. Trúnaðarflokkaðar upplýsingar ESB skulu fluttar á milli þjónustustofnana og húsnæðis utan svæða sem eru vernduð með hlutkenndum hætti:

a) hafa skal sem almenna reglu að trúnaðarflokkaðar upplýsingar ESB séu sendar á rafrænan hátt og verndaðar með dulkóðunartækjum sem eru samþykkt skv. 6. mgr. 10. gr.,

b) Þegar aðferðin, sem um getur í a-lið, er ekki notuð skulu trúnaðarflokkaðar upplýsingar ESB annað hvort fluttar:

i. með rafrænum miðlum (t.d. USB-lyklum, geisladiskum, hörðum diskum) vernduðum með dulkóðunartækjum sem eru samþykkt skv. 6. mgr. 10. gr., eða

ii. í öllum öðrum tilvikum, eftir staðlaðri uppskrift viðkomandi bærs öryggisyfirvalds og samkvæmt viðeigandi verndarráðstöfunum sem mælt er fyrir um í III. viðauka.

5. Í III. viðauka er kveðið á um framkvæmd efnisatriða þessarar greinar.

10. gr.

**Vernd trúnaðarflokkaðra upplýsinga ESB sem meðhöndlaðar eru í samskipta- og upplýsingakerfum.**

1. Upplýsingaöryggi (IA) í tengslum við samskipta- og upplýsingakerfi er sú tiltrú að slík kerfi muni vernda þær upplýsingar sem um þau fara og að þau virki eins og þörf er á, þegar þörf er á, undir stjórn lögmætra notenda. Skilvirkt upplýsingaöryggi skal tryggja viðeigandi leynd, heilleika, aðgengi, óhrekjanleika og áreiðanleika. Upplýsingaöryggi skal byggt á áhættustjórnunarferli.

2. „Samskipta- og upplýsingakerfi“ merkir öll kerfi sem gera kleift að meðhöndla upplýsingar í rafrænni mynd. Samskipta- og upplýsingakerfi skal samanstanda af öllum þeim tilföngum sem eru nauðsynleg til þess að það geti starfað, þ.m.t. grunnvirki, skipulag, starfsfólk og uppspretta upplýsinga. Ákvörðun þessi gildir um samskipta- og upplýsingakerfi (CIS) þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar.

3. Trúnaðarflokkaðar upplýsingar ESB skal meðhöndla innan samskipta- og upplýsingakerfis eins og hugtakið upplýsingaöryggi býður.

4. Votta ber öll samskipta- og upplýsingakerfi samkvæmt vottunarferli. Vottun miðar að því að tryggja að allar viðeigandi öryggisráðstafanir hafi verið gerðar og að fullnægjandi verndarstigi trúnaðarflokkaðra upplýsinga ESB og samskipta- og upplýsingakerfa hafi verið náð í samræmi við ákvörðun þessa. Í vottunaryfirlýsingunni skal koma fram það hæsta stig trúnaðarflokkunar sem heimilt er að meðhöndla upplýsingar samkvæmt í tilteknu samskipta- og upplýsingakerfi, ennfremur þeir skilmálar og þau skilyrði sem við eiga.

5. Samskipta- og upplýsingakerfi, þar sem meðhöndlun upplýsinga á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar fer fram, skal vernda þannig að ekki sé hægt að stofna upplýsingunum í hættu óviljandi með rafsegulgeislun (TEMPEST-öryggisráðstafanir).

6. Þegar trúnaðarflokkaðar upplýsingar ESB eru verndaðar með dulkóðunartækjum skal samþykkja slík tæki á eftirfarandi hátt:

a) leynd upplýsinga á trúnaðarstiginu LEYNDARMÁL ESB eða ofar skal vernda með dulkóðunartækjum sem ráðið samþykkir sem vottunaryfirvald dulkóðunar (CAA) samkvæmt tilmælum öryggisnefndarinnar,

b) leynd upplýsinga á trúnaðarstiginu TRÚNAÐARMÁL ESB eða TAKMARKAÐUR AÐGANGUR ESB skal vernda með dulkóðunartækjum sem aðalframkvæmdastjóri ráðsins (hér á eftir nefndur „aðalframkvæmdastjórinn“) samþykkir sem vottunaryfirvald dulkóðunar samkvæmt tilmælum öryggisnefndarinnar.

Þrátt fyrir ákvæði b-liðar er heimilt að tryggja leynd trúnaðarflokkaðra upplýsinga ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða TAKMARKAÐUR AÐGANGUR ESB í innlendum kerfum aðildarríkjanna með dulkóðunartækjum sem vottunaryfirvald dulkóðunar í aðildarríki samþykkir.

7. Nota ber samþykkt dulkóðunartæki þegar rafræn sending trúnaðarflokkaðra upplýsinga ESB fer fram. Þrátt fyrir þessa kröfu má beita sértæku verklagi eða sérstakri, tæknilegri samsetningu í neyðartilvikum, eins og fram kemur í IV. viðauka.

8. Bær stjórnvöld aðalskrifstofu ráðsins annars vegar og aðildarríkjanna hins vegar skulu koma á fót eftirtalinni starfsemi á sviði upplýsingaöryggis:

a) yfirvaldi á sviði upplýsingaöryggis (IAA),

b) TEMPEST-yfirvaldi (TA),

c) vottunaryfirvaldi dulkóðunar (CAA),

d) yfirvaldi á sviði dulkóðaðrar dreifingar (CDA).

9. Bær stjórnvöld aðalskrifstofu ráðsins annars vegar og aðildarríkjanna hins vegar skulu koma á fót eftirfarandi fyrir hvert og eitt kerfi:

a) yfirvaldi á sviði öryggisvottunar,

b) framkvæmdaryfirvaldi á sviði upplýsingaöryggis.

10. Í IV. viðauka er kveðið á um framkvæmd efnisatriða þessarar greinar.

11. gr.

**Iðnaðaröryggi.**

1. Iðnaðaröryggi er gerð ráðstafana til að tryggja vernd trúnaðarflokkaðra upplýsinga ESB af hálfu verktaka eða undirverktaka þegar samningaviðræður í aðdraganda samningsgerðar standa yfir og á líftíma trúnaðarflokkaðra verktakasamninga. Slíkir samningar fela ekki í sér aðgang að upplýsingum á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB.

2. Aðalskrifstofa ráðsins getur með verktakasamningi treyst iðnfyrirtækjum eða öðrum rekstrareiningum, sem eru skráð í aðildarríki eða þriðja ríki og hafa gert samning eða gengið frá stjórnsýslusamkomulagi í samræmi við a- eða b-lið 2. mgr. 12. gr., fyrir verkefnum sem fela í sér eða leiða af sér aðgang að eða meðhöndlun eða geymslu trúnaðarflokkaðra upplýsinga ESB.

3. Aðalskrifstofa ráðsins, sem samningsyfirvald, skal tryggja að lágmarksviðmiðunum um iðnaðaröryggi, sem eru settar fram í ákvörðun þessari og vísað er til í viðkomandi verktakasamningi, sé fylgt þegar trúnaðarflokkaðir verktakasamningar eru gerðir við iðnfyrirtæki eða aðrar rekstrareiningar.

4. Stjórnvald á sviði þjóðaröryggis (NSA), tilgreint öryggisyfirvald (DSA) eða hvað annað bært yfirvald hvers aðildarríkis sem er skal tryggja, að því marki sem innlend lög og reglugerðir heimila, að verktakar og undirverktakar, sem eru skráðir á yfirráðasvæði þess, geri allar viðeigandi ráðstafanir til verndar trúnaðarflokkuðum upplýsingum ESB, þegar samningaviðræður í aðdraganda samningsgerðar standa yfir og trúnaðarflokkaður samningur kemur til framkvæmda.

5. Stjórnvald á sviði þjóðaröryggis, tilgreint öryggisyfirvald eða hvað annað bært öryggisyfirvald hvers aðildarríkis sem er skal tryggja, í samræmi við innlend lög og reglugerðir, að verktakar eða undirverktakar sem eru skráðir í fyrrnefndu aðildarríki og eiga hlutdeild í trúnaðarflokkuðum verktakasamningum eða samningum um undirverktöku og krefjast aðgangs að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB innan starfsstöðva sinna, annað hvort við framkvæmd slíkra samninga eða í aðdraganda þeirra, hafi öryggisvottun starfsstöðvar (FSC) á viðeigandi stigi trúnaðarflokkunar.

6. Viðkomandi stjórnvald á sviði þjóðaröryggis, tilgreint öryggisyfirvald eða hvað annað bært öryggisyfirvald sem er skal, í samræmi við innlend lög og reglugerðir og þær lágmarksviðmiðanir sem mælt er fyrir um í I. viðauka, veita starfsfólki verktaka eða undirverktaka, sem vegna framkvæmdar trúnaðarflokkaðs samnings þarfnast aðgangs að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB, öryggisvottun starfsfólks (PSC).

7. Í V. viðauka er kveðið á um framkvæmd efnisatriða þessarar greinar.

12. gr.

**Skipti á trúnaðarflokkuðum upplýsingum við þriðju ríki og alþjóðastofnanir.**

1. Ákveði ráðið að þörf sé á að skiptast á trúnaðarflokkuðum upplýsingum ESB við þriðja ríki eða alþjóðastofnun skal setja viðeigandi regluramma þar um.

2. Til þess að setja slíkan regluramma og skilgreina gagnkvæmar reglur um vernd trúnaðarflokkaðra upplýsinga sem skiptst er á:

a) skal ráðið gera samninga um öryggisverklag vegna skipta á trúnaðarflokkuðum upplýsingum og verndar þeirra (hér á eftir nefndir „samningar um upplýsingaöryggi“ eða

b) getur aðalframkvæmdastjórinn gengið frá stjórnsýslusamkomulagi skv. 17. mgr. VI. viðauka, þar sem almenna reglan er sú að stig þeirra trúnaðarflokkuðu upplýsinga ESB sem til stendur að miðla er ekki hærra en TAKMARKAÐUR AÐGANGUR ESB.

3. Samningar um upplýsingaöryggi eða stjórnsýslusamkomulag, sem um getur í 2. mgr., skal innihalda ákvæði sem tryggja að þegar þriðju ríki eða alþjóðastofnanir taka við trúnaðarflokkuðum upplýsingum ESB séu slíkar upplýsingar verndaðar á viðeigandi hátt í samræmi við það stig trúnaðarflokkunar sem þær hafa og samkvæmt lágmarksviðmiðunum sem samsvara að minnsta kosti þeim sem mælt er fyrir um í ákvörðun þessari.

4. Ráðið tekur, í hverju tilviki fyrir sig, ákvörðun þess efnis að miðla til þriðja ríkis eða alþjóðastofnunar trúnaðarflokkuðum upplýsingum ESB, sem eru upprunnar í ráðinu, eftir eðli og innihaldi slíkra upplýsinga, vitneskjuþörf viðtakanda og eftir þeim ávinningi sem Evrópusambandið hefur af afhendingu þeirra. Ef ráðið er ekki útgefandi þeirra trúnaðarflokkuðu upplýsinga sem óskað er eftir að verði miðlað skal aðalskrifstofa ráðsins leita eftir skriflegu samþykki útgefanda fyrir miðlun þeirra. Ef eigi reynist unnt að ganga úr skugga um hver útgefandinn er skal ráðið taka á sig ábyrgð hins fyrrnefnda.

5. Matsheimsóknir skulu skipulagðar til að fá fullvissu um skilvirkni þeirra öryggisráðstafana sem eru til staðar í þriðja ríki og alþjóðastofnun til verndar trúnaðarflokkuðum upplýsingum ESB sem afhentar eru eða skipst er á.

6. Í VI. viðauka er kveðið á um framkvæmd efnisatriða þessarar greinar.

13. gr.

**Brot á öryggisreglum og stofnun trúnaðarflokkaðra upplýsinga ESB í hættu.**

1. Brot á öryggisreglum er afleiðing athafnar eða athafnaleysis einstaklings sem gengur gegn þeim öryggisreglum sem mælt er fyrir um í ákvörðun þessari.

2. Trúnaðarflokkuðum upplýsingum ESB er stofnað í hættu ef þeim, sem afleiðing brots á öryggisreglum, hefur, að hluta til eða öllu leyti, verið miðlað til einstaklinga sem er óheimill aðgangur að þeim.

3. Brot á öryggisreglum eða grunur um brot á öryggisreglum skal þegar í stað tilkynnt viðkomandi bæru öryggisyfirvaldi.

4. Þegar vitað er eða gild ástæða er til að ætla að trúnaðarflokkuðum upplýsingum ESB hafi verið stofnað í hættu eða að slíkar upplýsingar hafi tapast, skal viðkomandi bært öryggisyfirvald gera allar viðeigandi ráðstafanir, í samræmi við viðeigandi lög og reglugerðir, til að:

a) upplýsa útgefandann,

b) tryggja að málið sé rannsakað af starfsfólki, sem tengist ekki brotinu með beinum hætti, í því skyni að leiða fram staðreyndir málsins,

c) meta hvort hagsmunir ESB eða aðildarríkjanna hafi hugsanlega skaðast,

d) komið verði með viðeigandi hætti í veg fyrir að slíkt endurtaki sig og e) tilkynna hlutaðeigandi yfirvöldum um þær aðgerðir sem gripið er til.

5. Einstaklingur, sem er ábyrgur fyrir broti á þeim öryggisreglum sem mælt er fyrir um í ákvörðun þessari, má eiga von á að verða beittur agavaldi samkvæmt gildandi ákvæðum og reglugerðum. Einstaklingur, sem er ábyrgur fyrir því að stofna trúnaðarflokkuðum upplýsingum ESB í hættu eða að tapa slíkum upplýsingum, má eiga von á að verða beittur agavaldi og/eða að verða lögsóttur samkvæmt gildandi lögum, ákvæðum og reglugerðum.

14. gr.

**Ábyrgð á framkvæmd.**

1. Ráðið skal gera allar nauðsynlegar ráðstafanir til að tryggja að gætt sé heildarsamræmis þegar ákvæðum ákvörðunar þessarar er beitt.

2. Aðalframkvæmdastjórinn skal, í tengslum við meðhöndlun og geymslu trúnaðarflokkaðra upplýsinga ESB eða annarra trúnaðarflokkaðra upplýsinga, gera allar nauðsynlegar ráðstafanir til að tryggja að embættismenn og annað starfsfólk aðalskrifstofu ráðsins, starfsfólk sem er kallað til starfa á aðalskrifstofu ráðsins og verktakar á vegum hennar beiti ákvæðum ákvörðunar þessarar í húsnæði sem ráðið notar og er innan aðalskrifstofu þess, einnig í húsnæði tengiskrifstofa þess í þriðju ríkjum.

3. Aðildarríki skulu gera allar viðeigandi ráðstafanir, í samræmi við innlend lög og reglugerðir hvers og eins, til að tryggja að þegar trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar eða geymdar virði eftirtaldir aðilar ákvæði ákvörðunar þessarar:

a) starfsfólk fastanefnda aðildarríkjanna hjá Evrópusambandinu og sendimenn ríkja sem sækja fundi ráðsins eða stofnana þess, sem annast undirbúning, eða sem taka þátt í annarri starfsemi ráðsins,

b) annað starfsfólk innlendra stjórnvalda aðildarríkjanna, þ.m.t. starfsfólk sem er kallað til starfa hjá þeim stjórnvöldum, hvort sem það starfar á yfirráðasvæði aðildarríkjanna eða erlendis,

c) aðrir einstaklingar í aðildarríkjunum sem í krafti starfa sinna hafa tilskilda aðgangsheimild að trúnaðarflokkuðum upplýsingum ESB og d) verktakar frá aðildarríkjunum, hvort sem er á yfirráðasvæði aðildarríkjanna eða erlendis.

15. gr.

**Öryggisskipan í ráðinu.**

1. Ráðið skal, sem þátt í því hlutverki þess að gæta heildarsamræmis þegar ákvæðum ákvörðunar þessarar er beitt, samþykkja:

a) samninga sem um getur í a-lið 2. mgr. 12. gr.,

b) ákvarðanir sem heimila miðlun trúnaðarflokkaðra upplýsinga ESB til þriðju ríkja og alþjóðastofnana,

c) árlega eftirlitsáætlun sem aðalframkvæmdastjórinn gerir tillögu um og öryggisnefndin mælir með vegna eftirlits með þjónustustofnunum og húsnæði á vegum aðildarríkjanna og með embættum og stofnunum ESB, sem stofnsett eru samkvæmt ákvæðum 2. kafla í V. bálki sáttmálans um Evrópusambandið, ennfremur með Evrópulögreglunni og Evrópsku réttaraðstoðinni, einnig matsheimsóknir til þriðju ríkja og alþjóðastofnana til þess að fá vissu fyrir skilvirkni þeirra ráðstafana sem gerðar eru til verndar trúnaðarflokkuðum upplýsingum ESB og d) öryggisstefnu eins og gert er ráð fyrir í 1. mgr. 6. gr.

2. Aðalframkvæmdastjórinn er öryggisyfirvald aðalskrifstofu ráðsins. Sem slíkur skal aðalframkvæmdastjórinn:

a) framkvæma og endurskoða stefnu ráðsins á sviði öryggismála,

b) samræma öll öryggismál sem varða vernd trúnaðarflokkaðra upplýsinga og skipta máli fyrir starfsemi ráðsins, í samstarfi við stjórnvöld aðildarríkjanna á sviði þjóðaröryggis,

c) veita embættismönnum aðalskrifstofu ráðsins og öðrum starfsmönnum öryggisvottun ESB fyrir starfsfólk í samræmi við 3. mgr. 7. gr. áður en þeim er heimilaður aðgangur að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar,

d) skipa fyrir, eftir því sem við á, um rannsóknir á raunverulegri eða meintri stofnun trúnaðarflokkaðra upplýsinga í hættu, sem eru í vörslu ráðsins eða upprunnar hjá því, eða á tapi þeirra og óska eftir aðstoð hlutaðeigandi öryggisyfirvalda við slíkar rannsóknir,

e) framkvæma reglubundið eftirlit með öryggisfyrirkomulagi til verndar trúnaðarflokkuðum upplýsingum í húsnæði aðalskrifstofu ráðsins,

f) framkvæma reglubundið eftirlit með öryggisfyrirkomulagi til verndar trúnaðarflokkuðum upplýsingum ESB hjá embættum og stofnunum ESB, sem stofnsett eru samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, Evrópulögreglunni og Evrópsku réttaraðstoðinni, ennfremur hjá aðstandendum hættustjórnunaraðgerða, sem stofnað er til samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, og sérstökum fulltrúum ESB (EUSR) og meðlimum í hópum þeirra,

g) framkvæma reglubundið eftirlit, í samstarfi og samráði við hlutaðeigandi stjórnvald á sviði þjóðaröryggis, með öryggisfyrirkomulagi til verndar trúnaðarflokkuðum upplýsingum ESB í þjónustustofnunum og húsnæði aðildarríkjanna,

h) samræma öryggisráðstafanir í samstarfi við hlutaðeigandi bær stjórnvöld þeirra aðildarríkja sem ábyrg eru fyrir vernd trúnaðarflokkaðra upplýsinga og, eftir því sem við á, í þriðju ríkjum eða alþjóðastofnunum, meðal annars öryggisráðstafanir sem lúta að eðli þeirrar ógnar sem steðjar að öryggi trúnaðarflokkaðra upplýsinga ESB og leiðum til verndar gegn henni,

i. ganga frá stjórnsýslusamkomulagi þar er um getur í b-lið 2. mgr. 12. gr. og j) fara í upphafsmatsheimsóknir og reglubundnar matsheimsóknir til þriðju ríkja eða alþjóðastofnana til að fá fullvissu um skilvirkni þeirra ráðstafana sem beitt er til verndar trúnaðarflokkuðum upplýsingum ESB sem eru afhentar þessum aðilum eða sem skipst er á við þá.

Öryggisdeild aðalskrifstofu ráðsins skal vera aðalframkvæmdastjóranum til aðstoðar við að sinna þessum skyldum.

3. Aðildarríkjunum ber, í því skyni að hrinda ákvæðum 3. mgr. 14. gr. í framkvæmd:

a) að tilnefna stjórnvald á sviði þjóðaröryggis sem er ábyrgt fyrir öryggisfyrirkomulagi til verndar trúnaðarflokkuðum upplýsingum ESB til þess að:

i. trúnaðarflokkaðar upplýsingar ESB í vörslu innlendrar deildar, stofnunar eða embættis, sem er opinbert eða einkarekið, í heimalandi eða erlendis, séu verndaðar samkvæmt ákvæðum ákvörðunar þessarar,

ii. öryggisfyrirkomulag til verndar trúnaðarflokkuðum upplýsingum ESB sé undir reglubundnu eftirliti,

iii. allir einstaklingar, sem starfa hjá innlendri stjórnsýslu eða hjá verktaka sem kann að verða veittur aðgangur að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar, hafi viðeigandi öryggisvottun eða fái, með öðrum hætti, fullar heimildir með skírskotun til þess hlutverks sem þeir gegna, í samræmi við innlend lög og reglugerðir,

iv. öryggisáætlanir séu gerðar, eftir því sem nauðsyn krefur, í því skyni að lágmarka hættu á því að trúnaðarflokkuðum upplýsingum ESB sé stofnað í hættu eða á því að þær tapist,

v. öryggismál, sem varða vernd trúnaðarflokkaðra upplýsinga ESB, séu samræmd í samstarfi við önnur bær innlend stjórnvöldum, meðal annars þau sem um getur í ákvörðun þessari og vi) brugðist sé við viðeigandi beiðnum um öryggisvottun frá embættum og stofnunum ESB, sem stofnsett eru samkvæmt ákvæðum 2. kafla í V. bálki sáttmálans um Evrópusambandið sem, frá Evrópulögreglunni og Evrópsku réttaraðstoðinni, ennfremur frá aðstandendum hættustjórnunaraðgerða, sem stofnað er til samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, og frá sérstökum fulltrúum ESB (EUSR) og hópum þeirra.

Stjórnvöld á sviði þjóðaröryggis eru talin upp í viðbæti C,

b) að tryggja að bær yfirvöld þeirra veiti upplýsingar og ráðleggingar til ríkisstjórna sinna og í gegnum þær til ráðsins um eðli þeirrar ógnar sem steðjar að öryggi trúnaðarflokkaðra upplýsinga ESB leiðir til verndar gegn henni.

16. gr.

**Öryggisnefndin.**

1. Öryggisnefnd er hér með komið á fót. Hún skal skoða og meta öll öryggismál sem falla undir gildissvið ákvörðunar þessarar og beina tilmælum til ráðsins eftir því sem við á.

2. Öryggisnefndina skipa fulltrúar stjórnvalda aðildarríkjanna á sviði þjóðaröryggis með þátttöku eins fulltrúa framkvæmdastjórnarinnar og utanríkisþjónustu Evrópusambandsins. Aðalframkvæmdastjórinn eða tilnefndur fulltrúi hans skal gegna formennsku í nefndinni. Nefndin kemur saman samkvæmt fyrirmælum ráðsins eða að beiðni aðalframkvæmdastjórans eða stjórnvalds á sviði þjóðaröryggis.

Heimilt er að bjóða fulltrúum embætta og stofnana ESB, sem eru stofnsett samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, og fulltrúum Evrópulögreglunnar og Evrópsku réttaraðstoðarinnar að sitja fundi nefndarinnar þegar álitamál, sem varða þá aðila, eru rædd.

