II

(Muut kuin lainsäätämisjärjestyksessä hyväksyttävät säädökset)

ASETUKSET

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2023/203,

annettu 27 päivänä lokakuuta 2022,

Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1139 soveltamissäännöistä komission asetusten (EU) N:o 1321/2014, (EU) N:o 965/2012, (EU) N:o 1178/2011 ja (EU) 2015/340 ja komission täytäntöönpanoasetusten (EU) 2017/373 ja (EU) 2021/664 soveltamisalaan kuuluvia organisaatioita sekä komission asetusten (EU) N:o 748/2012, (EU) N:o 1321/2014, (EU) N:o 965/2012, (EU) N:o 1178/2011, (EU) 2015/340 ja (EU) N:o 139/2014 ja komission täytäntöönpanoasetusten (EU) 2017/373 ja (EU) 2021/664 soveltamisalaan kuuluvia toimivaltaisia viranomaisia varten ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien hallintaa koskevien vaatimusten osalta sekä komission asetusten (EU) N:o 1178/2011, (EU) N:o 748/2012, (EU) N:o 965/2012, (EU) N:o 139/2014, (EU) N:o 1321/2014 ja (EU) 2015/340 ja komission täytäntöönpanoasetusten (EU) 2017/373 ja (EU) 2021/664 muuttamisesta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan unionin lentoturvallisuusviraston perustamisesta, Euroopan parlamentin ja neuvoston asetusten (EY) N:o 2111/2005, (EY) N:o 1008/2008, (EU) N:o 996/2010, (EU) N:o 376/2014 ja direktiivien 2014/30/EU ja 2014/53/EU muuttamisesta sekä Euroopan parlamentin ja neuvoston asetusten (EY) N:o 552/2004 ja (EY) N:o 216/2008 ja neuvoston asetuksen (ETY) N:o 3922/91 ([1]) kumoamisesta 4 päivänä heinäkuuta 2018 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1139 ja erityisesti sen 17 artiklan 1 kohdan b alakohdan, 27 artiklan 1 kohdan a alakohdan, 31 artiklan 1 kohdan b alakohdan, 43 artiklan 1 kohdan b alakohdan, 53 artiklan 1 kohdan a alakohdan sekä 62 artiklan 15 kohdan c alakohdan,

sekä katsoo seuraavaa:

(1) Jatkuvan lentokelpoisuuden hallintaorganisaatioiden ja huolto-organisaatioiden on asetuksen (EU) 2018/1139 liitteessä II olevan 3.1 kohdan b alakohdassa vahvistettujen keskeisten vaatimusten mukaan luotava johtamisjärjestelmä turvallisuusriskien hallitsemiseksi ja pidettävä sitä yllä.

(2) Asetuksen (EU) 2018/1139 liitteessä IV olevan 3.3 kohdan b alakohdassa ja 5 kohdan b alakohdassa vahvistettujen keskeisten vaatimusten mukaan myös lentokoulutusorganisaatioiden, matkustamomiehistön koulutusorganisaatioiden, lentomiehistön ilmailulääketieteen keskusten ja simulaatiokoulutuslaitteiden käyttäjien on luotava johtamisjärjestelmä turvallisuusriskien hallitsemiseksi ja pidettävä sitä yllä.

(3) Asetuksen (EU) 2018/1139 liitteessä V olevan 8.1 kohdan c alakohdassa vahvistettujen keskeisten vaatimusten mukaan lentotoiminnan harjoittajien on luotava johtamisjärjestelmä turvallisuusriskien hallitsemiseksi ja pidettävä sitä yllä.

(4) Lisäksi ilmaliikenteen hallinnan ja lennonvarmistuspalvelun tarjoajien, U-space-palveluntarjoajien ja yksinoikeudella toimivien yhteisen tietopalvelun tarjoajien sekä lennonjohtajien koulutusorganisaatioiden ja ilmailulääketieteen keskusten on asetuksen (EU) 2018/1139 liitteessä VIII olevan 5.1 kohdan c alakohdassa ja 5.4 kohdan b alakohdassa vahvistettujen keskeisten vaatimusten mukaan luotava johtamisjärjestelmä turvallisuusriskien hallitsemiseksi ja pidettävä sitä yllä.

([1]) EUVL L 212, 22.8.2018, s. 1.

(5) Turvallisuusriskeillä voi olla erilaisia alkulähteitä, kuten puutteet suunnittelussa tai kunnossapidossa, ihmisen suorituskykyyn liittyvät näkökohdat, ympäristöuhkat ja tietoturvauhkat. Sen vuoksi näissä Euroopan unionin lentoturvallisuusviraston, jäljempänä 'virasto', sekä kansallisten toimivaltaisten viranomaisten ja edellä olevissa johdanto-osan kappaleissa tarkoitettujen organisaatioiden luomissa hallintojärjestelmissä olisi otettava huomioon sattumanvaraisista tapahtumista johtuvien turvallisuusriskien lisäksi myös sellaisista tietoturvauhkista johtuvat turvallisuusriskit, joissa pahantahtoisessa tarkoituksessa toimivat henkilöt saattavat hyödyntää olemassa olevia puutteita. Tällaiset tietoturvariskit lisääntyvät siviili-ilmailuympäristössä jatkuvasti, sillä nykyiset tietojärjestelmät ovat yhä useammin yhteenliitettyjä ja entistä yleisemmin pahantahtoisten toimijoiden kohteina.

(6) Tietojärjestelmiin liittyvät riskit eivät rajoitu mahdollisiin kyberavaruuteen kohdistuviin hyökkäyksiin, vaan niihin kuuluvat myös prosesseihin ja menettelyihin sekä ihmisten suorituskykyyn mahdollisesti vaikuttavat uhkat.

(7) Organisaatioista suuri osa käyttää jo digitaalisen tiedon ja datan suojaamiseen kansainvälisiä standardeja, kuten ISO 27001 -standardia. Näissä standardeissa ei välttämättä oteta täysin huomioon kaikkia siviili-ilmailun erityispiirteitä. Tästä syystä on tarpeen asettaa vaatimuksia sellaisten tietoturvariskien hallitsemiseksi, joilla saattaa olla vaikutusta ilmailun turvallisuuteen.

(8) On olennaisen tärkeää, että vaatimukset kattavat kaikki ilmailun eri osa-alueet ja niiden rajapinnat, koska ilmailu on varsin yhteenliitetty järjestelmien järjestelmä. Sen vuoksi niitä olisi sovellettava kaikkiin komission asetusten (EU) N:o 748/2012 ([2]), (EU) N:o 1321/2014 ([3]), (EU) N:o 965/2012 ([4]), (EU) N:o 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) N:o 139/2014 ([7]) ja täytäntöönpanoasetuksen (EU) 2021/664 ([8]) soveltamisalaan kuuluviin organisaatioihin ja toimivaltaisiin viranomaisiin, myös niihin, joilla jo vaaditaan olevan unionin ilmailun turvallisuusalan lainsäädännön mukainen hallintojärjestelmä. Jotkin organisaatiot olisi kuitenkin jätettävä tämän asetuksen soveltamisalan ulkopuolelle asianmukaisen oikeasuhteisuuden varmistamiseksi niiden ilmailujärjestelmälle aiheuttamiin pienempiin tietoturvariskeihin nähden.

(9) Tässä asetuksessa säädetyillä vaatimuksilla olisi varmistettava johdonmukainen soveltaminen kaikilla ilmailun osa-alueilla, ja vaatimusten vaikutuksen kyseisillä osa-alueilla jo sovellettavaan unionin ilmailun turvallisuusalan lainsäädäntöön olisi oltava mahdollisimman vähäinen.

([2]) Komission asetus (EU) N:o 748/2012, annettu 3 päivänä elokuuta 2012, ilma-alusten ja niihin liittyvien tuotteiden, osien ja laitteiden lentokelpoisuus- ja ympäristösertifiointia sekä suunnittelu- ja tuotanto-organisaatioiden sertifiointia koskevista täytäntöönpanosäännöistä (EUVL L 224, 21.8.2012, s. 1).

([3]) Komission asetus (EU) N:o 1321/2014, annettu 26 päivänä marraskuuta 2014, ilma-alusten sekä ilmailutuotteiden, osien ja laitteiden jatkuvan lentokelpoisuuden ylläpidosta ja näihin tehtäviin osallistuvien organisaatioiden ja henkilöstön hyväksymisestä (EUVL L 362, 17.12.2014, s. 1).

([4]) Komission asetus (EU) N:o 965/2012, annettu 5 päivänä lokakuuta 2012, lentotoimintaan liittyvistä teknisistä vaatimuksista ja hallinnollisista menettelyistä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 mukaisesti (EUVL L 296, 25.10.2012, s. 1).

([5]) Komission asetus (EU) N:o 1178/2011, annettu 3 päivänä marraskuuta 2011, siviili-ilmailun lentomiehistöä koskevien teknisten vaatimusten ja hallinnollisten menettelyjen säätämisestä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 nojalla (EUVL L 311, 25.11.2011, s. 1).

([6]) Komission asetus (EU) 2015/340, annettu 20 päivänä helmikuuta 2015, lennonjohtajien lupakirjoja ja todistuksia koskevista teknisistä vaatimuksista ja hallinnollisista menettelyistä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 mukaisesti, komission täytäntöönpanoasetuksen (EU) N:o 923/2012 muuttamisesta ja komission asetuksen (EU) N:o 805/2011 kumoamisesta (EUVL L 63, 6.3.2015, s. 1).

([7]) Komission asetus (EU) N:o 139/2014, annettu 12 päivänä helmikuuta 2014, lentopaikkoihin liittyvistä vaatimuksista ja hallinnollisista menettelyistä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008 mukaisesti (EUVL L 44, 14.2.2014, s. 1).

([8]) Komission täytäntöönpanoasetus (EU) 2021/664, annettu 22 päivänä huhtikuuta 2021, U-spacen sääntelykehyksestä (EUVL L 139, 23.4.2021, s. 161).

(10) Tässä asetuksessa säädetyt vaatimukset eivät saisi vaikuttaa komission täytäntöönpanoasetuksen (EU) 2015/1998 ([9]) liitteessä olevassa 1.7 kohdassa eivätkä Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148 ([10]) 14 artiklassa vahvistettuihin tietoturva- ja kyberturvallisuusvaatimuksiin.

(11) Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/696 ([11]) V osaston ”Ohjelman turvallisuus” 33–43 artiklassa säädettyjen turvallisuusvaatimusten katsotaan vastaavan tässä asetuksessa säädettyjä vaatimuksia, paitsi tämän asetuksen liitteessä II olevan IS.I.OR.230 kohdan osalta, jota olisi noudatettava.

(12) Oikeusvarmuuden vuoksi tässä asetuksessa määritellyn termin ’tietoturva’ tulkinnan, joka kuvastaa termin yleistä käyttöä siviili-ilmailussa maailmanlaajuisesti, olisi katsottava olevan yhdenmukainen direktiivin (EU) 2016/1148 4 artiklan 2 kohdassa määritellyn termin ’verkko- ja tietojärjestelmien turvallisuus’ kanssa. Tätä asetusta sovellettaessa käytettävää tietoturvan määritelmää ei saisi tulkita direktiivissä (EU) 2016/1148 vahvistetusta verkko- ja tietojärjestelmien turvallisuuden määritelmästä poikkeavaksi.

(13) Jotta vältetään oikeudellisten vaatimusten päällekkäisyys silloin, kun tämän asetuksen soveltamisalaan kuuluviin organisaatioihin jo sovelletaan johdanto-osan 10 ja 11 kappaleessa tarkoitetuista unionin säädöksistä johtuvia turvavaatimuksia, jotka vaikutukseltaan vastaavat tämän asetuksen säännöksiä, kyseisten turvavaatimusten noudattamista olisi pidettävä tässä asetuksessa säädettyjen vaatimusten noudattamisena.

(14) Tämän asetuksen soveltamisalaan kuuluvien organisaatioiden, joihin jo sovelletaan täytäntöönpanoasetuksesta (EU) 2015/1998 tai asetuksesta (EU) 2021/696 taikka molemmista johtuvia turvavaatimuksia, olisi täytettävä myös tämän asetuksen liitteen II (osa IS.I.OR.230 ”Tietoturvaa koskeva ulkoinen ilmoitusjärjestelmä”) vaatimukset, koska kummassakaan asetuksessa ei ole säännöksiä tietoturvapoikkeamien ulkoisesta ilmoittamisesta.

(15) Kattavuuden vuoksi asetuksia (EU) N:o 1178/2011, (EU) N:o 748/2012, (EU) N:o 965/2012, (EU) N:o 139/2014, (EU) N:o 1321/2014, (EU) 2015/340 sekä täytäntöönpanoasetuksia (EU) 2017/373 ([12]) ja (EU) 2021/664 olisi muutettava, jotta tietoturvan hallintajärjestelmälle tässä asetuksessa asetetut vaatimukset voidaan ottaa käyttöön näissä asetuksissa säädettyjen hallintojärjestelmien kanssa sekä vahvistaa toimivaltaisia viranomaisia koskevat vaatimukset edellä mainittuja tietoturvan hallintavaatimuksia täytäntöönpanevien organisaatioiden valvonnan osalta.

(16) Jotta organisaatioilla olisi riittävästi aikaa varmistaa, että uusia sääntöjä ja menettelyjä noudatetaan, tätä asetusta olisi sovellettava kolmen vuoden kuluttua sen voimaantulosta, lukuun ottamatta täytäntöönpanoasetuksessa (EU) 2017/373 määriteltyä Euroopan geostationaarisen navigointilisäjärjestelmän (EGNOS) lennonvarmistuspalvelun tarjoajaa, jonka osalta sitä olisi sovellettava meneillään olevan EGNOS-järjestelmän ja -palvelujen asetuksen (EU) 2021/696 mukaisen turvallisuusjärjestelyjen hyväksynnän vuoksi 1 päivästä tammikuuta 2026.

