KOMISJONI OTSUS (EL) 2022/640,

7. aprill 2022,

peamiste julgeolekuvaldkonna osalejate rolle ja vastutusvaldkondi käsitlevate rakenduseeskirjade kohta

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 249,

võttes arvesse komisjoni 13. märtsi 2015. aasta otsust (EL, Euratom) 2015/443 komisjoni julgeoleku kohta, ([1])

võttes arvesse komisjoni 13. märtsi 2015. aasta otsust (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta ([2])

ning arvestades järgmist:

(1) Otsuseid (EL, Euratom) 2015/443 ja (EL, Euratom) 2015/444 kohaldatakse kõigi komisjoni talituste ja objektide suhtes.

(2) Vajaduse korral võetakse otsuse (EL, Euratom) 2015/444 artikli 60 kohaselt vastu seda otsust täiendavad või toetavad rakenduseeskirjad.

(3) Turvameetmed, mida võetakse ELi salastatud teabe kaitsmiseks kogu selle olelusringi jooksul, peaksid eelkõige vastama asjaomase teabe salastatuse tasemele.

(4) Komisjoni side- ja infosüsteemide kaitse turvameetmed on sätestatud komisjoni otsuses (EL, Euratom) 2017/46, ([3]) eelkõige artiklis 3 „Komisjoni IT turbe põhimõtted“ ja artiklis 9 „Süsteemide omanikud“.

(5) Peamiste julgeolekuvaldkonna osalejate rolle ja vastutusvaldkondi käsitlevate rakenduseeskirjade eesmärk on esitada suuniseid nende ülesannete täitmisega seotud eelduste ja kohustuste kohta, mis on sätestatud otsustes (EL, Euratom) 2015/443 ja (EL, Euratom) 2015/444.

(6) Otsuse (EL, Euratom) 2015/444 artikli 36 lõikes 7 on sätestatud komisjoni julgeolekuasutuse sisse seatavad mitu täiendavat julgeolekuga seotud asutust. Nende asutuste ülesanded on sätestatud käesolevas otsuses.

(7) Otsuse (EL, Euratom) 2015/444 kohaselt kuulub kohalike julgeolekuametnike ja registri kontrolliametnike konkreetsesse vastutusalasse ELi salastatud teabe kaitse nende talituses.

(8) Komisjon võttis 4. mail 2016 vastu otsuse, ([4]) millega volitatakse julgeolekuküsimuste eest vastutavat komisjoni liiget võtma komisjoni nimel ja tema vastutusel vastu otsuse (EL, Euratom) 2015/444 artiklis 60 sätestatud rakenduseeskirjad, ning seejärel võttis julgeolekuküsimuste eest vastutav komisjoni liige 13. aprillil 2021 komisjoni nimel ja tema vastutusel vastu otsuse, ([5]) millega delegeeritakse need rakenduseeskirjad omakorda personalihalduse ja julgeoleku peadirektoraadi peadirektorile,

([1]) ELT L 72, 17.3.2015, lk 41.
([2]) ELT L 72, 17.3.2015, lk 53.
([3]) Komisjoni 10. jaanuari 2017. aasta otsus (EL, Euratom) 2017/46 Euroopa Komisjoni side- ja infosüsteemide turvalisuse kohta (ELT L 6, 11.1.2017, lk 40).
([4]) 4. mai 2016. aasta otsus C(2016) 2797 (final) julgeolekuga seotud volituse kohta.
([5]) 13. aprilli 2021. aasta otsus C(2021) 2684 (final), millega antakse edasidelegeeritud volitused, mis on antud komisjoni otsusega C(2016) 2797 julgeolekuga seotud volituste kohta.

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

1. PEATÜKK

Üldsätted

Artikkel 1

Sisu ja kohaldamisala

1. Käesoleva otsusega määratakse kindlaks nende peamiste julgeolekuvaldkonna osalejate rollid ja vastutusvaldkonnad, kes kaitsevad komisjonis ELi salastatud teavet kooskõlas otsustega (EL, Euratom) 2015/443 ja (EL, Euratom) 2015/444.

2. Käesolevat otsust kohaldatakse kõigi komisjoni talituste suhtes ja kõigil komisjoni objektidel.

2. PEATÜKK

Personalihalduse ja julgeoleku peadirektoraat

Artikkel 2

Komisjoni julgeolekuasutus

1. Personalihalduse ja julgeoleku peadirektoraadi julgeolekudirektoraadi direktorist saab otsuse (EL, Euratom) 2015/444 artiklis 7 osutatud komisjoni julgeolekuasutus.

