KOMISJONI OTSUS (EL, Euratom) 2018/559,

6. aprill 2018,

milles sätestatakse rakenduseeskirjad otsuse (EL, Euratom) 2017/46 (Euroopa Komisjoni side- ja infosüsteemide turvalisuse kohta) artikli 6 jaoks

EUROOPA KOMISJON,

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

võttes arvesse Euroopa Aatomienergiaühenduse asutamislepingut,

võttes arvesse komisjoni 10. jaanuari 2017. aasta otsust (EL, Euratom) 2017/46 Euroopa Komisjoni side- ja infosüsteemide turvalisuse kohta, [1] eriti selle artiklit 6,

ning arvestades järgmist:

(1) Seoses otsuse (EL, Euratom) 2017/46 vastuvõtmisega peab komisjon vaatama läbi, ajakohastama ja koondama kokku rakenduseeskirjad, mis on seotud kehtetuks tunnistatud komisjoni otsusega C(2006) 3602 komisjoni kasutatavate side- ja infosüsteemide turvalisuse kohta.

(2) Turvalisusküsimuste eest vastutavale komisjoni liikmele on täielikus kooskõlas sisemiste eeskirjade ja menetlustega antud otsuse (EL, Euratom) 2017/46 [2] artikli 13 kohane volitus kehtestada rakenduseeskirjad.

(3) Otsuse C(2006) 3602 rakenduseeskirjad tuleks seega kehtetuks tunnistada,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

1. PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Käesoleva otsuse reguleerimisese ja kohaldamisala on esitatud otsuse (EL, Euratom) 2017/46 artiklis 1.

2. Käesoleva otsuse sätteid kohaldatakse kõigi side- ja infosüsteemide suhtes. Käesolevas otsuses sätestatud kohustusi ei kohaldata siiski selliste side- ja infosüsteemide suhtes, kus töödeldakse ELi salastatud teavet. Nende süsteemidega seotud asjakohased kohustused määravad kindlaks süsteemide omanikud ja komisjoni julgeolekuasutus kooskõlas komisjoni otsusega (EL, Euratom) 2015/444 [3].

3. Käesoleva otsuse 2. peatükis antakse ülevaade IT turbega seotud töökorralduse ja kohustuste praktilisest rakendamisest. Käesoleva otsuse 3. peatükis antakse ülevaade otsuse (EL, Euratom) 2017/46 artikliga 6 seotud protsessidest.

Artikkel 2

Mõisted

Käesolevas otsuses kasutatakse otsuse (EL, Euratom) 2017/46 artiklis 2 määratletud mõisteid. Lisaks kasutatakse käesolevas otsuses järgmisi mõisteid:

1) „krüptovahendite heakskiitmise asutus“ – seda funktsiooni täidab personalihalduse ja julgeoleku peadirektoraadi alluvuses olev komisjoni julgeolekuasutus;

---

[1] ELT L 6, 11.1.2017, lk 40.

[2] Komisjoni 8. novembri 2017. aasta otsus C(2017) 7428 final, millega antakse volitus võtta vastu rakenduseeskirjad, standardid ja suunised, mis käsitlevad Euroopa Komisjonis side- ja infosüsteemide turvet.

[3] Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta (ELT L 72, 17.3.2015, lk 53).

2) „välisvõrguühendus“ – mis tahes elektrooniline ühendus komisjoni sisevõrgu ja mingi muu võrgu, sealhulgas Interneti vahel. See mõiste ei hõlma kolmandate isikute võrke, mida pakutakse lepingute alusel ja mis on komisjoni sisevõrgu osaks;

3) „võtmehoiustus“ – kord krüptovõtmete koopiate hoidmiseks ühe või mitme eraldiseisva isiku juures, tagades ülesannete lahus hoidmise, eesmärgiga võimaldada nende taastamine operatiivkoopia kaotamise korral. Võtmed võib jagada kaheks või mitmeks osaks, millest igaüht hoitakse eri isiku juures, tagamaks, et tervet võtit ei oleks ühelgi isikul;

4) „RASCI“ – lühend, mis tähistab kohustuste määramist järgmiste indikaatorite alusel:

   a) „vastutav“ (R – *responsible*) – kohustatud tegutsema ja võtma vastu otsuseid, et saavutada vajalikud tulemused;

   b) „vastutusele võetav“ (A – *accountable*) – kohustatud andma vastust toimingute, otsuste ja soorituse kohta;

   c) „toetav“ (S – *supports*) – kohustatud töötama ülesande lõpuleviimiseks koos vastutava isikuga;

   d) „konsulteeritud“ (C – *consulted*) – isik, kellelt, küsitakse nõu või arvamust;

   e) „teavitatud“ (I – *informed*) – asjakohase teabega kursis hoitud.