(17) Tässä asetuksessa säädetyt vaatimukset perustuvat viraston antamaan lausuntoon nro 03/2021 ([13]), jonka se on antanut asetuksen (EU) 2018/1139 75 artiklan 2 kohdan b ja c alakohdan ja 76 artiklan 1 kohdan mukaisesti.

([9]) Komission täytäntöönpanoasetus (EU) 2015/1998, annettu 5 päivänä marraskuuta 2015, yksityiskohtaisista toimenpiteistä ilmailun turvaamista koskevien yhteisten perusvaatimusten täytäntöönpanemiseksi (EUVL L 299, 14.11.2015, s. 1).

([10]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

([11]) Euroopan parlamentin ja neuvoston asetus (EU) 2021/696, annettu 28 päivänä huhtikuuta 2021, unionin avaruusohjelman ja Euroopan unionin avaruusohjelmaviraston perustamisesta sekä asetusten (EU) N:o 912/2010, (EU) N:o 1285/2013 ja (EU) N:o 377/2014 ja päätöksen N:o 541/2014/EU kumoamisesta (EUVL L 170, 12.5.2021, s. 69).

([12]) Komission täytäntöönpanoasetus (EU) 2017/373, annettu 1 päivänä maaliskuuta 2017, ilmaliikenteen hallinta- ja lennonvarmistuspalvelujen sekä muiden ilmaliikenteen hallintaverkon toimintojen palveluntarjoajia koskevista yhteisistä vaatimuksista ja näiden palveluntarjoajien valvonnasta, asetuksen (EY) N:o 482/2008 sekä täytäntöönpanoasetusten (EU) N:o 1034/2011, (EU) N:o 1035/2011 ja (EU) 2016/1377 kumoamisesta ja asetuksen (EU) N:o 677/2011 (EUVL L 62, 8.3.2017, s. 1)

([13]) https://www.easa.europa.eu/document-library/opinions

(18) Tässä asetuksessa säädetyt vaatimukset ovat asetuksen (EU) 2018/1139 127 artiklalla perustetun yhteisten turvallisuussääntöjen soveltamista siviili-ilmailun alalla käsittelevän komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Kohde

Tässä asetuksessa vahvistetaan vaatimukset, jotka organisaatioiden ja toimivaltaisten viranomaisten on täytettävä

a) tunnistaakseen ja hallitakseen sellaisia tietoturvariskejä, jotka saattavat vaikuttaa tieto- ja viestintäteknisiin järjestelmiin ja siviili-ilmailussa käytettävään dataan,

b) havaitakseen tietoturvatapahtumat ja tunnistaakseen niistä ne, joita pidetään mahdollisesti ilmailun turvallisuuteen vaikuttavina tietoturvapoikkeamina,

c) reagoidakseen näihin tietoturvapoikkeamiin ja palautuakseen niistä.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan seuraaviin organisaatioihin:

a) asetuksen (EU) N:o 1321/2014 liitteen II (145 osa) osaston A soveltamisalaan kuuluvat huolto-organisaatiot, lukuun ottamatta niitä, jotka osallistuvat yksinomaan asetuksen (EU) N:o 1321/2014 liitteen Vb (ML osa) mukaiseen ilma-alusten huoltoon;

b) asetuksen (EU) N:o 1321/2014 liitteen Vc (CAMO osa) osaston A soveltamisalaan kuuluvat jatkuvan lentokelpoisuuden hallintaorganisaatiot, lukuun ottamatta niitä, jotka osallistuvat yksinomaan asetuksen (EU) N:o 1321/2014 liitteen Vb (ML osa) mukaiseen ilma-alusten jatkuvan lentokelpoisuuden hallintaan;

c) asetuksen (EU) N:o 965/2012 liitteen III (osa ORO) soveltamisalaan kuuluvat lentotoiminnan harjoittajat, lukuun ottamatta niitä, jotka osallistuvat yksinomaan seuraavien ilma-alusten käyttöön lentotoiminnassa:

   i) ELA2-ilma-alukset, sellaisena kuin ne määritellään asetuksen (EU) N:o 748/2012 1 artiklan 2 kohdan j alakohdassa;

   ii) yksimoottoriset potkurikäyttöiset lentokoneet, joiden suurin käytettävä matkustajapaikkaluku on enintään 5 ja joita ei luokitella vaativiksi moottorikäyttöisiksi ilma-aluksiksi, kun ne lähtevät samalta lento- tai toimintapaikalta ja laskeutuvat samalle lento- tai toimintapaikalle ja harjoittavat näkölentosääntöjen (VFR) mukaista lentotoimintaa päivällä;

   iii) yksimoottoriset helikopterit, joiden suurin käytettävä matkustajapaikkaluku on enintään 5 ja joita ei ole luokiteltu vaativiksi moottorikäyttöisiksi ilma-aluksiksi, kun ne lähtevät samalta lento- tai toimintapaikalta ja laskeutuvat samalle lento- tai toimintapaikalle ja harjoittavat näkölentosääntöjen (VFR) mukaista lentotoimintaa päivällä.

d) asetuksen (EU) N:o 1178/2011 liitteen VII (osa ORA) soveltamisalaan kuuluvat hyväksytyt koulutusorganisaatiot, lukuun ottamatta niitä, jotka osallistuvat koulutustoimintaan yksinomaan asetuksen (EU) N:o 748/2012 1 artiklan 2 kohdan j alakohdassa määritellyillä ELA2-ilma-aluksilla tai yksinomaan teoriakoulutukseen;

e) lentomiehistön ilmailulääketieteen keskukset, joihin sovelletaan asetuksen (EU) N:o 1178/2011 liitettä VII (osa ORA);

f) asetuksen (EU) N:o 1178/2011 liitteen VII (osa ORA) soveltamisalaan kuuluvat lentoa simuloivien koulutuslaitteiden (FSTD) käyttäjät, lukuun ottamatta niitä, jotka osallistuvat FSTD-laitteiden käyttöön yksinomaan asetuksen (EU) N:o 748/2012 1 artiklan 2 kohdan j alakohdassa määriteltyjen ELA2-ilma-alusten osalta;

g) asetuksen (EU) 2015/340 liitteen III (osa ATCO.OR) soveltamisalaan kuuluvat lennonjohtajien koulutusorganisaatiot ja lennonjohtajien ilmailulääketieteen keskukset;

h) organisaatiot, joihin sovelletaan täytäntöönpanoasetuksen (EU) 2017/373 liitettä III (osa ATM/ANS.OR), lukuun ottamatta seuraavia palveluntarjoajia:

i) lennonvarmistuspalvelun tarjoajat, joilla on mainitussa liitteessä olevan ATM/ANS.OR.A.010 kohdan mukainen rajoitettu hyväksyntätodistus;

ii) lentotiedotuspalvelun tarjoajat, jotka antavat toiminnastaan mainitussa liitteessä olevan ATM/ANS.OR.A.015 kohdan mukaisen ilmoituksen;

i) U-space-palveluntarjoajat ja yksinoikeudella toimivat yhteisen tietopalvelun tarjoajat, joihin sovelletaan täytäntöönpanoasetusta (EU) 2021/664.

2. Tätä asetusta sovelletaan tämän asetuksen 6 artiklassa ja komission delegoidun asetuksen (EU) 2022/1645 ([14]) 5 artiklassa tarkoitettuihin toimivaltaisiin viranomaisiin sekä Euroopan unionin lentoturvallisuusvirastoon, jäljempänä 'virasto'.

3. Tätä asetusta sovelletaan myös siihen toimivaltaiseen viranomaiseen, joka vastaa asetuksen (EU) N:o 1321/2014 liitteen III (66 osa) mukaisten ilma-aluksen huoltohenkilöstön lupakirjojen myöntämisestä, voimassaolon jatkamisesta, muuttamisesta, keskeyttämisestä tai peruuttamisesta.

4. Tämä asetus ei vaikuta täytäntöönpanoasetuksen (EU) 2015/1998 liitteessä olevassa 1.7 kohdassa eikä direktiivin (EU) 2016/1148 14 artiklassa vahvistettuihin tietoturva- ja kyberturvallisuusvaatimuksiin.

3 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) 'tietoturvalla' verkko- ja tietojärjestelmien luottamuksellisuuden, eheyden, aitouden ja käytettävyyden säilyttämistä;

2) 'tietoturvatapahtumalla' järjestelmän, palvelun tai verkkotilan tunnistettua poikkeamaa, joka viittaa tietoturvapolitiikan mahdolliseen rikkomiseen tai tietoturvan valvontatoimien laiminlyöntiin taikka aiemmin tuntemattomaan tilanteeseen, jolla voi olla merkitystä tietoturvan kannalta;

3) 'poikkeamalla' mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti direktiivin (EU) 2016/1148 4 artiklan 7 kohdassa määriteltyyn verkko- ja tietojärjestelmien turvallisuuteen;

4) 'tietoturvariskillä' tietoturvatapahtuman mahdollisuudesta organisaation siviili-ilmailutoiminnalle, omaisuudelle, yksityishenkilöille tai muille organisaatioille aiheutuvaa riskiä. Tietoturvariskeihin liittyy mahdollisuus, että uhkissa hyödynnetään tieto-omaisuuden tai tieto-omaisuusryhmän haavoittuvuuksia;

([14]) Komission delegoitu asetus (EU) 2022/1645, annettu 14 päivänä heinäkuuta 2022, Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1139 soveltamista koskevista säännöistä siltä osin kuin on kyse ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien hallintaa koskevista vaatimuksista komission asetusten (EU) N:o 748/2012 ja (EU) N:o 139/2014 soveltamisalaan kuuluville organisaatioille sekä komission asetusten (EU) N:o 748/2012 ja (EU) N:o 139/2014 muuttamisesta (EUVL L 248, 26.9.2022, s. 18).

5) 'uhkalla' tietoturvaloukkauksen mahdollisuutta, joka on olemassa, kun on yhteisö, olosuhde, toimi tai tapahtuma, joka voisi aiheuttaa vahinkoa;

6) 'haavoittuvuudella' sellaista omaisuuden tai järjestelmän, menetelmien, suunnittelun, toteutuksen tai tietoturvatoimenpiteiden vikaa tai heikkoutta, jota voitaisiin hyödyntää ja joka johtaisi tietoturvapolitiikan rikkomiseen tai loukkaamiseen.

4 artikla

Organisaatioita ja toimivaltaisia viranomaisia koskevat vaatimukset

1. Edellä 2 artiklan 1 kohdassa tarkoitettujen organisaatioiden on täytettävä tämän asetuksen liitteen II (osa IS.I.OR) vaatimukset.

2. Edellä 2 artiklan 2 ja 3 kohdassa tarkoitettujen toimivaltaisten viranomaisten on täytettävä tämän asetuksen liitteen I (osa IS.AR) vaatimukset.

5 artikla

Muusta unionin lainsäädännöstä johtuvat vaatimukset

1. Jos 2 artiklan 1 kohdassa tarkoitettu organisaatio täyttää direktiivin (EU) 2016/1148 14 artiklan mukaisesti säädetyt turvavaatimukset, jotka vastaavat tässä asetuksessa säädettyjä vaatimuksia, kyseisten turvavaatimusten täyttäminen katsotaan tässä asetuksessa säädettyjen vaatimusten täyttämiseksi.

2. Jos 2 artiklan 1 kohdassa tarkoitettu organisaatio on Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 ([15]) 10 artiklan mukaisesti vahvistetuissa jäsenvaltioiden kansallisissa siviili-ilmailun turvaohjelmissa tarkoitettu lentotoiminnan harjoittaja tai yhteisö, täytäntöönpanoasetuksen (EU) 2015/1998 liitteessä olevaan 1.7 kohtaan sisältyvien kyberturvallisuusvaatimusten katsotaan vastaavan tässä asetuksessa säädettyjä vaatimuksia, lukuun ottamatta tämän asetuksen liitteessä II olevaa IS.I.OR.230 kohtaa, jota on noudatettava sellaisenaan.

3. Jos 2 artiklan 1 kohdassa tarkoitettu organisaatio on asetuksessa (EU) 2021/696 tarkoitetun Euroopan geostationaarisen navigointilisäjärjestelmän (EGNOS) lennonvarmistuspalvelun tarjoaja, mainitun asetuksen V osaston 33–43 artiklaan sisältyvien turvavaatimusten katsotaan vastaavan tässä asetuksessa säädettyjä vaatimuksia, lukuun ottamatta tämän asetuksen liitteessä II olevaa IS.I.OR.230 kohtaa, jota on noudatettava sellaisenaan.

4. Komissio voi virastoa ja direktiivin (EU) 2016/1148 11 artiklassa tarkoitettua yhteistyöryhmää kuultuaan antaa ohjeita tässä asetuksessa ja direktiivissä (EU) 2016/1148 säädettyjen vaatimusten vastaavuuden arvioimista varten.