2. Komisjoni julgeolekuasutus täidab oma ülesandeid otsusega (EL, Euratom) 2015/444 sätestatud järgmistes valdkondades kooskõlas käesoleva otsuse artiklitega 3–7:

a) personali turvalisus,

b) füüsiline julgeolek,

c) ELi salastatud teabe haldamine,

d) ELi salastatud teavet töötleva mis tahes side- ja infosüsteemi akrediteerimine,

e) tööstusjulgeolek ning

f) salastatud teabe vahetamine.

3. Komisjoni julgeolekuasutus tagab kohalike julgeolekuametnike ja nende asetäitjate ning registri kontrolliametnike ja nende asetäitjate vastutusvaldkondade ja kohustuste alase kohustusliku koolituse.

Artikkel 3

Infokindluse asutus

Infokindluse asutus vastutab ELi salastatud teabe kaitse puhul järgmise tegevuse eest:

a) infokindluse turbe põhimõtete ja turvasuuniste väljatöötamine ning nende tulemuslikkuse ja asjakohasuse jälgimine;

b) krüptovahenditega seotud tehnilise teabe kaitse ja haldamine;

c) tagamine, et infokindluse meetmed vastavad sobilikul viisil komisjoni julgeoleku- ja hankepõhimõtetele;

d) tagamine, et krüptovahendid valitakse vastavalt nende kõlblikkuse ja valiku põhimõtetele;

e) konsulteerimine süsteemide omanike ja tagajate, julgeolekuvaldkonna osalejate ja kasutajate esindajatega seoses infokindluse tagamise põhimõtete ja turvasuunistega.

Artikkel 4

Turvalisuse akrediteerimise asutus

1. Komisjoni julgeolekuasutus vastutab otsuse 2015/444 artikli 18 nõuetele vastavate turvaalade ning ELi salastatud teavet töötlevate side- ja infosüsteemide akrediteerimise eest.

2. Komisjoni talitused konsulteerivad turvalisuse akrediteerimise asutusega, koordineerides tegevust oma kohaliku julgeolekuametniku ja kohaliku informaatika turvalisuse ametnikuga, kui talitus kavatseb:

a) luua turvaala;

b) kasutada side- ja infosüsteemi ELi salastatud teabe töötlemiseks;

c) paigaldada muid seadmeid salastatud teabe töötlemiseks, sh ühenduse loomine kolmanda isiku side- ja infosüsteemiga.

Turvalisuse akrediteerimise asutus esitab selle tegevuse kohta nõuandeid nii kavandamise, rajamise kui ka arendamise ajal.

3. ELi salastatud teavet ei tohi turvaalas ega side- ja infosüsteemis töödelda enne seda, kui turvalisuse akrediteerimise asutus on andnud akrediteeringu ELi salastatud teabe asjakohase taseme jaoks.

4. Turvaala akrediteerimise nõuded on muu hulgas järgmised:

a) turvaala kavade kinnitamine;

b) välistöövõtjate tehtavate tööde mis tahes lepingute kinnitamine, võttes arvesse tööstusjulgeoleku nõudeid, näiteks mis tahes nõudeid, mille kohaselt peavad töövõtjatel ja nende töötajatel olema salastatud teabele juurdepääsu load;

c) kõigi nõutavate deklaratsioonide ja vastavussertifikaatide olemasolu;

d) turvaala füüsiline kontroll, mille eesmärk on veenduda, et ehitusmaterjalid ja -meetodid, juurdepääsu kontroll, turvaseadmed ja muud elemendid vastavad komisjoni julgeolekuasutuse esitatud nõuetele;

e) elektromagnetilise kiirguse vastaste meetmete kontroll mis tahes tehniliselt kaitstud turvaalade puhul;

f) turvaala turvanõuete rakendamise korra kinnitamine.

5. ELi salastatud teabe töötlemiseks kasutatava side- ja infosüsteemi akrediteerimise nõuded on muu hulgas järgmised:

a) süsteemi akrediteerimise strateegia koostamine;

b) side- ja infosüsteemi turvaplaani kontroll riskijuhtimise põhimõtete kohaselt;

c) side- ja infosüsteemi turvanõuete rakendamise korra kontroll;

d) turvalisuse akrediteerimise asutuse kindlaks määratud kõigi muude nõutavate turbedokumentide kontroll;

e) krüpteerimistehnoloogia mis tahes kasutuse heakskiitmine;

f) elektromagnetilise kiirguse vastaste meetmete kontroll side- ja infosüsteemi puhul, mis hakkab töötlema tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teavet;

g) side- ja infosüsteemi kontroll, mille eesmärk on veenduda, et dokumenteeritud turvameetmeid rakendatakse õigesti.