2. PEATÜKK

TÖÖKORRALDUS JA KOHUSTUSED

Artikkel 3

Rollid ja kohustused

Käesoleva otsuse artiklitega 4–8 seotud rollid ja kohustused on määratud kindlaks RASCI mudeli alusel lisas.

Artikkel 4

Kooskõla komisjoni infoturbepõhimõtetega

1. Personalihalduse ja julgeoleku peadirektoraat vaatab komisjoni IT turbe põhimõtted ning nendega seotud standardid ja suunised läbi, tagamaks, et need on kooskõlas komisjoni üldiste turbepõhimõtetega, eelkõige komisjoni otsusega (EL, Euratom) 2015/443 ([1]) ja otsusega (EL, Euratom) 2015/444.

2. Personalihalduse ja julgeoleku peadirektoraat võib komisjoni muude talituste palvel vaadata läbi nende IT turbe põhimõtted või muud IT turbe dokumendid, tagamaks, et need on komisjoni infoturbepõhimõtetega kooskõlas. Komisjoni asjaomase talituse juhataja tagab, et vastuolud kõrvaldatakse.

3. Personalihalduse ja julgeoleku peadirektoraat, kes vastutab infoturbe eest, teeb koostööd informaatika peadirektoraadiga, tagamaks, et IT turbe protsessides võetakse täielikult arvesse otsuses (EL, Euratom) 2015/443, eelkõige selle artiklites 3 ja 9 sätestatud liigitust ja turbepõhimõtteid.

3. PEATÜKK

IT TURBE PROTSESSID

Artikkel 5

Krüpteerimistehnoloogiad

1. ELi salastatud teabe kaitsmiseks krüpteerimistehnoloogiate kasutamine peab olema kooskõlas otsusega (EL, Euratom) 2015/444.

2. Otsuse selle kohta, kas krüpteerimistehnoloogiaid kasutatakse salastamata teabe kaitsmiseks, teeb iga side- ja infosüsteemi omanik, võttes arvesse nii riske, mida krüpteerimise maandab, kui ka riske, mida krüpteerimine tekitab.

3. Krüpteerimistehnoloogiate kasutamise peab krüptovahendite heakskiitmise asutus alati enne nende kasutamist heaks kiitma, välja arvatud juhul, kui krüpteerimistehnoloogiaid kasutatakse üksnes salastamata teabe konfidentsiaalsuse kaitsmiseks selle edastamise ajal ning kui kasutatakse võrgusuhtluse standardprotokolle.

([1]) Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41).

4. Selleks et salvestatud andmeid saaks taastada, kui dekrüpteerimisvõti ei ole kättesaadav, tagavad komisjoni talitused, et kõigi dekrüpteerimisvõtmete varukoopiaid hoitakse võtmehoiustussüsteemis, välja arvatud juhul, kui tegemist on käesoleva artikli lõikes 3 osutatud erandiga. Krüpteeritud andmed taastatakse dekrüpteerimisvõtmete varukoopiate abil ainult siis, kui selleks on krüptovahendite heakskiitmise asutuse kindlaks määratud standardi kohane luba.

5. Krüpteerimistehnoloogiate kasutamisele heakskiidu saamise taotlused dokumenteeritakse ametlikult ja need sisaldavad side- ja infosüsteemi, kaitstavate andmete, kasutatavate tehnoloogiate ja nendega seotud turbenõuete rakendamise korra üksikasju. Süsteemi omanik peab need heakskiidutaotlused allkirjastama.