3. Öryggisnefndin skal skipuleggja starfsemi sína þannig að hún geti sett fram tilmæli um sértæk öryggissvið. Nefndin skal stofna undirhóp sérfræðinga um málefni upplýsingaöryggis og aðra undirhópa sérfræðinga eftir því sem nauðsyn krefur. Nefndin útbýr skipunarbréf fyrir slíka undirhópa sérfræðinga og tekur við skýrslum frá þeim um starfsemi þeirra, meðal annars og þegar það á við, öllum tilmæli sem er beint til ráðsins.

17. gr.

**Fyrri ákvörðun skipt út.**

1. Ákvörðun þessi ógildir og kemur í stað ákvörðunar ráðsins 2001/264/EB frá 19. mars 2001 um samþykkt öryggisreglna ráðsins ([[2]](#footnote-2)).

2. Allar trúnaðarflokkaðar upplýsingar ESB, sem eru flokkaðar í samræmi við ákvörðun 2001/264/EB, skal vernda áfram í samræmi við viðeigandi ákvæði ákvörðunar þessarar.

18. gr.

**Gildistaka.**

Ákvörðun þessi öðlast gildi á þeim degi sem hún birtist í Stjórnartíðindum Evrópusambandsins.

Gjört í Brussel 31. mars 2011.

*Fyrir hönd ráðsins,*

Völner P.

*forseti.*

VIÐAUKAR

I*.* VIÐAUKI

Öryggi með tilliti til starfsfólks.

II. VIÐAUKI

Hlutkennt öryggi.

III. VIÐAUKI

Umsjón með trúnaðarflokkuðum upplýsingum.

IV. VIÐAUKI

Vernd trúnaðarflokkaðra upplýsinga ESB sem meðhöndlaðar eru í upplýsingakerfum.

V. VIÐAUKI

Iðnaðaröryggi.

VI.VIÐAUKI

Skipti á trúnaðarflokkuðum upplýsingum við þriðju ríki og alþjóðastofnanir.

--------------------------------------------------

*I. VIÐAUKI*

**ÖRYGGI MEÐ TILLITI TIL STARFSFÓLKS**

I. INNGANGUR

1. Í viðauka þessum er kveðið á um framkvæmd efnisatriða 7. gr. Í viðaukanum er einkum mælt fyrir um viðmið vegna ákvörðunar um hvort heimila skuli einstaklingi, að teknu tilliti til hollustu hans, trúverðugleika og áreiðanleika, aðgang að trúnaðarflokkuðum upplýsingum ESB og um verklag við könnun og innan stjórnsýslunnar sem fylgja ber í því sambandi.

2. Hugtakið „öryggisvottun starfsfólks“ vísar í viðauka þessum til öryggisvottunar starfsfólks innanlands og/eða öryggisvottunar ESB fyrir starfsfólk, sbr. skilgreiningu í viðbæti A.

II. AÐGANGUR AÐ TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM ESB HEIMILAÐUR

3. Einungis skal heimila einstaklingi aðgang að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar eftir að:

a) vitneskjuþörf hans hefur verið ákvörðuð,

b) hann hefur hlotið öryggisvottun starfsfólks á viðeigandi stigi eða hefur á annan hátt fengið fullt umboð vegna starfssvið síns í samræmi við innlend lög og reglugerðir og c) hann hefur verið upplýstur um öryggisreglur og verklag vegna verndar trúnaðarflokkaðra upplýsinga ESB og hefur gengist við ábyrgð sinni að því er varðar vernd slíkra upplýsinga.

4. Sérhvert aðildarríki og aðalskrifstofa ráðsins skulu auðkenna þær stöður í skipulagi sínu sem krefjast aðgangs að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar og krefjast því öryggisvottunar starfsfólks á viðeigandi stigi.

III. KRÖFUR VEGNA ÖRYGGISVOTTUNAR STARFSFÓLKS

5. Eftir að hafa móttekið beiðni frá til þess bærum aðila er stjórnvald á sviði þjóðaröryggis eða önnur til þess bær landsyfirvöld ábyrg fyrir því að tryggja að bakgrunnsskoðanir fari fram á þeim ríkisborgurum þeirra sem þurfa aðgang að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar. Viðmiðunarreglur um bakgrunnsskoðun skulu vera í samræmi við innlend lög og reglugerðir.

6. Hafi viðkomandi einstaklingur búsetu á yfirráðasvæði annars aðildarríkis eða þriðja ríkis skulu bær landsyfirvöld óska aðstoðar frá bæru stjórnvaldi í búseturíkinu í samræmi við innlend lög og reglugerðir. Aðildarríkin skulu aðstoða hvert annað við framkvæmd bakgrunnsskoðana í samræmi við innlend lög og reglugerðir.

7. Bær stjórnvöld á sviði þjóðaröryggis eða önnur innlend stjórnvöld geta, sé slíkt heimilt samkvæmt innlendum lögum og reglugerðum, gert bakgrunnsskoðun á erlendum ríkisborgurum sem þurfa aðgang að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar. Viðmiðunarreglur fyrir bakgrunnsskoðun skulu vera í samræmi við innlend lög og reglugerðir.

**Viðmið fyrir bakgrunnsskoðun.**

8. Taka skal ákvörðun um hollustu, trúverðugleika og áreiðanleika einstaklings, til þess að veita megi honum öryggisvottun starfsfólks vegna aðgangs að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar, með því að framkvæma bakgrunnsskoðun. Bært landsyfirvald skal vinna heildarmat byggt á niðurstöðum slíkrar bakgrunnsskoðunar. Engin ein neikvæð niðurstaða skal nauðsynlega teljast ástæða synjunar um öryggisvottun starfsfólks. Þær grunnviðmiðanir sem styðjast ber við hvað það varðar ættu m.a. að vera, að því marki sem innlend lög og reglugerðir heimila, rannsókn á því hvort viðkomandi einstaklingur:

a) hefur stundað eða gert tilraun til að stunda, lagt á ráðin með öðrum eða aðstoðað og hvatt annan til að stunda hvers kyns njósnir, hryðjuverastarfsemi, skemmdarverk, landráð eða uppreisnaráróður,

b) er, eða hefur verið, samstarfsmaður njósnara, hryðjuverkamanna, skemmdarverkamanna eða einstaklinga, sem af gildri ástæðu eru grunaðir um slíkt athæfi, eða samstarfsmaður fulltrúa skipulagsheilda eða erlendra ríkja, þ.m.t. erlendar leyniþjónustur, sem gæti ógnað öryggi ESB og/eða aðildarríkja, nema fyrrnefnd samtök hafi haft tilteknar heimildir meðan á opinberum skyldustörfum stóð,

c) er, eða hefur verið, meðlimur hvaða skipulagsheildar sem er sem með ofbeldisaðgerðum, niðurrifsstarfsemi eða öðrum ólöglegum aðferðum reynir, meðal annars, að steypa ríkisstjórn aðildarríkis, breyta stjórnskipan aðildarríkis eða breyta formgerð eða stefnu ríkisstjórnar þess,

d) er, eða hefur verið, stuðningsmaður einhverrar þeirrar skipulagsheildar sem er lýst í c-lið eða hefur haft náin tengsl við meðlimi slíkra skipulagsheilda,

e) hefur að yfirlögðu ráði haldið eftir, rangfært eða falsað mikilvægar upplýsingar, einkum um öryggismál, eða hefur að yfirlögðu ráði farið með ósannindi við útfyllingu spurningalista um öryggi með tilliti til starfsfólks eða meðan á viðtali um öryggismál stóð,

f) hefur verið dæmdur fyrir hegningarlagabrot, eitt eða fleiri,

g) á að baki sögu um að vera háður áfengi, að hafa notað ólögleg lyf og/eða misnotað lögleg lyf,

h) er, eða hefur verið, þátttakandi í athæfi sem kann að valda hættu á að viðkomandi sé berskjaldaður gagnvart fjárkúgun eða þrýstingi,

i) hafi með gerðum sínum eða í töluðu máli sýnt af sér óheiðarleika, óhollustu, óáreiðanleika eða ótrygglyndi,

j) hafi alvarlega eða endurtekið brotið öryggisreglur eða hafi gert tilraun til eða tekist að drýgja óleyfilegan verknað í tengslum við samskipta- og upplýsingakerfi,

k) gæti verið líklegur til að verða fyrir þrýstingi (t.d. með því að hafa eitt ríkisfang eða fleiri utan ESB eða þrýstingi af hálfu skyldmenna eða náinna samstarfsmanna sem gætu verið berskjaldaðir gagnvart erlendum leyniþjónustum, hryðjuverkahópum eða öðrum niðurrifssamtökum eða einstaklingum með stefnumál sem kunna að ógna öryggishagsmunum ESB og/eða aðildarríkja).

9. Fjárhagslegur bakgrunnur og sjúkrasaga geta einnig talist skipta máli meðan á bakgrunnsskoðun stendur, eftir því sem við á og í samræmi við innlend lög og reglugerðir.

10. Skapgerð, hegðun og aðstæður maka, sambýlings eða náins aðstandanda geta einnig talist skipta máli meðan á bakgrunnsskoðun stendur, eftir því sem við á og í samræmi við innlend lög og reglugerðir.

**Rannsóknarkröfur vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB.**

*Fyrsta öryggisvottun starfsfólks.*

11. Fyrsta öryggisvottun starfsfólks vegna aðgangs að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB og LEYNDARMÁL ESB skal byggð á bakgrunnsskoðun sem nær til síðustu 5 ára eða spannar tímabilið frá 18 ára aldri fram til líðandi stundar, eftir því hvort tímabilið er styttra, og skal skoðunin taka til eftirtalinna þátta:

a) frágangs innlends spurningalista vegna öryggis með tilliti til starfsfólks fyrir það stig trúnaðarflokkaðra upplýsinga ESB sem viðkomandi einstaklingur kann að þurfa aðgang að; eftir frágang spurningalistans skal senda hann bæru öryggisyfirvaldi,

b) könnunar á því hver viðkomandi er, hvert ríkisfang hans/hennar er og þjóðerni — sannprófunar á fæðingardegi og fæðingarstað og um hvaða einstakling er að ræða. Ganga skal úr skugga um hvert ríkisfang viðkomandi einstaklings er og/eða þjóðerni, fyrr og nú; í því felst mat á því hvort viðkomandi sé berskjaldaður gagnvart þrýstingi frá erlendum aðilum, t.d. vegna fyrri búsetu eða fyrri tengsla og

c) athugunar á skýrslum á lands- og staðarvísu — upplýsinga úr skýrslum um þjóðaröryggi og miðlægum sakaskrám, ef þær síðarnefndu fyrirfinnast og/eða athugunar á öðrum sambærilegum skrám stjórnvalda og lögreglu. Kanna ber skrár embætta sem framfylgja lögum og hafa lögsögu þar sem viðkomandi einstaklingur hefur haft búsetu eða starfað.

12. Upphafleg veiting öryggisvottunar starfsfólks vegna aðgangs að upplýsingum á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB skal byggð á bakgrunnsskoðun sem nær til síðustu 10 ára eða spannar tímabilið frá 18 ára aldri fram til líðandi stundar, eftir því hvort tímabilið er styttra. Ef viðtöl fara fram sbr. e-lið skal bakgrunnsskoðun taka að minnsta kosti til síðustu 7 ára, eða spanna tímabilið frá 18 ára aldri fram til líðandi stundar, eftir því hvort tímabilið er styttra. Auk þeirra viðmiða sem bent er á í 8. mgr. hér að framan skal skoða eftirtalda þætti, að því marki sem innlend lög og reglugerðir heimila, áður en veitt er öryggisvottun starfsfólks fyrir trúnaðarstigið ALGJÖRT LEYNDARMÁL ESB; einnig má rannsaka þessa þætti áður en veitt er öryggisvottun starfsfólks fyrir trúnaðarstigin TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB, þar sem þess er krafist samkvæmt innlendum lögum og reglugerðum:

a) fjárhagsstaða — afla skal upplýsinga um fjármál viðkomandi einstaklings til þess að meta hvort hann sé berskjaldaður gagnvart þrýstingi erlendis frá eða innanlands vegna alvarlegra fjárhagserfiðleika, eða til þess að greina óútskýrða auðlegð,

b) menntun — afla skal upplýsinga til þess að sannreyna menntunarbakgrunn viðkomandi einstaklings í skólum, háskólum og öðrum menntastofnunum sem hann hefur gengið í frá 18 ára aldri eða yfir tímabil sem viðkomandi skoðunaryfirvald telur við eiga,

c) starfsreynsla — afla skal upplýsinga um núverandi starf og fyrri störf, þar sem vísað er til heimilda eins og starfsferilsskráa, skýrslna um árangur eða dugnað í starfi og til vinnuveitenda eða yfirmanna,

d) herþjónusta — þar sem það á við, sannreyna skal þá þjónustu sem viðkomandi einstaklingur gegndi í hernum og með hvaða hætti hann var leystur undan herþjónustu og e) viðtöl — sé kveðið á um og séu þau heimil samkvæmt innlendum lögum, taka skal viðtal eða viðtöl við viðkomandi einstakling. Þá skal taka viðtöl við einstaklinga sem eru í stöðu til þess að leggja óhlutdrægt mat á bakgrunn viðkomandi einstaklings, athafnir hans, hollustu, trúverðugleika og áreiðanleika. Sé venja innanlands að viðfang bakgrunnsskoðunar afhendi meðmæli skal kalla þann er þau gefur til viðtals, nema gild ástæða sé til að láta það ógert.

13. Heimilt er að fram fari viðbótarskoðun, ef nauðsyn krefur, í samræmi við innlend lög og reglugerðir til að leiða í ljós allar tiltækar upplýsingar um einstakling sem skipta máli og að færa sönnur á eða hrekja neikvæðar upplýsingar.

*Endurnýjun öryggisvottunar starfsfólks.*

14. Eftir að öryggisvottun starfsfólks er veitt í fyrsta sinn og að því tilskildu að viðkomandi einstaklingur hafi starfað óslitið hjá innlendu stjórnvaldi eða á aðalskrifstofu ráðsins og þurfi áframhaldandi aðgang að trúnaðarflokkuðum upplýsingum ESB, skal endurskoða öryggisvottun starfsfólks fyrir hann til endurnýjunar með minnst 5 ára millibili vegna vottunar fyrir ALGJÖRT LEYNDARMÁL ESB og minnst 10 ára millibili vegna vottunar fyrir LEYNDARMÁL ESB og TRÚNAÐARMÁL ESB, sem reiknast frá þeim degi þegar tilkynnt var um niðurstöðu síðustu bakgrunnsskoðunar sem öryggisvottun starfsfólks byggðist á. Allar bakgrunnsskoðanir vegna endurnýjunar öryggisvottunar starfsfólks skulu spanna tímabilið frá því að síðasta skoðun fór fram.

15. Skoða skal þá þætti sem eru tilgreindir í 11. og 12. mgr. vegna endurnýjunar á öryggisvottun starfsfólks.

16. Leggja skal fram beiðnir um endurnýjun tímanlega, að teknu tilliti til þess tíma sem bakgrunnsskoðanir krefjast. Engu að síður getur bært stjórnvald, hafi viðkomandi stjórnvald á sviði þjóðaröryggis eða annað bært innlent stjórnvald móttekið viðeigandi beiðni um endurnýjun og tilsvarandi spurningalista um öryggi með tilliti til starfsfólks áður en öryggisvottun starfsfólks er útrunnin og nauðsynlegri bakgrunnsskoðun er ekki lokið, framlengt gildistíma gildandi öryggisvottunar starfsfólks um allt að 12 mánuði, ef slíkt er heimilt samkvæmt innlendum lögum og reglugerðum. Sé bakgrunnsskoðun enn ekki lokið að loknu þessu 12 mánaða tímabili skal fela viðkomandi einstaklingi störf þar sem öryggisvottunar starfsfólks er ekki krafist.

*Verklag við öryggisvottun starfsfólks innan aðalskrifstofu ráðsins.*

17. Stjórnvald aðalskrifstofu ráðsins á sviði öryggismála skal áframsenda fullgerðan spurningalista um öryggi með tilliti til starfsfólks vegna embættismanna og annarra starfsmanna aðalskrifstofu ráðsins til bærs stjórnvalds á sviði þjóðaröryggis þess aðildarríkis þar sem viðkomandi einstaklingur er ríkisborgari og óska eftir að bakgrunnsskoðun verði gerð fyrir það stig trúnaðarflokkaðra upplýsinga ESB sem fyrrnefndur einstaklingur mun þurfa aðgang á.

18. Þegar aðalskrifstofa ráðsins fær í hendur upplýsingar viðvíkjandi bakgrunsskoðun sem varða einstakling, sem hefur sótt um öryggisvottun starfsfólks ESB, skal aðalskrifstofa ráðsins tilkynna viðkomandi bæru stjórnvaldi á sviði þjóðaröryggis um það í samræmi við viðeigandi reglur og reglugerðir.

19. Að lokinni bakgrunnsskoðun skal viðkomandi bært stjórnvald á sviði þjóðaröryggis tilkynna öryggisyfirvaldi aðalskrifstofu ráðsins um niðurstöðu slíkrar skoðunar og nota staðlað eyðublað fyrir slík bréfaskipti sem öryggisnefndin mælir fyrir um.

a) Leiði niðurstöður bakgrunnsskoðunarinnar til fullvissu um að ekki sé vitað um neitt neikvætt sem myndi gefa tilefni til efasemda um hollustu, trúverðugleika og áreiðanleika viðkomandi einstaklings getur ráðningaryfirvald aðalskrifstofu ráðsins veitt viðkomandi einstaklingi öryggisvottun starfsfólks ESB og heimilað aðgang að trúnaðarflokkuðum upplýsingum ESB upp að viðeigandi trúnaðarstigi fram að tilgreindri dagsetningu.

b) Leiði niðurstöður bakgrunnsskoðunarinnar ekki til slíkrar fullvissu skal ráðningaryfirvald aðalskrifstofu ráðsins tilkynna það viðkomandi einstaklingi sem getur óskað eftir áheyrn hjá fyrrnefndu ráðningaryfirvaldi. Ráðningaryfirvaldið getur beðið bært stjórnvald á sviði þjóðaröryggis um allar frekari skýringar sem það getur veitt í samræmi við innlend lög og reglugerðir. Séu fyrrnefndar niðurstöður staðfestar skal ekki veita viðkomandi öryggisvottun ESB fyrir starfsfólk.

20. Viðeigandi lög og reglugerðir, sem gilda í viðkomandi aðildarríki, einnig þau sem fjalla um áfrýjun, skulu taka til bakgrunnsskoðunarinnar og þeirra niðurstaðna sem fást. Ákvörðunum ráðningaryfirvalds aðalskrifstofu ráðsins má áfrýja samkvæmt starfsmannareglum sem gilda um embættismenn Evrópusambandsins og ráðningarskilmálum sem varða aðra starfsmenn Evrópusambandsins, sem mælt er fyrir um í reglugerð (EBE, KBE, KSE) nr. 259/68 ([[3]](#footnote-3)) (hér á eftir nefnd „starfsmannareglurnar og ráðningarskilmálar“).

21. Sú fullvissa sem öryggisvottun ESB fyrir starfsfólks er byggð á, að því gefnu að hún haldi gildi sínu, skal ná til allra verkefna sem viðkomandi einstaklingi eru falin á aðalskrifstofu ráðsins eða hjá framkvæmdastjórninni.

22. Ef starfstími einstaklings byrjar ekki innan 12 mánaða frá því að ráðningaryfirvaldi aðalskrifstofu ráðsins er tilkynnt um niðurstöðu bakgrunnsskoðunarinnar, eða verði 12 mánaða hlé á störfum einstaklings, og starfi hann ekki á þeim tíma hjá aðalskrifstofu ráðsins eða gegni starfi hjá landsbundnu stjórnvaldi aðildarríkis, skal niðurstöðunni vísað til viðkomandi bærs stjórnvalds á sviði þjóðaröryggis því til staðfestingar að hún haldi gildi sínu og sé viðeigandi.

23. Fái aðalskrifstofa ráðsins vitneskju um upplýsingar þess efnis að hætta sé á að einstaklingur, sem hefur gilda öryggisvottun ESB fyrir starfsfólk, stofni öryggi í hættu skal aðalskrifstofa ráðsins tilkynna viðkomandi bæru stjórnvaldi á sviði þjóðaröryggis um það samkvæmt viðeigandi reglum og reglugerðum. Tilkynni stjórnvald á sviði þjóðaröryggis aðalskrifstofu ráðsins að sú fullvissa sem er veitt skv. a-lið 19. mgr. í tengslum við einstakling, sem hefur gilda öryggisvottun ESB fyrir starfsfólk, eigi ekki lengur við, getur ráðningaryfirvald aðalskrifstofu ráðsins beðið um hverja þá skýringu sem viðkomandi stjórnvald á sviði þjóðaröryggis getur veitt samkvæmt innlendum lögum og reglugerðum. Ef neikvæðar upplýsingar eru staðfestar skal afturkalla öryggisvottun ESB fyrir starfsfólk og loka fyrir aðgang viðkomandi einstaklings að trúnaðarflokkuðum upplýsingum ESB og útiloka hann frá störfum sem gera slíkan aðgang mögulegan eða þar sem hann gæti skapað hættu á öryggisbresti.

24. Sérhverja ákvörðun þess efnis að svipta embættismann aðalskrifstofu ráðsins eða annan starfsmann öryggisvottun ESB fyrir starfsfólk skal tilkynna hlutaðeigandi einstaklingi, og ástæður fyrir þeim gjörningi ef við á, sem getur óskað eftir áheyrn hjá ráðningaryfirvaldinu. Upplýsingar, sem stjórnvald á sviði þjóðaröryggis lætur í té, eru með fyrirvara um viðeigandi lög og reglugerðir sem gilda í hlutaðeigandi aðildarríki, einnig þau sem gilda um áfrýjun. Ákvörðunum ráðningaryfirvalds aðalskrifstofu ráðsins má áfrýja í samræmi við starfsmannareglurnar og ráðningarskilmála.

25. Innlendir sérfræðingar, sem kallaðir eru til að gegna stöðu á aðalskrifstofu ráðsins sem krefst öryggisvottunar ESB fyrir starfsfólk, skulu leggja fram hjá öryggisyfirvaldi aðalskrifstofu ráðsins gilda innlenda öryggisvottun starfsfólks, sem heimilar aðgang að trúnaðarflokkuðum upplýsingum ESB, áður en þeir hefja störf.

*Skrár yfir öryggisvottun starfsfólks.*

26. Halda skal skrá yfir innlenda öryggisvottun starfsfólks og öryggisvottun ESB fyrir starfsfólk sem veitt er vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB, annars vegar hjá sérhverju aðildarríki og hins vegar hjá aðalskrifstofu ráðsins. Þessar skrár skulu innihalda að lágmarki það stig trúnaðarflokkaðra upplýsinga ESB sem viðkomandi einstaklingi er veittur aðgangur að (TRÚNAÐARMÁL ESB eða ofar), dagsetningu öryggisvottunar starfsfólks og gildistíma.

27. Bært öryggisyfirvald getur gefið út vottorð um öryggisvottun starfsfólks (PSCC) sem sýnir það stig trúnaðarflokkaðra upplýsinga ESB sem heimilt er að veita viðkomandi einstaklingi aðgang á (TRÚNAÐARMÁL ESB eða ofar), gildistökudag viðeigandi innlendrar öryggisvottunar starfsfólks vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB eða gildistökudag öryggisvottunar ESB fyrir starfsfólk og þann dag þegar gildistími sjálfs vottorðsins rennur út.

