Euroopa Liidu
Nõukogu

Brüssel, 18. juuli 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	14. juuli 2022
Saaja:	Nõukogu peasekretariaat
Komisjoni dok nr:	C(2022) 4882 final - ANNEX
Teema:	LISA järgmise dokumendi juurde: KOMISJONI DELEGEERITUD MÄÄRUS, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014

Käesolevaga edastatakse delegatsioonidele dokument C(2022) 4882 final - ANNEX.

Lisatud: C(2022) 4882 final - ANNEX

EUROOPA
KOMISJON

Brüssel, 14.7.2022
C(2022) 4882 final

ANNEX

LISA

järgmise dokumendi juurde:

KOMISJONI DELEGEERITUD MÄÄRUS,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1139 rakendamise eeskirjad nõuete osas, mis on seotud selliste infoturvariskide juhtimisega, mis võivad mõjutada komisjoni määrustega (EL) nr 748/2012 ja (EL) nr 139/2014 hõlmatud organisatsioonide lennuohutust, ning muudetakse komisjoni määrusi (EL) nr 748/2012 ja (EL) nr 139/2014

LISA

INFOTURVE – ORGANISATSIOONIDELE ESITATAVAD NÕUDED

[IS.D.OR-OSA]

IS.D.OR.100 Kohaldamisala

Käesoleva osaga kehtestatakse nõuded, mida käesoleva määruse artiklis 2 osutatud organisatsioonid peavad täitma.

IS.D.OR.200 Infoturbe halduse süsteem

a) Organisatsioon kehtestab artiklis 1 sätestatud eesmärkide täitmiseks infoturbe halduse süsteemi ning rakendab ja hoiab seda töös, tagamaks, et organisatsioon:

1) kehtestab infoturvapoliitika, milles sätestatakse organisatsiooni üldpõhimõtted seoses infoturberiskide võimaliku mõjuga lennuohutusele;

2) teeb kindlaks ja vaatab läbi infoturvariskid kooskõlas punktiga IS.D.OR.205;

3) määrab kindlaks infoturvariski käsitlemise meetmed ja rakendab neid kooskõlas

punktiga IS.D.OR.210;

4) rakendab infoturbealast sisearuandluskava kooskõlas punktiga IS.D.OR.215;

5) kooskõlas punktiga IS.D.OR.220 määrab kindlaks meetmed, mida on vaja infoturvasündmuste avastamiseks, ja rakendab neid meetmeid, teeb kindlaks juhtumid, mida käsitatakse intsidentidena, mis võivad mõjutada lennuohutust, välja arvatud punkti IS.D.OR.205 alapunkti e kohaselt lubatud juhud, ning reageerib nendele infoturvaintsidentidele ja võtab meetmeid neist taastumiseks;

6) rakendab meetmeid, millest pädev asutus on teatanud kui viivitamatust reageeringust lennuohutust mõjutavale infoturvaintsidendile või turvaaugule;

7) võtab kooskõlas punktiga IS.D.OR.225 asjakohaseid meetmeid pädeva asutuse teatatud puuduste kõrvaldamiseks;

8) rakendab punkti IS.D.OR.230 kohast välisaruandluskava, et pädev asutus saaks võtta asjakohaseid meetmeid;

9) järgib punkti IS.D.OR.235 nõudeid, kui sõlmib punktis IS.D.OR.200 osutatud tegevuse mis tahes osa kohta allhankelepingu mõne muu organisatsiooniga;

10) järgib punkti IS.D.OR.240 kohaseid nõudeid töötajatele;

11) järgib punkti IS.D.OR.245 kohaseid andmesäilitusnõudeid;

12) jälgib organisatsiooni vastavust käesoleva määruse nõuetele ja annab puuduste kohta tagasisidet vastutavale juhatajale või projekteerimisorganisatsioonide puhul projekteerimisorganisatsiooni juhile, et tagada parandusmeetmete tõhus rakendamine;

13) kaitseb kogu sellise teabe konfidentsiaalsust, mida organisatsioon võib olla saanud teistelt organisatsioonidelt, vastavalt teabe tundlikkustasemele, ilma et see piiraks intsidentidest teatamise suhtes kohaldatavate nõuete järgimist.

b) Artiklis 1 osutatud nõuete pidevaks täitmiseks peab organisatsioon rakendama pidevat täiustamisprotsessi kooskõlas punktiga IS.D.OR.260.