6. Kui akrediteerimisnõuded on edukalt täidetud, siis väljastab turvalisuse akrediteerimise asutus ametliku loa turvaalas või side- ja infosüsteemis ELi salastatud teabe töötlemiseks kuni märgitud ELi salastatud teabe salastatuse maksimaalse tasemeni ja kuni viieks aastaks, olenevalt töödeldava ELi salastatud teabe salastatuse tasemest ja tekkivatest riskidest.

7. Kui antakse teada turvaala või side- ja infosüsteemi turvarikkumisest või kavandatud turvameetmete märkimisväärsest muutusest, siis vaatab turvalisuse akrediteerimise asutus ELi salastatud teabe töötlemise loa läbi ja võib vajaduse korral selle kuni kindlaks tehtud probleemide lahendamiseni kehtetuks tunnistada.

Artikkel 5

TEMPEST-asutus

1. Tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teavet töötleva side- ja infosüsteemi kaitseks rakendatakse TEMPEST-turvameetmeid ja neid võib rakendada ka tasemel RESTREINT UE/EU RESTRICTED salastatud teabe töötlemise puhul.

2. TEMPEST-asutus vastutab nende meetmete kinnitamise eest, mis võetakse, et kaitsta ELi salastatud teavet, et selline teave ei satuks ohtu tahtmatu elektromagnetkiirguse tõttu.

3. Kui ELi salastatud teavet töötleva side- ja infosüsteemi omanik esitab vastava taotluse, siis väljastab TEMPEST-asutus nende TEMPEST-turvameetmete kirjelduse, mis on teabe salastatuse taseme jaoks sobilikud.

4. TEMPEST-asutus teeb tasemel CONFIDENTIAL UE/EU CONFIDENTIAL või kõrgemal tasemel ELi salastatud teavet töötlevate turvaalade ning side- ja infosüsteemide akrediteerimise ajal tehnilised katsed ning väljastab TEMPEST-sertifikaadi, kui katsed on edukad.

5. TEMPEST-sertifikaadis tuleb märkida vähemalt:

a) katse kuupäev;

b) TEMPEST-turvameetmete kirjeldus koos objektide plaaniga;

c) sertifikaadi kehtivusaeg;

d) mis tahes muudatused, mille korral sertifikaat kaotab kehtivuse;

e) TEMPEST-asutuse allkiri.

6. Kohalik julgeolekuametnik või salastatud koosoleku korraldamise eest vastutav isik, kes kooskõlastab oma tegevust kohaliku julgeolekuametnikuga, võib esitada TEMPEST-asutusele taotluse, et ta kontrolliks koosolekuruume ja veenduks, et need on tehniliselt turvalised.

Artikkel 6

Krüptovahendite heakskiitmise asutus

1. Krüptovahendite heakskiitmise asutus vastutab krüpteerimistehnoloogia kasutamise heakskiitmise eest.

2. Ta väljastab suunised krüpteerimistehnoloogia kasutamise ja heakskiitmise nõuete kohta.

3. Krüptovahendite heakskiitmise asutus kiidab krüpteerimislahenduste kasutamise heaks süsteemi omaniku taotluse alusel. Heakskiidu andmiseks tuleb rahuldavalt hinnata vähemalt järgmist:

a) kaitstava teabe turvavajadused;

b) lahenduses kasutatava side- ja infosüsteemi ülevaade;

c) olemuslike ja jääkriskide hinnang;

d) kavandatava lahenduse kirjeldus;

e) krüpteerimislahenduse turvanõuete rakendamise kord.

4. Krüptovahendite heakskiitmise asutus peab heakskiidetud krüpteerimislahenduste registrit.

Artikkel 7

Krüptomaterjalide jaotamise asutus

1. Krüptomaterjalide jaotamise asutus vastutab ELi salastatud teabe kaitseks kasutatavate krüptomaterjalide (peamiselt krüpteerimisseadmed, krüptovõtmed, sertifikaadid ja seotud autenturid) järgmistele isikutele jaotamise eest:

a) komisjoni talitustele või kasutajatele väliste osaliste hallatavate side- ja infosüsteemide jaoks;

b) komisjonivälistele organisatsioonidele või kasutajatele komisjoni hallatavate side- ja infosüsteemide jaoks.

2. Krüptomaterjalide jaotamise asutus võib delegeerida kolmandatele isikutele krüptomaterjalide jaotamise teistele talitustele kooskõlas otsuse 2015/443 artikli 17 lõikega 3.