**Undanþágur frá kröfunni um öryggisvottun starfsfólks.**

28. Aðgangur einstaklinga í aðildarríkjum, sem hafa fulla heimild vegna starfa sinna, að trúnaðarupplýsingum ESB skal ákveðinn í samræmi við innlend lög og reglugerðir. Veita ber þeim einstaklingum leiðbeiningar um öryggisskyldur sínar með tilliti til þess að vernda trúnaðarflokkaðar upplýsingar ESB.

IV. MENNTUN OG VITUND Á SVIÐI ÖRYGGISMÁLA

29. Allir einstaklingar, sem veitt hefur verið öryggisvottun starfsfólks, skulu staðfesta skriflega að þeir hafi skilið skuldbindingar sínar með tilliti til þess að vernda trúnaðarflokkaðar upplýsingar ESB og afleiðingar þess ef slakað er á gerðum kröfum vegna trúnaðarflokkaðra upplýsinga ESB. Aðildarríkin og aðalskrifstofa ráðsins skulu, eftir því sem við á, halda skrá yfir slíkar skriflegar staðfestingar.

30. Öllum einstaklingum, sem heimilaður hefur verið aðgangur að eða þurfa að meðhöndla trúnaðarflokkaðar upplýsingar ESB, skal í upphafi gerð grein fyrir og leiðbeint reglulega um ógn við öryggi og er þeim skylt að tilkynna viðkomandi öryggisyfirvöldum án tafar um sérhverja aðkomu eða aðgerð sem þeir telja grunsamlega eða óvenjulega.

31. Öllum einstaklingum, sem hætta í starfi sem krefst aðgangs að trúnaðarflokkuðum upplýsingum ESB, skal gerð grein fyrir skuldbindingum sínum með tilliti til áframhaldandi verndar trúnaðarflokkaðra upplýsinga ESB og skulu, eftir því sem við á, staðfesta þær skriflega.

V. SÉRSTAKAR AÐSTÆÐUR

32. Heimili innlend lög og reglugerðir slíkt getur öryggisvottun starfsfólks, sem bært landsyfirvald aðildarríkis veitir vegna aðgangs að innlendum trúnaðarflokkuðum upplýsingum, heimilað, tímabundið og meðan þess er beðið að veitt sé innlend öryggisvottun starfsfólks vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB, innlendum embættismönnum aðgang að trúnaðarflokkuðum upplýsingum ESB upp að jafngildu stigi og tilgreint er í samsvörunartöflunni í viðbæti B, þegar slíkur tímabundinn aðgangur er nauðsynlegur í þágu ESB. Stjórnvöld á sviði þjóðaröryggis skulu upplýsa öryggisnefndina um það ef innlend lög og reglugerðir heimila ekki slíkan tímabundinn aðgang að trúnaðarflokkuðum upplýsingum ESB.

33. Ráðningaryfirvaldi aðalskrifstofu ráðsins er heimilt, beri brýna nauðsyn til og sé slíkt fullkomlega réttlætanlegt vegna þjónustuhagsmuna og meðan þess er beðið að lokið sé fullri bakgrunnsskoðun og að höfðu samráði við hlutaðeigandi stjórnvald á sviði þjóðaröryggis í því aðildarríki þar sem viðkomandi einstaklingur er ríkisborgari og með fyrirvara um niðurstöðu undanfarandi athuguna því til staðfestingar að ekki sé vitað um neinar neikvæðar upplýsingar, að veita embættismönnum aðalskrifstofu ráðsins og öðrum starfsmönnum tímabundna heimild til að ganga að trúnaðarflokkuðum upplýsingum ESB vegna sérstaks verkefnis. Slíkar tímabundnar heimildir skulu ekki gilda lengur en í 6 mánuði og skulu ekki veita aðgang að upplýsingum á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB. Allir einstaklingar, sem hafa fengið tímabundna heimild, skulu staðfesta skriflega að þeir hafa skilið skuldbindingar sínar með tilliti til þess að vernda trúnaðarflokkaðar upplýsingar ESB og afleiðingar þess að stofna trúnaðarflokkuðum upplýsingum ESB í hættu. Aðalskrifstofa ráðsins skal halda skrá yfir slíkar skriflegar staðfestingar.

34. Eigi að skipa einstakling í stöðu sem krefst öryggisvottunar starfsfólks einu stigi ofar þeirri sem hann hefur fyrir, getur skipunin verið til bráðabirgða að því tilskildu að:

a) yfirmaður viðkomandi einstaklings færi skrifleg rök fyrir brýnni þörf á að fyrrnefndum einstaklingi sé veittur aðgangur að trúnaðarflokkuðum upplýsingum ESB á hærra stigi,

b) aðgangur sé takmarkaður við sérstaka þætti trúnaðarflokkaðra upplýsinga ESB til notkunar við lausn viðkomandi verkefnis,

c) viðkomandi einstaklingur hafi gilda innlenda öryggisvottun starfsfólks eða öryggisvottun ESB fyrir starfsfólk,

d) vinna sé hafin við að afla heimildar fyrir það aðgangsstig sem staðan krefst,

e) bær stjórnvöld hafi gert fullnægjandi athuganir á því að viðkomandi einstaklingur hafi ekki gerst sekur um alvarleg eða endurtekin brot á öryggisreglum,

f) bært stjórnvald hafi samþykkt verkefni viðkomandi einstaklings og g) að sú skráningarstofa eða undirskráningarstofa sem er ábyrg skrái undanþáguna, m.a. lýsingu á þeim upplýsingum sem aðgangur var heimilaður að.

35. Nota ber það verklag sem lýst er hér að framan þegar um ræðir aðgang í eitt skipti að trúnaðarflokkuðum upplýsingum ESB einu stigi ofar en það sem viðkomandi einstaklingur hefur verið fengið öryggisvottun fyrir. Ekki skal grípa ítrekað til þessa verklags.

36. Aðildarríki og aðalframkvæmdastjórinn geta veitt, skriflega ef þess er kostur, einstaklingum, sem hafa ekki tilskilda öryggisvottun starfsfólks, aðgang að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB í mjög sérstökum undantekningartilvikum, t.d. í sendiferðum í fjandsamlegu umhverfi eða á tímum vaxandi alþjóðlegrar spennu þegar neyðarráðstafanir krefjast þess, einkum í því skyni að bjarga mannslífum, að því tilskildu að slík heimild sé algerlega nauðsynleg og að engin réttmæt ástæða sé til að draga hollustu, trúverðugleika og áreiðanleika viðkomandi einstaklings í efa. Halda skal skrá yfir slíka heimild sem lýsir þeim upplýsingum sem aðgangur var samþykktur að.

37. Þegar um ræðir upplýsingar á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB, skal takmarka þennan neyðaraðgang við þá ríkisborgara ESB sem hefur verið heimilaður aðgangur, annaðhvort að innlendu ígildi ALGJÖRS LEYNDARMÁLS ESB eða að upplýsingum á trúnaðarstiginu LEYNDARMÁL ESB.

38. Tilkynna ber öryggisnefndinni um þau tilfelli þegar gripið er til þess verklags sem um getur í 36. og 37. mgr.

39. Kveði innlend lög og reglugerðir aðildarríkjanna á um strangari reglur um tímabundnar heimildir, bráðabirgðaverkefni, aðgang í eitt skipti eða neyðaraðgang fyrir einstaklinga að trúnaðarflokkuðum upplýsingum, skulu þær verklagsreglur sem gert er ráð fyrir samkvæmt þessum hluta einungis koma til framkvæmda með þeim takmörkunum sem mælt er fyrir um í viðeigandi innlendum lögum og reglugerðum.

40. Öryggisnefndin skal fá í hendur ársskýrslu um þau tilvik þegar gripið er til þeirra verklagsreglna sem mælt er fyrir um í þessum hluta.

VI. ÞÁTTTAKA Í FUNDUM RÁÐSINS

41. Einstaklingar, sem eru tilnefndir til setu á fundum ráðsins eða stofnana þess sem annast undirbúning þar sem ræddar eru upplýsingar á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar, geta, með fyrirvara um ákvæði 28. mgr., einungis gert það að fenginni staðfestingu á stöðu öryggisvottunar viðkomandi einstaklings. Hlutaðeigandi stjórnvöld skulu senda öryggisdeild aðalskrifstofu ráðsins staðfestingu vottorðs um öryggisvottun starfsfólks eða aðra staðfestingu á öryggisvottun starfsfólks vegna fulltrúanna eða viðkomandi fulltrúi leggi slíka staðfestingu fram sjálfur í undantekningartilvikum. Eftir atvikum er heimilt að notast við sameiginlegan lista yfir nöfn, þar sem fram kemur viðeigandi staðfesting á öryggisvottun starfsfólks.

42. Hlutaðeigandi bært stjórnvald skal upplýsa aðalskrifstofu ráðsins þegar innlend öryggisvottun starfsfólks vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB er afturkölluð af öryggisástæðum í tilviki einstaklings sem ber að sitja fundi ráðsins eða stofnana þess sem annast undirbúning.

VII. HUGSANLEGUR AÐGANGUR AÐ TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM ESB

43. Þegar einstaklingar eiga að starfa í aðstæðum þar sem þeir geta hugsanlega haft aðgang að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða ofar skulu þeir fá viðeigandi öryggisvottun eða einatt fylgd.

44. Boðberar, verðir og fylgdarmenn skulu fá öryggisvottun á viðeigandi stigi eða vera öðruvísi skoðaðir með viðeigandi hætti í samræmi við innlend lög og reglugerðir, þeim skal leiðbeint um öryggisverklag til verndar trúnaðarflokkuðum upplýsingum ESB og skulu fá fræðslu um þær skyldur sem á þeim hvíla, þ.e. að vernda þær upplýsingar sem þeim er treyst fyrir.

*II. VIÐAUKI*

**HLUTKENNT ÖRYGGI**

I. INNGANGUR

1. Í viðauka þessum er kveðið á um framkvæmd efnisatriða 8. gr. Mælt er fyrir um lágmarkskröfur um hlutkennda vernd húsnæðis, bygginga, skrifstofa, rýma og annarra svæða þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar og geymdar, þ.m.t. svæði sem hýsa samskipta- og upplýsingakerfi.

2. Ráðstafanir vegna hlutkennds öryggis skulu miða að því að koma í veg fyrir óheimilan aðgang að trúnaðarflokkuðum upplýsingum ESB með því að:

a) tryggja að trúnaðarflokkaðar upplýsingar ESB séu meðhöndlaðar og geymdar á viðeigandi hátt,

b) gera ráð fyrir aðgreiningu starfsfólks með tilliti til aðgangs að trúnaðarflokkuðum upplýsingum ESB á grundvelli vitneskjuþarfar og, þar sem það á við, öryggisvottunar þeirra,

c) fyrirbyggja, hindra og koma upp um óleyfilegar aðgerðir og d) meina óviðkomandi aðila aðgang í laumi eða með innbroti.

II. KRÖFUR OG RÁÐSTAFANIR VEGNA HLUTKENNDS ÖRYGGIS.

3. Velja ber ráðstafanir vegna hlutkennds öryggis á grundvelli hættumats sem til þess bær stjórnvöld gera. Aðalskrifstofa ráðsins og aðildarríkin skulu hvort um sig nýta sér áhættustjórnunarferli til þess að vernda trúnaðarflokkaðar upplýsingar ESB í húsnæði sínu til þess að tryggt sé að notað sé stig hlutkenndrar verndar sem svarar til þeirrar áhættu sem metin hefur verið. Áhættustjórnunarferlið skal miðað við alla þætti sem máli skipta, einkum:

a) stig trúnaðarflokkaðra upplýsinga ESB,

b) form og magn trúnaðarflokkaðra upplýsinga ESB, með það í huga að mikið magn eða stórt safn trúnaðarflokkaðra upplýsinga ESB geti kallað á að strangari verndarráðstöfunum sé beitt,

c) nánasta umhverfi og skipulag þeirra bygginga eða svæða sem hýsa trúnaðarflokkaðar upplýsingar ESB og d) mat á ógn sem stafar af leyniþjónustum sem beita sér gegn Evrópusambandinu eða aðildarríkjum og af skemmdarverkum, hryðjuverkastarfsemi, niðurrifsstarfsemi eða annarri glæpastarfsemi.

4. Bært öryggisyfirvald ákveður, með því að beita hugtakinu lagskiptar varnir, rétta samsetningu ráðstafana vegna hlutkennds öryggis sem gera skal. Þær geta verið fólgnar í eftirfarandi þáttum, einum eða fleiri:

a) aflokun svæðis: hlutkennd aflokun sem ver mörk svæðis sem krefst verndar,

b) ágangsskynjunarkerfi: nota má ágangsskynjunarkerfi til að auka það öryggi sem aflokun svæðis veitir eða í rýmum og byggingum í stað öryggisvarða eða þeim til hjálpar.

c) aðgangsstýringu: beita má aðgangsstýringu við lóð, byggingu eða byggingar á lóð eða svæðum eða í tengslum við rými inni í byggingu. Framkvæma má aðgangsstýringu með rafeindatækni eða eftir rafvélrænum leiðum, með aðgerðum öryggisvarða og/eða móttökustjóra eða með öðrum hlutkenndum hætti.

d) öryggisvörðum: heimilt er að ráða til starfa öryggisverði, sem eru þjálfaðir, undir eftirliti og, ef nauðsyn krefur, hafa viðeigandi öryggisvottun, meðal annars til að standa gegn einstaklingum sem leggja á ráðin um leynilegan ágang,

e) lokuðu sjónvarpskerfi (CCTV): öryggisvörðum er heimilt að nota lokað sjónvarpskerfi til þess að sannreyna atvik og viðvaranir frá ágangsskynjunarkerfi á stórum lóðum eða svæðismörkum,

f) öryggisljósabúnaði: heimilt er að nota öryggisljósabúnað til þess að standa gegn óviðkomandi einstaklingi og skapa nauðsynlega lýsingu fyrir öryggisverði að sinna skilvirku eftirliti beint eða til þess að slíkt eftirlit geti farið fram óbeint með lokuðu sjónvarpskerfi,

g) hvaða öðrum viðeigandi hlutkenndum ráðstöfunum sem er til þess að fyrirbyggja eða koma upp um óheimilan aðgang eða koma í veg fyrir að trúnaðarflokkaðar upplýsingar ESB tapist eða skemmist.

5. Heimila má til þess bæru stjórnvaldi að gera leit við inngang og útgang því til varnar að komið sé inn með óleyfilegt efni eða að trúnaðarflokkaðar upplýsingar ESB séu fjarlægðar úr húsnæði eða byggingum með óleyfilegum hætti.

6. Þegar hætta er á að trúnaðarflokkaðar upplýsingar ESB séu sýnilegar, jafnvel af slysni, skal grípa til viðeigandi ráðstafana til að bregðast við þeirri hættu.

7. Þegar um ræðir nýja aðstöðu skal skilgreina kröfur um hlutkennt öryggi og virkniforskriftir þeirra sem hluta af skipulagi og hönnun aðstöðunnar. Þegar um ræðir þá aðstöðu sem fyrir er skal fullnægja kröfum um hlutkennt öryggi eins og frekast er unnt.

III. BÚNAÐUR FYRIR HLUTKENNDA VERND TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB.

8. Bært öryggisyfirvald skal tryggja, þegar aflað er búnaðar (t.d. öryggisgáma, tætara, hurðarlæsinga, rafrænna aðgangsstýrikerfa, ágangsskynjunarkerfa, viðvörunarkerfa) fyrir hlutkennda vernd trúnaðarflokkaðra upplýsinga ESB, að búnaðurinn uppfylli samþykkta tæknistaðla og lágmarkskröfur.

9. Tækniforskrift búnaðar sem er notaður við hlutkennda vernd trúnaðarflokkaðra upplýsinga ESB skal sett fram í öryggisleiðbeiningum sem öryggisnefndin skal samþykkja.

10. Reglulegt eftirlit skal fara fram með öryggiskerfum og reglulegt viðhald á búnaði. Í viðhaldi skal taka mið af niðurstöðu eftirlits til þess að tryggt sé að búnaðurinn virki áfram með hámarksafköstum.

11. Í hvert sinn sem eftirlit fer fram skal endurmeta virkni einstakra öryggisráðstafana og öryggiskerfisins í heild.

IV. SVÆÐI VERNDUÐ MEÐ HLUTKENNDUM HÆTTI

12. Koma skal upp tvenns konar svæðum, sem eru vernduð með hlutkenndum hætti, eða innlendu jafngildi þeirra, vegna hlutkenndrar verndar trúnaðarflokkaðra upplýsinga ESB:

a) stjórnsýslusvæðum og b) öryggissvæðum (þ.m.t. tæknileg öryggissvæði).

Allar vísanir til stjórnsýslusvæða og öryggissvæða, þ.m.t. tæknileg öryggissvæði, í ákvörðun þessari skal túlka þannig að vísi einnig til innlends jafngildis þeirra.

13. Viðkomandi bært öryggisyfirvald skal staðfesta að svæði uppfylli kröfur til þess að verða auðkennt sem stjórnsýslusvæði, öryggissvæði eða tæknilegt öryggissvæði.

14. Að því er stjórnsýslusvæði varðar:

a) skal komið upp sýnilega afmörkuðu svæði sem gerir kleift að hafa eftirlit með einstaklingum og, þar sem því verður komið við, farartækjum.

b) skulu einungis einstaklingar, sem hafa fullt leyfi viðkomandi bærs stjórnvalds, fá aðgang án fylgdar og c) skal öllum öðrum einstaklingum ávallt fylgt eða þeir vera háðir sambærilegu eftirliti.

15. Að því er öryggissvæði varðar:

a) skal komið upp sýnilega afmörkuðu og vernduðu svæði, þar sem haft er eftirlit með allri gegnumferð, jafnt inn sem út, með notkun aðgangskorts eða kerfis sem ber kennsl á einstaklinga,

b) skulu einungis einstaklingar, sem hafa öryggisvottun og sérstaka heimild til innkomu á svæðið á grundvelli vitneskjuþarfar, fá aðgang án fylgdar,

c) skal öllum öðrum einstaklingum ávallt fylgt eða þeir vera háðir sambærilegu eftirliti.

16. Þegar innkoma á öryggissvæði felur í sér í reynd beinan aðgang að trúnaðarflokkuðum upplýsingum sem þar eru geymdar, gilda eftirfarandi viðbótarkröfur:

a) gefa skal skýrt til kynna hæsta stig trúnaðarflokkunar þeirra upplýsinga sem eru venjulega geymdar á svæðinu,

b) allir gestir skulu hafa sérstaka heimild til innkomu á svæðið, þeim skal ávallt fylgt og þeir skulu hafa viðeigandi öryggisvottun, nema ráðstafanir séu gerðar til að tryggja að aðgangur að trúnaðarflokkuðum upplýsingum ESB sé útilokaður.

17. Auðkenna ber öryggissvæði, sem eru vernduð gegn hlerunum, sem tæknileg öryggissvæði. Eftirfarandi viðbótarkröfur gilda:

a) slík svæði skulu búin ágangsskynjunarkerfi, vera læst þegar enginn er á þeim og vöktuð þegar starfsemi fer þar fram. Hafa ber eftirlit með öllum lyklum í samræmi við ákvæði VI. hluta,

b) allir einstaklingar og allt efni, sem fer inn á slík svæði, skulu háð eftirliti,

c) slík svæði skulu háð hlutkenndu og/eða tæknilegu eftirliti reglubundið, eins og viðkomandi bært öryggisyfirvald gerir kröfu um. Fyrrnefnt eftirlit skal einnig fara fram í kjölfar óleyfilegrar innkomu eða ef grunsemdir vakna um slíka innkomu og d) Engar óleyfilegar fjarskiptaleiðslur, óleyfilegir símar eða önnur óleyfileg samskiptatæki og rafmagnstæki eða rafrænn búnaður skal vera á fyrrnefndum svæðum.

18. Þrátt fyrir ákvæði d-liðar 17. mgr. skal viðkomandi bært öryggisyfirvaldi skoða öll samskiptatæki og rafmagnstæki eða rafrænan búnað fyrst, áður en þau eða hann er notaður á svæðum þar sem fundir eru haldnir eða vinna fer fram, m.a. með upplýsingar á trúnaðarstiginu LEYNDARMÁL ESB eða ofar, og þar sem veruleg hætta er talin steðja að trúnaðarflokkuðum upplýsingum ESB, til þess að tryggt sé að ekki sé hægt að senda skiljanlegar upplýsingar með slíkum tækjum eða búnaði, fyrir slysni eða ólöglega, út fyrir mörk öryggissvæðisins.

19. Öryggissvæði, þar sem vaktmenn eru ekki til staðar allan sólarhringinn skulu, eftir því sem við, yfirfarin í lok venjulegs vinnutíma og af og til utan hans, nema ágangsskynjunarkerfi sé til staðar.

20. Setja má upp tímabundin öryggissvæði og tæknileg öryggissvæði innan stjórnsýslusvæðis vegna leynilegs fundar eða í öðrum svipuðum tilgangi.

21. Taka ber saman reglur um öryggi verklags fyrir sérhvert öryggissvæði þar sem mælt er fyrir um:

a) stig trúnaðarflokkaðra upplýsinga ESB sem heimilt er að meðhöndla og geymdar á svæðinu,

b) eftirlit og verndarráðstafanir sem skal viðhalda,

c) hvaða einstaklingar hafi aðgangsheimild að svæðinu án fylgdar með skírskotun til vitneskjuþarfar og öryggisvottunar,

d) verklagsreglur um fylgd eða vernd trúnaðarflokkaðra upplýsinga ESB þegar öðrum einstaklingum er heimilaður aðgangur að svæðinu, eftir því sem við á,

e) sérhverjar aðrar viðeigandi ráðstafanir og verklagsreglur.

22. Rammgerðum hólfum skal komið upp innan öryggissvæða. Viðkomandi bært öryggisyfirvald skal samþykkja veggi, gólf, loft, glugga og læsanlegar hurðir sem skulu og veita sambærilega vernd og öryggisgeymslur sem eru samþykktar fyrir geymslu trúnaðarflokkaðra upplýsinga ESB á sama stigi trúnaðarflokkunar.

V. HLUTKENNDAR VERNDARRÁÐSTAFANIR VEGNA MEÐHÖNDLUNAR OG GEYMSLU TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB

23. Trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB, er heimilt að meðhöndla:

a) á öryggissvæði,

b) á stjórnsýslusvæði, að því tilskildu að trúnaðarflokkaðar upplýsingar ESB séu verndaðar gegn aðgangi einstaklinga sem hafa ekki heimild eða

c) utan öryggissvæðis eða stjórnsýslusvæða, að því tilskildu að handhafi hinna trúnaðarflokkuðu upplýsinga ESB fari með þær í samræmi við ákvæði 28. til 40. mgr. III. viðauka og hafi skuldbindið sig til þess að virða sérstakar ráðstafanir sem mælt er fyrir um í öryggisleiðbeiningum sem viðkomandi bært öryggisyfirvald hefur gefið út í því skyni að tryggja að trúnaðarflokkaðar upplýsingar ESB séu verndaðar gegn aðgangi aðila sem ekki hafa aðgangsheimild.