c) Organisatsioon dokumenteerib kooskõlas punktiga IS.D.OR.250 kõik olulised protsessid, menetlused, rollid ja kohustused, mida on vaja punkti IS.D.OR.200 alapunkti a järgimiseks, ning kehtestab korra asjaomaste dokumentide muutmiseks. Kõnealuste protsesside, menetluste, rollide ja kohustustega seotud muudatusi hallatakse kooskõlas punktiga IS.D.OR.255.

d) Organisatsiooni poolt punkti IS.D.OR.200 alapunkti a täitmiseks kehtestatud protsessid, menetlused, rollid ja kohustused peavad vastama organisatsiooni tegevuse laadile ja keerukusele, lähtudes selle tegevusega kaasnevate infoturvariskide hindamisest, ning need võib integreerida muudesse olemasolevatesse juhtimissüsteemidesse, mida organisatsioon juba rakendab.

e) Ilma et see piiraks kohustust täita määruses (EL) nr 376/2014[1] sätestatud aruandlusnõudeid ja punkti IS.D.OR.200 alapunkti a alapunktis 13 sätestatud nõudeid, võib pädev asutus anda organisatsioonile loa mitte rakendada alapunktides a–d osutatud nõudeid ja punktides IS.D.OR.205–IS.D.OR.260 sisalduvaid asjaomaseid nõudeid, kui organisatsioon tõendab kõnealust pädevat asutust rahuldaval viisil, et toimingud, mida ta teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab, ei põhjusta ei talle endale ega teistele organisatsioonidele infoturvariske, mis võivad mõjutada lennuohutust. See luba põhineb infoturvariskide dokumenteeritud hindamisel, mille teostab organisatsioon või kolmas isik kooskõlas punktiga IS.D.OR.205 ning mille on läbi vaadanud ja heaks kiitnud pädev asutus.

Pädev asutus vaatab kõnealuse loa kehtivuse üle pärast kohaldatavat järelevalveauditi tsüklit ja iga kord, kui organisatsiooni tööde maht muutub.

IS.D.OR.205 Infoturbe halduse süsteem

a) Organisatsioon teeb kindlaks kõik oma elemendid, mida võivad ähvardada infoturvariskid. Need hõlmavad järgmist:

1) toimingud, mida organisatsioon teostab, rajatised, mida ta pakub, ressursid, mis talle eraldatakse ja teenused, mida ta osutab;

2) seadmed, süsteemid, andmed ja teave, mis aitavad kaasa alapunktis 1 loetletud elementide toimimisele.

b) Organisatsioon teeb kindlaks liidesed, mis tal on teiste organisatsioonidega ja mis võivad vastastikku põhjustada infoturvariske.

c) Alapunktides a ja b osutatud elementide ja liideste puhul teeb organisatsioon kindlaks infoturvariskid, mis võivad mõjutada lennuohutust. Organisatsioon teeb iga kindlakstehtud riski puhul järgmist:

1) määrab riskitaseme vastavalt organisatsiooni kehtestatud ja eelnevalt kindlaks määratud liigitusele;

2) seostab iga riski ja selle taseme alapunktide a ja b kohaselt kindlaks määratud asjakohase elemendi või liidesega.

Alapunktis 1 osutatud eelnevalt kindlaksmääratud liigituse puhul võetakse arvesse ohustsenaariumi esinemise võimalust ja selle ohutusalaste tagajärgede raskusastet. Sellele liigitusele tuginedes ja võttes arvesse, kas organisatsioonil on toimingute jaoks struktureeritud ning korratav riskijuhtimisprotsess, peab organisatsioon suutma kindlaks teha, kas risk on vastuvõetav või tuleb seda käsitleda kooskõlas punktiga IS.D.OR.210.

([1]) Euroopa Parlamendi ja nõukogu 3. aprilli 2014. aasta määrus (EL) nr 376/2014, mis käsitleb tsiviillennunduses toimunud juhtumitest teatamist ning juhtumite analüüsi ja järelmeid, millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 996/2010 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2003/42/EÜ ja komisjoni määrused (EÜ) nr 1321/2007 ja (EÜ) nr 1330/2007 (ELT L 122, 24.4.2014, lk 18).