6 artikla

Toimivaltainen viranomainen

1. Rajoittamatta asetuksen (EU) 2021/696 36 artiklassa tarkoitettuja turvallisuusjärjestelyjen hyväksyntälautakunnalle annettuja tehtäviä, tämän asetuksen noudattamisen todentamisesta ja valvonnasta vastaava viranomainen on

a) 2 artiklan 1 kohdan a alakohdassa tarkoitettujen organisaatioiden osalta asetuksen (EU) N:o 1321/2014 liitteen II (145 osa) mukaisesti nimetty toimivaltainen viranomainen;

b) 2 artiklan 1 kohdan b alakohdassa tarkoitettujen organisaatioiden osalta asetuksen (EU) N:o 1321/2014 liitteen Vc (CAMO osa) mukaisesti nimetty toimivaltainen viranomainen;

([15]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 300/2008, annettu 11 päivänä maaliskuuta 2008, yhteisistä siviili-ilmailun turvaamista koskevista säännöistä ja asetuksen (EY) N:o 2320/2002 kumoamisesta (EUVL L 97, 9.4.2008, s. 72).

c) 2 artiklan 1 kohdan c alakohdassa tarkoitettujen organisaatioiden osalta asetuksen (EU) N:o 965/2012 liitteen III (osa ORO) mukaisesti nimetty toimivaltainen viranomainen;

d) 2 artiklan 1 kohdan d–f alakohdassa tarkoitettujen organisaatioiden osalta asetuksen (EU) N:o 1178/2011 liitteen VII (osa ORA) mukaisesti nimetty toimivaltainen viranomainen;

e) 2 artiklan 1 kohdan g alakohdassa tarkoitettujen organisaatioiden osalta asetuksen (EU) 2015/340 6 artiklan 2 kohdan mukaisesti nimetty toimivaltainen viranomainen;

f) 2 artiklan 1 kohdan h alakohdassa tarkoitettujen organisaatioiden osalta täytäntöönpanoasetuksen (EU) 2017/373 4 artiklan 1 kohdan mukaisesti nimetty toimivaltainen viranomainen;

g) 2 artiklan 1 kohdan i alakohdassa tarkoitettujen organisaatioiden osalta tapauksen mukaan täytäntöönpanoasetuksen (EU) 2021/664 14 artiklan 1 tai 2 kohdan mukaisesti nimetty toimivaltainen viranomainen.

2. Jäsenvaltiot voivat tämän asetuksen soveltamiseksi nimetä riippumattoman ja itsenäisen yksikön hoitamaan 1 kohdassa tarkoitetut toimivaltaisten viranomaisten tehtävät ja velvollisuudet. Tällöin on otettava käyttöön koordinointitoimenpiteitä kyseisen yksikön ja 1 kohdassa tarkoitettujen toimivaltaisten viranomaisten välillä sen varmistamiseksi, että kaikkia vaatimuksia, jotka organisaation on täytettävä, valvotaan tehokkaasti.

3. Virasto tekee yhteistyötä Euroopan unionin avaruusohjelmaviraston (EUSPA) ja asetuksen (EU) 2021/696 36 artiklassa tarkoitetun turvallisuusjärjestelyjen hyväksyntäviranomaisen kanssa noudattaen kaikilta osin salassapitovelvollisuutta, henkilötietojen suojaa ja turvallisuusluokiteltujen tietojen suojaa koskevia sääntöjä varmistaakseen EGNOS-lennonvarmistuspalvelun tarjoajaan sovellettavien vaatimusten tehokkaan valvonnan.

7 artikla

Merkityksellisten tietojen toimittaminen verkko- ja tietoturvasta vastaavalle toimivaltaiselle viranomaiselle

Niiden viranomaisten, jotka tämän asetuksen mukaan ovat toimivaltaisia, on ilman aiheetonta viivytystä annettava direktiivin (EU) 2016/1148 8 artiklan mukaisesti nimetylle keskitetylle yhteyspisteelle kaikki merkitykselliset tiedot, jotka sisältyvät direktiivin (EU) 2016/1148 5 artiklan mukaisesti määritettyjen keskeisten palvelujen tarjoajien tämän asetuksen liitteessä II olevan IS.I.OR.230 kohdan ja delegoidun asetuksen 2022/1645 liitteessä I olevan IS.D.OR.230 kohdan mukaisesti toimittamiin ilmoituksiin.

8 artikla

Asetuksen (EU) N:o 1178/2011 muuttaminen

Muutetaan asetuksen (EU) N:o 1178/2011 liitteet VI (osa ARA) ja VII (osa ORA) tämän asetuksen liitteen III mukaisesti.

9 artikla

Asetuksen (EU) N:o 748/2012 muuttaminen

Muutetaan asetuksen (EU) N:o 748/2012 liite I (21 osa) tämän asetuksen liitteen IV mukaisesti.

10 artikla

Asetuksen (EU) N:o 965/2012 muuttaminen

Muutetaan asetuksen (EU) N:o 965/2012 liitteet II (osa ARO) ja III (osa ORO) tämän asetuksen liitteen V mukaisesti.

11 artikla

Asetuksen (EU) N:o 139/2014 muuttaminen

Muutetaan asetuksen (EU) N:o 139/2014 liite II (osa ADR.AR) tämän asetuksen liitteen VI mukaisesti.

12 artikla

Asetuksen (EU) N:o 1321/2014 muuttaminen

Muutetaan asetuksen (EU) N:o 1321/2014 liitteet II (145 osa), III (66 osa) ja Vc (CAMO osa) tämän asetuksen liitteen VII mukaisesti.

13 artikla

Asetuksen (EU) 2015/340 muuttaminen

Muutetaan asetuksen (EU) 2015/340 liitteet II (osa ATCO.AR) ja III (osa ATCO.OR) tämän asetuksen liitteen VIII mukaisesti.

14 artikla

Täytäntöönpanoasetuksen (EU) 2017/373 muuttaminen

Muutetaan täytäntöönpanoasetuksen (EU) 2017/373 liitteet II (osa ATM/ANS.AR) ja III (osa ATM/ANS.OR) tämän asetuksen liitteen IX mukaisesti.

15 artikla

Täytäntöönpanoasetuksen (EU) 2021/664 muuttaminen

Muutetaan täytäntöönpanoasetus (EU) 2021/664 seuraavasti:

1) Korvataan 15 artiklan 1 kohdan f alakohta seuraavasti:

”f) ottavansa käyttöön täytäntöönpanoasetuksen (EU) 2017/373 liitteessä III olevassa osastossa D olevan ATM/ANS.OR.D.010 kohdan mukaisen turvatoimien hallintajärjestelmän sekä täytäntöönpanoasetuksen (EU) 2023/203 liitteen II (osa IS.I.OR) mukaisen tietoturvan hallintajärjestelmän ja pitävänsä niitä yllä.”

2) Lisätään 18 artiklaan l alakohta seuraavasti:

”l) perustettava ja toteutettava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen tietoturvan hallintajärjestelmä sekä pidettävä sitä yllä.”

16 artikla

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Sitä sovelletaan 22 päivästä helmikuuta 2026.

Täytäntöönpanoasetuksen (EU) 2017/373 soveltamisalaan kuuluvan EGNOS-lennonvarmistuspalvelun tarjoajan osalta sitä sovelletaan kuitenkin 1 päivästä tammikuuta 2026.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 27 päivänä lokakuuta 2022.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

TIETOTURVA – VIRANOMAISIA KOSKEVAT VAATIMUKSET

[OSA IS.AR]

IS.AR.100 Soveltamisala

IS.AR.200 Tietoturvan hallinnan käsikirja (ISMS)

IS.AR.205 Tietoturvariskien arviointi

IS.AR.210 Tietoturvariskien käsittely

IS.AR.215 Tietoturvapoikkeamat – havaitseminen, reagointi ja palautuminen

IS.AR.220 Tietoturvan hallinnan teettäminen alihankintana

IS.AR.225 Henkilöstövaatimukset

IS.AR.230 Tietojen tallentaminen

IS.AR.235 Jatkuva parantaminen

IS.AR.100 Soveltamisala

Tässä osassa vahvistetaan hallintaa koskevat vaatimukset, jotka tämän asetuksen 2 artiklan 2 kohdassa tarkoitettujen toimivaltaisten viranomaisten on täytettävä.

Vaatimukset, jotka kyseisten toimivaltaisten viranomaisten on täytettävä sertifiointi-, valvonta- ja vaatimustenmukaisuuden varmistamistoimiensa suorittamiseksi, sisältyvät tämän asetuksen 2 artiklan 1 kohdassa ja delegoidun asetuksen (EU) 2022/1645 2 artiklassa tarkoitettuihin asetuksiin.

IS.AR.200 Tietoturvan hallinnan käsikirja (ISMS)

a) Toimivaltaisen viranomaisen on 1 artiklassa vahvistettujen tavoitteiden saavuttamiseksi perustettava, otettava käyttöön ja ylläpidettävä tietoturvan hallintajärjestelmä (ISMS), jolla varmistetaan, että toimivaltainen viranomainen

   1) laatii tietoturvapolitiikan, jossa vahvistetaan tietoturvariskejä koskevat toimivaltaisen viranomaisen yleiset periaatteet ilmailun turvallisuuteen mahdollisesti kohdistuvien vaikutusten osalta;

   2) tunnistaa tietoturvariskit ja tarkastelee niitä IS.AR.205 kohdan mukaisesti;

   3) määrittelee ja ottaa käyttöön IS.AR.210 kohdan mukaiset tietoturvariskien käsittelytoimenpiteet;

   4) määrittelee ja ottaa käyttöön tarvittavat toimenpiteet tietoturvatapahtumien havaitsemiseksi IS.AR.215 kohdan mukaisesti ja tunnistaa ne tapahtumat, joita pidetään sellaisina vaaratilanteina, joilla saattaa olla vaikutusta ilmailun turvallisuuteen, sekä reagoi kyseisiin tietoturvapoikkeamiin ja palautuu niistä;

   5) täyttää IS.AR.220 kohdan vaatimukset, jos jokin osa IS.AR.200 kohdassa kuvatusta toiminnasta teetetään alihankintana muilla organisaatioilla;

   6) täyttää IS.AR.225 kohdassa olevat henkilöstövaatimukset;

   7) täyttää IS.AR.230 kohdassa olevat tietojen tallentamista koskevat vaatimukset;

   8) valvoo, että sen oma organisaatio täyttää tämän asetuksen vaatimukset, ja antaa IS.AR.225 kohdan a alakohdassa tarkoitetulle henkilölle palautetta havainnoista korjaavien toimien tehokkaan täytäntöönpanon varmistamiseksi;

9) suojaa kaikkien sellaisten tietojen luottamuksellisuuden, joita toimivaltaisella viranomaisella mahdollisesti on sen valvonnan piiriin kuuluvista organisaatioista, sekä tämän asetuksen liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan ja delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti perustettujen organisaation ulkoisten ilmoitusjärjestelmien kautta saatujen tietojen luottamuksellisuuden;

10) ilmoittaa virastolle muutoksista, jotka vaikuttavat toimivaltaisen viranomaisen valmiuteen suorittaa tehtävänsä ja hoitaa tässä asetuksessa määritellyt velvollisuutensa;

11) määrittelee ja ottaa käyttöön menettelyt asiaankuuluvien tietojen jakamiseksi tarpeen mukaan, käytännöllisesti ja oikea-aikaisesti muiden toimivaltaisten viranomaisten ja virastojen sekä tämän asetuksen soveltamisalaan kuuluvien organisaatioiden avustamiseksi tehokkaiden turvariskiarviointien tekemisessä niiden toiminnasta.

b) Täyttääkseen jatkuvasti 1 artiklassa tarkoitetut vaatimukset toimivaltaisen viranomaisen on otettava käyttöön IS.AR.235 kohdan mukainen jatkuvan parantamisen prosessi.

c) Toimivaltaisen viranomaisen on dokumentoitava kaikki IS.AR.200 kohdan a alakohdan noudattamisen edellyttämät keskeiset prosessit, menettelyt, tehtävät ja vastuut sekä otettava käyttöön prosessi dokumentoinnin muuttamiseksi.

d) Niiden prosessien, menettelyjen, tehtävien ja vastuiden, jotka toimivaltainen viranomainen on laatinut IS.AR.200 kohdan a alakohdan noudattamiseksi, on kyseiseen toimintaan liittyvien tietoturvariskien arvioinnin perusteella vastattava organisaation toiminnan luonnetta ja vaativuutta, ja ne voidaan sisällyttää muihin olemassa oleviin hallintajärjestelmiin, jotka toimivaltainen viranomainen on jo ottanut käyttöön.

IS.AR.205 Tietoturvariskien arviointi

a) Toimivaltaisen viranomaisen on tunnistettava kaikki ne osa-alueet omassa organisaatiossaan, jotka voivat altistua tietoturvariskeille. Näihin kuuluvat

1) toimivaltaisen viranomaisen toiminta, tilat ja resurssit sekä ne palvelut, joita toimivaltainen viranomainen käyttää, tarjoaa, vastaanottaa tai ylläpitää;

2) edellä 1 kohdassa tarkoitettujen osa-alueiden toiminnassa käytettävät laitteet, järjestelmät, data ja tiedot.

b) Toimivaltaisen viranomaisen on tunnistettava ne rajapinnat, joita sen omalla organisaatiolla on muiden organisaatioiden kanssa ja jotka voivat johtaa keskinäiseen altistumiseen tietoturvariskeille.

c) Toimivaltaisen viranomaisen on tunnistettava a ja b alakohdassa tarkoitettujen osa-alueiden ja rajapintojen osalta tietoturvariskit, joilla saattaa olla vaikutusta ilmailun turvallisuuteen.

Toimivaltaisen viranomaisen on kunkin tunnistetun riskin osalta

1) määritettävä riskitaso toimivaltaisen viranomaisen ennalta määrittelemän luokituksen mukaan;

2) yhdistettävä kukin riski ja sen taso a ja b alakohdan mukaisesti tunnistettuun vastaavaan osa-alueeseen tai rajapintaan.

Edellä 1 kohdassa tarkoitetussa ennalta määritellyssä luokituksessa on otettava huomioon uhkaskenaarion toteutumismahdollisuus ja sen turvallisuusvaikutusten merkittävyys. Tämän luokituksen avulla ja ottaen huomioon, onko toimivaltaisella viranomaisella jäsennelty ja toistettavissa oleva toiminnan riskienhallintaprosessi, toimivaltaisen viranomaisen on pystyttävä määrittämään, onko riski hyväksyttävä vai onko sitä tarpeen käsitellä IS.AR.210 kohdan mukaisesti.