24. Geyma skal trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB, í hentugum læstum skrifstofuhúsgögnum á stjórnsýslusvæði eða öryggissvæði. Þær má geyma tímabundið utan öryggissvæðis eða stjórnsýslusvæðis, að því tilskildu að handhafi þeirra hafi skuldbindið sig til þess að virða sérstakar ráðstafanir sem viðkomandi bært öryggisstjórnvald hefur mælt fyrir um.

25. Heimilt er að meðhöndla trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB:

a) á öryggissvæði,

b) á stjórnsýslusvæði, að því tilskildu að trúnaðarflokkaðar upplýsingar ESB séu verndaðar fyrir aðgangi einstaklinga sem hafa ekki heimild eða

c) utan öryggissvæðis eða stjórnsýslusvæðis, að því tilskildu að handhafi:

i. fari með trúnaðarflokkaðar upplýsingar ESB í samræmi við ákvæði 28. til 40. mgr. III. viðauka,

ii. hafi skuldbindið sig til þess að virða sérstakar ráðstafanir sem mælt er fyrir um í öryggisleiðbeiningum sem viðkomandi bært öryggisstjórnvald hefur gefið út í því skyni að tryggja að trúnaðarflokkaðar upplýsingar ESB séu verndaðar gegn aðgangi aðila sem ekki hafa aðgangsheimild,

iii. hafi hinar trúnaðarflokkuðu upplýsingar ESB ávallt í eigin umsjá og iv. hafi tilkynnt viðkomandi skráningarstofu að um pappírsskjöl sé að ræða.

26. Geyma skal trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB og LEYNDARMÁL ESB, á öryggissvæði í öryggisgeymslu eða rammgerðu hólfi.

27. Meðhöndla ber trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB á öryggissvæði.

28. Geyma ber trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB, á öryggissvæði að einu af eftirfarandi skilyrðum uppfylltum:

a) í öryggisgeymslu í samræmi við ákvæði 8. mgr., að viðbættum einum eða fleiri eftirfarandi eftirlitsþáttum:

i. stöðugri vernd eða sannprófun sem vottaðir öryggisverðir eða vaktmenn annast,

ii. samþykktu ágangsskynjunarkerfi ásamt með öryggisvörðum í viðbragðsstöðu

eða

b) í rammgerðu hólfi, búnu ágangsskynjunarkerfi, ásamt með öryggisvörðum í viðbragðsstöðu.

29. Reglur sem gilda um flutning trúnaðarflokkaðra upplýsinga ESB utan svæða, sem eru vernduð með hlutkenndum hætti, eru settar fram í III. viðauka.

VI. EFTIRLIT MEÐ LYKLUM OG TALNAKÓÐUM SEM ERU NOTAÐIR TIL AÐ VERNDA TRÚNAÐARFLOKKAÐAR UPPLÝSINGAR ESB

30. Viðkomandi bært öryggisyfirvald skal útlista verklag við umsjón með lyklum og talnakóðum fyrir skrifstofur, rými, rammgerð hólf og öryggisgeymslur. Fyrrnefnt verklag er til verndar gegn aðgangi þeirra sem ekki hafa aðgangsheimild.

31. Lágmarksfjöldi einstaklinga, sem þurfa að þekkja talnakóða, skulu leggja þá á minnið. Breyta ber talnakóðum fyrir öryggisgeymslur og rammgerð hólf þar sem trúnaðarflokkaðar upplýsingar ESB eru geymdar:

a) ávallt þegar breyting verður á því starfsfólki sem þekkir talnakóðana,

b) ávallt þegar upplýsingum hefur verið stofnað í hættu eða grunur leikur á um það,

c) þegar viðhald eða viðgerð hefur farið fram á lás og

d) á 12 mánaða fresti að minnsta kosti.

--------------------------------------------------

*III. VIÐAUKI*

**UMSJÓN MEÐ TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM**

I. INNGANGUR

1. Í viðauka þessum er kveðið á um framkvæmd efnisatriða 9. gr. Þar er mælt fyrir um stjórnsýsluráðstafanir til eftirlits með trúnaðarflokkuðum upplýsingum ESB á líftíma þeirra, til þess að greiða fyrir því að unnt sé að fyrirbyggja, koma upp um og bæta fyrir stofnun slíkra upplýsinga í hættu eða tap þeirra af ásettu ráði eða slysni.

II. UMSJÓN MEÐ FLOKKUN

**Flokkun og merkingar.**

2. Upplýsingar skulu flokkaðar þarfnist þær verndar með tilliti til leyndar.

3. Útgefandi trúnaðarflokkaðra upplýsinga ESB ber ábyrgð á ákvörðun stigs trúnaðarflokkunar í samræmi við viðeigandi flokkunarleiðbeiningar og vegna dreifingar upplýsinganna í fyrsta sinn.

4. Ákveða skal stig trúnaðarflokkaðra upplýsinga ESB samkvæmt ákvæðum 2. mgr. 2. gr. og með vísan til þeirrar öryggisstefnu sem samþykkja skal samkvæmt 3. mgr. 3. gr.

5. Viðeigandi trúnaðarflokkun skal koma fram með skýrum og réttum hætti, hvort sem hinar trúnaðarflokkuðu upplýsingar ESB eru á pappír, munnlegar, rafrænar eða á einhveri annarri mynd.

6. Einstakir hlutar ákveðinna skjala (þ.e. blaðsíður, málsgreinar, hlutar, viðaukar, viðbætar, viðhengi og fylgiskjöl) kunna að þarfnast mismunandi flokkunar og skulu merktir í samræmi við það, m.a. þegar skjölin eru geymd í rafræni mynd.

7. Heildarstig trúnaðarflokkunar skjals eða skrár skal a.m.k. vera jafn hátt og sá hluti skjalsins sem hefur hæsta trúnaðarstig. Þegar upplýsingum úr margvíslegum heimildum er safnað saman skal yfirfara lokaafurðina til að ákvarða heildarstig trúnaðarflokkunar hennar, þar eð hún kann að kalla á hærri flokkun en einstakir hlutar hennar.

8. Skjöl, sem innihalda hluta með mismunandi stigum trúnaðarflokkunar, skulu þannig uppbyggð, eins og við verður komið, að auðvelt sé að greina hluta með ólík stig trúnaðarflokkunar og skilja þá frá ef nauðsyn krefur.

9. Trúnaðarstig bréfs eða orðsendingar, sem inniheldur fylgiskjöl, skal vera jafn hátt og hæsta trúnaðarstig fylgiskjala þess eða hennar. Útgefandinn skal gefa skýrt til kynna, með viðeigandi merkingu, trúnaðarstig bréfsins eða orðsendingarinnar þegar það eða hún er skilin frá fylgiskjölunum, t.d.:

TRÚNAÐARMÁL ESB

Án viðhengis eða viðhengja, TAKMARKAÐUR AÐGANGUR ESB.

**Merkingar.**

10. Auk einnar þeirra merkinga trúnaðarflokkunar, sem settar er fram í 2. mgr. 2. gr., geta trúnaðarflokkaðar upplýsingar ESB haft viðbótarmerkingar eins og:

a) kennimerki sem auðkennir útgefanda,

b) viðvaranir, táknorð eða upphafsstafaorð sem tilgreina það athafnasvið sem skjalið tengist, sérstaka dreifingu á grundvelli vitneskjuþarfar eða notkunartakmarkanir,

c) merkingar sem gefa til kynna birtingarmöguleika,

d) eftir atvikum, eftir hvaða dag eða tiltekinn viðburð heimilt er að lækka trúnaðarstig upplýsinganna eða aflétta trúnaðarflokkun þeirra,

**Skammstöfun flokkunarmerkinga.**

11. Heimilt er að nota staðlaða skammstöfun flokkunarmerkinga til þess að gefa til kynna stig trúnaðarflokkunar einstakra málsgreina í texta. Skammstafanir geta ekki komið í stað óstyttra flokkunarmerkinga.

12. Heimilt er að nota eftirfarandi staðlaðar skammstafanir í trúnaðarflokkuðum skjölum ESB til þess að gefa til kynna stig trúnaðarflokkaðra kafla eða textahluta sé textinn styttri en ein blaðsíða:

ALGJÖRT LEYNDARMÁL ESB AL-ESB

LEYNDARMÁL ESB L-ESB

TRÚNAÐARMÁL ESB T-ESB

TAKMARKAÐUR AÐGANGUR ESB TA-ESB

**Tilurð trúnaðarflokkaðra upplýsinga ESB.**

13. Þegar trúnaðarskjal ESB er undirbúið:

a) skal merkja sérhverja blaðsíðu viðeigandi stigi trúnaðarflokkunar með skírum hætti,

b) skal tölusetja sérhverja blaðsíðu,

c) skal skjalið hafa tilvísunarnúmer og tilgreint efnissvið sem er ekki sem slíkt trúnaðarflokkaðar upplýsingar, nema það sé þannig merkt,

d) skal skjalið vera dagsett,

e) skulu skjöl á trúnaðarstiginu LEYNDARMÁL ESB eða ofar, hafa númer eintaks á hverri síðu, standi til að dreifa þeim í nokkrum eintökum.

14. Ef ekki er hægt að beita ákvæði 13. mgr. gagnvart trúnaðarflokkuðum upplýsingum ESB skal gera aðrar viðeigandi ráðstafanir í samræmi við öryggisleiðbeiningar sem ákveða skal skv. 2. mgr. 6. gr.

**Lækkun trúnaðarstigs trúnaðarflokkaðra upplýsinga ESB og aflétting trúnaðarflokkunar.**

15. Samfara tilurð trúnaðarflokkaðra upplýsinga ESB skal útgefandinn gefa til kynna, þegar því verður komið við og einkum í tilviki upplýsinga á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB, hvort lækka megi trúnaðarstig eða aflétta trúnaðarflokkun þeirra á tilteknum degi eða eftir tiltekinn viðburð.

16. Aðalskrifstofa ráðsins skal yfirfara reglulega trúnaðarflokkaðar upplýsingar ESB, sem hún hefur í sinni vörslu, til að ganga úr skugga um hvort viðkomandi stig trúnaðarflokkunar sé enn í gildi. Aðalskrifstofa ráðsins skal koma á stofn kerfi sem gerir kleift að yfirfara flokkunarstig skráðra trúnaðarflokkaðra upplýsinga ESB, sem það gefur út, eigi sjaldnar en á 5 ára fresti. Slík endurskoðun er ónauðsynleg hafi útgefandinn gefið til kynna frá upphafi að trúnaðarstig upplýsinganna verði sjálfkrafa lækkað eða trúnaðarkvöð aflétt og að upplýsingarnar hafi verið merktar í samræmi við það.

III. SKRÁNING TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB MEÐ TILLITI TIL ÖRYGGIS

17. Tilnefna skal ábyrga skráningarstofu fyrir sérhverja skipulagseiningu innan aðalskrifstofu ráðsins og á vegum innlendra stjórnvalda aðildarríkjanna, þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar, til þess að tryggt sé að trúnaðarflokkaðar upplýsingar ESB séu meðhöndlaðar í samræmi við ákvörðun þessa. Skráningarstofur skulu stofnsettar sem öryggissvæði, eins og þau eru skilgreind í II. viðauka.

18. Í ákvörðun þessari merkir skráning með tilliti til öryggis (hér á eftir nefnd „skráning“) að beita verklagsreglum sem lúta að skráningu lífsferils efnis, þ.m.t. dreifing þess og eyðing.

19. Allt efni á trúnaðarstiginu TRÚNAÐARMÁL ESB og ofar skal skrá í tilnefndum skráningarstofum þegar það berst skipulagseiningu eða fer þaðan.

20. Miðlæg skráningarstofa innan aðalskrifstofu ráðsins skal halda skrá yfir allar trúnaðarflokkaðar upplýsingar sem ráðið og aðalskrifstofa ráðsins miðla til þriðju ríkja og alþjóðastofnana og yfir allar trúnaðarflokkaðar upplýsingar sem berast frá þriðju ríkjum og alþjóðastofnunum.

21. Í tilfelli samskipta- og upplýsingakerfis getur skráningarferlið farið fram innan kerfisins sjálfs.

22. Ráðið skal, í þágu öryggis, samþykkja öryggisstefnu vegna skráningar trúnaðarflokkaðra upplýsinga ESB.

Skráningarstofur upplýsinga sem eru flokkaðar ALGJÖRT LEYNDARMÁL ESB

23. Tilnefna ber skráningarstofu í aðildarríkjunum og innan aðalskrifstofu ráðsins sem gegnir hlutverki miðlægs stjórnvalds sem annast móttöku og sendingu upplýsinga á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB. Heimilt er, ef nauðsyn krefur, að tilnefna undirskáningarstofur sem meðhöndla slíkar upplýsingar með tilliti til skráningar.

24. Fyrrnefndum undirskráningarstofum er óheimilt að senda skjöl merkt ALGJÖRT LEYNDARMÁL ESB beint til annarra undirskráningarstofa sömu miðlægu skráningarstofunnar sem annast skjöl flokkuð ALGJÖRT LEYNDARMÁL ESB eða til utanaðkomandi aðila, án ótvíræðs skriflegs samþykkis þeirrar síðastnefndu.

IV. AFRITUN OG ÞÝÐING TRÚNAÐARFLOKKAÐRA SKJALA ESB

25. Óheimilt er að afrita eða þýða skjöl merkt ALGJÖRT LEYNDARMÁL ESB án fyrirfram skriflegs samþykkis útgefandans.

26. Hafi útgefandi skjala á trúnaðarstiginu LEYNDARMÁL ESB og neðar ekki sett fram viðvaranir vegna afritunar eða þýðingar er heimilt að afrita eða þýða slík skjöl samkvæmt fyrirmælum handhafa þeirra.

27. Þær öryggisráðstafanir sem eiga við um frumrit skjalsins skulu gilda um afrit og þýðingar þess.

V. FLUTNINGUR TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB

28. Flutningur trúnaðarflokkaðra upplýsinga ESB er háður verndarráðstöfunum sem settar eru fram í 30. til 40. mgr. Þegar trúnaðarflokkaðar upplýsingar ESB eru fluttar í rafræni mynd er heimilt, þrátt fyrir ákvæði 4. mgr. 9. gr., að auka við neðangreindar verndarráðstafanir með viðeigandi tæknilegum gagnráðstöfunum, sem viðkomandi bært öryggisyfirvald mælir fyrir um, í því skyni að lágmarka hættu á tapi slíkra upplýsinga eða að þeim sé stofnað í hættu.

29. Viðkomandi bær öryggisyfirvöld innan aðalskrifstofu ráðsins og í aðildarríkjunum skulu gefa út fyrirmæli um flutning trúnaðarflokkaðra upplýsinga ESB í samræmi við ákvörðun þessa.

**Innan byggingar eða sjálfstæðrar húsaþyrpingar.**

30. Trúnaðarflokkaðar upplýsingar ESB sem fluttar eru innan byggingar eða sjálfstæðrar húsaþyrpingar skulu huldar til að varna því að innihaldið verði skoðað.

31. Þegar upplýsingar á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB eru fluttar innan byggingar eða sjálfstæðrar húsaþyrpingar skal flytja þær í traustu umslagi sem er einungis merkt nafni viðtakanda.

Innan ESB:

32. Búið skal um trúnaðarflokkaðar upplýsingar ESB sem fluttar eru milli bygginga eða athafnasvæða innan ESB þannig að þær séu varðar gegn óleyfilegri uppljóstrun.

33. Flutningur upplýsinga, sem eru flokkaðar upp að trúnaðarstiginu LEYNDARMÁL ESB innan ESB, skal fara fram með einum eftirfarandi hátta:

a) með boðbera hers, stjórnarvalda eða stjórnarpóstbera, eftir atvikum,

b) með boðsendingu, að því tilskildu að:

i. trúnaðarflokkaðar upplýsingar ESB fari ekki vörslu burðarmannsins, nema þær séu geymdar samkvæmt þeim kröfum sem settar eru fram í II. viðauka,

ii. trúnaðarflokkaðar upplýsingar ESB séu ekki opnaðar á leiðinni eða lesnar á opinberum stöðum,

iii. viðkomandi einstaklingar séu upplýstir um þá ábyrgð sem þeir bera með tilliti til öryggis,

iv. viðkomandi einstaklingum sé útvegað boðberavottorð, ef nauðsyn krefur,

c) með almennri póstþjónustu eða sendingarþjónustu, að því tilskildu að:

i. viðkomandi stjórnvald á sviði þjóðaröryggis samþykki fyrrnefnda þjónustu í samræmi við innlend lög og reglugerðir,

ii. viðkomandi þjónusta geri viðeigandi verndarráðstafanir eftir lágmarkskröfum sem mæla skal fyrir í öryggisleiðbeiningum skv. 2. mgr. 6. gr.

Þegar flutningur fer fram frá einu aðildarríki til annars gilda ákvæði c-liðar einungis um upplýsingar sem eru flokkaðar upp að trúnaðarstiginu TRÚNAÐARMÁL ESB.

34. Efni á trúnaðarstiginu TRÚNAÐARMÁL ESB og LEYNDARMÁL ESB (t.d. búnaður eða vélbúnaður) og ekki er hægt að flytja með þeim hætti er um getur í 33. mgr., skal flytja sem farm með flutningafyrirtækjum í samræmi við ákvæði V. viðauka.

35. Boðberar hers, stjórnvalda eða stjórnarpóstberar skulu, eftir atvikum, flytja upplýsingar á trúnaðarstiginu ALGJÖRT LEYNDARMÁL ESB á milli bygginga eða athafnasvæða innan ESB.

**Frá ESB til yfirráðasvæðis þriðja ríkis.**

36. Búa skal um trúnaðarflokkaðar upplýsingar ESB, sem eru fluttar frá ESB til yfirráðasvæðis þriðja ríkis, þannig að þær séu varðar gegn óleyfilegri uppljóstun.

37. Flutningur upplýsinga á trúnaðarstiginu TRÚNAÐARMÁL ESB og LEYNDARMÁL ESB frá ESB til yfirráðasvæðis þriðja ríkis skal fara fram með einum eftirfarandi hátta:

a) með boðbera hers eða stjórnarpóstbera,

b) handborið, að því tilskildu að:

i. pakkinn hafi opinbert innsigli eða þannig sé búið um hana að gefið sé til kynna að um opinbera sendingu sé að ræða sem sé undanskilin toll- eða öryggisskoðun,

ii. viðkomandi einstaklingar hafi boðberavottorð þar sem auðkenni sendingarinnar kemur fram ásamt heimild þeirra til að flytja hana,

iii. trúnaðarflokkaðar upplýsingar ESB fari ekki úr vörslu handhafans, nema þær séu geymdar samkvæmt þeim kröfum sem settar eru fram í II. viðauka,

iv. trúnaðarflokkaðar upplýsingar ESB séu ekki opnaðar á leiðinni eða lesnar á opinberum stöðum og

v) viðkomandi einstaklingar séu upplýstir um þá ábyrgð sem þeir bera með tilliti til öryggis.

38. Flutningur upplýsinga á trúnaðarstiginu TRÚNAÐARMÁL ESB og LEYNDARMÁL ESB sem ESB miðlar til þriðja ríkis eða alþjóðastofnunar, skal fara fram samkvæmt viðeigandi ákvæðum samkvæmt samningi um upplýsingaöryggi eða stjórnsýslusamkomulagi sbr. a- eða b-lið 2. mgr. 12. gr.

39. Þá er og heimilt að flytja upplýsingar á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB með almennri póstþjónustu eða sendingarþjónustu.

40. Boðberar hers eða stjórnarpóstberar skulu annast flutning upplýsinga á trúnaðarstiginu ALJGÖRT LEYNDARMÁL ESB frá ESB til yfirráðasvæðis þriðja ríkis.

VI. EYÐING TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB.

41. Trúnaðarskjölum ESB, sem ekki er lengur þörf fyrir, má eyða, samanber þó viðeigandi ákvæði og reglugerðir um geymslu skjala.

42. Ábyrg skráningarstofa eyðir skjölum, sem ber að skrá skv. 2. mgr. 9. gr., samkvæmt fyrirmælum frá handhafa eða bærs stjórnvalds. Uppfæra ber færslubækur og aðrar skráningarupplýsingar til samræmis.

43. Eyða ber skjölum á trúnaðarstiginu LEYNDARMÁL ESB eða ALGJÖRT LEYNDARMÁL ESB í viðurvist vitna sem eru vottuð a.m.k. til jafns við trúnaðarflokkunarstig þess skjals sem er eytt.

44. Skráningaryfirvaldið og vitnið, þegar nærveru þess síðarnefnda er krafist, skulu undirrita eyðingarvottorð sem er skráð á skráningarstofunni. Skráningarstofan skal varðveita eyðingarvottorð skjala, sem eru flokkuð LEYNDARMÁL ESB, í a.m.k. 10 ár og skjala, sem eru flokkuð TRÚNAÐARMÁL ESB og LEYNDARMÁL ESB, í a.m.k. 5 ár.

45. Eyða ber trúnaðarflokkuðum skjölum, þ.m.t. skjöl á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB, með aðferðum sem eru í samræmi við viðeigandi viðmiðanir ESB eða jafngildar viðmiðanir eða með aðferðum sem aðildarríki hafa samþykktar eftir innlendum tæknistöðlum til þess að koma í veg fyrir endurgerð að hluta eða að öllu leyti.

46. Eyðing geymslumiðla í tölvum sem eru notaðir fyrir trúnaðarflokkaðar upplýsingar ESB skal vera í samræmi við ákvæði 36. mgr. IV. viðauka.

VII. EFTIRLIT OG MATSHEIMSÓKNIR

47. Hugtakið „eftirlit“ tekur hér á eftir til:

a) eftirlits skv. 3. mgr. 9. gr. og e-, f- og g-lið 2. mgr. 15. gr. eða

b) matsheimsóknar skv. 5. mgr. 12. gr.,

í því skyni að meta skilvirkni ráðstafana sem eru gerðar til verndar trúnaðarflokkuðum upplýsingum ESB.

48. Eftirlit skal m.a. fara fram til þess að:

a) tryggja að fylgt sé nauðsynlegum lágmarksviðmiðunum um vernd trúnaðarflokkaðra upplýsinga ESB sem mælt er fyrir um í ákvörðun þessari,

b) leggja áherslu á mikilvægi öryggis og skilvirkrar áhættustjórnunar innan þeirra eininga þar sem eftirlit fer fram,

c) unnt sé að mæla með gagnráðstöfunum til að draga úr sérstökum áhrifum þess þegar leynd trúnaðarflokkaðra upplýsinga, heilleiki þeirra eða aðgengi að þeim fer forgörðum og d) styrkja yfirstandandi áætlanir öryggisyfirvalda á sviði fræðslu og vitundarvakningar í öryggismálum.

49. Fyrir lok hvers almanaksárs skal ráðið samþykkja þá eftirlitsáætlun sem gert er ráð fyrir í c-lið 1. mgr. 15. gr. fyrir komandi ár. Dagsetja ber eftirlit í hverju tilviki fyrir sig í samráði við viðkomandi embætti eða stofnun ESB, aðildarríki, þriðja ríki eða alþjóðastofnun.

**Framkvæmd eftirlits.**

50. Eftirlit skal fara fram með það að markmiði að skoða viðeigandi ákvæði, reglur og verklag sem gilda innan þeirrar rekstrareiningar sem eftirlitið varðar og sannreyna hvort starfsvenjur viðkomandi rekstrareiningar samræmist þeim grundvallarsetningum og lágmarksviðmiðunum sem mælt er fyrir um í ákvörðun þessari og þeim ákvæðum sem gilda um skipti á trúnaðarflokkuðum upplýsingum við þá rekstareiningu.