3. Krüptomaterjalide jaotamise asutus tagab, et kõik krüptomaterjalid saadetakse turvaliste kanalite kaudu, mida kaitstakse igasuguse rikkumise eest ja mis suudavad sellise rikkumise tuvastada, kooskõlas julgeolekunormidega, mida kohaldatakse nende materjalidega kaitstava ELi salastatud teabe salastatuse taseme suhtes.

4. Krüptomaterjalide jaotamise asutus esitab suuniseid iga sellise komisjoni talituse kohalikule julgeolekuametnikule ja vajaduse korral kohalikule informaatika turvalisuse ametnikule, mis osaleb krüptomaterjalide koostamises, jaotamises või kasutamises.

5. Krüptomaterjalide jaotamise asutus tagab, et jaotamise käigus määratakse kindlaks sobilik turvanõuete rakendamise kord.

3. PEATÜKK

Komisjoni talitused

Artikkel 8

Talituste juhatajad

1. Iga talituse juhataja nimetab:

a) talituse või kabineti kohaliku julgeolekuametniku ning vajaduse korral tema asetäitja(d);

b) iga ELi salastatud teabe registrit pidava talituse registri kontrolliametniku ning vajaduse korral tema asetäitja(d);

c) iga ELi salastatud teavet töötleva side- ja infosüsteemi omaniku.

2. Talituse juhataja taotleb enne kohalike julgeolekuametnike, nende asetäitjate, registri kontrolliametnike ja nende asetäitjate nimetamist personalihalduse ja julgeoleku peadirektoraadi julgeolekudirektoraadi direktori heakskiitu.

3. Talituse juhataja määrab kohaliku julgeolekuametnikuga konsulteerides kindlaks kõik ametikohad, millel töötavad inimesed vajavad ELi salastatud teabele juurdepääsu luba. Neile ametikohtadele kandideerivaid inimesi teavitatakse värbamise ajal nõudest omandada salastatud teabele juurdepääsu luba.

4. Kõigi ELi salastatud teavet valdavate talituste juhatajad vastutavad vajaduse korral hädaolukorras evakueerimise ja hävitamise plaanide rakendamise eest. Plaanid peavad sisaldama alternatiivi olukordadeks, kui talituse juhatajaga ei ole võimalik ühendust võtta.

Artikkel 9

ELi salastatud teavet töötlevate side- ja infosüsteemide omanikud

1. Süsteemi omanik võtab ELi salastatud teavet töötleva side- ja infosüsteemi rakendamise projekti puhul võimalikult kiiresti ühendust turvalisuse akrediteerimise asutusega, et teha kindlaks asjakohased turvastandardid ja -nõuded ning alustada turvalisuse akrediteerimist.

2. Süsteemi omanik tagab, et turvameetmed vastavad turvalisuse akrediteerimise asutuse nõuetele ning et side- ja infosüsteem ei töötle ELi salastatud teavet enne akrediteerimist.

3. Süsteemi omanik võtab ühendust krüptovahendite heakskiitmise asutusega, et saada heakskiit mis tahes krüpteerimistehnoloogia kasutamisele. Süsteemide omanikud ei kasuta tootmissüsteemides krüpteerimistehnoloogiat enne sellele eelneva heakskiidu saamist.

4. Süsteemi omanik konsulteerib side- ja infosüsteemi turvalisuse asjus talituse kohaliku informaatika turvalisuse ametnikuga.

5. Süsteemi omanik vaatab süsteemi suhtes kohaldatavad turvameetmed, sh selle turvaplaani, vähemalt kord aastas läbi.

6. Kui side- ja infosüsteemis toimub turvaintsident, mille tõttu ei saa side- ja infosüsteem enam ELi salastatud teavet piisavalt kaitsta, siis teavitab süsteemi omanik kohalikku julgeolekuametnikku ja võtab viivitamata ühendust turvalisuse akrediteerimise asutusega, et küsida nõu, kuidas tegutseda. Sel juhul võidakse akrediteerimine peatada ja süsteem kuni sobiliku parandusmeetme võtmiseni kasutusest kõrvaldada.

7. Süsteemi omanik toetab turvalisuse akrediteerimise asutust alati täiel määral, kui asutus täidab side- ja infosüsteemi akrediteerimisega seotud ülesandeid.