Selleks et riskihindamisi oleks vastastikku hõlpsam võrrelda, võetakse alapunkti 1 kohasel riskitaseme määramisel arvesse asjakohast teavet, mis on kogutud koostöös alapunktis b osutatud organisatsioonidega.

d) Organisatsioon vaatab alapunktide a, b ja c kohaselt tehtud riskihindamise läbi ja ajakohastab seda kõikidel järgmistel juhtudel:

1) infoturvariskiga seotud elemendid on muutunud;

2) organisatsiooni ja teiste organisatsioonide vahelised liidesed või teiste organisatsioonide teatatud riskid on muutunud;

3) riskide kindlakstegemiseks, analüüsimiseks ja liigitamiseks kasutatud teave või teadmised on muutunud;

4) infoturvaintsidente analüüsides on saadud uusi teadmisi.

IS.D.OR.210 Infoturvariski käsitlemine

a) Organisatsioon töötab välja meetmed punkti IS.D.OR.205 kohaselt kindlaks tehtud vastuvõetamatute riskide käsitlemiseks, rakendab neid õigel ajal ja kontrollib nende jätkuvat tõhusust. Need meetmed võimaldavad organisatsioonil teha järgmist:

1) kontrollida asjaolusid, mis aitavad kaasa ohustsenaariumi tõhusale esinemisele;

2) vähendada ohustsenaariumi realiseerumisest tulenevaid tagajärgi lennuohutusele;

3) vältida riske.

Kõnealuste meetmetega ei kaasne uusi võimalikke vastuvõetamatuid riske lennuohutusele.

b) Punkti IS.D.OR.240 alapunktides a ja b osutatud isikut ja organisatsiooni teisi mõjutatud töötajaid teavitatakse punkti IS.D.OR.205 kohaselt tehtud riskihindamise tulemustest, asjaomastest ohustsenaariumidest ja rakendatavatest meetmetest.

Organisatsioon teavitab ka selliseid organisatsioone, kellega tal on punkti IS.D.OR.205 alapunkti b kohane liides, mis tahes riskidest, mida kumbki organisatsioon teisega jagab.

IS.D.OR.215 Infoturbealane sisearuandluskava

a) Organisatsioon kehtestab asutusesisese aruandluskava, mis võimaldab talletada ja hinnata infoturvasündmusi, sealhulgas neid, millest tuleb teatada vastavalt punktile IS.D.OR.230.

b) Kõnealune kava ja punktis IS.D.OR.220 osutatud protsess peavad võimaldama organisatsioonil teha järgmist:

1) välja selgitada, milliseid alapunkti a kohaselt teatatud juhtumeid peetakse infoturvaintsidentideks või turvaaukudeks, mis võivad mõjutada lennuohutust;

2) teha kindlaks alapunkti 1 kohaselt avastatud infoturvaintsidentide ja turvaaukude põhjused ning neid mõjutavad tegurid ning käsitleda neid infoturvariskide juhtimise protsessi osana kooskõlas punktidega IS.D.OR.205 ja IS.D.OR.220;

3) tagada, et hinnatakse kogu teadaolevat asjakohast teavet, mis on seotud alapunkti 1 kohaselt kindlaks tehtud infoturvaintsidentide ja turvaaukudega;

4) vajaduse korral tagada, et rakendatakse meetodit teabe asutusesiseseks levitamiseks.

c) Kõik allhankelepingu alusel tegutsevad organisatsioonid, kes põhjustavad asjaomasele organisatsioonile infoturvariske, mis võivad mõjutada lennuohutust, peavad teavitama organisatsiooni infoturvasündmustest. Kõnealune teave esitatakse konkreetsetes allhankelepingutes kehtestatud korras ja seda hinnatakse vastavalt alapunktile b.

d) Organisatsioon teeb uurimise käigus koostööd kõigi teiste organisatsioonidega, kes on märkimisväärselt panustanud oma tegevusega seotud infoturbesse.

e) Organisatsioon võib selle aruandlussüsteemi integreerida muude aruandlussüsteemidega, mida ta on juba rakendanud.