51. Eftirlit skal framkvæmt í tveimur áföngum. Koma skal á undirbúningsfundi með viðkomandi rekstrareiningu, ef nauðsyn krefur, áður en sjálft eftirlitið fer fram. Að undirbúningsfundinum loknum skal eftirlitshópurinn koma á, í samráði við fyrrnefnda rekstrareiningu, ítarlegri eftirlitsáætlun sem tekur til allra sviða öryggismála. Eftirlitshópurinn skal fá aðgang að öllum stöðum, þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar, einkum skráningarstofum og tengistöðum samskipta- og upplýsingakerfa.

52. Sameiginlegur eftirlitshópur aðalskrifstofu ráðsins og ráðsins bera ábyrgð á framkvæmd eftirlits innan innlendrar stjórnsýslu aðildarríkjanna í nánu samstarfi við embættismenn þeirrar rekstrareiningar sem eftirlitið varðar.

53. Sameiginlegur eftirlitshópur aðalskrifstofu ráðsins og ráðsins bera ábyrgð á framkvæmd eftirlits í þriðju ríkjum og alþjóðastofnunum í nánu samstarfi við embættismenn viðkomandi þriðju ríkja og alþjóðastofnana þar sem eftirlitið fer fram.

54. Öryggisdeild aðalskrifstofu ráðsins skal annast eftirlit, með aðstoð sérfræðinga stjórnvalds á sviði þjóðaröryggis á því yfirráðasvæði þar sem viðkomandi embætti eða stofnun er staðsett, innan embætta og stofnana ESB, sem eru stofnsett samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, og innan Evrópulögreglunnar og Evrópsku réttaraðstoðarinnar. Öryggismálaskrifstofa framkvæmdastjórnarinnar (ECSD) getur komið að málum skiptist hún reglulega á trúnaðarflokkuðum upplýsingum ESB við þau embætti eða stofnanir sem um er að ræða.

55. Í tilviki eftirlits hjá embættum og stofnunum ESB, sem stofnsett eru samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, Evrópulögreglunni og Evrópsku réttaraðstoðinni og hjá þriðju ríkjum og alþjóðastofnunum, skal óska eftir aðstoð sérfræðinga innlendra stjórnvalda á sviði þjóðaröryggis samkvæmt ítarlegri tilhögun sem öryggisnefndin skal samþykkja.

**Eftirlitsskýrslur.**

56. Þegar eftirlitinu er lokið skal kynna þeirri rekstrareiningu sem það varðar helstu niðurstöður og tilmæli. Að því loknu skal taka saman skýrslu um eftirlitið sem öryggisyfirvald aðalskrifstofu ráðsins (öryggisdeildin) ber á byrgð á. Hafi tillaga verið gerð um úrbætur og tilmæli lögð fram skal í skýrslunni benda á einstök atriði niðurstöðum hennar til stuðnings. Skýrslan skal framsend viðkomandi yfirvaldi þeirrar rekstrareiningar sem eftirlitið varðar.

57. Að því er varðar eftirlit sem fer fram hjá innlendri stjórnsýslu aðildarríkja:

a) skulu drög að eftirlitsskýrslunni framsend viðkomandi stjórnvaldi á sviði þjóðaröryggis því til staðfestingar að hún sé í raun rétt og að hún innihaldi engar upplýsingar sem eru flokkaðar ofar en TAKMARKAÐUR AÐGANGUR ESB,

b) skal dreifa eftirlitsskýrslum til meðlima öryggisnefndarinnar og til öryggismálaskrifstofu framkvæmdastjórnarinnar, nema stjórnvald á sviði þjóðaröryggis í viðkomandi aðildarríki óski eftir að almenn dreifing fari ekki fram; skýrslan skal vera á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB.

Taka ber saman reglulega skýrslu, sem öryggisyfirvald aðalskrifstofu ráðsins (öryggisdeildin) ber ábyrgð á, í því skyni að draga fram lærdóm af því eftirliti sem er lokið í aðildarríkjum á tilteknu tímabili og öryggisnefndin yfirfer.

58. Að því er varðar matsheimsóknir til þriðju ríkja og alþjóðastofnana skal skýrslunni dreift til öryggisnefndarinnar og öryggismálaskrifstofu framkvæmdastjórnarinnar. Skýrslan skal a.m.k. vera á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB. Sannreyna ber allar úrbætur í framhaldsheimsókn og gefa öryggisnefndinni skýrslu um þær.

59. Að því er varðar eftirlit hjá embættum og stofnunum ESB, sem stofnsett eru samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið, Evrópulögreglunni og Evrópsku réttaraðstoðinni skal eftirlitsskýrslum dreift til meðlima öryggisnefndarinnar og til öryggismálaskrifstofu framkvæmdastjórnarinnar. Drög að eftirlitsskýrslunni skal framsenda viðkomandi embætti eða stofnun því til staðfestingar að hún sé í raun rétt og að hún innihaldi engar upplýsingar sem eru flokkaðar ofar en TAKMARKAÐUR AÐGANGUR ESB. Sannreyna ber allar úrbætur í framhaldsheimsókn og gefa öryggisnefndinni skýrslu um þær.

60. Öryggisyfirvald aðalskrifstofu ráðsins framkvæmir reglulega eftirlit hjá skipulagseiningum á aðalskrifstofu ráðsins í þeim tilgangi sem mælt er fyrir um í 48. mgr.

**Gátlisti vegna eftirlits.**

61. Öryggisyfirvald aðalskrifstofu ráðsins (öryggisdeildin) skal taka saman og uppfæra gátlista vegna eftirlits með öryggi yfir atriði sem sannreyna á meðan eftirlitið stendur yfir. Framsenda skal öryggisnefndinni gátlistann.

62. Upplýsinga, sem eru nauðsynlegar til þess að fylla gátlistann út, skal einkum aflað meðan á eftirlitinu stendur hjá þeim aðila sem annast stjórn öryggismála hjá þeirri rekstrareiningu sem eftirlitið varðar. Gátlistann skal trúnaðarflokka í samráði við þá rekstrareiningu sem eftirlitið varðar eftir að lokið er við að færa inn nákvæm svör. Gátlistinn er ekki hluti af eftirlitsskýrslunni.

--------------------------------------------------

*IV. VIÐAUKI*

**VERND TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB SEM MEÐHÖNDLAÐAR ERU Í UPPLÝSINGAKERFUM**

I. INNGANGUR

1. Í viðauka þessum er kveðið á um framkvæmd efnisatriða 10. gr.

2. Eftirtaldir eiginleikar og hugtök upplýsingaöryggis eru nauðsynleg vegna öryggis og til þess að aðgerðir innan upplýsingakerfisins virki rétt:

áreiðanleiki: trygging fyrir því að upplýsingar séu ósviknar og upprunnar frá réttum aðila,

aðgengi: sá eiginleiki að upplýsingar séu aðgengilegar og nothæfar að fram kominni beiðni frá viðurkenndri rekstrareiningu,

leynd: sá eiginleiki að upplýsingum sé ekki uppljóstrað án heimildar til óviðkomandi einstaklinga, rekstrareininga eða vinnsluferla,

Heilleiki: sá eiginleiki að nákvæmni og fullkomleiki upplýsinga og tilfanga sé tryggður,

óhrekjanleiki: sá eiginleiki að unnt sé að sanna að tiltekin aðgerð eða atburður hafi átt sér stað, þannig að ógerlegt sé að neita því síðar.

II. MEGINIREGLUR UM UPPLÝSINGAÖRYGGI

3. Ákvæðin sem sett eru fram hér að aftan eru grundvöllur öryggis sérhvers samskipta- og upplýsingakerfis þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar. Ítarlegar kröfur um hvernig þessum ákvæðum skuli beitt eru skilgreindar í öryggisstefnu og -leiðbeiningum um upplýsingaöryggi.

**Öryggisáhættustjórnun.**

4. Öryggisáhættustjórnun er óaðskiljanlegur þáttur í því að skilgreina, þróa og viðhalda samskipta- og upplýsingakerfi. Áhættustjórnun (mat, meðferð, staðfesting og samskipti) skal komið til leiðar sem ítrekunarferli í samvinnu fulltrúa eigenda kerfisins, verkefnastjórna, rekstrarstjórna og öryggisvottunaryfirvalda, þar sem stuðst er við sannreynd, gagnsæ og fullkomlega skiljanleg áhættumatsferli. Notkunarsvið samskipta- og upplýsingakerfa og tilfanga þeirra skal skilgreina með skýrum hætti allt frá upphafi notkunar áhættustjórnunarferlisins.

5. Bær stjórnvöld skulu yfirfara hugsanlega ógn sem kann að steðja að samskipta- og upplýsingakerfinu og viðhalda uppfærðu og nákvæmu ógnarmati sem gefur rétta mynd af ríkjandi rekstrarumhverfi. Þau skulu bæta stöðugt þekkingu sína á málefnum varnarleysis og endurskoða reglulegulega mat þess til að geta fylgt þeim breytingum sem umhverfi upplýsingatækninnar tekur.

6. Markmiðið með viðbrögðum við hættu, sem steðjar að öryggi, er að beita röð öryggisráðstafana sem skapar viðunandi jafnvægi milli krafna notenda, kostnaðar og eftirstandandi öryggisáhættu.

7. Þær sértöku kröfur, umfang og stig einstakra atriða, sem viðkomandi yfirvald á sviði öryggisvottunar ákveður vegna vottunar samskipta- og upplýsingakerfis, skulu svara til þeirrar áhættu sem áætluð er, að teknu tilliti til allra þátta sem skipta máli, þ.m.t. stig trúnaðarflokkaðra upplýsinga ESB sem eru meðhöndlaðar í samskipta- og upplýsingakerfinu. Vottun skal fela í sér formlega yfirlýsingu um eftirstandandi áhættu og viðurkenningu ábyrgs yfirvalds á þeirri áhættu.

**Öryggi á líftíma samskipta- og upplýsingakerfisins.**

8. Gerð er krafa um að öryggi samskipta- og upplýsingakerfisins sé tryggt allan líftíma þess, frá byrjun uns það er tekið úr notkun.

9. Tilgreina ber hlutverk og milliverkun sérhvers geranda, sem er hluti af samskipta- og upplýsingakerfi með tilliti til öryggis þess, fyrir sérhvern fasa líftímans.

10. Sérhvert samskipta- og upplýsingakerfi, þ.m.t. tæknilegar öryggisráðstafanir þess og aðrar öryggisráðstafanir, skal öryggisprófa meðan á vottunarferlinu stendur til þess að tryggt sé að viðeigandi áreiðanleikastigi sé náð og að ljóst sé að þær komi til framkvæmda, séu samþættar og skipað saman með réttum hætti.

11. Öryggismat, eftirlit og endurskoðun skal fara reglulega fram meðan samskipta- og upplýsingakerfi er í rekstri og því við haldið og þegar sérstakar aðstæður koma upp.

12. Gögn um öryggi samskipta- og upplýsingakerfis skulu aukin á líftíma þess sem er órjúfanlegur þáttur í því ferli að hafa stjórn á breytingum og samskipan.

**Bestu starfsvenjur.**

13. Aðalskrifstofa ráðsins og aðildarríkin skulu þróa í sameiningu bestu starfsvenjur til verndar trúnaðarflokkaðra upplýsinga ESB sem eru meðhöndlaðar í samskipta- og upplýsingakerfi. Í viðmiðunarreglum um bestu starfsvenjur skulu tíundaðar öryggisráðstafanir sem lúta að tækni, hlutkenndum þáttum, skipulagi og verklagi viðvíkjandi samskipta- og upplýsingakerfi og fela í sér rökstudda skilvirkni þegar sporna skal gegn ógnum og varnarleysi.

14. Byggja ber vernd trúnaðarflokkaðra upplýsinga ESB, sem eru meðhöndlaðar í samskipta- og upplýsingakerfi, á reynslu rekstrareininga sem koma að upplýsingaöryggi innan og utan ESB.

15. Útbreiðsla og eftirfarandi notkun bestu starfsvenja skal stuðla að því að jafngildu áreiðanleikastigi sé náð fyrir hin ýmsu samskipta- og upplýsingakerfi sem aðalskrifstofa ráðsins og aðildarríki, sem meðhöndla trúnaðarflokkaðar upplýsingar ESB, reka.

**Lagskiptar varnir.**

16. Grípa skal til margháttaðra tæknilegra og annars konar öryggisráðstafana, sem eru skipulagðar í mörgum lögum, í því skyni að draga úr þeirri áhættu sem steðjar að samskipta- og upplýsingakerfum. Eftirtaldir þættir eru fólgnir í fyrrnefndri lagskiptingu:

a) hindrun: öryggisráðstafanir til að afstýra því að gerðar séu áætlanir um að ráðast á samskipta- og upplýsingakerfið,

b) forvarnir: öryggisráðstafanir til að hindra eða stöðva árás á samskipta- og upplýsingakerfið,

c) greining: öryggisráðstafanir til að koma upp um árás á samskipta- og upplýsingakerfið,

d) mótstöðuafl: öryggisráðstafanir til að takmarka áhrif árásar við lágmarksfjölda upplýsinga eða tilfanga innan samskipta- og upplýsingakerfis og að koma í veg fyrir frekara tjón og e) endurheimt: öryggisráðstafanir til að koma á öruggu ástandi samskipta- og upplýsingakerfis á ný.

Sveigjanleiki slíkra öryggisráðstafana er ákvarðaður að undangengnu áhættumati,.

17. Viðkomandi bær stjórnvöld skulu tryggja að þau geti brugðist við tilvikum, sem geta náð út fyrir mörk með tilliti til skipulags og út fyrir landamæri ríkja, í því skyni að samræma viðbrögð og deila upplýsingum um þau tilvik og hættu sem þeim fylgir (viðbragðsgeta í neyðartilvikum sem varða tölvuöryggi).

**Meginregla um lágmark og lágmarksréttindi.**

18. Virkni, búnaður og þjónusta, sem er nauðsynleg til að uppfylla rekstrarkröfur, skal einungis hagnýtt til þess að koma í veg fyrir óþarfa áhættu.

19. Notendur samskipta- og upplýsingakerfisins og ferli, sem gerð eru sjálfvirk, skulu aðeins fá þann aðgang, réttindi eða heimildir sem þau þarfnast til að vinna sín verk, til þess að takmarka megi skemmdir af slysni, vegna mistaka eða vegna óheimilar notkunar á föngum samskipta- og upplýsingakerfisins.

20. Liður í vottunarferlinu skal vera að sannreyna þá skráningaraðferð sem tiltekið samskipta- og upplýsingakerfi notar, þar sem þess gerist þörf.

**Vitund um upplýsingaöryggi.**

21. Vitund um hættu og tiltækar öryggisráðstafanir er grundvallaratriði í þeirri viðleitni að vernda öryggi samskipta- og upplýsingakerfis. Mikilvægt er að allt það starfsfólk sem kemur að samskipta- og upplýsingakerfi á líftíma þess, þ.m.t. notendur, hafi skilning á eftirtöldum þáttum:

a) að öryggisbrestur geti skaðað samskipta- og upplýsingakerfi verulega,

b) hugsanlegum skaða sem aðrir geta orðið fyrir og samtenging og víxltengsl kunna að valda og c) ábyrgð sérhvers einstaklings á öryggi samskipta- og upplýsingakerfisins eftir því hvaða hlutverki hver og einn gegnir innan kerfisins og í verkferlum.

22. Öllu starfsfólki, sem kemur að málum, þ.m.t. yfirstjórn og notendur kerfisins, er skylt að þiggja þjálfun á sviði upplýsingaöryggis og vitundarvakningar, til þess að tryggt sé að það geri sér grein fyrir þeirri ábyrgð sem það ber með tilliti til öryggis.

**Mat og viðurkenning öryggisvarnings innan upplýsingatækninnar.**

23. Ákvarða ber það stig tiltrúar á öryggisráðstöfunum, skilgreint sem áreiðanleikastig, eftir að niðurstöður áhættustjórnunarferlisins liggja fyrir og í samræmi við viðeigandi stefnumörkun og leiðbeiningar í öryggismálum.

24. Staðfesta ber áreiðanleikastig með því að beita viðurkenndu verklagi á alþjóðavísu eða viðurkenndum innlendum aðferðum og verklagi. Í þessu felst einkum og sér í lagi mat, eftirlit og endurskoðun.

25. Innlent vottunaryfirvald dulkóðunar í aðildarríki skal meta og samþykkja dulkóðunartæki til verndar trúnaðarflokkuðum upplýsingum ESB.

26. Áður en ráðið eða aðalframkvæmdastjórinn leggur til að dulkóðunartæki skuli samþykkt skv. 6. mgr. 10. gr. skulu þau hafa staðist mat óháðs aðila, þ.e. hæfs yfirvalds á viðkomandi sviði (AQUA) í aðildarríki sem hefur ekki komið að hönnun eða framleiðslu tækisins. Hversu nákvæmt mat óháðs aðila skal vera fer eftir ætluðu hæsta flokkunarstigi þeirra trúnaðarflokkuðu upplýsinga ESB sem fyrrnefndum tækjum er ætlað að vernda. Ráðið skal samþykkja öryggisstefnu fyrir mat og vottun dulkóðunartækjanna.

27. Ráðinu eða aðalframkvæmdastjóranum, eftir því sem við á, er heimilt, þar sem slíkt er réttlætanlegt af sérstökum rekstrarástæðum og eftir tilmælum öryggisnefndarinnar, að falla frá kröfum skv. 25. og 26. mgr. og veita bráðabirgðasamþykki fyrir tiltekið tímabil í samræmi við þær verklagsreglur sem mælt er fyrir um í 6. mgr. 10. gr.

28. Hæft yfirvald viðkomandi sviði (AQUA) skal vera vottunaryfirvald dulkóðunar í aðildarríki sem hefur fengið vottun til þess að framkvæma framhaldsmat dulkóðunartækja til verndar trúnaðarflokkuðum upplýsingum ESB.

29. Ráðið samþykkir öryggisstefnu vegna hæfis og samþykkis öryggistækja í upplýsingatækni sem ekki eru dulkóðunartæki.

**Flutningur innan öryggissvæða.**

30. Heimilt er, þrátt fyrir ákvæði ákvörðunar þessarar og þegar trúnaðarflokkaðar upplýsingar ESB eru fluttar til innan öryggissvæða, að dreifa upplýsingum án þess að notast við dulkóðun eða með því að notast við dulkóðun á lægra stigi, allt eftir þeirri niðurstöðu sem áhættustjórnunarferlið gefur og að fengnu samþykki yfirvalds á sviði öryggisvottunar.

**Örugg samtenging samskipta- og upplýsingakerfa.**

31. Að því er varðar ákvörðun þessa merkir samtenging beina tengingu tveggja eða fleiri upplýsingatæknikerfa í þeim tilgangi að deila gögnum og öðrum uppsprettum upplýsinga (t.d. samskiptum) í eina eða fleiri áttir.

32. Samskipta- og upplýsingakerfi skal meðhöndla sérhver samtengd upplýsingatæknikerfi sem væru þau óáreiðanleg og gera verndarráðstafanir til að fylgjast með skiptum á trúnaðarflokkuðum upplýsingum.

33. Framfylgja ber eftirfarandi grunnkröfum vegna allra samtenginga samskipta- og upplýsingakerfis við önnur upplýsingatæknikerfi:

a) viðkomandi bær yfirvöld skulu samþykkja viðskipta- eða rekstrarkröfur fyrir slíkar samtengingar,

b) samtengingarnar skulu meðhöndlaðar í áhættustjórnunar- og vottunarferli og þarfnast samþykkis bærs yfirvalds á sviði öryggisvottunar og

c) virkja skal jaðarverndarþjónustu (BPS) á mörkum allra samskipta- og upplýsingakerfa.

34. Eigi skal tengja saman vottað samskipta- og upplýsingakerfi og óvarið netkerfi eða almenningsnetkerfi, nema samskipta- og upplýsingakerfið hafi vottað jaðarverndarþjónustu sem er uppsett í slíkum tilgangi á milli samskipta- og upplýsingakerfisins og hins óvarða almenningsnetkerfis. Bært yfirvald á sviði upplýsingaöryggis skal yfirfara og bært yfirvald á sviði öryggisvottunar skal samþykkja öryggisráðstafanir vegna slíkra samtenginga.

Þegar hið óvarða kerfi eða almenningsnetkerfið er notað eingöngu sem flutningstæki og dulkóðunartæki, sem er samþykkt skv. 10. gr., hefur dulkóðað gögnin, skal eigi líta svo á að slík tenging sé samtenging.

35. Bein eða flæðandi samtenging samskipta- og upplýsingakerfis, sem er vottað til þess að meðhöndla ALGJÖRT LEYNDARMÁL ESB, og óvarins kerfis eða almenningsnetkerfis er bönnuð.

**Geymslumiðlar fyrir rafræna gagnavinnslu.**

36. Geymslumiðlum fyrir rafræna gagnavinnslu skal eytt samkvæmt verklagi sem viðkomandi bært öryggisyfirvald samþykkir.

37. Geymslumiðla fyrir rafræna gagnavinnslu skal endurnýta, með því að lækka trúnaðarstig þeirra eða aflétta af þeim trúnaðarflokkun í samræmi við öryggisstefnu sem komið skal á skv. 1. mgr. 6. gr.

**Neyðarástand.**

38. Þrátt fyrir ákvæði ákvörðunar þessarar er heimilt að beita þeim sérstöku verklagsreglum sem er lýst hér að aftan ef neyðarástand skapast, t.d. meðan yfirvofandi eða raunverulegt hættuástand ríkir, átök, stríðsástand eða í sérstökum rekstraraðstæðum.

39. Trúnaðarflokkaðar upplýsingar ESB má flytja með því að nota dulkóðunartæki, sem hafa verið vottuð fyrir lægra stig trúnaðarflokkunar, eða án dulkóðunar með samþykki viðkomandi bærs yfirvalds, ef seinkun myndi valda skaða sem vegur þyngra en sá skaði sem uppljóstrun hins trúnaðarflokkaða efnis gæti haft í för með sér og ef:

a) sendandinn og viðtakandinn ráða ekki yfir þeirri aðstöðu til dulkóðunar sem krafist er eða yfir neinni aðstöðu til dulkóðunar og b) ekki er hægt að flytja hið trúnaðarflokkaða efni eftir öðrum leiðum.

40. Trúnaðarflokkaðar upplýsingar, sem eru fluttar við þær aðstæður sem settar eru fram í 38. mgr., skulu ekki hafa neinar merkingar eða ábendingar sem aðgreina þær frá upplýsingum sem ekki eru trúnaðarflokkaðar eða unnt er að vernda með tiltækum dulkóðunartækjum. Tilkynna ber viðtakendum um viðeigandi stig trúnaðarflokkunar án tafar eftir öðrum leiðum.

41. Þurfi að grípa til ákvæðis 38. mgr. skal gefa viðkomandi bæru yfirvaldi og öryggisnefndinni skýrslu um það eftir á.