Artikkel 10

Infokindluse rakendusasutus

Iga side- ja infosüsteemi infokindluse rakendusasutus teeb järgmist:

a) määrab kindlaks turbedokumendid kooskõlas turbe tegevuspõhimõtete ja turbesuunistega, eelkõige turvaplaaniga, süsteemiga seotud turvanõuete rakendamise korra ja krüptograafilised dokumendid, mida kasutatakse side- ja infosüsteemi akrediteerimisel;

b) osaleb süsteemispetsiifiliste tehnilise turvalisuse meetmete, seadmete ja tarkvara valimises ja katsetamises, teostab järelevalvet nende rakendamise üle ja tagab nende turvalise paigaldamise, konfigureerimise ja haldamise kooskõlas asjakohaste turbedokumentidega;

c) osaleb TEMPEST-turvameetmete ja seadmete valimises, kui seda turvaplaanis nõutakse, ning tagab koostöös TEMPEST-asutusega, et need paigaldatakse turvaliselt ja neid hooldatakse;

d) teeb järelevalvet süsteemi käitamisega seotud turvanõuete rakendamise korra rakendamise ja kohaldamise üle;

e) haldab ja töötleb koostöös krüptomaterjalide jaotamise asutusega krüptovahendeid, et tagada krüptomaterjalide ja kontrollimisvahendite säilitamine ning vajaduse korral krüpteerimisvariantide genereerimine;

f) viib ellu turvaanalüüse ja läbivaatamisi ning teeb katseid, eelkõige et koostada turvalisuse akrediteerimise asutuse nõudel asjakohaseid riskiaruandeid;

g) pakub side- ja infosüsteemispetsiifilist infokindluse alast koolitust;

h) rakendab ja kasutab side- ja infosüsteemispetsiifilisi turvameetmeid.

4. PEATÜKK

Kohalik julgeolekuametnik

Artikkel 11

Kohaliku julgeolekuametniku nimetamine

1. Kohalik julgeolekuametnik ja tema asetäitjad on ametnikud või ajutised teenistujad.

2. Kõigil kohalikel julgeolekuametnikel ja nende asetäitjatel on kehtivad julgeolekuload, et saada juurdepääs ELi salastatud teabele kuni tasemeni SECRET UE/EU SECRET ning vajaduse korral kuni tasemeni TRES SECRET UE/EU TOP SECRET. Kohalikud julgeolekuametnikud ja nende asetäitjad peavad hankima enne ametisse nimetamist julgeolekuload.

3. Komisjoni esindused võivad esitada komisjoni julgeolekuasutusele taotluse, et ta teeks erandi lõigetes 1 ja 2 märgitud nõuetest.

Artikkel 12

Turvaalade turvanõuete rakendamise kord

1. Asjaomase komisjoni talituse kohalik julgeolekuametnik koostab iga oma vastutusalasse kuuluva turvaala turvanõuete rakendamise korra.

2. Kohalik julgeolekuametnik tagab, et turvanõuete rakendamise kord vastab järgmistele nõuetele:

a) tööajal lubatakse turvaalasse saatjata siseneda ainult töötajatel, kellel on kehtiv julgeolekuluba ja põhjendatud vajadus saada juurdepääs tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud dokumentidele;

b) töövälisel ajal lubatakse turvaalasse saatjata siseneda ainult talituse julgeolekuametnikul, turvaala registri kontrolliametnikul/kontrolliametnikel, nende asetäitjatel ning personalihalduse ja julgeoleku peadirektoraadi julgeolekudirektoraadi volitatud töötajatel;

c) ilma komisjoni julgeolekuasutuse eelneva loata ei lubata turvaalasse tuua salvestus- ja sideseadmeid, näiteks mobiiltelefone, arvuteid, kaameraid või muid nutiseadmeid; mis tahes erandeid tuleb komisjoni julgeolekuasutuselt eelnevalt taotleda; kohalik julgeolekuametnik tegutseb kontaktpunktina;

d) kõiki asutusesiseseid või -väliseid töötajaid, kes vajavad turvaalale juurdepääsu, aga ei vasta punktis a märgitud kriteeriumidele, peab nõuetekohaselt volitatud töötaja turvaalas pidevalt saatma ja nende järele valvama; iga selline juurdepääs turvaalale kantakse logiraamatusse, mida hoitakse turvaala sissepääsu juures;

e) kohalik julgeolekuametnik tagab, et turvaala jälgivad sissetungituvastuse süsteemid on pidevalt kasutusel ja toimivad nõuetekohaselt, ning ta haldab kõiki sellega seotud paroole, võtmeid, PIN-koode ning muid juurdepääsu- ja autentimismehhanisme;

f) turvaalaga seotud häiretest teatatakse personalihalduse ja julgeoleku peadirektoraadi julgeolekudirektoraadile, kes teavitab viivitamata kohalikku julgeolekuametnikku;

g) selle talituse kohalik julgeolekuametnik, kus turvaala asub, peab registrit kõigist pärast häiret või turvaintsidenti toimunud sekkumistest;