IS.D.OR.220 Infoturvaintsidendid – nende avastamine, neile reageerimine ja nendest taastumine

a) Organisatsioon rakendab punkti IS.D.OR.205 kohaselt tehtud riskihindamise tulemuste ja punkti IS.D.OR.210 kohaselt tehtud riskikäsitluse tulemuste põhjal meetmeid, et teha kindlaks sellised intsidendid ja turvaaugud, mille puhul võivad realiseeruda vastuvõetamatud riskid ja mis võivad mõjutada lennuohutust. Kõnealused avastamismeetmed võimaldavad organisatsioonil teha järgmist:

1) avastada kõrvalekalded eelnevalt kindlaks määratud funktsionaalse tulemuslikkuse lähtetasemetest;

2) anda hoiatus, et kõrvalekalde korral aktiveerida nõuetekohased reageerimismeetmed.

b) Organisatsioon rakendab meetmeid, et reageerida alapunkti a kohaselt kindlaks tehtud sündmusele, mis võib muutuda või olla muutunud infoturvaintsidendiks. Kõnealused reageerimismeetmed võimaldavad organisatsioonil teha järgmist:

1) reageerida alapunkti a alapunktis 2 osutatud hoiatustele, aktiveerides eelnevalt kindlaks määratud vahendid ja tegevussuunad;

2) piirata rünnaku levikut ja vältida ohustsenaariumi täielikku realiseerumist;

3) kontrollida punkti IS.D.OR.205 alapunktis a kindlaks määratud asjaomaste elementide tõrkeolekut.

c) Organisatsioon rakendab infoturvaintsidentidest taastumiseks meetmeid, sealhulgas vajaduse korral erakorralisi meetmeid. Kõnealused taastumismeetmed võimaldavad organisatsioonil:

1) kõrvaldada intsidendi põhjustanud olukorra või muuta intsidendi ohutase vastuvõetavaks;

2) saavutada punkti IS.D.OR.205 alapunktis a kindlaks määratud asjaomaste elementide ohutus ajavahemiku jooksul, mille organisatsioon on taastumiseks eelnevalt kindlaks määranud.

IS.D.OR.225 Reageerimine pädeva asutuse teatatud puudustele

a) Kui pädevalt asutuselt saadakse teade puuduse kohta, teeb organisatsioon järgmist:

1) selgitab välja nõuetele mittevastavuse algpõhjuse või -põhjused ja nõuetele mittevastavust soodustavad tegurid;

2) töötab välja parandusmeetmete kava;

3) tõendab pädevat asutust rahuldaval viisil, et nõuetele mittevastavus on kõrvaldatud.

b) Alapunktis a osutatud meetmed võetakse pädeva asutusega kokkulepitud aja jooksul.

IS.D.OR.230 Infoturbealane välisaruandluskava

a) Organisatsioon rakendab infoturbealast aruandlussüsteemi, mis vastab määruses (EL) nr 376/2014 ning selle delegeeritud õigusaktides ja rakendusaktides sätestatud nõuetele, kui kõnealust määrust organisatsiooni suhtes kohaldatakse.

b) Ilma et see piiraks määruses (EL) nr 376/2014 sätestatud kohustusi, tagab organisatsioon, et ta teavitab oma pädevat asutust kõigist infoturvaintsidentidest või turvaaukudest, mis võivad kujutada endast märkimisväärset riski lennuohutusele. Lisaks kohaldatakse järgmist:

1) kui selline intsident või turvaauk mõjutab õhusõidukit või sellega seotud süsteemi või komponenti, teatab organisatsioon sellest ka projekti kinnituse omanikule;

2) kui selline intsident või turvaauk mõjutab organisatsioonis kasutatavat süsteemi või komponenti, teatab organisatsioon sellest süsteemi või komponendi konstrueerimise eest vastutavale organisatsioonile.

c) Organisatsioon edastab alapunktis b osutatud olukordade kohta teavet järgmiselt:

1) pädevat asutust ja vajaduse korral projekti kinnituse omanikku või süsteemi või komponendi projekteerimise eest vastutavat organisatsiooni teavitatakse kohe, kui organisatsioon asjaomasest olukorrast teada saab;

2) pädevat asutust ja vajaduse korral projekti kinnituse omanikku või süsteemi või komponendi projekteerimise eest vastutavat organisatsiooni teavitatakse nii kiiresti kui võimalik, kuid mitte hiljem kui 72 tundi pärast seda, kui organisatsioon asjaomasest olukorrast teada saab, välja arvatud erakorraliste takistavate asjaolude korral.

Teade koostatakse pädeva asutuse määratud vormis ja see peab sisaldama kogu asjakohast teavet, mida organisatsioon on olukorra kohta kogunud;

3) pädevale asutusele ja vajaduse korral projekti kinnituse omanikule või süsteemi või komponendi projekteerimise eest vastutavale organisatsioonile esitatakse järelaruanne, milles on üksikasjalikult kirjeldatud meetmeid, mida organisatsioon on intsidendist taastumiseks võtnud või kavatseb võtta, ning meetmeid, mida ta kavatseb võtta samasuguste infoturvaintsidentide vältimiseks tulevikus.