III. STARFSEMI OG YFIRVÖLD Á SVIÐI UPPLÝSINGAÖRYGGIS

42. Eftirfarandi starfsemi á sviði upplýsingaöryggis skal komið á í aðildarríkjunum og á aðalskrifstofu ráðsins. Eigi er gerð krafa um að starfsemi þessi fari fram innan einstakra skipulagseininga. Þær skulu hafa aðskilin umboð. Samt sem áður er heimilt að sameina eða samþætta þessa starfsemi og skyldur, sem henni fylgja, innan sömu skipulagseiningar eða skipta henni upp milli mismunandi skipulagseininga, að því tilskildu að komið sé í veg fyrir innri hagsmunaárekstra eða árekstra milli verkefna.

**Yfirvald á sviði upplýsingaöryggis.**

43. Yfirvald á sviði upplýsingaöryggis ber ábyrgð á:

a) að þróa öryggisstefnu og öryggisleiðbeiningar á sviði upplýsingaöryggis og að vakta skilvirkni og viðeiganleika þeirra,

b) að vernda og annast um tæknilegar upplýsingar sem tengjast dulkóðunartækjum,

c) að tryggja að þær ráðstafanir á sviði upplýsingaöryggis, sem er kosið að gera til verndar trúnaðarflokkuðum upplýsingum ESB, samræmist viðeigandi stefnumiðum sem segja fyrir um hæfi þeirra og val,

d) að tryggja að dulkóðunartæki séu valin í samræmi við þau stefnumið sem segja fyrir um hæfi þeirra og val,

e) að samræma þjálfun í og vitund um upplýsingaöryggi,

f) að hafa samráð við söluaðila kerfisins, þá sem annast öryggi og fulltrúa notenda um mál er varða öryggisstefnu og -leiðbeiningar á sviði upplýsingaöryggis og g) að tryggja að viðeigandi sérþekking sé til staðar í sérfræðiundirnefndum öryggisnefndarinnar vegna málefna á sviði upplýsingaöryggis.

**TEMPEST-yfirvald.**

44. TEMPEST-yfirvald ber ábyrgð á því að tryggja að samskipta- og upplýsingakerfi séu í samræmi við stefnumið og leiðbeiningar TEMPEST. Það samþykkir gagnráðstafanir TEMPEST viðvíkjandi uppsetningu og tækjum til verndar trúnaðarflokkuðum upplýsingum ESB upp að skilgreindu stigi trúnaðarflokkunar í rekstrarumhverfi sínu.

**Vottunaryfirvald dulkóðunar.**

45. Vottunaryfirvald dulkóðunar ber ábyrgð á því að tryggja að dulkóðunartæki séu í samræmi við innlend stefnumið varðandi dulkóðun eða stefnumið ráðsins varðandi dulkóðun. Það veitir samþykki sitt fyrir dulkóðunartæki til verndar trúnaðarflokkuðum upplýsingum ESB upp að skilgreindu stigi trúnaðarflokkunar í rekstrarumhverfi sínu. Að því er aðildarríkin varðar ber vottunaryfirvald dulkóðunar auk þess ábyrgð á því að meta dulkóðunartæki.

**Yfirvald á sviði dulkóðaðrar dreifingar.**

46. Yfirvald á sviði dulkóðaðrar dreifingar ber ábyrgð á:

a) umsjón með og reikningsskilum á dulkóðuðu efni ESB,

b) að tryggja að viðeigandi verklagsreglum sé framfylgt og leiðir séu fundnar til að standa reikningsskil og skila öruggri meðhöndlun á öllu dulkóðuðu efni ESB og til að geyma það og dreifa því og c) að tryggja flutning dulkóðaðs efnis ESB til eða frá einstaklingum eða þjónustustofnunum sem nota það.

**Yfirvald á sviði öryggisvottunar.**

47. Yfirvald á sviði öryggisvottunar fyrir sérhvert kerfi ber ábyrgð á:

a) að tryggja að samskipta- og upplýsingakerfi sé í samræmi við viðeigandi öryggisstefnu og öryggisleiðbeiningar, útvega samþykkisyfirlýsingu fyrir samskipta- og upplýsingakerfi þess efnis að það geti meðhöndlað trúnaðarflokkaðar upplýsingar ESB upp að skilgreindu stigi trúnaðarflokkunar í rekstrarumhverfi sínu, settir séu fram skilmálar og skilyrði vottunarinnar og viðmið vegna krafna um endurnýjað samþykki,

b) að koma á öryggisvottunarferli í samræmi við viðeigandi stefnumál, þar sem skilyrði fyrir samþykki samskipta- og upplýsingakerfis, sem heyrir undir það, koma fram með skýrum hætti,

c) að skilgreina áætlun um öryggisvottun, þar sem sett er fram hversu nákvæmt vottunarferlið þarf að vera til þess að svara til þess áreiðanleikastigs sem krafist er,

d) að yfirfara og samþykkja gögn sem varða öryggismál, þ.m.t. yfirlýsingar um áhættustjórnun og eftirstandandi áhættu, yfirlýsingar um kerfismiðaðar öryggiskröfur, gögn um sannprófun framkvæmdar öryggisráðstafana og öryggisverkhættir, og að tryggja að þau séu í samræmi við reglur ráðsins um og stefnu þess í öryggismálum,

e) að kanna hvernig öryggisráðstöfunum er beitt með tilliti til samskipta- og upplýsingakerfisins með því að framkvæma öryggismat, eftirlit eða endurskoðun eða ábyrgjast að þessir verkþættir fari fram,

f) að skilgreina öryggiskröfur (t.d. vottunarstig starfsfólks) sem skulu gilda um trúnaðarstöður sem tengjast samskipta- og upplýsingakerfinu,

g) að staðfesta val samþykktra dulkóðunartækja og TEMPEST-tækja sem eru notuð til að tryggja öryggi samskipta- og upplýsingakerfis,

h) að samþykkja eða, ef við á, taka þátt í að samþykkja, ásamt með öðrum, samtengingu tiltekins samskipta- og upplýsingakerfis við annað samskipta- og upplýsingakerfi og i) að hafa samráð við söluaðila kerfisins, þá sem annast öryggi og fulltrúa notenda um framkvæmd öryggisáhættustjórnunar, einkum með tilliti til eftirstandandi áhættu, og um hvaða skilmálar og skilyrði skuli gilda um samþykkisyfirlýsinguna.

48. Yfirvald aðalskrifstofu ráðsins á sviði öryggisvottunar ber ábyrgð á vottun allra samskipta- og upplýsingakerfa sem eru í rekstri og heyra undir verksvið aðalskrifstofu ráðsins.

49. Viðkomandi yfirvald aðildarríkis á sviði öryggisvottunar ber ábyrgð á vottun samskipta- og upplýsingakerfis og íhluta þeirra sem eru í rekstri og heyra undir verksvið aðildarríkis.

50. Sameiginlegt öryggisvottunarráð (SAB) ber ábyrgð á vottun samskipta- og upplýsingakerfa sem heyra undir verkvið bæði yfirvalds aðalskrifstofu ráðsins á sviði öryggisvottunar og yfirvalds aðildarríkis á sviði öryggisvottunar. Í ráðinu situr fulltrúi yfirvalds á sviði öryggisvottunar frá sérhverju aðildarríki og fulltrúi yfirvalds ráðsins á sviði öryggisvottunar tekur þátt í störfum þess. Öðrum rekstrareiningum með búnað sem tengir saman línur í samskipta- og upplýsingakerfi skal boðið að sækja fundi ráðsins þegar viðkomandi kerfi er til umfjöllunar.

Fulltrúi yfirvalds aðalskrifstofu ráðsins á sviði öryggisvottunar fer með formennsku í sameiginlega öryggisvottunarráðinu. Ákvarðanir ráðsins skulu teknar með samhljóða samþykki fulltrúa yfirvalda á sviði öryggisvottunar frá stofnunum, aðildarríkjum og öðrum rekstrareiningum með búnað sem tengir saman línur í samskipta- og upplýsingakerfinu. Ráðið gefur öryggisnefndinni reglubundnar skýrslur um starfsemi sína og tilkynnir henni um allar vottunaryfirlýsingar.

**Framkvæmdaryfirvald upplýsingaöryggis.**

51. Framkvæmdaryfirvald upplýsingaöryggis fyrir sérhvert kerfi ber ábyrgð á:

a) vinnslu öryggisgagna í samræmi við stefnumið og reglur á sviði öryggismála, einkum yfirlýsingum um kerfismiðaðar öryggiskröfur, þ.m.t. yfirlýsing um eftirstandandi áhættu, öryggisverkhættir og áætlun um dulkóðun í vottunarferli samskipta- og upplýsingakerfisins,

b) þátttöku í vali og prófun á kerfismiðuðum og tæknilegum öryggisráðstöfunum, -tækjum og -hugbúnaði til þess að hafa eftirlit með því hvernig þeim er beitt og til þess að tryggja að þeim sé komið fyrir, skipað saman og viðhaldið í samræmi við viðeigandi öryggisgögn,

c) þátttöku í vali á TEMPEST-öryggisráðstöfunum og -tækjum ef þess er krafist í yfirlýsingu um kerfismiðaðar öryggiskröfur og því að tryggja að þeim sé komið fyrir á öruggan hátt og viðhaldið í samstarfi við TEMPEST yfirvaldið,

d) vöktun þess hvernig öryggisverkhættir koma til framkvæmda og hvernig þeim er beitt og því að fela eiganda kerfisins ábyrgð á rekstraröryggi, þar sem það á við,

e) umsjón og meðferð dulkóðunartækja, því að tryggja varðveislu dulkóðaðs efnis og eftirlitsskylds efnis og, ef þess er krafist, að tryggja gerð dulkóðunartákna,

f) endurskoðun og prófunum á öryggisgreiningu, einkum í tengslum við vinnslu viðeigandi skýrslna um áhættu, eftir því sem viðkomandi yfirvald á sviði öryggisvottunar gerir kröfu um,

g) sértækri þjálfun í upplýsingaöryggi vegna samskipta- og upplýsingakerfa,

h) beitingu og framfylgd sértækra öryggisráðstafana vegna samskipta- og upplýsingakerfa.

--------------------------------------------------

*V. VIÐAUKI*

**IÐNAÐARÖRYGGI**

I. INNGANGUR

1. Í viðauka þessum er kveðið á um framkvæmd efnisatriða 11. gr. Mælt er fyrir um almenn öryggisákvæði sem gilda um iðnfyrirtæki eða aðrar rekstrareiningar í samningaviðræðum í aðdraganda samningsgerðar og allan líftíma trúnaðarflokkaðra verktakasamninga sem aðalskrifstofa ráðsins gerir.

2. Ráðið skal samþykkja stefnu um iðnaðaröryggi, þar sem einkum eru tilgreindar ítarlegar kröfur um öryggisvottun starfsstöðva, öryggisskilmála (SAL), heimsóknir, sendingu og flutning trúnaðarflokkaðra upplýsinga ESB.

II. ÖRYGGISÞÆTTIR Í TRÚNAÐARFLOKKUÐUM VERKTAKASAMNINGI

**Leiðbeiningar um trúnaðarflokkun (SCG).**

3. Áður en útboð er hafið eða trúnaðarflokkaðir verktakasamningar gerðir skal aðalskrifstofa ráðsins, sem samningsyfirvald, ákvarða trúnaðarflokkun allra upplýsinga, sem bjóðendur og verktakar fá aðgang að, ásamt trúnaðarflokkun allra upplýsinga sem viðkomandi verktaki mun taka saman. Aðalskrifstofa ráðsins skal í þessu skyni taka saman leiðbeiningar um trúnaðarflokkun sem nota skal við framkvæmd samningsins.

4. Eftirfarandi meginreglur gilda þegar ákvarða skal trúnaðarflokkun ólíkra þátta trúnaðarflokkaðs verktakasamnings:

a) Aðalskrifstofa ráðsins skal, þegar leiðbeiningar um trúnaðarflokkun eru teknar saman, taka tillit til viðeigandi öryggisafstöðu, m.a. til þeirrar trúnaðarflokkunar sem útgefandi veittra upplýsinga hefur gefið þeim og samþykkt að nota skuli vegna samningsins.

b) heildarstig trúnaðarflokkunar verktakasamningsins skal ekki vera lægra en hæsta trúnaðarstig staks þáttar hans og c) aðalskrifstofa ráðsins skal, þar sem það á við, hafa samráð við stjórnvöld aðildarríkjanna á sviði þjóðaröryggis og/eða tilgreind öryggisyfirvöld þeirra eða hvaða annað viðkomandi bært öryggisyfirvald sem er, verði breytingar gerðar á trúnaðarflokkun upplýsinga, sem verktakar taka saman eða láta í té í tengslum við framkvæmd verktakasamnings, og þegar leiðbeiningum um trúnaðarflokkun er breytt síðar meir.

**Öryggisskilmálar.**

5. Öryggiskröfum vegna einstakra samninga skal lýst í öryggisskilmálum. Öryggisskilmálar skulu, eftir því sem við á, innihalda leiðbeiningar um trúnaðarflokkun og er óaðskiljanlegur hluti trúnaðarflokkaðs verktakasamnings eða samnings um undirverktöku.

6. Öryggisskilmálar skulu innihalda ákvæði sem skylda viðkomandi verktaka og/eða undirverktaka til þess að uppfylla þær lágmarksviðmiðanir sem mælt er fyrir um í ákvörðun þessari. Uppfylli verktaki ekki þessar lágmarksviðmiðanir getur það verið nægilegt tilefni til að segja verktakasamningi upp.

**Öryggisleiðbeiningar vegna áætlana og/eða verkefna (PSI).**

7. Viðkomandi samningsyfirvald, sem er tilnefnt til þess að stjórna viðkomandi áætlun eða verkefni, getur tekið saman sérstakar öryggisleiðbeiningar vegna áætlana og/eða verkefna, allt eftir umfangi þeirra og feli þær í sér aðgang að, meðhöndlun á eða geymslu trúnaðarflokkaðra upplýsinga ESB. Stjórnvöld aðildarríkjanna á sviði þjóðaröryggis og/eða tilgreind öryggisyfirvöld þeirra eða hvaða annað bært öryggisyfirvald sem er, sem á aðild að viðkomandi áætlun og/eða verkefni, skulu samþykkja öryggisleiðbeiningar vegna áætlana og/eða verkefna og kunna þær að innihalda frekari öryggiskröfur.

III. ÖRYGGISVOTTUN STARFSSTÖÐVAR (FSC)

8. Stjórnvald á sviði þjóðaröryggis eða tilgreint öryggisyfirvald eða hvert annað bært öryggisyfirvald aðildarríkis sem er veitir öryggisvottun starfsstöðvar sem gefur til kynna, í samræmi við innlend lög og reglugerðir, að iðnfyrirtæki eða önnur rekstrareining geti verndað trúnaðarflokkaðar upplýsingar ESB á viðeigandi stigi trúnaðarflokkunar (TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB) innan starfsstöðva sinna. Leggja ber öryggisvottun starfsstöðvar fyrir aðalskrifstofu ráðsins, sem viðkomandi samningsyfirvald, áður en verktaki eða undirverktaki eða hugsanlegur verktaki eða undirverktaki fær eða honum er veittur aðgangur að trúnaðarflokkuðum upplýsingum ESB.

9. Viðkomandi stjórnvald á sviði þjóðaröryggis eða tilgreint öryggisyfirvald skal, þegar það gefur út öryggisvottun starfsstöðvar, að minnsta kosti:

a) meta heilindi iðnfyrirtækisins eða annarrar rekstrareiningar,

b) meta eignarhald, yfirráð eða þann möguleika að hafa óréttmæt áhrif sem geta talist öryggisáhætta,

c) sannreyna að viðkomandi iðnfyrirtæki eða sérhver önnur rekstrareining hafi komið á öryggiskerfi í viðkomandi starfsstöð, sem tekur til allra viðeigandi öryggisráðstafana sem eru nauðsynlegar til verndar upplýsingum eða efni á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB, sem uppfyllir þær kröfur sem mælt er fyrir um í ákvörðun þessari,

d) sannreyna að fyrir stjórnendur, eigendur og starfsfólk, sem skulu hafa aðgang að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB, hafi staða starfsfólks með tilliti til öryggis verið staðfest í samræmi við þær kröfur sem mælt er fyrir um í ákvörðun þessari,

e) sannreyna að iðnfyrirtæki eða sérver önnur rekstrareining hafi skipað öryggisfulltrúa starfsstöðvarinnar sem er ábyrgur gagnvart stjórnendum hennar fyrir því að framfylgja öryggisskyldum innan slíkrar rekstrareiningar.

10. Aðalskrifstofa ráðsins skal, þar sem við á og sem samningsyfirvald, tilkynna viðkomandi stjórnvaldi á sviði þjóðaröryggis og/eða tilgreindu öryggisyfirvaldi eða hvaða öðru bæru öryggisyfirvaldi sem er að krafist sé öryggisvottunar starfsstöðvar í aðdraganda samningsgerðar eða vegna framkvæmdar samnings. Krefjast ber öryggisvottunar starfsstöðvar eða öryggisvottunar starfsfólks í aðdraganda samningsgerðar, ef nauðsynlegt reynist að láta trúnaðarflokkaðar upplýsingar ESB á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB í té meðan útboðsferlið stendur yfir.

11. Viðkomandi samningsyfirvald skal ekki ganga frá trúnaðarflokkuðum verktakasamningi við bjóðanda, sem er valinn, áður en fengin er staðfesting frá stjórnvaldi á sviði þjóðaröryggis og/eða tilgreindu öryggisyfirvaldi eða hvaða öðru bæru öryggisyfirvaldi sem er í því aðildarríki þar sem verktakinn eða undirverktakinn er skráður þess efnis að viðeigandi öryggisvottun starfsstöðvar hafi verið gefin út, þar sem þess er krafist.

12. Viðkomandi stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald eða hvað annað bært öryggisyfirvald sem er, sem hefur gefið út öryggisvottun starfsstöðvar, skal tilkynna aðalskrifstofu ráðsins, sem samningsyfirvaldi, um breytingar sem hafa áhrif á öryggisvottun starfsstöðvar. Tilkynna ber stjórnvaldi á sviði þjóðaröryggis og/eða tilgreindu öryggisyfirvaldi eða öðru bæru öryggisyfirvaldi um slíkar breytingar ef um samning við undirverktaka er að ræða.

13. Afturkalli viðkomandi stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald eða hvaða annað bært öryggisyfirvald sem er öryggisvottun starfsstöðvar, gefur það aðalskrifstofu ráðsins, sem samningsyfirvaldi, nægilega ástæðu til að segja trúnaðarflokkuðum verktakasamningi upp eða útiloka bjóðanda frá samkeppninni.

IV. TRÚNAÐARFLOKKAÐIR VERKTAKASAMNINGAR OG SAMNINGAR UM UNDIRVERKTÖKU

14. Séu bjóðanda afhentar trúnaðarflokkaðar upplýsingar ESB í aðdraganda samningsgerðar skal útboðið innihalda ákvæði sem skyldar bjóðanda, sem leggur ekki fram tilboð eða er ekki valinn, til að skila öllum trúnaðarflokkuðum skjölum innan tiltekins frests.

15. Eftir að trúnaðarflokkaður verktakasamningur eða samningur um undirverktöku hefur verið gerður skal aðalskrifstofa ráðsins, sem samningsyfirvald, tilkynna stjórnvaldi á sviði þjóðaröryggis og/eða tilgreindu öryggisyfirvaldi eða hvaða öðru bæru öryggisyfirvaldi sem er, sem viðkomandi verktaki eða undirverktaki fellur undir, um öryggisákvæði hins trúnaðarflokkaða samnings.

16. Þegar slíkum samningum er sagt upp, skal aðalskrifstofa ráðsins, sem samningsyfirvald (og/eða viðkomandi stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald eða hvaða annað bært öryggisyfirvald sem er, eftir því sem við á, ef um samning um undirverktöku er að ræða) þegar í stað tilkynna það viðkomandi stjórnvaldi á sviði þjóðaröryggis og/eða tilgreindu öryggisyfirvaldi eða hvaða öðru bæru öryggisyfirvaldi sem er í því aðildarríki þar sem verktakinn eða undirverktakinn er skráður.

17. Almenna reglan er að gerð er krafa um að verktakinn eða undirverktakinn skili samningsyfirvaldinu aftur öllum trúnaðarflokkuðum upplýsingum ESB, sem það hefur undir höndum, við uppsögn trúnaðarflokkaðs verktakasamnings eða samnings um undirverktöku.

18. Í öryggisskilmálum skal setja sértæk ákvæði um förgun trúnaðarflokkaðra upplýsinga ESB meðan á framkvæmd verktakasamnings stendur eða við uppsögn hans.

19. Sé viðkomandi verktaka eða undirverktaka heimilað að halda eftir trúnaðarflokkuðum upplýsingum ESB eftir uppsögn samnings, ber að virða áfram þær lágmarksviðmiðanir sem mælt er fyrir um í ákvörðun þessari og skal verktakinn eða undirverktakinn tryggja leynd trúnaðarflokkaðra upplýsinga ESB.

20. Setja ber fram skilyrði, sem gilda um samninga verktaka við undirverktaka, í útboðsgögnunum og samningnum.

21. Verktaki skal afla heimildar aðalskrifstofu ráðsins, sem samningsyfirvaldi, áður en hann gerir samning við undirverktaka um einhverja hluta trúnaðarflokkaðs samnings. Óheimilt er að gera samning um undirverktöku við iðnfyrirtæki eða aðrar rekstrareiningar sem eru skráðar í ríki utan ESB og ekki hafa gengið frá samning um upplýsingaöryggi við ESB.

22. Viðkomandi verktaki ber ábyrgð á því að tryggt sé að öll starfsemi undirverktaka fari fram eftir þeim lágmarksviðmiðunum sem mælt er fyrir um í ákvörðun þessari og skal ekki afhenda undirverktaka trúnaðarflokkaðar upplýsingar ESB án skriflegs fyrirframsamþykkis viðkomandi samningsyfirvalds.

23. Viðkomandi samningsyfirvald skal gæta réttinda útgefanda, með tilliti til trúnaðarflokkaðra upplýsinga ESB sem verða til hjá verktakanum eða undirverktakanum eða sem þeir meðhöndla.

V. HEIMSÓKNIR Í TENGSLUM VIÐ TRÚNAÐARFLOKKAÐA SAMNINGA

24. Þegar aðalskrifstofa ráðsins, verktakar eða undirverktakar, þarfnast aðgangs að upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB á athafnasvæði hvers annars vegna framkvæmdar trúnaðarflokkaðs samnings, skal skipuleggja heimsóknir í samráði við viðkomandi stjórnvöld á sviði þjóðaröryggis og/eða tilgreind öryggisyfirvöld eða hvaða annað viðkomandi bært öryggisyfirvald sem er. Stjórnvöld á sviði þjóðaröryggis og/eða tilgreind öryggisyfirvöld geta, engu að síður og í tengslum við sérstök verkefni, samþykkt verklag sem gerir kleift að skipuleggja slíkar heimsóknir milliliðalaust.

25. Allir þeir sem fara í fyrrnefndar heimsóknir skulu hafa viðeigandi öryggisvottun starfsfólks og „vitneskjuþörf“ vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB sem tengjast samningi aðalskrifstofu ráðsins.

26. Þeir sem fara í fyrrnefndar heimsóknir skulu eingöngu fá aðgang að þeim trúnaðarflokkuðu upplýsingum ESB sem varða tilgang heimsóknarinnar.