h) võetakse kasutusele menetlused, mida rakendatakse turvaalas antud häire või toimunud muu hädaolukorra puhul, sh töötajate evakueerimine ning komisjoni julgeolekuasutuse vastutusalasse kuuluva hädaolukordadele reageerimise rühma ja vajaduse korral asutuseväliste hädaabiteenistuste kiire tegevuse tagamine;

i) kohalik julgeolekuametnik teatab komisjoni julgeolekuasutusele viivitamata kõigist turvaalas toimunud või sellega seotud turvarikkumistest, et määrata kindlaks sobilik reageerimisviis;

j) turvaala eraldiseisvad bürood, ruumid ja seifid hoitakse lukus alati, kui keegi nendes või nende juures ei viibi;

k) töötajad väldivad salastatud teabe arutamist turvaala koridorides või muudel üldkasutatavatel aladel, kui läheduses viibivad vastava loata isikud.

Artikkel 13

Turvavõtmed ja koodid

1. Kohaliku julgeolekuametniku üldisesse vastutusalasse kuulub turvaalas või sellele juurdepääsu saamiseks kasutatavate võtmete ja koodide nõuetekohane käsitsemine ja säilitamine. Võtmeid ja koode säilitatakse seifis ja neid kaitstakse vähemalt samal tasemel kui materjali, millele nende abil saab juurdepääsu.

2. Kohalik julgeolekuametnik peab registrit seifidest ja turvakambritest ning ajakohastatud nimekirja kõigist töötajatest, kellel on neile saatjata juurdepääs.

3. Kohalik julgeolekuametnik peab registrit seifide ja turvakambrite võtmetest ning töötajatest, kellele need antakse. Iga antud võtme kohta säilitatakse kinnitust, mis sisaldab teavet võtme tunnusandmete, saaja, saamise kuupäeva ja kellaaja kohta.

4. Võtmed ja koodid antakse ainult töötajatele, kellel on ELi salastatud teabe tundmistarve ja kellele on antud sellele juurdepääsu saamiseks sobilik luba. Kui need tingimused ei ole enam täidetud, siis võtab kohalik julgeolekuametnik mis tahes võtme tagasi.

5. Kohalik julgeolekuametnik hoiab varuvõtmeid ja kirjalikku märget iga koodi kohta eraldi suletud, läbipaistmatutes, allkirjastatud ja kuupäevaga ümbrikutes, mille annavad võtmete eest vastutavad töötajad. Neid ümbrikke hoitakse seifis, mis on sobilik kõnealuses seifis või turvakambris hoitava kõige salajasema materjali hoidmiseks.

6. Kui koodi või võtme vahetamise korral on ümbrikul märke selle rikkumisest või kahjustamisest, siis käsitleb kohalik julgeolekuametnik seda turvaintsidendina ja annab sellest viivitamata komisjoni julgeolekuasutusele teada.

7. Turvaalades muudetakse seifikoode kohaliku julgeolekuametniku järelevalve all. Koode vahetatakse iga 12 kuu tagant ja järgmistel juhtudel:

a) võetakse vastu uus seif või paigaldatakse uus lukk (eelkõige tuleb viivitamata muuta vaikimisi määratud koode);

b) eeldatakse salajasuse kahjustamist või see on toimunud;

c) koodi teadev isik ei vaja enam juurdepääsu.

8. Kohalik julgeolekuametnik peab registrit lõikes 7 osutatud koodide muutmise kuupäevadest.

Artikkel 14

ELi salastatud teabe hädaolukorras evakueerimise ja hävitamise plaanid

1. Kohalik julgeolekuametnik aitab talituse juhatajal koostada ELi salastatud teabe hädaolukorras evakueerimise ja hävitamise plaanid, lähtudes personalihalduse ja julgeoleku peadirektoraadi esitatud suunistest.

2. Kohalik julgeolekuametnik tagab, et mis tahes seadmed, mis on vajalikud lõikes 1 märgitud plaanide elluviimiseks, on kergesti kättesaadavad ja neid hoitakse heas töökorras.

3. Kohalik julgeolekuametnik vaatab koos lõikes 1 märgitud plaanides nimetatud ametnikega iga 12 kuu tagant läbi plaanide valmisoleku astme ja võtab mis tahes meetmeid, mis on vajalikud nende ajakohastamiseks.

Artikkel 15

Julgeolekuload

1. Kohalik julgeolekuametnik peab registrit talituse kõigist ametikohtadest, mille puhul nõutakse komisjoni julgeolekuluba, ning nendel ametikohtadel töötavatest inimestest. Julgeolekuloa nõue tuleb märkida värbamisprotsessi käigus teatesse vaba ametikoha kohta ja kandidaati tuleb sellest vestluse ajal teavitada.