6. Krüpteerimistehnoloogiate kasutamisele heakskiidu saamise taotlusi hindab krüptovahendite heakskiitmise asutus avaldatud standardite ja nõuete alusel.

Artikkel 6

IT turbe inspekteerimine

1. Personalihalduse ja julgeoleku peadirektoraat inspekteerib IT turvet, et kontrollida, kas IT turbe meetmed on kooskõlas komisjoni IT turbe põhimõtetega, ja et kontrollida nende kontrollimeetmete terviklust.

2. Personalihalduse ja julgeoleku peadirektoraat võib IT turvet inspekteerida

a) omal algatusel,

b) infoturbe juhtnõukogu nõudmisel,

c) süsteemi omaniku palvel,

d) turvaintsidendi tõttu või

e) tulenevalt teatavat süsteemi ohustava suure riski tuvastamisest.

3. Andmete omanikud võivad nõuda IT turbe inspekteerimist enne side- ja infosüsteemis oma teabe salvestamist.

4. Inspekteerimise tulemused dokumenteeritakse ametlikus aruandes, mis esitatakse süsteemi omanikule ja mille koopia edastatakse kohalikule informaatika turvalisuse ametnikule (LISO) ning mis sisaldab järeldusi ja soovitusi selle kohta, kuidas parandada side- ja infosüsteemi vastavust IT turbe põhimõtetele. Personalihalduse ja julgeoleku peadirektoraat teavitab olulistest probleemidest ja soovitustest infoturbe juhtnõukogu.

5. Personalihalduse ja julgeoleku peadirektoraat jälgib soovituste elluviimist.

6. Kui see on asjakohane, hõlmab IT turbe inspekteerimine süsteemi omanikule nii sisemiste kui ka väliste teenuseosutajate poolt pakutavate teenuste, ruumide ja seadmete inspekteerimist.

Artikkel 7

Juurdepääs välisvõrkude kaudu

1. Personalihalduse ja julgeoleku peadirektoraat kehtestab eeskirjad standardiga, milles käsitletakse komisjoni side- ja infosüsteemide ning välisvõrkude vahelise juurdepääsu lubamist.

2. Eeskirjades eristatakse eri liiki välisvõrguühendusi ja nähakse igat liiki ühenduse jaoks ette asjakohased turbeeeskirjad, sealhulgas see, kas asjaomane asutus peab ühenduseks eelnevalt loa andma, nagu mainitud käesoleva artikli lõikes 4.

3. Kui see on nõutud, antakse luba ametliku taotluse alusel ja ametliku heakskiitmisprotsessi kohaselt. Heakskiit kehtib teatava aja jooksul ja see tuleb saada enne ühenduse aktiveerimist.

4. Loa andmise eest vastutab üldiselt personalihalduse ja julgeoleku peadirektoraat, kuid mõnda liiki ühenduse puhul võib ta selle otsuse (EL, Euratom) 2015/443 artikli 17 lõike 3 kohaselt omal äranägemisel ning lõikes 8 sätestatud tingimustest lähtudes delegeerida.

5. Selleks et kaitsta komisjoni side- ja infosüsteeme ning võrke loata juurdepääsu või muude turvarikkumiste ohu eest, võib luba andev üksus kehtestada lisaturbenõuded, mille täitmine on heakskiidu saamise tingimuseks.

6. Komisjonis osutab võrguteenuseid tavaliselt informaatika peadirektoraat. Komisjoni muu talitus, millel on võrk, mida ei paku informaatika peadirektoraat, peab enne selle kasutamist saama infoturbe juhtnõukogu nõusoleku. Komisjoni talitus dokumenteerib taotluse tegevusega seotud põhjendused ja näitab, et võrgukontrollid on piisavad sissetulevate ja väljaminevate infovoogude kontrollimise nõuete täitmiseks.

7. Side- ja infosüsteemi omanik määrab kohaliku informaatika turvalisuse ametniku abiga kindlaks turbenõuded süsteemile välise juurdepääsu jaoks ning tagab selle turvalisuse kaitsmiseks asjakohaste meetmete rakendamise.