Järelaruanne esitatakse kohe, kui need meetmed on kindlaks määratud, ja see koostatakse pädeva asutuse määratud vormis.

IS.D.OR.235 Allhankelepingu sõlmimine infoturbe haldamiseks

a) Kui organisatsioon sõlmib punktis IS.D.OR.200 osutatud tegevuse mis tahes osa teostamiseks allhankelepingu mõne muu organisatsiooniga, peab ta tagama, et lepinguga hõlmatud tegevus vastab käesoleva määruse nõuetele ja et lepingupartner töötab tema järelevalve all. Organisatsioon tagab, et allhanketegevusega seotud riske juhitakse nõuetekohaselt.

b) Organisatsioon tagab, et pädeval asutusel on taotluse korral juurdepääs allhankelepingu alusel tegutsevale organisatsioonile, et teha kindlaks käesolevas määruses sätestatud kohaldatavate nõuete jätkuv järgimine.

IS.D.OR.240 Töötajatele esitatavad nõuded

a) Organisatsiooni vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht, kes on määratud määruse (EL) nr 748/2012 ja määruse (EL) nr 139/2014 kohaselt, nagu on osutatud käesoleva määruse artikli 2 punkti 1 alapunktides a ja b, vastutab organisatsiooni esindajana selle eest, et organisatsioonis on kõiki käesoleva määrusega nõutavaid toiminguid võimalik rahastada ja ellu viia. See isik peab tegema järgmist:

1) tagama, et käesoleva määruse nõuete täitmiseks on olemas kõik vajalikud vahendid;

2) kehtestama punkti IS.D.OR.200 alapunkti a alapunktis 1 osutatud infoturvapoliitika ja seda edendama;

3) tõendama, et tal on olemas põhiteadmised käesoleva määruse kohta.

b) Vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht määrab isiku või isikute rühma, et tagada organisatsiooni vastavus käesoleva määruse nõuetele, ning määrab kindlaks oma volituste ulatuse. Kõnealune isik või isikute rühm allub otse vastutavale juhatajale või projekteerimisorganisatsiooni puhul selle juhile ning tal

peavad olema oma kohustuste täitmiseks vajalikud teadmised, taust ja kogemused. Menetlustes tuleb kindlaks määrata, kes asendab konkreetset isikut tema pikemal äraolekul.

c) Vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht määrab isiku või isikute rühma, kes vastutab punkti IS.D.OR.200 alapunkti a alapunktis 12 osutatud vastavuskontrolli eest.

d) Kui organisatsioon kasutab organisatsioonilisi infoturbestruktuure, -põhimõtteid, -protsesse ja -menetlusi koos teiste organisatsioonidega või oma organisatsiooni selliste valdkondadega, mille puhul kinnitust või deklaratsiooni ei nõuta, võib vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht delegeerida oma ülesanded ühisele vastutavale isikule.

Sel juhul lepivad organisatsiooni vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht ja ühine vastutav isik kokku koordineerimismeetmed, et tagada infoturbehalduse nõuetekohane integreerimine organisatsiooni.

e) Vastutav juhatajavõi projekteerimisorganisatsiooni juht või alapunktis d osutatud ühine vastutav isik vastutab organisatsiooni esindajana punkti IS.D.OR.200 rakendamiseks vajalike organisatsiooniliste struktuuride, põhimõtete, protsesside ja menetluste ning nende haldamise eest organisatsioonis.

f) Organisatsioonis kehtestatakse kord, millega tagatakse, et käesoleva lisaga hõlmatud toiminguteks on piisaval arvul töötajaid.

g) Organisatsioonis kehtestatakse kord, millega tagatakse, et alapunktis f osutatud töötajatel on oma ülesannete täitmiseks vajalik pädevus.

h) Organisatsioonis kehtestatakse kord, millega tagatakse, et töötajad on teadlikud neile määratud rollide ja ülesannetega seotud kohustustest.

i) Organisatsioon peab tagama, et selliste töötajate identiteedi ja usaldusväärsuse nõuetekohase kontrolli, kellel on juurdepääs infosüsteemidele ja andmetele, mille suhtes kohaldatakse käesoleva määruse nõudeid.