2. Kohalik julgeolekuametnik teeb kõigi ELi salastatud teabele juurdepääsu saamiseks esitatud julgeolekulubade taotluste järelevalvet. Kohalik julgeolekuametnik on julgeolekulubade asjus talituse kontaktpunkt ja suhtleb komisjoni julgeolekuasutusega.

3. Kohalik julgeolekuametnik esitab taotluse, et algatada asjaomasele töötajale julgeolekuloa andmise menetlus, ning tagab, et töötaja esitab riikliku julgeolekukontrolli küsimustiku viivitamata komisjoni julgeolekuasutusele.

4. Kohalik julgeolekuametnik tagab, et talituse julgeolekukontrolli läbinud töötajad osalevad julgeolekuloa saamiseks kohustuslikus ELi salastatud teabe infotunnis.

5. Kohalik julgeolekuametnik suhtleb korrapäraselt talituse personaliosakonnaga, et saada teavet julgeolekuloa nõudega ametikohtadel toimunud kõigi muutuste kohta, ning teavitab komisjoni julgeolekuasutust viivitamata kõigist sellistest muutustest.

6. Kohalik julgeolekuametnik teavitab komisjoni julgeolekuasutust uute julgeolekukontrolli läbinud töötajate saabumisest, kes asuvad tööle julgeolekuluba nõudval ametikohal.

7. Kohalik julgeolekuametnik tagab, et talituse töötajad läbivad salastatud teabele juurdepääsu loa uuendamise menetluse nõutud tähtpäevaks. Kõiki töötajaid, kes keelduvad menetluse läbimisest, kohustatakse minema üle ametikohale, mille puhul ei nõuta julgeolekuluba.

Artikkel 16

ELi salastatud teabe register

1. Kui talitus haldab ELi salastatud teabe registrit, siis kontrollib kohalik julgeolekuametnik registri kontrolliametnike tegevust, mille puhul töödeldakse ELi salastatud teavet, ning ELi salastatud teavet kaitsvate julgeolekunormide järgimist.

2. Kohalik julgeolekuametnik teeb vähemalt iga 12 kuu tagant ning registri kontrolliametniku või tema asetäitja vahetumise korral järgmised kontrollid:

a) ELi salastatud teabe registri dokumentide valimi kontroll, et veenduda nende seisundis ja salastatud dokumentide registri täpsuses;

b) ELi salastatud teabe registrist ELi salastatud teabe väljastamise ja selle sinna kandmise kinnituste ja edastusdokumentide valimi kontroll;

c) hävitamisaktide valimi kontroll.

3. Kohalik julgeolekuametnik teeb vähemalt kord kuus salastatud dokumentide registri ja hiljuti laekunud salastatud dokumentide pistelisi kontrolle, et veenduda, et dokumendid registreeritakse nõuetekohaselt.

4. Kõik kontrollid registreeritakse salastatud dokumentide registri logisse.

Artikkel 17

Muud julgeolekualased kohustused

Kohaliku julgeolekuametniku muud julgeolekualased kohustused märgitakse julgeolekuteates, mis käsitleb eelkõige inimeste, objektide, muu vara ja teabe füüsilist julgeolekut.

5. PEATÜKK

Registri kontrolliametnik

Artikkel 18

Registri kontrolliametniku nimetamine

1. Registri kontrolliametnik ja tema asetäitjad on ametnikud või ajutised teenistujad.

2. Kõigil registri kontrolliametnikel ja nende asetäitjatel on kehtivad julgeolekuload, et saada juurdepääs ELi salastatud teabele kuni tasemeni SECRET UE/EU SECRET ning vajaduse korral kuni tasemeni TRES SECRET UE/EU TOP SECRET. Registri kontrolliametnikud ja nende asetäitjad peavad enne ametisse nimetamist hankima julgeolekuload.

3. Komisjoni esindused võivad esitada komisjoni julgeolekuasutusele taotluse, et ta teeks erandi lõigetes 1 ja 2 märgitud nõuetest.

Artikkel 19

Kohustused

1. Registri kontrolliametnikud registreerivad tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabe julgeoleku kaalutlustel, kui:

a) see saabub komisjoni talitusse või saadetakse sealt välja või

b) see saabub side- ja infosüsteemi või saadetakse sealt välja.