8. Välisvõrguühendustega seoses rakendatud turbemeetmed tuginevad teadmisvajaduse ja vähimate õiguste põhimõttele, mis tagab, et isikud saavad ainult sellist teavet ja sellised juurdepääsuõigused, mida neil on vaja komisjoni jaoks ametlike ülesannete täitmiseks.

9. Kõiki välisvõrguühendusi filtreeritakse ja jälgitakse, et avastada võimalikke turvarikkumisi.

10. Kui ühendused luuakse selleks, et võimaldada side- ja infosüsteemide sisseostmist, sõltub loa andmine artiklis 8 kirjeldatud menetluse edukast lõpetamisest.

Artikkel 8

Side- ja infosüsteemide sisseostmine

1. Käesoleva otsuse kohaldamisel käsitatakse side- ja infosüsteemi sisseostetuna, kui seda pakutakse kolmandast isikust töövõtjaga sõlmitud lepingu alusel ning side- ja infosüsteem asub lepingu kohaselt väljaspool komisjoni ruume. See hõlmab üksikuid või mitmeid sisseostetud side- ja infosüsteeme või muid IT-teenuseid ja andmekeskuseid väljaspool komisjoni ruume ning komisjoni andmekogumite töötlemist välisüksuste poolt.

2. Side- ja infosüsteemi sisseostmise puhul võetakse järgmiselt arvesse töödeldava teabe tundlikkust või salastatust:

a) side- ja infosüsteem, milles töödeldakse ELi salastatud teavet, akrediteeritakse kooskõlas otsusega (EL, Euratom) 2015/444; sellele eelneb konsulteerimine komisjoni turvalisuse akrediteerimise asutusega. Süsteeme, milles töödeldakse ELi salastatud teavet, ei osteta sisse;

b) ELi salastamata teavet töötleva süsteemi omanik rakendab proportsionaalsed meetmed, et tegeleda turbevajadustega kooskõlas asjakohaste juriidiliste kohustuste või teabe tundlikkusega, võttes arvesse sisseostmise riske. Personalihalduse ja julgeoleku peadirektoraat võib kehtestada lisanõudeid;

c) sisseostetud arendusprojektides võetakse arvesse välja töötatud koodi ja arenduses kasutatud testandmete tundlikkust.

3. Sisseostetud side- ja infosüsteemi suhtes kohaldatakse peale otsuse (EL, Euratom) 2017/46 artiklis 3 sätestatute järgmisi põhimõtteid:

a) sisseostukokkulepped peavad olema sellised, millega välditakse konkreetsetest pakkujatest sõltumist;

b) turbekorralduse sisseostmisel tuleb minimeerida kolmanda üksuse töötajate võimalused pääseda juurde komisjoni andmetele või neid muuda;

c) kolmanda üksuse töötajad, kellel on sisseostetud side- ja infosüsteemile juurdepääs, peavad esitama konfidentsiaalsus-kokkulepped;

d) side- ja infosüsteemi sisseostmise kohta peab olema side- ja infosüsteemide registris märge.

4. Süsteemi omanik teeb andmete omaniku osalusel järgmist:

a) hindab sisseostmisega seotud riske ja dokumenteerib need;

b) kehtestab asjakohased turbenõuded;

c) konsulteerib kõigi muude ühendatud side- ja infosüsteemide omanikega, tagamaks, et nende turbenõuded on hõlmatud;

d) tagab, et sisseostuleping sisaldab asjakohaseid turbenõudeid ja õigusi;

e) täidab kõik muud nõuded, mis on sätestatud korras, millele on osutatud käesoleva artikli lõikes 8.

Need meetmed viiakse lõpule enne ühe või mitme side- ja infosüsteemi sisseostmiseks lepingu või muu kokkuleppe sõlmimist.

5. Selleks et täita kindlaks määratud turbenõudeid, juhivad süsteemide omanikud sissostmisega seotud riske side- ja infosüsteemi kasutusaja jooksul.

6. Süsteemide omanikud tagavad, et kolmandast isikust töövõtjad on kohustatud teavitama komisjoni viivitamata kõigist IT turbe intsidentidest, mis komisjoni sisseostetud side- ja infosüsteemi mõjutavad.