IS.D.OR.245 Andmete säilitamine

a) Organisatsioon registreerib oma infoturbehaldustoimingud.

1) Organisatsioon tagab järgmiste dokumentide arhiveerimise ja jälgitavuse:

i) kõik punkti IS.D.OR.200 alapunkti e kohaselt saadud load ja nendega seotud turvariskihindamised;

ii) punkti IS.D.OR.200 alapunkti a alapunktis 9 osutatud allhankelepingud;

iii) teave punkti IS.D.OR.200 alapunktis d osutatud peamiste protsesside kohta;

iv) teave punktis IS.D.OR.205 osutatud riskihindamise käigus kindlaks tehtud riskide kohta koos punktis IS.D.OR.210 osutatud asjakohaste riskikäsitlusmeetmetega;

v) andmed punktides IS.D.OR.215 ja IS.D.OR.230 osutatud aruandluskavade kohaselt teatatud infoturvaintsidentide ja turvaaukude kohta;

vi) teave selliste infoturvasündmuste kohta, mida võib avastamata infoturvaintsidentide või turvaaukude kindlakstegemiseks olla vaja uuesti hinnata.

2) Alapunkti 1 alapunktis i osutatud teavet säilitatakse vähemalt viis aastat pärast asjaomase loa kehtivuse lõppemist.

3) Alapunkti 1 alapunktis ii osutatud teavet säilitatakse vähemalt viis aastat pärast allhankelepingu muutmist või lõpetamist.

4) Alapunkti 1 alapunktides iii, iv ja v osutatud teavet säilitatakse vähemalt viis aastat.

5) Alapunkti 1 alapunktis vi osutatud teavet säilitatakse seni, kuni asjaomased infoturvasündmused on organisatsiooni kehtestatud perioodilisusega ümber hinnatud.

b) Organisatsioon registreerib infoturbehaldustöötajate kvalifikatsiooni ja kogemused.

1) Töötajate kvalifikatsiooni ja kogemusi käsitlevat teavet säilitatakse seni, kuni isik töötab organisatsiooni heaks, ja vähemalt kolm aastat pärast seda, kui asjaomane isik on organisatsioonist lahkunud.

2) Töötajate taotlusel tagatakse neile juurdepääs oma isiklikele dokumentidele. Lisaks esitab organisatsioon lahkuvatele töötajatele nende taotlusel koopia isiklikest dokumentidest.

c) Dokumentide vorming sätestatakse organisatsiooni tegevuskorras.

d) Dokumente säilitatakse nii, et need oleks kaitstud rikkumise, muutmise ja varguse eest, ning vajaduse korral määratakse kindlaks teabe salastatusaste. Organisatsioon kasutab asjakohaseid vahendeid dokumentide tervikluse ja autentsuse säilitamiseks ning tagab, et neile pääsevad juurde ainult lubatud isikud.

IS.D.OR.250 Infoturbehalduse käsiraamat

a) Organisatsioon teeb pädevale asutusele kättesaadavaks infoturbehalduse käsiraamatu ning vajaduse korral kõik selles viidatud käsiraamatud ja menetlused, mis sisaldavad järgmist teavet:

1) vastutava juhataja või projekteerimisorganisatsiooni puhul selle juhi allkirjastatud dokument, milles kinnitatakse, et organisatsioon tegutseb pidevas kooskõlas käesoleva lisaga ja infoturbehalduse käsiraamatuga. Kui vastutav juhataja või projekteerimisorganisatsiooni puhul selle juht ei ole organisatsiooni tegevjuht, peab kinnituse allkirjastama ka organisatsiooni tegevjuht;

2) punkti IS.D.OR.240 alapunktides b ja c osutatud isiku(te) ametinimetus(ed), nimi (nimed), kohustused, vastutus, ülesanded ja volitused;

3) vajaduse korral punkti IS.D.OR.240 alapunktis d osutatud isiku(te) ametinimetus(ed), nimi (nimed), kohustused, vastutus, ülesanded ja volitused;

4) organisatsiooni infoturvapoliitika, millele on osutatud punkti IS.D.OR.200 alapunkti a alapunktis 1;

5) töötajate arvu ja kategooriate ning töötajate olemasolu planeerimiseks kasutatava süsteemi üldine kirjeldus vastavalt punkti IS.D.OR.240 nõuetele;