2. Registri kontrolliametnikud registreerivad kõik tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabe olelusringi sündmused. Registri kontrolliametnikud tagavad ka, et registreeritakse kogu tasemel RESTREINT UE/EU RESTRICTED või võrdväärsel tasemel salastatud teave, mida vahetatakse kolmandate riikide ja rahvusvaheliste organisatsioonidega. Seda tehakse kooskõlastades tegevust peasekretariaadi hallatud ELi salastatud teabe registriga.

3. Registri kontrolliametnik kannab tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud dokumendid salastatud dokumentide registrisse ja tagab, et neid säilitatakse turvaliselt ELi salastatud teabe registris.

4. Registri kontrolliametnik abistab komisjoni töötajaid tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud teabe koostamisel ja saatmisel.

5. Kui tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud dokumente saadakse teistelt talitustelt või välistelt osalejatelt, siis tagab registri kontrolliametnik, et saatjale esitatakse nõuetekohaselt vastuvõtu kinnitus.

6. Enne seda, kui registri kontrolliametnik lubab töötajal saada juurdepääsu ELi salastatud teabe registris sisalduvale salastatud dokumendile, küsib ametnik kohalikult julgeolekuametnikult kinnitust, et töötaja on saanud komisjoni julgeolekuasutuse julgeolekuloa.

7. Registri kontrolliametnik kannab logisse kõik ELi salastatud teabe registrisse sisenenud ja sealt väljunud töötajad, kellel ei ole saatjata juurdepääsu luba, ning saadab neid nende külastuse ajal.

8. Kui töötaja võtab ELi salastatud teabe registrist dokumendi selle lugemiseks, siis tagab registri kontrolliametnik, et see töötaja on kursis asjakohaste kompenseerivate turvameetmetega ja et töötaja tagastab dokumendi niipea, kui ta seda enam ei vaja. Registri kontrolliametnik tuletab töötajatele meelde, et nad tagastaksid sellised dokumendid võimalikult kiiresti.

9. ELi salastatud teabe registrist väljastatakse kullerisertifikaat, kui salastatud dokumendid viiakse käsipostiga väljapoole registri asukohariiki.

10. Üksikasjalikud juhised registri kontrolliametnikele salastatud dokumentide registreerimiseks esitatakse julgeolekuteates.

Artikkel 20

Salastatuse taseme alandamine ja salastatuse kustutamine

Registri kontrolliametnik abistab päritolutalitusi registreeritud ELi salastatud teabe läbivaatamisel, et teha kindlaks, kas algne salastatuse tase on jätkuvalt asjakohane või kas dokumendi salastatuse taset saab alandada või salastatuse kustutada.

Artikkel 21

Hävitamine

1. Registri kontrolliametnikud vastutavad tasemel CONFIDENTIEL UE/EU CONFIDENTIAL ja kõrgemal tasemel salastatud teabe nõuetekohasel viisil hävitamise eest, vajaduse korral julgeolekukontrolli läbinud tunnistajate kohalolul.

2. Registri kontrolliametnikud kannavad tasemel CONFIDENTIEL UE/EU CONFIDENTIAL ja kõrgemal tasemel salastatud teabe hävitamise salastatud dokumentide registrisse ning säilitavad vastavaid hävitamisakte ELi salastatud teabe registris.

Artikkel 22

Lisaülesanded

1. Registri kontrolliametnikud annavad kohalikule julgeolekuametnikule kogu vajaliku abi, kui kohalik julgeolekuametnik teeb ELi salastatud teabe registri järelevalvet.

2. Registri kontrolliametnik annab eeldatud või toimunud turvaintsidentidest teada kohalikule julgeolekuametnikule, kes omakorda teatab neist komisjoni julgeolekuasutusele.

3. Registri kontrolliametnik, kes haldab tasemel CONFIDENTIEL UE/EU CONFIDENTIAL või kõrgemal tasemel salastatud koosolekut korraldava komisjoni talituse ELi salastatud teabe registrit, valmistab ette ELi salastatud teabe, mida koosoleku ajal käsitletakse, ning kooskõlastab tegevust koosoleku korraldajaga, et tagada kõigi dokumentide ja kinnituste käitlemine kehtivate normide kohaselt.

6. PEATÜKK

Lõppsätted

Artikkel 23

Läbipaistvus

Käesolevast otsusest antakse teada komisjoni töötajatele ja kõigile teistele isikutele, kelle suhtes see kehtib, ning otsus avaldatakse *Euroopa Liidu Teatajas*.

Artikkel 24

Käesolev otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Brüssel, 7. aprill 2022

Komisjoni nimel
presidendi eest
personalihalduse ja julgeoleku peadirektoraadi
peadirektor
Gertrud INGESTAD