7. Süsteemi omanik vastutab selle tagamise eest, et side- ja infosüsteem, sisseostuleping ja turbekorraldus vastaksid komisjoni info- ja IT turbe eeskirjadele.

8. Personalihalduse ja julgeoleku peadirektoraat kehtestab kooskõlas artikliga 10 punktides 1–7 osutatud kohustuste ja toimingute kohta üksikasjaliku standardi.

4. PEATÜKK

MUUD SÄTTED JA LÕPPSÄTTED

Artikkel 9

Läbipaistvus

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

Artikkel 10

Standardid

1. Käesoleva otsuse sätteid käsitletakse vajaduse korral üksikasjalikumalt standardites ja/või suunistes, mis võetakse vastu kooskõlas otsusega (EL, Euratom) 2017/46 ja otsusega C(2017) 7428. IT turbe standardites ja suunistes käsitletakse rakenduseeskirju ja otsust (EL, Euratom) 2017/46 seoses spetsiifiliste turbevaldkondadega üksikasjalikumalt vastavalt ISO 27001:2013 A lisale. Need standardid ja suunised põhinevad valdkonna parimatel tavadel ja valitakse välja selliselt, et need sobiksid kokku komisjoni IT-keskkonnaga.

2. Vajaduse korral töötatakse vastavalt ISO 27001:2013 A lisale välja standardid järgmistes valdkondades:

1) infoturbe korraldus;

2) töötajate turvalisus;

3) varahaldus;

4) juurdepääsukontroll;

5) krüptograafia;

6) füüsiline turvalisus ja keskkonnaohutus;

7) talitluskindlus;

8) teabeedastuse turve;

9) süsteemi soetamine, arendamine ja hooldamine;

10) suhted pakkujatega;

11) infoturbeintsidentide haldus;

12) talitluspidevuse haldamise infoturbe aspektid;

13) nõuetele vastavus.

3. Infoturbe juhtnõukogu kiidab käesoleva artikli lõigetes 1 ja 2 osutatud standardid enne nende vastuvõtmist heaks.

4. Otsuse C(2006) 3602 rakenduseeskirjad, mis on seotud käesoleva otsuse kohaldamisalaga, tunnistatakse kehtetuks.

5. 16. augusti 2006. aasta otsuse C(2006) 3602 alusel vastu võetud standardid ja suunised jäävad jõusse, kui nad ei ole vastuolus käesolevate rakenduseeskirjadega, kuni nad tunnistatakse kehtetuks või kuni nad asendatakse otsuse (EL, Euratom) 2017/46 artikli 13 alusel vastu võetavate standardite või suunistega.

Artikkel 11

Jõustumine

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

Brüssel, 6. aprill 2018

Komisjoni nimel
presidendi eest
komisjoni liige
Günther OETTINGER

LISA

ROLLID JA KOHUSTUSED (RASCI)

RASCI mudelis määratakse üksustele rollid, kasutades järgmisi lühendeid:

a) R – vastutav

b) A – vastutusele võetav

c) S – toetav

d) C – konsulteeritud

e) I – teavitatud

Protsess / Roll	Infoturbe juhtnõukogu	Personalihalduse ja julgeoleku peadirektoraat (julgeoleku direktoraat)	Komisjoni talitused	Süsteemi omanik	Andmete omanik	Kohalik informaatika turvalisuse ametnik	Informaatika peadirektoraat	Lepingulised töövõtjad
Kooskõla komisjoni infoturbepõhimõtetega		**R/A**	**S**				**S**	
Krüpteerimistehnoloogiad		**C**	**A**	**R**	**I**	**C**		
IT turbe inspekteerimine	**I**	**A/R**		**S**	**I**	**I**	**S**	
Juurdepääs välisvõrkude kaudu	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Side- ja infosüsteemide sisseostmine		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Infoturbe juhtnõukoguga konsulteeritakse seoses sisevõrkude kasutamisega muude komisjoni talituste poolt kui informaatika peadirektoraat.

[2] Sisseostetud side- ja infosüsteemi omanik on vastutav; kõigi muude selliste side- ja infosüsteemi omanikega, millega sisseostetud side- ja infosüsteem on ühendatud, konsulteeritakse.