VI. SENDING OG FLUTNINGUR TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB

27. Viðeigandi ákvæði 10. gr. og IV. viðauka gilda um rafræna sendingu trúnaðarflokkaðra upplýsinga ESB.

28. Viðeigandi ákvæði III. viðauka gilda, í samræmi innlend lög og reglugerðir, um flutning trúnaðarflokkaðra upplýsinga ESB.

29. Þegar senda á trúnaðarflokkað efni sem farm skal beita eftirfarandi meginreglum við ákvörðun öryggisfyrirkomulags:

a) tryggja ber öryggi á öllum stigum meðan á flutningi stendur frá upphafsstað til lokaákvörðunarstaðar,

b) miða ber verndarstig sendingar við hæsta stig trúnaðarflokkunar þess efnis sem hún samanstendur af,

c) þau fyrirtæki sem annast flutning skulu hljóta öryggisvottun starfsstöðvar á viðeigandi stigi. Í slíkum tilvikum skal starfsfólkið, sem meðhöndlar sendinguna, hljóta öryggisvottun samkvæmt ákvæðum I. viðauka,

d) áður en efni á trúnaðarstiginu TRÚNAÐARMÁL ESB eða LEYNDARMÁL ESB er flutt yfir landamæri skal sendandinn semja flutningsáætlun sem skal hljóta samþykki viðkomandi stjórnvalds á sviði þjóðaröryggis og/eða tilgreindra öryggisyfirvalda eða hvaða annars viðkomandi bærs öryggisyfirvalds,

e) ferðir milli staða skulu farnar beint án viðkomu eftir því sem frekast er unnt og þeim skal lokið eins fljótt og aðstæður leyfa,

f) þær leiðir sem eru farnar skulu, ávallt þegar því verður komið við, liggja um aðildarríki. Því aðeins skyldi fara leiðir gegnum ríki, önnur en aðildarríki, að viðkomandi stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald eða hvaða annað bært öryggisyfirvald sem er, í ríki sendandans og í ríki viðtakandans, heimili það.

VII. FLUTNINGUR TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB TIL VERKTAKA Í ÞRIÐJU RÍKJUM

30. Trúnaðarflokkaðar upplýsingar ESB skal flytja til verktaka og undirverktaka í þriðju ríkjum í samræmi við öryggisráðstafanir sem aðalskrifstofa ráðsins, sem samningsyfirvald, og viðkomandi stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald þess þriðja ríkis þar sem verktakinn er skráður koma sér saman um.

VIII. MEÐHÖNDLUN OG GEYMSLA UPPLÝSINGA Á TRÚNAÐARSTIGINU TAKMARKAÐUR AÐGANGUR ESB

31. Aðalskrifstofu ráðsins, sem samningsyfirvaldi, er heimilt, í samstarfi við viðkomandi stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald í hlutaðeigandi aðildarríki, að heimsækja starfsstöðvar verktaka og/eða undirverktaka, með vísan til samningsákvæða, til þess að sannreyna að viðeigandi öryggisráðstafanir til verndar trúnaðarflokkuðum upplýsingum ESB á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB, sem er krafist samkvæmt viðkomandi samningi, hafi verið gerðar.

32. Aðalskrifstofa ráðsins, sem samningsyfirvald, skal, eftir því sem þurfa þykir og samkvæmt innlendum lögum og reglugerðum, tilkynna stjórnvöldum á sviði þjóðaröryggis og/eða tilgreindum öryggisyfirvöldum eða hvaða öðru bæru öryggisyfirvaldi sem er um verktakasamninga eða samninga um undirverktöku sem innihalda upplýsingar á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB.

33. Ekki er krafist öryggisvottunar starfsstöðvar eða öryggisvottunar starfsfólks fyrir verktaka eða undirverktaka og starfsfólk þeirra vegna samninga sem aðalskrifstofa ráðsins gerir og innihalda upplýsingar á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB.

34. Aðalskrifstofa ráðsins, sem samningsyfirvald, skoðar svör við útboðum vegna verktakasamninga, þar sem krafist er aðgangs að upplýsingum á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB, þrátt fyrir kröfur um öryggisvottun starfsstöðvar eða öryggisvottun starfsfólks sem kunna að vera gerðar samkvæmt innlendum lögum og reglugerðum.

35. Þau skilyrði sem skulu gilda um samninga viðkomandi verktaka við undirverktaka skulu vera í samræmi við ákvæði 21. mgr.

36. Feli verktakasamningur í sér að upplýsingar á trúnaðarstiginu TAKMARKAÐUR AÐGANGUR ESB séu meðhöndlaðar í samskipta- og upplýsingakerfi, sem verktaki rekur, skal aðalskrifstofa ráðsins, sem samningsyfirvald, tryggja að í samningnum eða sérhverjum samningi um undirverktöku séu tilgreindar nauðsynlegar tækni- og stjórnsýslukröfur um vottun samskipta- og upplýsingakerfisins, sem svara til þeirrar áhættu sem er talin vera fyrir hendi, að teknu tilliti til allra viðeigandi þátta. Viðkomandi samningsyfirvald og stjórnvald á sviði þjóðaröryggis og/eða tilgreint öryggisyfirvald skulu semja um sín á milli um hversu víðtæk vottun fyrrnefnds samskipta- og upplýsingakerfis skal að vera.

--------------------------------------------------

*VI. VIÐAUKI*

**SKIPTI Á TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM VIÐ ÞRIÐJU RÍKI OG ALÞJÓÐASTOFNANIR**

I. INNGANGUR

1. Í viðauka þessum er kveðið á um framkvæmd efnisatriða 12. gr.

II. REGLURAMMI UM SKIPTI Á TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM

2. Ákveði ráðið að skipta á trúnaðarflokkuðum upplýsingum sé þörf í langan tíma,

— skal ganga frá samningi um upplýsingaöryggi eða

— skal ganga frá stjórnsýslusamkomulagi,

í samræmi við 2. mgr. 12. gr. og III. og IV. lið og á grundvelli tilmæla öryggisnefndarinnar.

3. Standi til að afhenda þriðju ríkjum eða alþjóðastofnunum, sem taka þátt í aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum (CSDP), trúnaðarflokkaðar upplýsingar ESB, sem teknar eru saman vegna slíkrar aðgerðar, og hvorugt þeirra regluramma er um getur í 2. mgr. er fyrirliggjandi, skal stjórna skiptum á trúnaðarflokkuðum upplýsingum ESB við þriðja ríki eða alþjóðastofnun, sem tekur þátt í aðgerðinni, í samræmi við ákvæði V. hluta og samkvæmt:

— rammasamningi um þátttöku,

— samningi um þátttöku sem er gerður sérstaklega vegna viðkomandi aðgerðar eða

— ef hvorugur ofangreindra samninga er fyrirliggjandi, samkvæmt stjórnsýslusamkomulagi sem er gert sérstaklega vegna viðkomandi aðgerðar.

4. Liggi reglurammi, er um getur í 2. og 3. mgr., ekki fyrir og sé ákveðið að miðla trúnaðarflokkuðum upplýsingum ESB til þriðja ríkis eða alþjóðastofnunar í sérstöku undantekningartilviki samkvæmt ákvæðum VI. hluta, skal leita eftir skriflegri tryggingu viðkomandi þriðja ríkis eða alþjóðastofnunar til að ábyrgjast að það eða hún verndi trúnaðarflokkaðar upplýsinga ESB, sem hefur verið miðlað, í samræmi við grundvallarsetningar og lágmarksviðmiðanir sem mælt er fyrir um í ákvörðun þessari.

III. SAMNINGAR UM UPPLÝSINGAÖRYGGI

5. Í samningum um upplýsingaöryggi skulu koma fram grundvallarsetningar og lágmarksviðmiðanir sem gilda um skipti á trúnaðarflokkuðum upplýsingum milli ESB og þriðja ríkis eða alþjóðastofnunar.

6. Í samningum um upplýsingaöryggi skal kveðið á um fyrirkomulag tæknilegrar framkvæmdar sem öryggisdeild aðalskrifstofu ráðsins, öryggismálaskrifstofa framkvæmdastjórnarinnar og bært öryggisyfirvald viðkomandi þriðja ríkis eða alþjóðastofnunar koma sér saman um. Með slíku fyrirkomulagi skal tekið mið af því verndarstigi sem gildandi öryggisreglur, skipulag og verklagsreglur í viðkomandi þriðja ríki eða alþjóðastofnun kveða á um. Öryggisnefndin skal samþykkja fyrrnefnt fyrirkomulag.

7. Ekki skal skiptast á trúnaðarflokkuðum upplýsingum ESB með rafrænum hætti nema skýrt sé kveðið á um það í viðeigandi samningi um upplýsingaöryggi eða samkvæmt fyrirkomulagi tæknilegrar framkvæmdar.

8. Í samningum um upplýsingaöryggi skal vera ákvæði um að öryggisdeild aðalskrifstofu ráðsins og öryggismálaskrifstofa framkvæmdastjórnarinnar skuli sammælast um, áður en skiptst er á trúnaðarflokkuðum upplýsingum samkvæmt viðeigandi samningi, að móttakandinn sé fær um að vernda og tryggja upplýsingar, sem hann fær afhentar, með viðeigandi hætti.

9. Þegar ráðið gengur frá samningi um upplýsingaöryggi skal tilnefna skráningarstofu hjá sérhverjum aðila sem gegnir hlutverki aðalviðtökustaðar og -sendingarstaðar fyrir skipti á trúnaðarflokkuðum upplýsingum.

10. Öryggisdeild aðalskrifstofu ráðsins skal, ásamt öryggismálaskrifstofu framkvæmdastjórnarinnar og í samráði við viðkomandi þriðja ríki eða alþjóðastofnun, fara í matsheimsóknir í því skyni að leggja mat á skilvirkni öryggisreglna, -skipulags og -verklags í viðkomandi þriðja ríki eða alþjóðastofnun. Matsheimsóknir þessar skulu fara fram samkvæmt viðeigandi ákvæðum III. viðauka og í þeim skal meta:

a) þann regluramma sem gildir um verndun trúnaðarflokkaðra upplýsinga,

b) öll sérkenni öryggisstefnunnar og skipulag öryggismála í viðkomandi þriðja ríki eða alþjóðastofnun sem geta haft áhrif á það stig trúnaðarflokkaðra upplýsinga sem kann að verða skiptst á.

c) þær öryggisráðstafanir og verklagsreglur sem er fylgt í raun og

d) verklag við öryggisvottun vegna þess stigs trúnaðarflokkaðra upplýsinga ESB sem til stendur að miðla.

11. Hópurinn, sem fer í matsheimsókn á vegum Evrópusambandsins, skal meta hvort öryggisreglur og -verklag í viðkomandi þriðja ríki eða alþjóðastofnun séu fullnægjandi til verndar trúnaðarflokkaðra upplýsinga ESB á viðeigandi trúnaðarstigi.

12. Niðurstöður slíkra heimsókna skulu lagðar fram í skýrslu, en á grundvelli hennar skal öryggisnefndin ákvarða hámarksstig trúnaðarflokkaðra upplýsinga ESB, sem heimilt er að skiptast á í pappírformi, og þar sem það á við í rafrænni mynd, við viðkomandi þriðja aðila, og ákvarða þau önnur sérstöku skilyrði sem gilda um skipti við þann aðila.

13. Leggja skal kapp á að fara í matsheimsókn til viðkomandi þriðja ríkis eða alþjóðastofnunar og meta til fulls ástand öryggismála, áður en öryggisnefndin samþykkir fyrirkomulag framkvæmdar, til þess að ganga úr skugga um eiginleika og skilvirkni þess öryggiskerfis sem er til staðar. Reynist hins vegar ekki unnt að fara í slíka heimsókn skal öryggisdeild aðalskrifstofu ráðsins gefa öryggisnefndinni eins ítarlega skýrslu og frekast er unnt, sem er byggð á þeim upplýsingum sem öryggisdeildinni eru tiltækar, þar sem öryggisnefndin er upplýst um gildandi öryggisreglur og skipulag öryggismála hjá viðkomandi þriðja ríki eða alþjóðastofnun.

14. Öryggisnefndin getur ákveðið, meðan þess er beðið að niðurstöður matsheimsóknar verði kannaðar, að engum trúnaðarflokkuðum upplýsingum ESB verði miðlað, eða kunni einungis að verða miðlað upp að ákveðnu trúnaðarstigi, eða getur ákveðið sérstök skilyrði sem skulu gilda um miðlun trúnaðarflokkaðra upplýsinga ESB til viðkomandi þriðja ríkis eða alþjóðastofnunar. Öryggideild aðalskrifstofu ráðsins skal tilkynna þetta viðkomandi þriðja ríki eða alþjóðastofnun.

15. Öryggideild aðalskrifstofu ráðsins skal, með gagnkvæmu samkomulagi við viðkomandi þriðja ríki eða alþjóðastofnun, fara með reglulegu millibili í framhaldsmatsheimsóknir í því skyni að sannreyna að það fyrirkomulag sem er til staðar standist þær lágmarksviðmiðanir sem samkomulag er um.

16. Eftir að samningur um upplýsingaöryggi hefur öðlast gildi og skipti á trúnaðarflokkuðum upplýsingum við viðkomandi þriðja ríki eða alþjóðastofnun eru hafin, getur öryggisnefndin ákveðið að breyta hámarksstigi trúnaðarflokkaðra upplýsinga ESB sem heimilt er að skiptast á í pappírsformi eða í rafræni mynd, einkum í ljósi framhaldsmatsheimsókna.

IV. STJÓRNSÝSLUSAMKOMULAG

17. Aðalframkvæmdastjórinn getur, að fengnu samþykki ráðsins og sé þörf á að skiptast í langan tíma á upplýsingum, sem að megin reglu til eru ekki á hærra trúnaðarstigi en TAKMARKAÐUR AÐGANGUR ESB, við þriðja ríki eða alþjóðastofnun og þegar öryggisnefndin hefur staðfest að viðkomandi aðili hafi ekki nægilega þróað öryggiskerfi til þess að hægt sé að gera samning um upplýsingaöryggi, gengið frá stjórnsýslusamkomulagi við viðkomandi yfirvöld í hlutaðeigandi þriðja ríki eða alþjóðastofnun.

18. Ráðið getur, í undantekningartilvikum og þegar nauðsynlegt er að smíða með hraði regluramma um skipti á trúnaðarflokkuðum upplýsingum af knýjandi rekstrarlegum ástæðum, ákveðið að ganga skuli frá stjórnsýslusamkomulagi vegna skipta á upplýsingum á hærra stigi trúnaðarflokkunar.

19. Almenna reglan er sú að stjórnsýslusamkomulag sé í formi bréfaskipta.

20. Matsheimsókn, er um getur í 10. mgr., skal farin og skýrsla send öryggisnefndinni, sem skal dæma hana fullnægjandi, áður en trúnaðarflokkuðum upplýsingum ESB er í raun miðlað til viðkomandi þriðja ríkis eða alþjóðastofnunar. Séu hins vegar óvenjulegar ástæður fyrir því að skipti á trúnaðarflokkuðum upplýsingum fari fram án tafar og vakin er athygli ráðsins á þeim ástæðum, er heimilt að miðla trúnaðarflokkuðum upplýsingum ESB, að því tilskildu að allt kapp sé lagt á að fyrrnefnd matsheimsókn sé farin eins fljótt og aðstæður leyfa.

21. Ekki skal skiptast á trúnaðarflokkuðum upplýsingum ESB með rafrænum hætti nema skýrt sé kveðið á um það í viðeigandi stjórnsýslusamkomulagi.

V. SKIPTI Á TRÚNAÐRFLOKKUÐUM UPPLÝSINGUM Í TENGSLUM VIÐ AÐGERÐIR TIL FRAMKVÆMDAR SAMEIGINLEGRI STEFNU Í ÖRYGGIS- OG VARNARMÁLUM

22. Rammasamningar um þátttöku mæla fyrir um þátttöku þriðju ríkja og alþjóðastofnana í aðgerðum til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum. Þessir samningar innihalda ákvæði um miðlun trúnaðarflokkaðra upplýsinga ESB, sem verða til vegna aðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, til þeirra þriðju ríkja og alþjóðastofnana sem taka þátt í fyrrnefndum aðgerðum. Hámarksstig þeirra trúnaðarflokkuðu upplýsinga ESB sem skipti eru heimil á skal vera TAKMARKAÐUR AÐGANGUR ESB vegna borgaralegra aðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum og TRÚNAÐARMÁL ESB vegna hernaðaraðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, nema kveðið sé á um annað í þeirri ákvörðun sem stofnar til hverrar og einnar aðgerðar af því tagi.

23. Samningar um þátttöku, sem eru gerðir sérstaklega vegna tiltekinnar aðgerðar til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, skulu innihalda ákvæði um miðlun trúnaðarflokkaðra upplýsinga ESB, sem verða til vegna þeirrar aðgerðar, til þeirra þriðju ríkja eða alþjóðastofnana sem taka þátt í henni. Hámarksstig þeirra trúnaðarflokkuðu upplýsinga ESB sem skipti eru heimil á skal vera TAKMARKAÐUR AÐGANGUR ESB vegna borgaralegra aðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum og TRÚNAÐARMÁL ESB vegna hernaðaraðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, nema kveðið sé á um annað í þeirri ákvörðun sem stofnar til hverrar og einnar aðgerðar af því tagi.

24. Stjórnsýslusamkomulag, sem er gert sérstaklega vegna þátttöku þriðja ríkis eða alþjóðastofnunar í tiltekinni aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, getur meðal annars tekið til miðlunar trúnaðarflokkaðra upplýsinga ESB, sem verða til vegna þeirrar aðgerðar, til fyrrnefnds þriðja ríkis eða alþjóðastofnunar. Slíkt sértækt stjórnsýslusamkomulag skal gert í samræmi við þær verklagsreglur sem settar eru fram í 17. og 18. mgr. IV. hluta. Hámarksstig þeirra trúnaðarflokkuðu upplýsinga ESB sem skipti eru heimil á skal vera TAKMARKAÐUR AÐGANGUR ESB vegna borgaralegra aðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum og TRÚNAÐARMÁL ESB vegna hernaðaraðgerða til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, nema kveðið sé á um annað í þeirri ákvörðun sem stofnar til hverrar og einnar aðgerðar af því tagi.

25. Ekki er gerð nein krafa um framkvæmdarráðstafanir eða matsheimsóknir áður en ákvæðin um miðlun trúnaðarflokkaðra upplýsinga ESB í tengslum við 22. 23. og 24. mgr. koma til framkvæmda.

26. Heimilt er, komi upp sérstök og knýjandi þörf til að grípa til aðgerða, að ganga frá sértæku stjórnsýslusamkomulagi, hafi viðkomandi gistiríki, sem hefur lögsögu þar sem aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum fer fram, ekki gengið frá samningi eða stjórnsýslusamkomulagi við ESB um upplýsingaöryggi vegna skipta á trúnaðarflokkuðum upplýsingum. Kveða ber á um þennan kost í ákvörðuninni um að stofna til aðgerðar til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum. Trúnaðarflokkaðar upplýsingar ESB, sem er miðlað við fyrrnefndar aðstæður, skulu takmarkaðar við þær sem verða til í tengslum við þá aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum sem um ræðir og ekki vera á hærra trúnaðarstigi en TAKMARKAÐUR AÐGANGUR ESB. Gistiríkið skal skuldbinda sig, samkvæmt fyrrnefndu sértæku stjórnsýslusamkomulagi, til þess að vernda trúnaðarflokkaðar upplýsingar ESB í samræmi við lágmarksviðmiðanir sem svara a.m.k. til þeirra sem mælt er fyrir um í ákvörðun þessari.

27. Í þeim ákvæðum um trúnaðarflokkaðar upplýsingar sem til stendur að rammasamningar um þátttöku, samningar um þátttöku, sem eru gerðir sérstaklega vegna tiltekinnar aðgerðar, og sértækt stjórnsýslusamkomulag, er um getur í 22.-24. mgr., feli í sér skal boðað að viðkomandi þriðja ríki eða alþjóðastofnun beri að tryggja að starfsfólk á þeirra vegum, sem er kallað er til starfa í hvaða aðgerð sem er, muni vernda trúnaðarflokkaðar upplýsingar ESB í samræmi við öryggisreglur ráðsins og frekari leiðbeiningar, sem bær yfirvöld gefa út, þ.m.t. valdlýsing aðgerðarinnar.

28. Ef samningur um upplýsingaöryggi er gerður síðar meir milli ESB og þriðja ríkis eða alþjóðastofnunar, sem tekur þátt í aðgerð, skal viðkomandi samningur um upplýsingaöryggi ganga framar hvaða rammasamningi um þátttöku sem er, samningi um þátttöku, sem er gerður sérstaklega vegna tiltekinnar aðgerðar, eða hvaða sértæku stjórnsýslusamkomulagi sem er, að því er varðar skipti á og meðhöndlun trúnaðarflokkaðra upplýsinga ESB.

29. Skipti á trúnaðarflokkuðum upplýsingum ESB í rafrænni mynd eru óheimil samkvæmt rammasamningi um þátttöku, samningi um þátttöku, sem er gerður sérstaklega vegna tiltekinnar aðgerðar, eða sértæku stjórnsýslusamkomulagi við þriðja ríki eða alþjóðastofnun, nema sérstaklega sé kveðið á um það í viðkomandi samningi eða samkomulagi.

30. Trúnaðarflokkuðum upplýsingum ESB, sem verða til í tengslum við aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, má uppljóstra til starfsfólks sem þriðju ríki eða alþjóðastofnanir kalla til starfa vegna umræddrar aðgerðar í samræmi við 22. til 29. mgr. Þegar slíku starfsfólki er heimilaður aðgangur að trúnaðarflokkuðum upplýsingum ESB í húsnæði eða samskipta- og upplýsingakerfi aðgerðar til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, skal gera ráðstafanir (þ.m.t. skráning trúnaðarflokkaðra upplýsinga ESB sem er uppljóstrað) til þess að draga úr hættu af tapi eða tilslökun. Skilgreina ber slíkar ráðstafanir í viðeigandi skjölum um áætlanir eða verkefna.

VI. SÉRSTÖK MIÐLUN TRÚNAÐARFLOKKAÐRA UPPLÝSINGA ESB Í UNDANTEKNINGARTILVIKUM

31. Þegar ekki er fyrirliggjandi reglurammi í samræmi við ákvæði III. til V. hluta og ráðið eða ein af stofnunum þess, sem annast undirbúning, ákveður að til staðar sé alveg sérstök þörf á að miðla til þriðja ríkis eða alþjóðastofnunar trúnaðarflokkuðum upplýsingum ESB, skal aðalskrifstofa ráðsins:

a) að því marki sem frekast er unnt, sannreyna hjá öryggisyfirvöldum viðkomandi þriðja ríkis eða alþjóðastofnunar að öryggisreglur, -skipulag og -verklag séu þannig að trúnaðarflokkaðar upplýsingar ESB, sem er miðlað til þess eða hennar, verði verndaðar samkvæmt viðmiðunum sem a.m.k. samsvara þeim sem mælt er fyrir um í ákvörðun þessari,

b) hvetja öryggisnefndina, á grundvelli fyrirliggjandi upplýsinga, til þess að gefa út tilmæli um þá tiltrú sem hafa má á öryggisreglum, -skipulagi og -verklagi í viðkomandi þriðja ríki eða alþjóðastofnun sem til stendur að miðla trúnaðarflokkuðum upplýsingum ESB til.