Riskiarvioiden keskinäisen vertailtavuuden helpottamiseksi 1 kohdan mukaisessa riskitason määrittämisessä on otettava koordinoidusti huomioon asiaankuuluvat tiedot, jotka on saatu b alakohdassa tarkoitettujen organisaatioiden kanssa.

d) Toimivaltaisen viranomaisen on tarkasteltava uudelleen ja päivitettävä a, b ja c alakohdan mukaisesti tehtyä riskinarviointia seuraavissa tilanteissa:

1) tietoturvariskien kohteena olevissa osa-alueissa on tehty muutoksia;

2) toimivaltaisen viranomaisen organisaation ja muiden organisaatioiden väliset rajapinnat tai muiden organisaatioiden ilmoittamat riskit ovat muuttuneet;

3) riskien tunnistamiseen, analysointiin ja luokitteluun käytetyt tiedot tai tietämys ovat muuttuneet;

4) tietoturvapoikkeamien analysoinnista on saatu uutta tietoa.

IS.AR.210 Tietoturvariskien käsittely

a) Toimivaltaisen viranomaisen on laadittava toimenpiteet IS.AR.205 kohdan mukaisesti tunnistettujen ei-hyväksyttävien riskien torjumiseksi, otettava ne käyttöön kohtuullisessa ajassa ja tarkistettava, että toimenpiteet säilyvät jatkuvasti tehokkaina. Näiden toimenpiteiden on mahdollistettava se, että toimivaltainen viranomainen

1) valvoo olosuhteita, jotka vaikuttavat uhkaskenaarion tosiasialliseen toteutumiseen;

2) vähentää uhkaskenaarion toteutumisesta ilmailun turvallisuudelle aiheutuvia seurauksia;

3) välttää riskit.

Toimenpiteet eivät saa aiheuttaa ilmailun turvallisuuteen mahdollisesti kohdistuvia uusia riskejä, joita ei voida hyväksyä.

b) IS.AR.225 kohdan a alakohdassa tarkoitetulle henkilölle ja muulle toimivaltaisen viranomaisen henkilöstölle, jota asia koskee, on annettava tieto IS.AR.205 kohdan mukaisesti tehdyn riskinarvioinnin tuloksista, vastaavista uhkaskenaarioista ja käyttöön otettavista toimenpiteistä.

Toimivaltaisen viranomaisen on myös annettava tieto kaikista toimivaltaisen viranomaisen ja organisaation yhteisistä riskeistä niille organisaatioille, joiden kanssa sillä on IS.AR.205 kohdan b alakohdan mukainen rajapinta.

IS.AR.215 Tietoturvapoikkeamat – havaitseminen, reagointi ja palautuminen

a) Toimivaltaisen viranomaisen on IS.AR.205 kohdan mukaisesti tehdyn riskinarvioinnin tulosten ja IS.AR.210 kohdan mukaisesti suoritetun riskien käsittelyn tulosten perusteella otettava käyttöön toimenpiteitä sellaisten tapahtumien havaitsemiseksi, jotka osoittavat ei-hyväksyttävien riskien toteutumismahdollisuutta ja joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Näiden havaitsemistoimenpiteiden on mahdollistettava se, että toimivaltainen viranomainen

1) tunnistaa poikkeamat ennalta määritetyistä toiminnallisen suorituskyvyn perustasoista;

2) antaa varoitukset asianmukaisten vastatoimien aktivoimiseksi, jos poikkeamia ilmenee.

b) Toimivaltaisen viranomaisen on otettava käyttöön toimenpiteet reagoidakseen kaikkiin a alakohdan mukaisesti tunnistettuihin tilanteisiin, jotka saattavat kehittyä tietoturvapoikkeamaksi tai joista on kehittynyt tietoturvapoikkeama. Näiden vastatoimenpiteiden on mahdollistettava se, että toimivaltainen viranomainen

1) reagoi omassa organisaatiossaan a alakohdan 2 alakohdassa tarkoitettuihin varoituksiin aktivoimalla ennalta määritellyt resurssit ja toimet;

2) estää hyökkäyksen leviämisen ja välttää uhkaskenaarion täysimääräisen toteutumisen;

3) hallitsee IS.AR.205 kohdan a alakohdassa määriteltyjen, kohteena olevien osa-alueiden vikatilaa.

c) Toimivaltaisen viranomaisen on otettava käyttöön tietoturvapoikkeamista palautumiseen tähtäävät toimenpiteet ja tarvittaessa myös hätätoimenpiteet. Näiden palautumistoimenpiteiden on mahdollistettava se, että toimivaltainen viranomainen

1) poistaa poikkeaman aiheuttaneen tilanteen tai rajoittaa sen siedettävälle tasolle;

2) saattaa IS.AR.205 kohdan a alakohdassa määritellyt kohteena olevat osa-alueet turvalliseen tilaan organisaationsa ennalta määrittämässä palautumisajassa.

IS.AR.220 Tietoturvan hallinnan teettäminen alihankintana

Teetettäessä osa IS.AR.200 kohdassa tarkoitetusta toiminnasta alihankintana muilla organisaatioilla toimivaltaisen viranomaisen on varmistettava, että alihankintana teetettävä toiminta on tämän asetuksen mukaista ja että alihankkijaorganisaatio työskentelee sen valvonnassa. Toimivaltaisen viranomaisen on varmistettava, että alihankintana teetettävään toimintaan liittyviä riskejä hallitaan asianmukaisesti.

IS.AR.225 Henkilöstövaatimukset

Toimivaltaisella viranomaisella on

a) oltava henkilö, jolla on valtuudet laatia ja ylläpitää tämän asetuksen täytäntöönpanon edellyttämät organisaatiorakenteet, toimintaperiaatteet, prosessit ja menettelyt.

Tällä henkilöllä on

1) oltava valtuudet käyttää täysimääräisesti resursseja, joita toimivaltainen viranomainen tarvitsee suorittaakseen kaikki tässä asetuksessa edellytetyt tehtävät;

2) oltava osoitettujen tehtävien hoitamiseksi tarvittava toimivallan siirto;

b) oltava käytössään prosessi sen varmistamiseksi, että sillä on riittävästi henkilöstöä tämän liitteen soveltamisalaan kuuluvien toimien suorittamiseen;

c) oltava käytössään prosessi sen varmistamiseksi, että b alakohdassa tarkoitetulla henkilöstöllä on tarvittava pätevyys tehtäviensä suorittamiseen;

d) oltava käytössään prosessi sen varmistamiseksi, että henkilöstö tuntee sille annettuihin rooleihin ja työtehtäviin liittyvät vastuut;

e) oltava varmuus siitä, että sen henkilöstön henkilöllisyys ja luotettavuus, jolla on pääsy tämän asetuksen vaatimusten mukaisiin tietojärjestelmiin ja dataan, on osoitettu asianmukaisesti.

IS.AR.230 Tietojen tallentaminen

a) Toimivaltaisen viranomaisen on pidettävä kirjaa tietoturvan hallinnastaan.

1) Toimivaltaisen viranomaisen on varmistettava, että seuraavat tiedot arkistoidaan ja että ne ovat jäljitettävissä:

i) IS.AR.200 kohdan a alakohdan 5 alakohdan kohdassa tarkoitetun toiminnan alihankintasopimukset;

ii) tiedot IS.AR.200 kohdan d alakohdassa tarkoitetuista keskeisistä prosesseista;

iii) tiedot IS.AR.205 kohdassa tarkoitetussa riskinarvioinnissa tunnistetuista riskeistä ja niihin liittyvistä IS.AR.210 kohdassa tarkoitetuista riskien käsittelytoimenpiteistä;

iv) tiedot tietoturvatapahtumista, joita saattaa olla tarpeen arvioida uudelleen havaitsemattomien tietoturvaan liittyvien poikkeamien tai haavoittuvuuksien paljastamiseksi.

2) Edellä 1 alakohdan i alakohdassa tarkoitetut tiedot on säilytettävä vähintään viiden vuoden ajan sopimuksen muuttamisesta tai irtisanomisesta.

3) Edellä 1 alakohdan ii ja iii alakohdassa tarkoitetut tiedot on säilytettävä vähintään viiden vuoden ajan.

4) Edellä 1 alakohdan iv alakohdassa tarkoitetut tiedot on säilytettävä, kunnes kyseiset tietoturvatapahtumat on arvioitu uudelleen toimivaltaisen viranomaisen laatimassa menettelyssä määritetyin väliajoin.

b) Toimivaltaisen viranomaisen on pidettävä kirjaa tietoturvan hallintaan osallistuvan oman henkilöstönsä pätevyydestä ja kokemuksesta

1) Henkilöstön pätevyyttä ja kokemusta koskevat tiedot on säilytettävä niin kauan kuin henkilö työskentelee toimivaltaisessa viranomaisessa ja vähintään kolme vuotta sen jälkeen, kun henkilö on jättänyt toimivaltaisen viranomaisen.

2) Henkilöstön jäsenille on heidän pyynnöstään annettava pääsy heidän henkilökohtaisiin asiakirjoihinsa. Lisäksi toimivaltaisen viranomaisen on pyynnöstä toimitettava heille jäljennös heidän henkilökohtaisista tiedoistaan, kun he jättävät toimivaltaisen viranomaisen.

c) Tietojen tallennusmuoto on määritettävä toimivaltaisen viranomaisen menettelyissä.

d) Tiedot on säilytettävä tavalla, joka varmistaa niiden suojaamisen vioittumiselta, muuttamiselta ja varkaudelta, ja niin, että tiedot tunnistetaan vaadittaessa niiden turvallisuusluokituksen mukaan. Toimivaltaisen viranomaisen on varmistettava, että tiedot säilytetään tavalla, joka varmistaa niiden eheyden ja aitouden sekä pääsyn tietoihin vain siihen oikeutetuille.

IS.AR.235 Jatkuva parantaminen

a) Toimivaltaisen viranomaisen on arvioitava oman tietoturvan hallintajärjestelmänsä tehokkuutta ja kypsyyttä käyttäen asianmukaisia suorituskykyindikaattoreita. Arviointi on tehtävä toimivaltaisen viranomaisen ennalta määrittelemän kalenterin mukaan tai tietoturvapoikkeaman jälkeen.

b) Jos a alakohdan mukaisesti tehdyn arvioinnin perusteella havaitaan puutteita, toimivaltaisen viranomaisen on toteutettava tarvittavat parannustoimenpiteet sen varmistamiseksi, että tietoturvan hallintajärjestelmä täyttää edelleen sovellettavat vaatimukset ja pitää tietoturvariskit hyväksyttävällä tasolla. Lisäksi toimivaltaisen viranomaisen on arvioitava uudelleen ne tietoturvan hallintajärjestelmän osa-alueet, joihin hyväksytyt toimenpiteet vaikuttavat.

LIITE II

TIETOTURVA – ORGANISAATIOITA KOSKEVAT VAATIMUKSET

[OSA IS.I.OR]

IS.I.OR.100 Soveltamisala

IS.I.OR.200 Tietoturvan hallinnan käsikirja (ISMS)

IS.I.OR.205 Tietoturvariskien arviointi

IS.I.OR.210 Tietoturvariskien käsittely

IS.I.OR.215 Tietoturvaa koskeva sisäinen ilmoitusjärjestelmä

IS.I.OR.220 Tietoturvapoikkeamat – havaitseminen, reagointi ja palautuminen

IS.I.OR.225 Reagointi toimivaltaisen viranomaisen ilmoittamiin havaintoihin

IS.I.OR.230 Tietoturvaa koskeva ulkoinen ilmoitusjärjestelmä

IS.I.OR.235 Tietoturvan hallinnan teettäminen alihankintana

IS.I.OR.240 Henkilöstövaatimukset

IS.I.OR.245 Tietojen tallentaminen

IS.I.OR.250 Tietoturvan hallinnan käsikirja (ISMM)

IS.I.OR.255 Tietoturvan hallintajärjestelmän muutokset

IS.I.OR.260 Jatkuva parantaminen

IS.I.OR.100 Soveltamisala

Tässä osassa vahvistetaan vaatimukset, jotka tämän asetuksen 2 artiklan 1 kohdassa tarkoitettujen organisaatioiden on täytettävä.