6) punkti IS.D.OR.200 rakendamise eest vastutavate võtmeisikute, sealhulgas punkti IS.D.OR.200 alapunkti a alapunktis 12 osutatud vastavuskontrolli funktsiooni eest vastutava(te) isiku(te) ametinimetus(ed), kohustused, vastutus, ülesanded ja volitused;

7) organisatsiooni skeem, milles on näidatud alapunktides 2 ja 6 osutatud isikute aruandlus- ja vastutusahelad;

8) punktis IS.D.OR.215 osutatud sisearuandluskava kirjeldus;

9) menetlused, milles täpsustatakse, kuidas organisatsioon tagab käesoleva osa nõuete täitmise, ning eelkõige:

   i) punkti IS.D.OR.200 alapunktis c osutatud dokumenteerimistoimingud;

   ii) menetlused, millega määratakse kindlaks, kuidas organisatsioon kontrollib punkti IS.D.OR.200 alapunkti a alapunktis 9 osutatud lepingulist tegevust;

   iii) alapunkti c kohane menetlus infoturbehalduse käsiraamatu muutmiseks;

10) loetelu nõuete täitmise alternatiivsetest meetoditest, mis on praegu heaks kiidetud.

b) Infoturbehalduse käsiraamatu esimene väljaanne kiidetakse heaks ja pädev asutus säilitab selle koopia. Infoturbehalduse käsiraamatut muudetakse vastavalt vajadusele, et tagada organisatsiooni infoturbe halduse süsteemi kirjelduse ajakohasus. Pädevale asutusele esitatakse koopia kõigist infoturbehalduse käsiraamatu muudatustest.

c) Infoturbehalduse käsiraamatu muudatusi hallatakse organisatsiooni kehtestatud korras. Pädev asutus peab heaks kiitma kõik muudatused, mille suhtes asjaomast korda ei kohaldata, ja muudatused, mis on seotud punkti IS.D.OR.255 alapunktis b osutatud muudatustega.

d) Organisatsioon võib infoturbehalduse käsiraamatu integreerida muude olemasolevate juhtkonna näidismaterjalide või käsiraamatutega, kui on olemas selged ristviited, mis näitavad, millised juhtkonna näidismaterjali või käsiraamatu osad vastavad käesolevas lisas esitatud eri nõuetele.

IS.D.OR.255 Infoturbe halduse süsteemi muudatused

a) Infoturbe halduse süsteemi muudatusi võib hallata ja neist võib pädevat asutust teavitada organisatsiooni väljatöötatud korras. Selle korra peab heaks kiitma pädev asutus.

b) Kui asjaomase infoturbe halduse süsteemi muudatuste suhtes ei kohaldata alapunktis a osutatud korda, peab organisatsioon esitama need pädevale asutusele heakskiidu taotlemiseks ning selle saamiseks.

Kõnealuste muudatuste suhtes kohaldatakse järgmist:

1) taotlus tuleb esitada enne muudatuse tegemist, et pädeval asutusel oleks võimalik kontrollida, kas organisatsioon vastab jätkuvalt käesolevas määruses sätestatud nõuetele, ning vajaduse korral muuta organisatsiooni sertifikaati ja sellele lisatud sertifitseerimistingimusi;

2) organisatsioon teeb pädevale asutusele kättesaadavaks kogu teabe, mida nõutakse muudatuse hindamiseks;

3) muudatust rakendatakse alles siis, kui pädevalt asutuselt on selle kohta saadud ametlik heakskiit;

4) organisatsioon peab selliste muudatuste rakendamise ajal tegutsema pädeva asutuse ettenähtud tingimustel.

IS.D.OR.260 Pidev täiustamine

a) Organisatsioon hindab asjakohaste tulemusnäitajate abil infoturbe halduse süsteemi tulemuslikkust ja küpsust. Hindamine toimub organisatsiooni poolt eelnevalt kindlaks määratud ajakava alusel või pärast infoturvaintsidenti.

b) Kui alapunkti a kohase hindamise käigus leitakse puudusi, võtab organisatsioon vajalikud parandusmeetmed selle tagamiseks, et infoturbe halduse süsteem vastaks jätkuvalt kohaldatavatele nõuetele ja et infoturvariskide tase oleks jätkuvalt vastuvõetav. Lisaks hindab organisatsioon uuesti infoturbe halduse süsteemi neid elemente, mida vastuvõetud meetmed mõjutavad.