32. Gefi öryggisnefndin út tilmæli þar sem mælt er með því að viðeigandi trúnaðarflokkuðum upplýsingum ESB verði miðlað, skal vísa málinu til nefndar fastafulltrúa (COREPER) sem tekur ákvörðun um miðlun þeirra.

33. Mæli öryggisnefndin ekki með því í tilmælum sínum að framsenda viðeigandi trúnaðarflokkaðar upplýsingar ESB:

a) vegna málefna, sem varða sameiginlega stefnu í utanríkis- og öryggismálum og/eða aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum, skal stjórnmála- og öryggisnefndin fjalla um málið og setja fram tilmæli vegna ákvörðunar nefndar fastafulltrúa,

b) vegna allra annarra málefna skal nefnd fastafulltrúa fjalla um málið og taka ákvörðun.

34. Nefnd fastafulltrúa getur ákveðið, þar sem það telst viðeigandi og með fyrirvara um fyrirfram skriflegt samþykki útgefandans, að heimilt sé að miðla hinum trúnaðarflokkuðu upplýsingum aðeins að hluta til eða einungis ef trúnaðarstig þeirra er lækkað eða ef trúnaði þeirra er aflétt áður, eða ákveðið að þær upplýsingar sem til stendur að miðla séu útbúnar án vísunar til uppruna eða upphaflegs stigs trúnaðarflokkunar ESB.

35. Aðalskrifstofa ráðsins skal, í kjölfar þeirrar ákvörðunar að miðla trúnaðarflokkuðum upplýsingum ESB, senda viðkomandi skjal, sem skal merkt hæft til miðlunar og því þriðja ríki eða alþjóðastofnun sem upplýsingunum hefur verið miðlað til. Áður en hinum trúnaðarflokkuðu upplýsingum ESB er miðlað eða jafnhliða eiginlegri miðlun þeirra, skal viðkomandi þriðji aðili skuldbinda sig skriflega til þess að vernda þær upplýsingar sem hann veitir viðtöku í samræmi við þær grundvallarsetningar og lágmarksviðmiðanir er um getur í ákvörðun þessari.

VII. HEIMILD TIL AÐ MIÐLA TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM ESB TIL ÞRIÐJU RÍKJA EÐA ALÞJÓÐASTOFNANA

36. Ráðið skal, ef reglurammi er til staðar í samræmi við ákvæði 2. mgr. vegna skipta á trúnaðarflokkuðum upplýsingum við þriðja ríki eða alþjóðastofnun, ákveða að heimila aðalframkvæmdastjóranum að miðla trúnaðarflokkuðum upplýsingum ESB til viðkomandi þriðja ríkis eða alþjóðastofnunar, í samræmi við meginregluna um samþykki útgefanda.

37. Sé reglurammi til staðar í samræmi við ákvæði 3. mgr. vegna skipta á trúnaðarflokkuðum upplýsingum við þriðja ríki eða alþjóðastofnun, skal aðalframkvæmdastjóranum heimilað að miðla trúnaðarflokkuðum upplýsingum ESB í samræmi við ákvörðunina um að stofna til aðgerðar til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum og meginregluna um samþykki útgefanda.

38. Aðalframkvæmdastjórinn getur falið háttsettum embættismönnum aðalskrifstofu ráðsins eða öðrum aðilum undir sinni stjórn í hendur þessar heimildir.

--------------------------------------------------

Viðbætar

Viðbætir A

Skilgreiningar**.**

Viðbætir B

Jafngildi trúnaðarflokkunar.

Viðbætir C

Skrá yfir stjórnvöld á sviði þjóðaröryggis.

Viðbætir D

Skrá yfir skammstafanir.

--------------------------------------------------

*Viðbætir A*

SKILGREININGAR

Í ákvörðun þessari er skilgreining eftirfarandi hugtaka sem hér segir:

„vottun“ merkir það ferli sem leiðir til formlegrar yfirlýsingar yfirvalds á sviði öryggisvottunar þess efnis að tiltekið kerfi sé samþykkt til að meðhöndla upplýsingar á skilgreindu trúnaðarstigi í sérstakri öryggisstillingu í rekstrarumhverfi þess og á viðunandi áhættustigi, á grundvelli þeirrar forsendu að gerð hafi verið röð samþykktra öryggisráðstafana tæknilegs, hlutkennds og skipulagslegs eðlis og sem varða verklag;

„tilföng“ merkir allt sem telst verðmætt fyrir tiltekna skipulagsheild, þá starfsemi sem hún stundar og áframhald þeirrar starfsemi, þ.m.t. upplýsingaveitur sem styðja við verkefni skipulagsheildarinnar;

„líftími samskipta- og upplýsingakerfis“ merkir allan þann tíma sem samskipta- og upplýsingakerfi er til, þ.m.t. innsetning þess, hugmyndalýsing, áætlanagerð, þarfagreining, hönnun, þróun, prófun, framgangur, rekstur, viðhald og ónýting;

„trúnaðarflokkaður verktakasamningur“ merkir samning sem aðalskrifstofa ráðsins gerir við verktaka vegna afhendingar vöru, verkframkvæmda eða þjónustustarfsemi, þar sem framkvæmd slíks samnings krefst eða felur í sér aðgang að eða tilurð trúnaðarflokkaðra upplýsinga ESB;

„trúnaðarflokkaður samningur um undirverktöku“ merkir samning verktaki aðalskrifstofu ráðsins gerir við annan verktaka (þ.e. undirverktaka) vegna afhendingar vöru, verkframkvæmda eða þjónustustarfsemi, þar sem framkvæmd slíks samnings krefst eða felur í sér aðgang að eða tilurð trúnaðarflokkaðra upplýsinga ESB;

„samskipta- og upplýsingakerfi“ — sjá 2. mgr. 10. gr.;

„verktaki“ merkir einstakling eða lögaðila sem býr yfir gerhæfi til þess að taka á sig samningsskuldbindingar;

„dulkóðunarefni“ merkir dulkóðunarlausnarvísi, vélbúnað til dulkóðunar og hugbúnaðareiningar, ásamt framleiðsluvörum, þ.m.t. smáatriði varðandi beitingu með tilheyrandi gögnum og kóðunarefni;

„aðgerð til framkvæmdar sameiginlegri stefnu í öryggis- og varnarmálum“ merkir hernaðarlega eða borgaralega hættustjórnunaraðgerð samkvæmt ákvæðum 2. kafla V. bálks sáttmálans um Evrópusambandið;

„aflétting trúnaðarflokkunar“ merkir að öll trúnaðarflokkun sé afnumin;

„lagskiptar varnir“ merkir að grípa til margháttaðra öryggisráðstafana sem eru skipulagðar varnir í mörgum lögum;

„tilgreint öryggisyfirvald“ merkir yfirvald sem ber ábyrgð gagnvart stjórnvaldi aðildarríkis á sviði þjóðaröryggis sem aftur ber ábyrgð á samskiptum við fyrirtæki eða aðrar rekstrareiningar vegna innlendrar stefnu í öllum málum er varða iðnaðaröryggi og á því að láta í té leiðbeiningar og aðstoð við framkvæmd hennar. Stjórnvald á sviði þjóðaröryggis eða hvaða annað bært yfirvald sem er getur gegnt hlutverki tilgreinds öryggisyfirvalds;

„skjal“ merkir skráðar upplýsingar óháð hlutkenndri mynd þeirra eða einkennum;

„lækkun trúnaðarstigs“ merkir að lækka stig trúnaðarflokkunar;

„trúnaðarflokkaðar upplýsingar ESB“ — sjá 1. mgr. 2. gr.;

„öryggisvottun starfsstöðvar“ merkir stjórnsýsluákvörðun stjórnvalds á sviði þjóðaröryggis eða tilgreinds öryggisyfirvalds um að tiltekin starfsstöð geti, með tilliti til öryggis, veitt trúnaðarflokkuðum upplýsingum ESB fullnægjandi vernd á tilgreindu stigi trúnaðarflokkunar og að starfsfólk hennar, sem þarfnast aðgangs að trúnaðarflokkuðum upplýsingum ESB, hafi verið veitt viðeigandi öryggisvottun og verið upplýst um viðeigandi öryggiskröfur sem nauðsynlegt er að uppfylla til þess að hafa aðgang að og vernda trúnaðarflokkaðar upplýsingar ESB;

„meðhöndlun“ trúnaðarflokkaðra upplýsinga ESB merkir allar hugsanlegar athafnir viðvíkjandi trúnaðarflokkuðum upplýsingum ESB á líftíma þeirra. Í meðhöndlun felst tilurð, vinnsla, flutningur, lækkun trúnaðarstigs, aflétting trúnaðar og eyðing. Að því er samskipta- og upplýsingakerfi varðar felur meðhöndlun einnig í sér söfnun upplýsinga, sýningu, sendingu og geymslu;

„handhafi“ merkir einstakling, með fullt umboð og staðfesta vitneskjuþörf, sem hefur í vörslu sinni hluta af trúnaðarflokkuðum upplýsingum ESB og ber í samræmi við það ábyrgð á vernd þeirra;

„iðnfyrirtæki eða önnur rekstrareining“ merkir rekstrareiningu sem kemur að því að afhenda vörur, vinna verk eða veita þjónustu. Um getur verið að ræða rekstrareiningu á sviði iðnaðar, viðskipta, þjónustu, vísinda, rannsókna, menntunar eða þróunar eða sjálfstætt starfandi einstakling;

„iðnaðaröryggi“ — sjá 1. mgr. 11. gr.;

„upplýsingaöryggi“ — sjá 1. mgr. 10. gr.;

„samtenging“ — sjá 31. mgr. IV. viðauka;

„umsjón með trúnaðarflokkuðum upplýsingum“ — sjá 1. mgr. 9. gr.;

„efni“ merkir öll skjöl eða vélar eða búnað sem hefur annaðhvort verið framleiddur eða er í framleiðslu;

„útgefandi“ merkir þá stofnun, embætti eða aðila innan ESB, aðildarríki, þriðja ríki eða alþjóðastofnun sem hefur stjórnað tilurð trúnaðarflokkaðra upplýsinga og/eða innleiðingu þeirra í skipulagseiningar ESB;

„öryggi með tilliti til starfsfólks“ — sjá 1. mgr. 7. gr.;

„öryggisvottun starfsfólks“ merkir annað hvort eða hvoru tveggja af eftirfarandi:

— „ESB öryggisvottun starfsfólks“ merkir, vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB, heimild ráðningaryfirvalds aðalskrifstofu ráðsins sem er veitt í samræmi við ákvörðun þessa að lokinni bakgrunnsskoðun sem bær yfirvöld aðildarríkis framkvæmir og staðfestir að heimilt sé að veita einstaklingi, að því tilskildu að „vitneskjuþörf“ hans hafi verið staðfest, aðgang að trúnaðarflokkuðum upplýsingum ESB upp að tilgreindu stigi (TRÚNAÐARMÁL ESB eða ofar) fram að tiltekinni dagsetningu. Sá einstaklingur sem þannig er lýst er sagður hafa „öryggisvottun“;

— „innlend öryggisvottun starfsfólks“ merkir, vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB, yfirlýsingu bærs yfirvalds aðildarríkis sem er gefin að lokinni bakgrunnsskoðun sem bær stjórnvöld aðildarríkis framkvæmir og staðfestir að heimilt sé að veita einstaklingi, að því tilskildu að „vitneskjuþörf“ hans hafi verið staðfest, aðgang að trúnaðarflokkuðum upplýsingum ESB upp að tilgreindu stigi (TRÚNAÐARMÁL ESB eða ofar) fram að tiltekinni dagsetningu. Sá einstaklingur sem þannig er lýst er sagður hafa „öryggisvottun“;

„vottorð um öryggisvottun starfsfólks“ merkir vottorð sem bært yfirvald gefur út sem staðfestingu þess að einstaklingur hafi öryggisvottun og hafi gilda innenda eða ESB öryggisvottun starfsfólks og sem sýnir það stig trúnaðarflokkaðra upplýsinga ESB sem veita má fyrrnefndum einstaklingi aðgang á (TRÚNAÐARMÁL ESB eða ofar), gildistíma viðeigandi öryggisvottunar starfsfólks og hvenær gildistími vottorðsins sjálfs rennur út;

„hlutkennt öryggi“ — sjá 1. mgr. 8. gr.;

„öryggisleiðbeiningar vegna áætlana og/eða verkefna“ merkir skrá yfir öryggisverklag sem er beitt í tilviki sérstakra áætlana og/eða verkefna í því augnamiði að staðla öryggisverklag. Heimilt er að endurskoða hana meðan á áætluninni og/eða verkefninu stendur;

„skráning“ — sjá 18. mgr. III. viðauka;

„eftirstandandi áhætta“ merkir þá áhættu sem eftir stendur þegar öryggisráðstafanir hafa verið gerðar, þar sem öllum ógnum hefur ekki verið mætt og ekki er unnt að útiloka allt varnarleysi;

„áhætta“ merkir þá tilhneigingu að ákveðin ógn þýði að unnt sé að notfæra sér innri og ytri veikleika skipulagsheildar eða einhverra þeirra kerfa sem hún nýtir og valda skipulagsheildinni og efnislegum og óefnislegum tilföngum hennar með því skaða. Mælikvarði hennar er samsetning á líkum á ógnum og áhrifum þeirra;

— „áhættusamþykki“ er sú ákvörðun að samþykkja að eftirstandandi áhætta sé áfram til staðar eftir að meðferð vegna áhættu er lokið;

— „áhættumat“ samanstendur af því að greina ógnir og veikleika og framkvæma tengda áhættugreiningu, þ.e. greiningu á líkum og áhrifum;

— „áhættukynning“ samanstendur af því að þróa meðvitund um áhættur meðal notenda samskipta- og upplýsingakerfa, upplýsa vottunaryfirvöld um slíkar áhættur og að gera rekstrarstjórnum grein fyrir þeim;

— „áhættumeðferð“ samanstendur af því að draga úr áhrifum, fjarlægja, minnka (með viðeigandi samsetningu tæknilegra, hlutkenndra og skipulagslegra ráðstafana eða verklagsráðstafana), flytja eða vakta áhættuna;

„öryggisskilmálar“ merkir samstæðu sérstakra samningsskilyrða sem viðkomandi samningsyfirvald gefur út og eru óaðskiljanlegur hluti sérhvers trúnaðarflokkaðs samnings, sem felur í sér aðgang að eða tilurð trúnaðarflokkaðra upplýsingar ESB, þar sem tilgreindar eru öryggiskröfur eða þeir þætti samningsins sem þarfnast öryggisverndar;

„leiðbeiningar um trúnaðarflokkun“ merkir skjal sem lýsir þeim þáttum áætlunar eða samnings sem eru trúnaðarflokkaðir og tilgreinir þau stig trúnaðarflokkunar sem við eiga. Heimilt er að útvíkka leiðbeiningar um trúnaðarflokkun allan líftíma viðkomandi áætlunar eða samnings og heimilt er að endurflokka eða lækka trúnaðarstig einstakra þátta upplýsinganna. Þegar leiðbeiningar um trúnaðarflokkun eru fyrir hendi skulu þær vera hluti af viðeigandi öryggisskilmálum;

„bakgrunnsskoðun“ merkir þær rannsóknir sem bært yfirvald aðildarríkis framkvæmir í samræmi við innlend lög og reglugerðir til þess að öðlast tryggingu fyrir því að ekkert neikvætt sé vitað sem gæti komið í veg fyrir að einstaklingur hljóti innlenda öryggisvottun starfsfólks eða öryggisvottun ESB fyrir starfsfólk vegna aðgangs að trúnaðarflokkuðum upplýsingum ESB upp að tilgreindu stigi (TRÚNAÐARMÁL ESB eða ofar);

„öryggisvinnumáti“ merkir ákvörðun skilyrða, sem samskipta- og upplýsingakerfi er rekið samkvæmt, sem er byggð á trúnaðarflokkun upplýsinga sem meðhöndlaðar eru og vottunarstigi, formlegri aðgangsviðurkenningu og vitneskjuþörf notenda upplýsinganna. Ferns konar vinnumáti fyrirfinnst til þess að meðhöndla eða flytja trúnaðarflokkaðar upplýsingar: eingilt form, hástigsform, sundurgreint form og fjölþrepaform:

— „eingilt form“ merkir vinnumáta þar sem allir einstaklingar með aðgang að samskipta- og upplýsingakerfinu hafa vottun á hæsta stig trúnaðarflokkunar vegna upplýsinga sem meðhöndlaðar eru í upplýsingakerfinu og hafa jafnfram almenna vitneskjuþörf vegna allra upplýsinga sem eru meðhöndlaðar í kerfinu;

— „hástigsform“ merkir vinnumáta þar sem allir einstaklingar með aðgang að samskipta- og upplýsingakerfinu hafa vottun á hæsta stigi trúnaðarflokkunar vegna upplýsinga sem meðhöndlaðar eru í samskipta- og upplýsingakerfinu, en allir einstaklingar með aðgang að því kerfi hafa ekki almenna vitneskjuþörf vegna upplýsinga sem eru meðhöndlaðar í því. Einstaklingur getur veitt aðgangsheimild að upplýsingum;

— „sundurgreint form“ merkir vinnumáta þar sem allir einstaklingar með aðgang að samskipta- og upplýsingakerfinu hafa vottun á hæsta stigi trúnaðarflokkunar vegna upplýsinga sem eru meðhöndlaðar í því kerfi, en allir einstaklingar með aðgang að kerfinu hafa ekki formlega heimild til að ganga að þeim upplýsingum sem þar eru meðhöndlaðar. Formleg heimild felur í sér formleg, miðlæg forráð yfir aðgangsstýringu sem eru aðskilin frá rétti einstaklings til að ákvarða aðgangsheimild;

— „fjölþrepaform“ merkir vinnumáta þar sem allir einstaklingar með aðgang að samskipta- og upplýsingakerfinu hafa ekki vottun á hæsta stigi trúnaðarflokkunar vegna upplýsinga sem eru meðhöndlaðar í því kerfi og allir einstaklingar með aðgang að fyrrnefndu kerfi hafa ekki almenna vitneskjuþörf vegna upplýsinga sem eru meðhöndlaðar í því;

„öryggisáhættustjórnunarferli“ merkir allt ferlið við að greina, hafa stjórn á og lágmarka óvissa atburði sem kunna að hafa áhrif á öryggi skipulagsheildar eða einhvers þess kerfis sem hún notar. Ferlið tekur til áhættutengdrar starfsemi í heild, þ.m.t. mat, meðferð, samþykki og samskipti;

„TEMPEST“ merkir rannsókn, athugun og eftirlit með því hvort rafsegulgeislun sé stofnað í hættu og aðferðir til að stemma stigu við slíku;

„ógn“ merkir hugsanlega orsök óæskilegs atviks sem gæti skaðað tiltekna skipulagsheild eða eitthvað þeirra kerfa sem hún notar. Slíkar ógnir geta verið af slysni eða ásettu ráði (illgirni) og einkennast af ógnandi þáttum, hugsanlegu takmarki og árásaraðferðum;

„varnarleysi“ merkir veikleika af hvaða tagi sem er sem ein ógn eða fleiri geta hagnýtt sér. Varnarleysi getur verið vanræksla eða tengst vanmætti stjórntækja, þ.e. styrkleika þeirra, heilleika eða samkvæmni og getur verið tæknilegs eðlis, af völdum verklags eða hlutkennds, skipulagslegs eða rekstrarlegs eðlis.

--------------------------------------------------

*Viðbætir B*

JAFNGILDI TRÚNAÐARFLOKKUNAR











(1) Diffusion Restreinte/Beperkte Verspreiding er ekki trúnaðarflokkað í Belgíu. Belgía meðhöndlar og verndar upplýsingar flokkaðar „TAKMARKAÐUR AÐGANGUR ESB“ með hætti sem jafngildir að minnsta kosti þeim viðmiðunum og því verklag sem er lýst í öryggisreglum ráðs Evrópusambandsins.

(2) Þýskaland: VS = Verschlusssache.

(3) Frakkland notar ekki flokkunina „RESTREINT“ í innlendu kerfi sínu. Frakkland meðhöndlar og verndar upplýsingar flokkaðar „TAKMARKAÐUR AÐGANGUR ESB“ með hætti sem jafngildir að minnsta kosti þeim viðmiðunum og því verklag sem er lýst í öryggisreglum ráðs Evrópusambandsins.

(4) Svíþjóð: merkingar vegna trúnaðarflokkunar í efri röð eru notaðar af varnarmálayfirvöldum og merkingar í neðri röð af öðrum yfirvöldum.

--------------------------------------------------

*Viðbætir C*

SKRÁ YFIR STJÓRNVÖLD Á SVIÐI ÞJÓÐARÖRYGGIS











*Viðbætir D*

SKRÁ YFIR SKAMMSTAFANIR

Upphafsstafaorð Merking

AQUA Appropriately Qualified Authority Til þess bært stjórnvald

BPS Boundary Protection Services Verndarþjónusta endimarka

CAA Crypto Approval Authority Vottunaryfirvald dulkóðunar

CCTV Closed Circuit Television Lokað sjónvarpskerfi

CDA Crypto Distribution Authorit Dreifingaryfirvald dulkóðunar.

CFSP Common Foreign and Security Policy Sameiginleg stefna í utanríkis- og öryggismálum (SSUÖ)

CIS Communication and Information Systems handling EUCI Samskipta- og upplýsingakerfi þar sem trúnaðarflokkaðar upplýsingar ESB eru meðhöndlaðar (EUCI)

COREPER Committee of Permanent Representative. Nefnd fastafulltrúa

CSDP Common Security and Defence Policy Sameiginleg stefna í öryggis- og varnarmálum (SSÖV)

DSA Designated Security Authority Tilgreint öryggisyfirvald

ECSD European Commission Security Directorate Öryggismálaskrifstofa framkvæmdastjórnarinnar

EUCI Classified Information Trúnaðarflokkaðar upplýsingar ESB

EUSR Special Representative Sérstakur fulltrúi ESB

FSC Facility Security Clearance Öryggisvottun starfsstöðvar

GSC General Secretariat of the Council Aðalskrifstofa ráðs Evrópusambandsins

IA Information Assurance Upplýsingaöryggi

IAA Information Assurance Authority Yfirvald á sviði upplýsingaöryggis.

IDS Instrusion Detection System Ágangsskynjunarkerfi

IT Information Technology Upplýsingatækni

NSA National Security Authority Stjórnvald á sviði þjóðaröryggis

PSC Personnel Security Clearance Öryggisvottun starfsfólks

PSCC Personnel Security Clearance Certificate Vottorð um öryggisvottun starfsfólks

PSI Programme/Project Security Instructions Öryggisleiðbeiningar vegna áætlana/verkefna.

SAA Security Accreditation Authority Yfirvald á sviði öryggisvottunar.

SAB Security Accreditation Board Öryggisvottunarráð

SAL Security Aspects Letter Öryggisskilmálar

SecOPs Security Operating Procedures Öryggisverkhættir

SCG Security Classification Guide Leiðbeiningar um trúnaðarflokkun

SSRS System-Specific Security Requirement Statement Yfirlýsing um kerfismiðaðar öryggiskröfur

TA TEMPEST Authority TEMPEST-yfirvald

1. () Stjtíð. ESB L 325, 11. 12. 2009, bls. 35. [↑](#footnote-ref-1)
2. () Stjtíð. EB L 101, 11. 4. 2001, bls. 1. [↑](#footnote-ref-2)
3. () Stjtíð. EB L 56, 4.3.1968, bls. 1. [↑](#footnote-ref-3)