IS.I.OR.200 Tietoturvan hallinnan käsikirja (ISMS)

a) Organisaation on 1 artiklassa vahvistettujen tavoitteiden saavuttamiseksi perustettava, otettava käyttöön ja ylläpidettävä tietoturvan hallintajärjestelmä (ISMS), jolla varmistetaan, että organisaatio

   1) laatii tietoturvapolitiikan, jossa vahvistetaan tietoturvariskejä koskevat organisaation yleiset periaatteet ilmailun turvallisuuteen mahdollisesti kohdistuvien vaikutusten osalta;

   2) tunnistaa tietoturvariskit ja tarkastelee niitä IS.I.OR.205 kohdan mukaisesti;

   3) määrittelee ja ottaa käyttöön IS.I.OR.210 kohdan mukaiset tietoturvariskien käsittelytoimenpiteet;

   4) ottaa käyttöön IS.I.OR.215 kohdan mukaisen tietoturvaa koskevan sisäisen ilmoitusjärjestelmän;

   5) määrittelee ja ottaa käyttöön tarvittavat toimenpiteet tietoturvatapahtumien havaitsemiseksi IS.I.OR.220 kohdan mukaisesti ja tunnistaa ne tapahtumat, joita pidetään sellaisina vaaratilanteina, joilla saattaa olla vaikutusta ilmailun turvallisuuteen, lukuun ottamatta IS.I.OR.205 kohdan e alakohdan sallimia tapauksia, sekä reagoi kyseisiin tietoturvapoikkeamiin ja palautuu niistä;

6) ottaa käyttöön toimenpiteet, joista toimivaltainen viranomainen on ilmoittanut välittömänä reaktiona sellaiseen tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen, joka vaikuttaa ilmailun turvallisuuteen;

7) toteuttaa toimivaltaisen viranomaisen ilmoittamien havaintojen korjaamiseksi asianmukaiset toimet IS.I.OR.225 kohdan mukaisesti;

8) ottaa käyttöön IS.I.OR.230 kohdan mukaisen ulkoisen ilmoitusjärjestelmän, jotta toimivaltainen viranomainen voi toteuttaa asianmukaiset toimet;

9) täyttää IS.I.OR.235 kohdan vaatimukset, jos jokin osa IS.I.OR.200 kohdassa tarkoitetusta toiminnasta teetetään alihankintana muilla organisaatioilla;

10) täyttää IS.I.OR.240 kohdassa säädetyt henkilöstövaatimukset;

11) täyttää IS.I.OR.245 kohdassa säädetyt tietojen tallentamista koskevat vaatimukset;

12) valvoo, että organisaatio täyttää tämän asetuksen vaatimukset, ja antaa vastuulliselle johtajalle palautetta havainnoista korjaavien toimien tehokkaan täytäntöönpanon varmistamiseksi;

13) suojaa muilta organisaatioilta mahdollisesti saamiensa tietojen luottamuksellisuuden tietojen turvallisuusluokan mukaan, sanotun kuitenkaan rajoittamatta sovellettavia poikkeamista ilmoittamista koskevia vaatimuksia.

b) Täyttääkseen jatkuvasti 1 artiklassa tarkoitetut vaatimukset organisaation on otettava käyttöön IS.I.OR.260 kohdan mukainen jatkuvan parantamisen prosessi.

c) Organisaation on IS.I.OR.250 kohdan mukaisesti dokumentoitava kaikki IS.I.OR.200 kohdan a alakohdan noudattamisen edellyttämät keskeiset prosessit, menettelyt, tehtävät ja vastuut sekä otettava käyttöön prosessi dokumentoinnin muuttamiseksi. Näiden prosessien, menettelyjen, tehtävien ja vastuiden muutoksia on hallittava IS.I.OR.255 kohdan mukaisesti.

d) Niiden prosessien, menettelyjen, tehtävien ja vastuiden, jotka organisaatio on laatinut IS.I.OR.200 kohdan a alakohdan noudattamiseksi, on kyseiseen toimintaan liittyvien tietoturvariskien arvioinnin perusteella vastattava organisaation toiminnan luonnetta ja vaativuutta, ja ne voidaan sisällyttää muihin olemassa oleviin hallintajärjestelmiin, jotka organisaatio on jo ottanut käyttöön.

e) Toimivaltainen viranomainen voi antaa organisaatiolle hyväksynnän, jonka mukaan sen ei tarvitse täyttää a–d alakohdassa tarkoitettuja vaatimuksia eikä IS.I.OR.205–IS.I.OR.260 kohdassa olevia asiaan liittyviä vaatimuksia, jos organisaatio osoittaa asianomaista viranomaista tyydyttävällä tavalla, että sen toiminta, tilat ja resurssit sekä ne palvelut, joita se tuottaa, tarjoaa, vastaanottaa ja ylläpitää, eivät aiheuta sellaisia tietoturvariskejä, joilla saattaa olla vaikutusta ilmailun turvallisuuteen sen itsensä tai muiden organisaatioiden osalta, sanotun kuitenkaan rajoittamatta velvoitetta täyttää asetukseen (EU) N:o 376/2014 sisältyvät ilmoitusvaatimukset ja IS.I.OR.200 kohdan a alakohdan 13 alakohdan vaatimukset. Hyväksynnän on perustuttava organisaation tai kolmannen osapuolen IS.I.OR.205 kohdan mukaisesti suorittamaan dokumentoituun tietoturvariskien arviointiin, jonka toimivaltainen viranomainen on tarkastanut ja hyväksynyt.

Toimivaltainen viranomainen tarkastelee hyväksynnän voimassaolon jatkumista sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia.

IS.I.OR.205 Tietoturvariskien arviointi

a) Organisaation on tunnistettava kaikki ne osa-alueet organisaatiossa, jotka voivat altistua tietoturvariskeille. Näihin kuuluvat muun muassa seuraavat:

1) organisaation toiminta, tilat ja resurssit sekä ne palvelut, joita organisaatio tuottaa, tarjoaa, vastaanottaa tai ylläpitää;

2) edellä 1 kohdassa lueteltujen osa-alueiden toiminnassa käytettävät laitteet, järjestelmät, data ja tiedot.

b) Organisaation on tunnistettava ne rajapinnat, joita sillä on muiden organisaatioiden kanssa ja jotka voivat johtaa keskinäiseen altistumiseen tietoturvariskeille.

c) Organisaation on tunnistettava a ja b alakohdassa tarkoitettujen osa-alueiden ja rajapintojen osalta tietoturvariskit, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Organisaation on kunkin tunnistetun riskin osalta

1) määritettävä riskitaso organisaation ennalta määrittelemän luokituksen mukaan;

2) yhdistettävä kukin riski ja sen taso a ja b alakohdan mukaisesti tunnistettuun vastaavaan osa-alueeseen tai rajapintaan.

Edellä 1 kohdassa tarkoitetussa ennalta määritellyssä luokituksessa on otettava huomioon uhkaskenaarion toteutumismahdollisuus ja sen turvallisuusvaikutusten merkittävyys. Tämän luokituksen perusteella ja ottaen huomioon, onko organisaatiolla jäsennelty ja toistettavissa oleva toiminnan riskienhallintaprosessi, organisaation on pystyttävä määrittämään, onko riski hyväksyttävä vai onko sitä tarpeen käsitellä IS.I.OR.210 kohdan mukaisesti.

Riskiarvioiden keskinäisen vertailtavuuden helpottamiseksi 1 kohdan mukaisessa riskitason määrittämisessä on otettava koordinoidusti huomioon asiaankuuluvat tiedot, jotka on saatu b alakohdassa tarkoitettujen organisaatioiden kanssa.

d) Organisaation on tarkasteltava uudelleen ja päivitettävä a, b ja tapauksen mukaan c tai e alakohdan mukaisesti tehtyä riskinarviointia seuraavissa tilanteissa:

1) tietoturvariskien kohteena olevissa osa-alueissa on tehty muutoksia;

2) organisaation ja muiden organisaatioiden väliset rajapinnat tai muiden organisaatioiden ilmoittamat riskit ovat muuttuneet;

3) riskien tunnistamiseen, analysointiin ja luokitteluun käytetyt tiedot tai tietämys ovat muuttuneet;

4) tietoturvapoikkeamien analysoinnista on saatu uutta tietoa.

e) Poiketen siitä, mitä c alakohdassa säädetään, organisaatioiden, joiden on noudatettava täytäntöönpanoasetuksen (EU) 2017/373 liitteen III (osa ATM/ANS.OR) osastoa C, on ilmailun turvallisuuteen kohdistuvien vaikutusten analyysin sijaan tehtävä ATM/ANS.OR.C.005 kohdassa vaadittu turvallisuustukiarvioinnin mukainen analyysi niiden palveluihin kohdistuvista vaikutuksista. Tämä turvallisuustukiarviointi on asetettava niiden ilmaliikennepalvelun tarjoajien saataville, joille organisaatio tarjoaa palveluja, ja kyseisten ilmaliikennepalvelun tarjoajat vastaavat ilmailun turvallisuuteen kohdistuvien vaikutusten arvioinnista.

IS.I.OR.210 Tietoturvariskien käsittely

a) Organisaation on laadittava toimenpiteet IS.I.OR.205 kohdan mukaisesti tunnistettujen ei-hyväksyttävien riskien torjumiseksi, otettava ne käyttöön ne kohtuullisessa ajassa ja tarkistettava, että toimenpiteet säilyvät jatkuvasti tehokkaina. Näiden toimenpiteiden on mahdollistettava se, että organisaatio

1) valvoo olosuhteita, jotka vaikuttavat uhkaskenaarion tosiasialliseen toteutumiseen;

2) vähentää uhkaskenaarion toteutumisesta ilmailun turvallisuudelle aiheutuvia seurauksia;

3) välttää riskit.

Toimenpiteet eivät saa aiheuttaa ilmailun turvallisuuteen mahdollisesti kohdistuvia uusia riskejä, joita ei voida hyväksyä.

b) IS.I.OR.240 kohdan a ja b alakohdassa tarkoitetulle henkilölle ja muulle organisaation henkilöstölle, jota asia koskee, on annettava tieto IS.I.OR.205 kohdan mukaisesti tehdyn riskinarvioinnin tuloksista, vastaavista uhkaskenaarioista ja käyttöön otettavista toimenpiteistä.

Organisaation on myös annettava tieto kaikista organisaatioille yhteisistä riskeistä niille organisaatioille, joiden kanssa sillä on IS.I.OR.205 kohdan b alakohdan mukainen rajapinta.

IS.I.OR.215 Tietoturvaa koskeva sisäinen ilmoitusjärjestelmä

a) Organisaation on perustettava sisäinen ilmoitusjärjestelmä, jonka avulla voidaan kerätä ja arvioida tietoturvatapahtumia, IS.I.OR.230 kohdan mukaisesti ilmoitettavat tapahtumat mukaan luettuina.

b) Tämän järjestelmän ja IS.I.OR.220 kohdassa tarkoitetun prosessin on mahdollistettava se, että organisaatio

1) tunnistaa, mitkä a alakohdan mukaisesti ilmoitetuista tapahtumista katsotaan sellaisiksi tietoturvaan liittyviksi poikkeamiksi tai haavoittuvuuksiksi, joilla saattaa olla vaikutusta ilmailun turvallisuuteen;

2) tunnistaa 1 kohdan mukaisesti tunnistettujen tietoturvaan liittyvien poikkeamien ja haavoittuvuuksien syyt ja myötävaikuttavat tekijät sekä käsittelee niitä osana IS.I.OR.205 ja IS.I.OR.220 kohdan mukaista tietoturvariskien hallintaprosessia;

3) varmistaa, että kaikki tiedossa olevat 1 kohdan mukaisesti tunnistettuja tietoturvaan liittyviä poikkeamia tai haavoittuvuuksia koskevat asiaankuuluvat tiedot arvioidaan;

4) varmistaa, että käytössä on menetelmä tietojen jakamiseen sisäisesti tarpeen mukaan.

c) Alihankkijaorganisaation, joka saattaa altistaa organisaation sellaisille tietoturvariskeille, joilla saattaa olla vaikutusta ilmailun turvallisuuteen, on ilmoitettava organisaatiolle tietoturvatapahtumista. Ilmoitukset on annettava sopimusjärjestelyissä vahvistettuja menettelyjä noudattaen, ja ne on arvioitava b alakohdan mukaisesti.

d) Organisaation on tehtävä tutkinnassa yhteistyötä muiden sellaisten organisaatioiden kanssa, joilla on merkittävä vaikutus tietoturvaan sen omassa toiminnassa.

e) Organisaatio voi yhdistää tämän ilmoitusjärjestelmän muihin ilmoitusjärjestelmiin, jotka se on jo ottanut käyttöön.

IS.I.OR.220 Tietoturvapoikkeamat – havaitseminen, reagointi ja palautuminen

a) Organisaation on IS.I.OR.205 kohdan mukaisesti tehdyn riskinarvioinnin tulosten ja IS.I.OR.210 kohdan mukaisesti suoritetun riskien käsittelyn tulosten perusteella otettava käyttöön toimenpiteitä sellaisten poikkeamien ja haavoittuvuuksien havaitsemiseksi, jotka osoittavat ei-hyväksyttävien riskien toteutumismahdollisuutta ja joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Näiden havaitsemistoimenpiteiden on mahdollistettava se, että organisaatio

1) tunnistaa poikkeamat ennalta määritetyistä toiminnallisen suorituskyvyn perustasoista;

2) antaa varoitukset asianmukaisten vastatoimien aktivoimiseksi, jos poikkeamia ilmenee.

b) Organisaation on otettava käyttöön toimenpiteet reagoidakseen kaikkiin a alakohdan mukaisesti tunnistettuihin tilanteisiin, jotka saattavat kehittyä tietoturvapoikkeamaksi tai joista on kehittynyt tietoturvapoikkeama. Näiden vastatoimien on mahdollistettava se, että organisaatio

1) reagoi a alakohdan 2 alakohdassa tarkoitettuihin varoituksiin aktivoimalla ennalta määritellyt resurssit ja toimet;

2) estää hyökkäyksen leviämisen ja välttää uhkaskenaarion täysimääräisen toteutumisen;

3) hallitsee IS.I.OR.205 kohdan a alakohdassa määriteltyjen, kohteena olevien osa-alueiden vikatilaa.

c) Organisaation on otettava käyttöön tietoturvapoikkeamasta palautumiseen tähtäävät toimenpiteet ja tarvittaessa myös hätätoimenpiteet. Näiden palautumistoimien on mahdollistettava se, että organisaatio

1) poistaa poikkeaman aiheuttaneen tilanteen tai rajoittaa sen siedettävälle tasolle;

2) saattaa IS.I.OR.205 kohdan a alakohdassa määritellyt kohteena olevat osa-alueet turvalliseen tilaan organisaation ennalta määrittelemässä palautumisajassa.

IS.I.OR.225 Reagointi toimivaltaisen viranomaisen ilmoittamiin havaintoihin

a) Saatuaan toimivaltaiselta viranomaiselta ilmoituksen havainnoista organisaation on

1) tunnistettava havaitun puutteen perussyyt ja myötävaikuttavat tekijät;

2) laadittava korjaustoimenpidesuunnitelma;

3) osoitettava toimivaltaista viranomaista tyydyttävällä tavalla, että vaatimustenvastaisuus on korjattu.

b) Edellä a alakohdassa tarkoitetut toimet on toteutettava toimivaltaisen viranomaisen kanssa sovitussa määräajassa.

IS.I.OR.230 Tietoturvaa koskeva ulkoinen ilmoitusjärjestelmä

a) Organisaation on otettava käyttöön tietoturvaa koskeva ilmoitusjärjestelmä, joka täyttää asetuksessa (EU) N:o 376/2014 sekä sen delegoiduissa säädöksissä ja täytäntöönpanosäädöksissä säädetyt vaatimukset, jos mainittua asetusta sovelletaan organisaatioon.

b) Organisaation on varmistettava, että kaikista tietoturvaan liittyvistä poikkeamista tai haavoittuvuuksista, joista saattaa aiheutua merkittävä riski ilmailun turvallisuudelle, ilmoitetaan sen toimivaltaiselle viranomaiselle, sanotun kuitenkaan rajoittamatta asetuksen (EU) N:o 376/2014 velvoitteiden soveltamista. Lisäksi:

1) jos tällainen poikkeama tai haavoittuvuus vaikuttaa ilma-alukseen tai siihen liittyvään järjestelmään tai komponenttiin, organisaation on ilmoitettava siitä myös suunnitteluhyväksynnän haltijalle;

2) jos tällainen poikkeama tai haavoittuvuus vaikuttaa organisaation käyttämään järjestelmään tai rakenneosaan, organisaation on ilmoitettava siitä järjestelmän tai rakenneosan suunnittelusta vastaavalle organisaatiolle.

c) Organisaation on raportoitava b alakohdassa tarkoitetuista tilanteista seuraavasti:

1) ilmoitus toimivaltaiselle viranomaiselle ja tarvittaessa suunnitteluhyväksynnän haltijalle taikka järjestelmän tai rakenneosan suunnittelusta vastaavalle organisaatiolle heti, kun tilanne on tullut organisaation tietoon;

2) raportti toimivaltaiselle viranomaiselle ja tarvittaessa suunnitteluhyväksynnän haltijalle taikka järjestelmän tai rakenneosan suunnittelusta vastaavalle organisaatiolle mahdollisimman pian, mutta kuitenkin enintään 72 tunnin kuluessa siitä, kun tilanne on tullut organisaation tietoon, ellei tämä poikkeuksellisten olosuhteiden vuoksi ole mahdotonta.

Raportti on laadittava toimivaltaisen viranomaisen määrittelemässä muodossa, ja sen on sisällettävä kaikki organisaation tiedossa olevat olennaiset tiedot tilanteesta;

3) seurantaraportti toimivaltaiselle viranomaiselle ja tarvittaessa suunnitteluhyväksynnän haltijalle taikka järjestelmän tai rakenneosan suunnittelusta vastaavalle organisaatiolle; seurantaraportissa yksityiskohtaiset tiedot toimista, jotka organisaatio on toteuttanut tai aikoo toteuttaa palautuakseen poikkeamasta, sekä toimista, joita se aikoo toteuttaa estääkseen vastaavat tietoturvapoikkeamat tulevaisuudessa.

Seurantaraportti on toimitettava heti, kun kyseiset toimet on yksilöity, ja se on laadittava toimivaltaisen viranomaisen määrittelemässä muodossa.

IS.I.OR.235 Tietoturvan hallinnan teettäminen alihankintana

a) Teetettäessä osa IS.I.OR.200 kohdassa tarkoitetusta toiminnasta alihankintana muilla organisaatioilla organisaation on varmistettava, että alihankintana teetettävä toiminta on tämän asetuksen mukaista ja että alihankkijaorganisaatio työskentelee sen valvonnassa. Organisaation on varmistettava, että alihankintana teetettävään toimintaan liittyviä riskejä hallitaan asianmukaisesti.

b) Organisaation on varmistettava, että toimivaltaisella viranomaisella on pyynnöstä pääsy alihankkijaorganisaatioon sen toteamiseksi, että tässä asetuksessa säädettyjä sovellettavia vaatimuksia noudatetaan edelleen.

IS.I.OR.240 Henkilöstövaatimukset

a) Tämän asetuksen 2 artiklassa tarkoitetun organisaation vastuullisella johtajalla, joka on tapauksen mukaan nimetty asetusten (EU) N:o 1321/2014, (EU) N:o 965/2012, (EU) N:o 1178/2011, (EU) 2015/340, täytäntöönpanoasetuksen (EU) 2017/373 tai täytäntöönpanoasetuksen (EU) 2021/664 mukaisesti, on oltava valtuudet varmistaa yrityksen puolesta, että kaikki tämän asetuksen edellyttämät toimet kyetään rahoittamaan ja toteuttamaan. Kyseisen henkilön on

1) varmistettava, että käytettävissä on kaikki tarvittavat resurssit tämän asetuksen vaatimusten täyttämiseksi;

2) laadittava IS.I.OR.200 kohdan a alakohdan 1 alakohdassa tarkoitettu tietoturvapolitiikka ja edistettävä sitä;

3) osoitettava, että hän ymmärtää tämän asetuksen keskeisen sisällön.

b) Vastuullisen johtajan on nimitettävä henkilö tai henkilöryhmä varmistamaan, että organisaatio noudattaa tämän asetuksen vaatimuksia, ja määriteltävä toimivaltansa laajuus. Kyseisen henkilön tai henkilöryhmän on raportoitava suoraan vastuulliselle johtajalle, ja hänellä on oltava asianmukaiset tiedot, tausta ja kokemus tehtäviensä hoitamiseen. Menetelmissä on määritettävä, kuka toimii kenenkin henkilön sijaisena pitkien poissaolojen aikana.

c) Vastuullisen johtajan on nimitettävä henkilö tai henkilöryhmä, joka vastaa IS.I.OR.200 kohdan a alakohdan 12 alakohdassa tarkoitetun vaatimustenmukaisuuden valvontatoiminnon hallinnoinnista.

d) Jos organisaatiolla on yhteiset tietoturvaa koskevat organisaatiorakenteet, periaatteet, prosessit ja menettelyt muiden organisaatioiden tai sen oman organisaation sellaisten osien kanssa, joita hyväksyntä tai ilmoitus ei kata, vastuullinen johtaja voi delegoida toimintansa yhteiselle vastuuhenkilölle.

Tällöin organisaation vastuullisen johtajan ja yhteisen vastuuhenkilön välillä on otettava käyttöön koordinointitoimenpiteet tietoturvan hallinnan asianmukaisen integroinnin varmistamiseksi organisaatiossa.

e) Vastuullisella johtajalla tai d alakohdassa tarkoitetulla yhteisellä vastuuhenkilöllä on oltava valtuudet luoda yrityksen puolesta IS.I.OR.200 kohdan täytäntöönpanemiseksi tarvittavat organisaatiorakenteet, periaatteet, prosessit ja menettelyt ja ylläpitää niitä.

f) Organisaatiolla on oltava käytössään prosessi sen varmistamiseksi, että sillä on riittävästi henkilöstöä tämän liitteen soveltamisalaan kuuluvien toimien suorittamiseen.

g) Organisaatiolla on oltava käytössään prosessi sen varmistamiseksi, että f alakohdassa tarkoitetulla henkilöstöllä on tarvittava pätevyys tehtäviensä suorittamiseen.

h) Organisaatiolla on oltava käytössään prosessi sen varmistamiseksi, että henkilöstö tuntee sille annettuihin rooleihin ja työtehtäviin liittyvät vastuut.

i) Organisaation on varmistettava, että sen henkilöstön henkilöllisyys ja luotettavuus, jolla on pääsy tämän asetuksen vaatimusten mukaisiin tietojärjestelmiin ja dataan, on osoitettu asianmukaisesti.

IS.I.OR.245 Tietojen tallentaminen

a) *Organisaation on pidettävä kirjaa tietoturvan hallinnastaan.*

1) Organisaation on varmistettava, että seuraavat tiedot arkistoidaan ja että ne ovat jäljitettävissä:

i) IS.I.OR.200 kohdan e alakohdan mukaiset mahdollisesti saadut hyväksynnät ja niihin liittyvät tietoturvariskien arvioinnit;

ii) IS.I.OR.200 kohdan a alakohdan 9 alakohdan kohdassa tarkoitetun toiminnan alihankintasopimukset;

iii) tiedot IS.I.OR.200 kohdan d alakohdassa tarkoitetuista keskeisistä prosesseista;

iv) tiedot IS.I.OR.205 kohdassa tarkoitetussa riskinarvioinnissa tunnistetuista riskeistä ja niihin liittyvistä IS.I.OR.210 kohdassa tarkoitetuista riskien käsittelytoimenpiteistä;

v) tiedot IS.I.OR.215 ja IS.I.OR.230 kohdassa tarkoitettujen ilmoitusjärjestelmien mukaisesti ilmoitetuista tietoturvaan liittyvistä poikkeamista ja haavoittuvuuksista;

vi) tiedot tietoturvatapahtumista, joita saattaa olla tarpeen arvioida uudelleen havaitsemattomien tietoturvaan liittyvien poikkeamien tai haavoittuvuuksien paljastamiseksi.

2) Edellä 1 alakohdan i alakohdassa tarkoitetut tiedot on säilytettävä vähintään viiden vuoden ajan hyväksynnän voimassaolon päättymisestä.

3) Edellä 1 alakohdan ii alakohdassa tarkoitetut tiedot on säilytettävä vähintään viiden vuoden ajan sopimuksen muuttamisesta tai irtisanomisesta.

4) Edellä 1 alakohdan iii, iv ja v alakohdassa tarkoitetut tiedot on säilytettävä vähintään viiden vuoden ajan.

5) Edellä 1 alakohdan vi alakohdassa tarkoitetut tiedot on säilytettävä, kunnes kyseiset tietoturvatapahtumat on arvioitu uudelleen organisaation laatimassa menettelyssä määritetyin väliajoin.

b) *Organisaation on pidettävä kirjaa tietoturvan hallintaan osallistuvan oman henkilöstönsä pätevyydestä ja kokemuksesta*

1) Henkilöstön pätevyyttä ja kokemusta koskevat tiedot on säilytettävä niin kauan kuin henkilö työskentelee organisaatiossa ja vähintään kolme vuotta sen jälkeen, kun henkilö on jättänyt organisaation.

2) Henkilöstön jäsenille on heidän pyynnöstään annettava pääsy heidän henkilökohtaisiin asiakirjoihinsa. Lisäksi organisaation on pyynnöstä toimitettava heille jäljennös heidän henkilökohtaisista tiedoistaan, kun he jättävät organisaation.

c) Tietojen tallennusmuoto on määritettävä organisaation menettelyissä.

d) Tiedot on säilytettävä tavalla, joka varmistaa niiden suojaamisen vioittumiselta, muuttamiselta ja varkaudelta, ja niin, että tiedot tunnistetaan vaadittaessa niiden turvallisuusluokituksen mukaan. Organisaation on varmistettava, että tiedot säilytetään tavalla, joka varmistaa niiden eheyden ja aitouden sekä pääsyn tietoihin vain siihen oikeutetuille.

IS.I.OR.250 Tietoturvan hallinnan käsikirja (ISMM)

a) Organisaation on asetettava toimivaltaisen viranomaisen saataville tietoturvan hallinnan käsikirja (ISMM) sekä tarvittaessa siihen liittyvät käsikirjat ja menettelyt, joihin viitataan ja jotka sisältävät

1) vastuullisen johtajan allekirjoittaman vakuutuksen, jossa vahvistetaan, että organisaatio toimii aina tämän liitteen ja tietoturvan hallinnan käsikirjan mukaisesti. Jos vastuullinen johtaja ei ole organisaation pääjohtaja, pääjohtajan on varmennettava vakuutus allekirjoituksellaan;

2) IS.I.OR.240 kohdan b ja c alakohdassa määritettyjen henkilöiden tehtävänimikkeet, nimet, työtehtävät, vastuuvelvollisuudet, vastuualueet ja valtuudet;

3) IS.I.OR.240 kohdan d alakohdassa määritetyn yhteisen vastuuhenkilön, jos sellainen on, tehtävänimikkeen, nimen, työtehtävät, vastuuvelvollisuudet, vastuualueet ja valtuudet;

4) IS.I.OR.200 kohdan a alakohdan 1 alakohdassa tarkoitetun organisaation tietoturvapolitiikan;

5) yleiskuvauksen henkilöstön lukumäärästä ja henkilöstöluokista sekä käytössä olevasta järjestelmästä, jolla henkilöstön käytettävyyttä suunnitellaan IS.I.OR.240 kohdan d alakohdassa vaaditun mukaisesti;

6) IS.I.OR.200 kohdan täytäntöönpanosta vastaavien keskeisten henkilöiden tehtävänimikkeet, nimet, työtehtävät, vastuuvelvollisuudet, vastuualueet ja valtuudet, mukaan lukien IS.I.OR.200 kohdan a alakohdan 12 alakohdassa tarkoitetusta vaatimustenmukaisuuden valvontatoiminnosta vastaavat henkilöt;

7) organisaatiokaavion, josta käyvät ilmi 2 ja 6 alakohdassa tarkoitettujen henkilöiden raportointi- ja vastuuketjut;

8) kuvauksen IS.I.OR.215 kohdassa tarkoitetusta sisäisestä ilmoitusjärjestelmästä;

9) menettelyt, joissa kuvataan, miten organisaatio varmistaa tämän osan noudattamisen, ja erityisesti

i) IS.I.OR.200 kohdan c alakohdassa tarkoitetun dokumentoinnin;

ii) menettelyt, joilla määritellään, miten organisaatio valvoo IS.I.OR.200 kohdan a alakohdan 9 alakohdassa tarkoitettua alihankintana teetettävää toimintaa;

iii) c alakohdassa tarkoitetun tietoturvan hallinnan käsikirjan muuttamismenettelyn;

10) yksityiskohtaiset tiedot voimassa olevista hyväksytyistä vaihtoehtoisista vaatimusten täyttämisen menetelmistä.

b) Tietoturvan hallinnan käsikirjan alkuperäiselle versiolle on saatava hyväksyntä, ja toimivaltaisen viranomaisen on säilytettävä sen jäljennös. Tietoturvan hallinnan käsikirjaa on tarvittaessa muutettava, jotta organisaation tietoturvan hallintajärjestelmän kuvaus pysyy ajantasaisena. Toimivaltaiselle viranomaiselle on toimitettava jäljennös kaikista tietoturvan hallinnan käsikirjaan tehdyistä muutoksista.

c) Tietoturvan hallinnan käsikirjaan tehtäviä muutoksia on hallittava organisaation laatimalla menettelyllä. Toimivaltaiselta viranomaiselta on saatava hyväksyntä kaikkiin muutoksiin, jotka eivät kuulu tämän menettelyn soveltamisalaan, ja kaikkiin muutoksiin, jotka liittyvät IS.I.OR.255 kohdan b alakohdassa tarkoitettuihin muutoksiin.

d) Organisaatio voi yhdistää tietoturvan hallinnan käsikirjan muihin sen laatimiin organisaation käsikirjoihin sillä edellytyksellä, että on olemassa selkeät ristiviittaukset, jotka osoittavat, mitkä organisaation käsikirjan osat vastaavat tässä liitteessä esitettyjä eri vaatimuksia.

IS.I.OR.255 Tietoturvan hallintajärjestelmän muutokset

a) Tietoturvan hallintajärjestelmän muutoksia voidaan hallita ja niistä voidaan ilmoittaa toimivaltaiselle viranomaiselle organisaation laatimalla menettelyllä. Menettelyn on oltava toimivaltaisen viranomaisen hyväksymä.

b) Sellaisten tietoturvan hallinnan käsikirjan muutosten osalta, jotka eivät kuulu a alakohdassa tarkoitetun menettelyn piiriin, organisaation on haettava ja saatava toimivaltaisen viranomaisen antama hyväksyntä.

Näiden muutosten osalta:

1) hakemus on toimitettava ennen kyseisten muutosten tekemistä, jotta toimivaltainen viranomainen voi todeta tämän asetuksen vaatimusten täyttyvän edelleen ja tarvittaessa muuttaa organisaation hyväksyntätodistusta ja sen liitteenä olevia hyväksyntäehtoja.

2) organisaation on asetettava toimivaltaisen viranomaisen saataville kaikki tiedot, joita se pyytää muutoksen arvioimiseksi;

3) muutos voidaan tehdä vasta, kun toimivaltaiselta viranomaiselta on saatu virallinen hyväksyntä;

4) organisaation on tällaisia muutoksia tehtäessä toimittava toimivaltaisen viranomaisen asettamin ehdoin.

IS.I.OR.260 Jatkuva parantaminen

a) Organisaation on arvioitava tietoturvan hallintajärjestelmän tehokkuutta ja kypsyyttä käyttäen asianmukaisia suorituskykyindikaattoreita. Arviointi on tehtävä organisaation ennalta määrittelemän kalenterin mukaan tai tietoturvapoikkeaman jälkeen.

b) Jos a alakohdan mukaisesti tehdyn arvioinnin perusteella havaitaan puutteita, organisaation on toteutettava tarvittavat parannustoimenpiteet sen varmistamiseksi, että tietoturvan hallintajärjestelmä täyttää edelleen sovellettavat vaatimukset ja pitää tietoturvariskit hyväksyttävällä tasolla. Lisäksi organisaation on arvioitava uudelleen ne tietoturvan hallintajärjestelmän osa-alueet, joihin hyväksytyt toimenpiteet vaikuttavat.

LIITE III

Muutetaan asetuksen (EU) N:o 1178/2011 liitteet VI (osa ARA) ja VII (osa ORA) seuraavasti:

1) Muutetaan liite VI (osa ARA) seuraavasti:

a) Lisätään ARA.GEN.125 kohtaan c alakohta seuraavasti:

"c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista."

b) Lisätään ARA.GEN.135 kohdan jälkeen ARA.GEN.135A kohta seuraavasti:

"**ARA.GEN.135A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki ARA.GEN.125 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee."

c) Lisätään ARA.GEN.200 kohtaan e alakohta seuraavasti:

"e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi."

d) Muutetaan ARA.GEN.205 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

"**ARA.GEN.205 Tehtävien antaminen**";

ii) Lisätään c alakohta seuraavasti:

"c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ORA.GEN.200A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma ARA.GEN.200 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät."

e) Lisätään ARA.GEN.300 kohtaan g alakohta seuraavasti:

"g) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ORA.GEN.200A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–f alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia."

f) Lisätään ARA.GEN.330 kohdan jälkeen ARA.GEN.330A kohta seuraavasti:

"**ARA.GEN.330A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa ARA.GEN.300 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava ARA.GEN.350 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos."

2) Muutetaan liite VII (osa ORA) seuraavasti:

Lisätään ORA.GEN.200 kohdan jälkeen ORA.GEN.200A kohta seuraavasti:

"**ORA.GEN.200A Tietoturvan hallintajärjestelmä**

ORA.GEN.200 kohdassa tarkoitetun hallintojärjestelmän lisäksi organisaation on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 mukainen tietoturvan hallintajärjestelmä."

LIITE IV

Muutetaan asetuksen (EU) N:o 748/2012 liite I (21 osa) seuraavasti:

1) Muutetaan sisällysluettelo seuraavasti:

a) Lisätään 21.B.20 kohdan otsikon jälkeen otsikko seuraavasti:

”21.B.20A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen”

b) Korvataan 21.B.30 kohdan otsikko seuraavasti:

”21.B.30 Tehtävien antaminen”;

c) Lisätään 21.B.240 kohdan otsikon jälkeen otsikko seuraavasti:

”21.B.240A Tietoturvan hallintajärjestelmän muutokset”

d) Lisätään 21.B.435 kohdan otsikon jälkeen otsikko seuraavasti:

”21.B.435A Tietoturvan hallintajärjestelmän muutokset”

2) Lisätään 21.B.15 kohtaan c alakohta seuraavasti:

”c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista.”

3) Lisätään 21.B.20 kohdan jälkeen 21.B.20A kohta seuraavasti:

”21.B.20A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki 21.B.15 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee.”

4) Lisätään 21.B.25 kohtaan e alakohta seuraavasti:

”e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi.”

5) Muutetaan 21.B.30 kohta seuraavasti:

a) Korvataan otsikko seuraavasti:

”21.B.30 Tehtävien antaminen”;

b) Lisätään c alakohta seuraavasti:

”c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa 21.A.139A ja 21.A.239A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma 21.B.25 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät.”

6) Lisätään 21.B.221 kohtaan g alakohta seuraavasti:

”g) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa 21.A.139A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–f alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia.”

7) Lisätään 21.B.240 kohdan jälkeen 21.B.240A kohta seuraavasti:

”**21.B.240A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa 21.B.221 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava 21.B.225 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos.”

8) Lisätään 21.B.431 kohtaan d alakohta seuraavasti:

”d) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa 21.A.239A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–c alakohdan noudattamisen lisäksi noudatettava seuraavia periaatteita:

1) toimivaltaisen viranomaisen on tarkasteltava niitä rajapintoja ja rajapintoihin liittyviä riskejä, joita sen valvomat organisaatiot ovat havainneet delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.205 kohdan b alakohdan mukaisesti;

2) jos eri organisaatioiden havaitsemissa keskinäisissä rajapinnoissa ja rajapintoihin liittyvissä riskeissä todetaan eroavuuksia, toimivaltaisen viranomaisen on tarkasteltava niitä uudelleen asianomaisten organisaatioiden kanssa ja tarvittaessa tehtävä asianmukaiset havainnot korjaavien toimien toteuttamisen varmistamiseksi;

3) jos 2 kohdan mukaisesti tarkastelluista asiakirjoista käy ilmi, että sellaisiin rajapintoihin, joissa organisaatiot ovat saman jäsenvaltion toisen toimivaltaisen viranomaisen valvonnassa, liittyy merkittäviä riskejä, asiasta on annettava tieto kyseessä olevalle toimivaltaiselle viranomaiselle.”

9) Lisätään 21.B.435 kohdan jälkeen 21.B.435A kohta seuraavasti:

”**21.B.435A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa 21.B.431 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava 21.B.433 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos.”

LIITE V

Muutetaan asetuksen (EU) N:o 965/2012 liitteet II (osa ARO) ja III (osa ORO) seuraavasti:

1) Muutetaan liite II (osa ARO) seuraavasti:

a) Lisätään ARO.GEN.125 kohtaan c alakohta seuraavasti:

"c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista."

b) Lisätään ARO.GEN.135 kohdan jälkeen ARO.GEN.135A kohta seuraavasti:

"**ARO.GEN.135A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki ARO.GEN.125 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee."

c) Lisätään ARO.GEN.200 kohtaan e alakohta seuraavasti:

"e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi."

d) Muutetaan ARO.GEN.205 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

"**ARO.GEN.205 Tehtävien antaminen**";

ii) Lisätään c alakohta seuraavasti:

"c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ORO.GEN.200A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma ARO.GEN.200 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät."

e) Lisätään ARO.GEN.300 kohtaan g alakohta seuraavasti:

"g) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ORO.GEN.200A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–f alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia."

f) Lisätään ARO.GEN.330 kohdan jälkeen ARO.GEN.330A kohta seuraavasti:

"**ARO.GEN.330A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa ARO.GEN.300 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava ARO.GEN.350 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos."

2) Muutetaan liite III (osa ORO) seuraavasti:

Lisätään ORO.GEN.200 kohdan jälkeen ORO.GEN.200A kohta seuraavasti:

"**ORO.GEN.200A Tietoturvan hallintajärjestelmä**

ORO.GEN.200 kohdassa tarkoitetun hallintojärjestelmän lisäksi lentotoiminnan harjoittajan on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 mukainen tietoturvan hallintajärjestelmä."

LIITE VI

Muutetaan asetuksen (EU) N:o 139/2014 liite II (osa ADR.AR) seuraavasti:

1) Lisätään ADR.AR.A.025 kohtaan c alakohta seuraavasti:

"c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista."

2) Lisätään ADR.AR.A.030 kohdan jälkeen ADR.AR.A.030A kohta seuraavasti:

"**ADR.AR.A.030A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki ADR.AR.A.025 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee."

3) Lisätään ADR.AR.B.005 kohtaan d alakohta seuraavasti:

"d) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi."

4) Muutetaan ADR.AR.B.010 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

"**ADR.AR.B.010 Tehtävien antaminen**";

ii) Lisätään c alakohta seuraavasti:

"c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ADR.OR.D.005A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma ADR.AR.B.005 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät."

5) Lisätään ADR.AR.C.005 kohtaan f alakohta seuraavasti:

"f) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ADR.OR.D.005A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–e alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia."

6) Lisätään ADR.AR.C.040 kohdan jälkeen ADR.AR.C.040A kohta seuraavasti:

"**ADR.AR.C.040A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa ADR.AR.C.005 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava ADR.AR.C.055 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista delegoidun asetuksen (EU) 2022/1645 liitteessä I (osa IS.D.OR) olevan IS.D.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos."

LIITE VII

Muutetaan asetuksen (EU) N:o 1321/2014 liitteet II (145 osa), III (66 osa) ja VII (CAMO osa) seuraavasti:

1) Muutetaan liite II (145 osa) seuraavasti:

a) Muutetaan sisällysluettelo seuraavasti:

i) Lisätään 145.A.200 kohdan otsikon jälkeen otsikko seuraavasti:

”145.A.200A Tietoturvan hallintajärjestelmä”;

ii) Lisätään 145.B.135 kohdan otsikon jälkeen otsikko seuraavasti:

”145.B.135A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen”

iii) Korvataan 145.B.205 kohdan otsikko seuraavasti:

”145.B.205 Tehtävien antaminen”;

iv) Lisätään 145.B.330 kohdan otsikon jälkeen otsikko seuraavasti:

”145.B.330A Tietoturvan hallintajärjestelmän muutokset”

b) Lisätään 145.A.200 kohdan jälkeen 145.A.200A kohta seuraavasti:

”145.A.200A **Tietoturvan hallintajärjestelmä**

Edellä 145.A.200 kohdassa tarkoitetun hallintojärjestelmän lisäksi huolto-organisaation on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 mukainen tietoturvan hallintajärjestelmä.”

c) Lisätään 145.B.125 kohtaan c alakohta seuraavasti:

”c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista.”

d) Lisätään 145.B.135 kohdan jälkeen 145.B.135A kohta seuraavasti:

”145.B.135A **Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki 145.B.125 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee."

e) Lisätään 145.B.200 kohtaan e alakohta seuraavasti:

"e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi."

f) Muutetaan 145.B.205 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

"145.B.205 **Tehtävien antaminen**";

ii) Lisätään c alakohta seuraavasti:

"c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa 145.A.200A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma 145.B.200 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät."

g) Lisätään 145.B.300 kohtaan g alakohta seuraavasti:

"g) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa 145.A.200A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–f alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia."

h) Lisätään 145.B.330 kohdan jälkeen 145.B.330A kohta seuraavasti:

"145.B.330A **Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa 145.B.300 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava 145.B.350 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos.”

2) Muutetaan liite III (66 osa) seuraavasti:

a) Lisätään sisällysluetteloon 66.B.10 kohdan otsikon jälkeen otsikko seuraavasti:

”66.B.15 Tietoturvan hallintajärjestelmä”;

b) Lisätään 66.B.10 kohdan jälkeen 66.B.15 kohta seuraavasti:

”66.B.15 **Tietoturvan hallintajärjestelmä**

Toimivaltaisen viranomaisen on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen tietoturvan hallintajärjestelmä.”

3) Muutetaan liite Vc (CAMO osa) seuraavasti:

a) Muutetaan sisällysluettelo seuraavasti:

i) Lisätään CAMO.A.200 kohdan otsikon jälkeen otsikko seuraavasti:

”CAMO.A.200A Tietoturvan hallintajärjestelmä”;

ii) Lisätään CAMO.B.135 kohdan otsikon jälkeen otsikko seuraavasti:

”CAMO.B.135A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen”;

iii) Korvataan CAMO.B.205 kohdan otsikko seuraavasti:

”CAMO.B.205 Tehtävien antaminen”;

iv) Lisätään CAMO.B.330 kohdan otsikon jälkeen otsikko seuraavasti:

”CAMO.B.330A Tietoturvan hallintajärjestelmän muutokset”

b) Lisätään CAMO.A.200 kohdan jälkeen CAMO.A.200A kohta seuraavasti:

”CAMO.A.200A **Tietoturvan hallintajärjestelmä**

CAMO.A.200 kohdassa tarkoitetun hallintojärjestelmän lisäksi organisaation on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 mukainen tietoturvan hallintajärjestelmä.”

c) Lisätään CAMO.B.125 kohtaan c alakohta seuraavasti:

”c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista.”

d) Lisätään CAMO.B.135 kohdan jälkeen CAMO.B.135A kohta seuraavasti:

”CAMO.B.135A **Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Viraston ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki CAMO.B.125 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee.”

e) Lisätään CAMO.B.200 kohtaan e alakohta seuraavasti:

”e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi.”

f) Muutetaan CAMO.B.205 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

”CAMO.B.205 **Tehtävien antaminen**”;

ii) Lisätään c alakohta seuraavasti:

”c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa CAMO.A.200A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma CAMO.B.200 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät."

g) Lisätään CAMO.B.300 kohtaan g alakohta seuraavasti:

"g) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa CAMO.A.200A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–f alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia."

h) Lisätään CAMO.B.330 kohdan jälkeen CAMO.B.330A kohta seuraavasti:

"CAMO.B.330A **Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa CAMO.B.300 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava CAMO.B.350 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos."

LIITE VIII

Muutetaan asetuksen (EU) 2015/340 liitteet II (osa ATCO.AR) ja III (osa ATCO.OR) seuraavasti:

1) Muutetaan liite II (osa ATCO.AR) seuraavasti:

a) Lisätään ATCO.AR.A.020 kohtaan c alakohta seuraavasti:

”c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista.”

b) Lisätään ATCO.AR.A.025 kohdan jälkeen ATCO.AR.A.025A kohta seuraavasti:

”**ATCO.AR.A.025A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki ATCO.AR.A.020 kohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee.”

c) Lisätään ATCO.AR.B.001 kohtaan e alakohta seuraavasti:

”e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi.”

d) Muutetaan ATCO.AR.B.005 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

”**ATCO.AR.B.005 Tehtävien antaminen**”;

ii) Lisätään c alakohta seuraavasti:

”c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ATCO.OR.C.001A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma ATCO.AR.B.001 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät."

e) Lisätään ATCO.AR.C.001 kohtaan f alakohta seuraavasti:

"f) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ATCO.OR.C.001A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–e alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia."

f) Lisätään ATCO.AR.E.010 kohdan jälkeen ATCO.AR.E.010A kohta seuraavasti:

"**ATCO.AR.E.010A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa ATCO.AR.C.001 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava ATCO.AR.C.010 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos."

2) Muutetaan liite III (osa ATCO.AR) seuraavasti:

Lisätään ATCO.OR.C.001 kohdan jälkeen ATCO.OR.C.001A kohta seuraavasti:

"**ATCO.OR.C.001A Tietoturvan hallintajärjestelmä**

ATCO.OR.C.001 kohdassa tarkoitetun hallintojärjestelmän lisäksi koulutusorganisaation on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 mukainen tietoturvan hallintajärjestelmä."

LIITE IX

Muutetaan täytäntöönpanoasetuksen (EU) 2017/373 liitteet II (osa ATM/ANS.AR) ja III (osa ATM/ANS.OR) seuraavasti:

1) Muutetaan liite II (osa ATM/ANS.AR) seuraavasti:

a) Lisätään ATM/ANS.AR.A.020 kohtaan c alakohta seuraavasti:

"c) Jäsenvaltion toimivaltaisen viranomaisen on mahdollisimman pian toimitettava virastolle turvallisuuden kannalta merkittävät tiedot, jotka tulevat esiin sen täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.230 kohdan mukaisesti saamista tietoturvailmoituksista."

b) Lisätään ATM/ANS.AR.A.025 kohdan jälkeen ATM/ANS.AR.A.025A kohta seuraavasti:

"**ATM/ANS.AR.A.025A Välitön reagointi ilmailun turvallisuuteen vaikuttavaan tietoturvaan liittyvään poikkeamaan tai haavoittuvuuteen**

a) Toimivaltaisen viranomaisen on otettava käyttöön järjestelmä, jolla kerätään, analysoidaan ja jaetaan asianmukaisesti tiedot, jotka koskevat niitä organisaatioiden ilmoittamia tietoturvaan liittyviä poikkeamia ja haavoittuvuuksia, joilla saattaa olla vaikutusta ilmailun turvallisuuteen. Tämä on toteutettava koordinoidusti muiden tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa vastaavien asiaankuuluvien viranomaisten kanssa ilmoitusjärjestelmien koordinoinnin ja yhteensopivuuden lisäämiseksi.

b) Virasto ottaa käyttöön järjestelmän voidakseen analysoida asianmukaisesti kaikki ATM/ANS.AR.A.020 kohdan c alakohdan mukaisesti saadut asiaankuuluvat turvallisuuden kannalta merkittävät tiedot ja toimittaa ilman aiheetonta viivytystä jäsenvaltioille ja komissiolle kaikki tiedot, mukaan lukien suositukset tai toteutettavat korjaavat toimet, jotka ovat tarpeen, jotta ne voivat reagoida oikea-aikaisesti ilmailun turvallisuuteen mahdollisesti vaikuttavaan tietoturvaan liittyvään sellaiseen poikkeamaan tai haavoittuvuuteen, jossa on mukana asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten soveltamisalaan kuuluvia tuotteita, osia, irrallisia varusteita, henkilöitä tai organisaatioita.

c) Saatuaan a ja b alakohdassa tarkoitetut tiedot toimivaltaisen viranomaisen on toteutettava asianmukaiset toimenpiteet, joilla puututaan tietoturvaan liittyvän poikkeaman tai haavoittuvuuden mahdolliseen vaikutukseen ilmailun turvallisuuteen.

d) Edellä c alakohdassa tarkoitetuista toimenpiteistä on ilmoitettava välittömästi kaikille henkilöille tai organisaatioille, joiden on asetuksen (EU) 2018/1139 ja sen delegoitujen säädösten ja täytäntöönpanosäädösten mukaan noudatettava niitä. Jäsenvaltion toimivaltaisen viranomaisen on ilmoitettava näistä toimenpiteistä myös virastolle ja, jos yhteinen toiminta on tarpeen, niiden muiden jäsenvaltioiden toimivaltaisille viranomaisille, joita asia koskee."

c) Lisätään ATM/ANS.AR.B.001 kohtaan e alakohta seuraavasti:

"e) Edellä a alakohdassa esitettyjen vaatimusten lisäksi toimivaltaisen viranomaisen perustaman ja ylläpitämän hallintojärjestelmän on oltava täytäntöönpanoasetuksen (EU) 2023/203 liitteen I (osa IS.AR) mukainen ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi."

d) Muutetaan ATM/ANS.AR.B.005 kohta seuraavasti:

i) Korvataan otsikko seuraavasti:

"**ATM/ANS.AR.B.005 Tehtävien antaminen**";

ii) Lisätään c alakohta seuraavasti:

”c) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ATM/ANS.OR.B.005A kohdan vaatimuksia, toimivaltainen viranomainen voi antaa tehtäviä päteville yksiköille a alakohdan mukaisesti tai jollekin asiaankuuluvalle viranomaiselle, joka vastaa tietoturvasta tai kyberturvallisuudesta jäsenvaltiossa. Tehtäviä antaessaan toimivaltaisen viranomaisen on varmistettava, että

1) pätevä yksikkö tai asianomainen viranomainen koordinoi ja ottaa huomioon kaikki ilmailun turvallisuuteen liittyvät näkökohdat;

2) pätevän yksikön tai asiaankuuluvan viranomaisen suorittamien sertifiointi- ja valvontatoimien tulokset sisällytetään organisaation yleisiin sertifiointi- ja valvontatiedostoihin;

3) sen oma ATM/ANS.AR.B.001 kohdan e alakohdan mukaisesti perustettu tietoturvan hallintajärjestelmä kattaa kaikki sen puolesta suoritettavat sertifiointiin ja jatkuvaan valvontaan liittyvät tehtävät.”

e) Lisätään ATM/ANS.AR.C.010 kohtaan d alakohta seuraavasti:

”d) Sen sertifioimista ja valvomista varten, että organisaatio noudattaa ATM/ANS.OR.B.005A kohdan vaatimuksia, toimivaltaisen viranomaisen on a–c alakohdan noudattamisen lisäksi tarkasteltava uudelleen niitä hyväksyntöjä, jotka on myönnetty tämän asetuksen IS.I.OR.200 kohdan e alakohdan tai delegoidun asetuksen (EU) 2022/1645 IS.D.OR.200 kohdan e alakohdan mukaisesti, sovellettavan valvonnan auditointisyklin mukaan ja aina, kun organisaation työn laajuuteen tehdään muutoksia.”

f) Lisätään ATM/ANS.AR.C.025 kohdan jälkeen ATM/ANS.AR.C.025A kohta seuraavasti:

”**ATM/ANS.AR.C.025A Tietoturvan hallintajärjestelmän muutokset**

a) Niiden muutosten osalta, joita hallinnoidaan ja joista ilmoitetaan toimivaltaiselle viranomaiselle täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan a alakohdan mukaisella menettelyllä, toimivaltaisen viranomaisen on sisällytettävä muutosten uudelleentarkastelu jatkuvaan valvontaansa ATM/ANS.AR.C.010 kohdassa vahvistettujen periaatteiden mukaisesti. Jos vaatimusten noudattamisessa havaitaan puutteita, toimivaltaisen viranomaisen on ilmoitettava asiasta organisaatiolle, pyydettävä lisämuutoksia ja toimittava ATM/ANS.AR.C.050 kohdan mukaisesti.

b) Muiden sellaisten muutosten osalta, jotka edellyttävät hyväksynnän hakemista täytäntöönpanoasetuksen (EU) 2023/203 liitteessä II (osa IS.I.OR) olevan IS.I.OR.255 kohdan b alakohdan mukaisesti:

1) saatuaan muutosta koskevan hakemuksen toimivaltaisen viranomaisen on ennen hyväksynnän antamista tarkistettava, täyttääkö organisaatio sovellettavat vaatimukset;

2) toimivaltaisen viranomaisen on vahvistettava edellytykset, joilla organisaatio voi toimia muutoksen toteuttamisen aikana;

3) kun toimivaltainen viranomainen on vakuuttunut siitä, että organisaatio täyttää sovellettavat vaatimukset, sen on hyväksyttävä muutos.”

2) Muutetaan liite III (osa ATM/ANS.OR) seuraavasti:

a) Lisätään ATM/ANS.OR.B.005 kohdan jälkeen ATM/ANS.OR.B.005A kohta seuraavasti:

”**ATM/ANS.OR.B.005A Tietoturvan hallintajärjestelmä**

ATM/ANS.OR.B.005 kohdassa tarkoitetun hallintojärjestelmän lisäksi palveluntarjoajan on ilmailun turvallisuuteen mahdollisesti vaikuttavien tietoturvariskien asianmukaisen hallinnan varmistamiseksi perustettava, toteutettava ja ylläpidettävä täytäntöönpanoasetuksen (EU) 2023/203 mukainen tietoturvan hallintajärjestelmä.”

b) Korvataan ATM/ANS.OR.D.010 kohta seuraavasti:

"**ATM/ANS.OR.D.010 Turvatoimien hallinta**

a) Lennonvarmistuspalvelujen ja ilmaliikennevirtojen säätelyn tarjoajien sekä verkon hallinnoijan on ATM/ANS.OR.B.005 kohdan mukaisen hallintojärjestelmänsä erottamattomana osana toteutettava turvatoimien hallintajärjestelmä, jolla varmistetaan

1) niiden tilojen ja henkilöstön turvallisuus siten, että laiton puuttuminen palvelujen tarjontaan voidaan estää;

2) niiden vastaanottamien, tuottamien tai muuten käyttämien operatiivisten tietojen turvaaminen siten, että näiden tietojen saanti on rajoitettu koskemaan vain siihen oikeutettuja henkilöitä.

b) Turvatoimien hallintajärjestelmässä on määriteltävä

1) prosessit ja menetelmät, jotka liittyvät turvariskien arviointiin ja vähentämiseen, turvatoimien valvontaan ja parantamiseen, turvakatselmuksiin ja aiemmista kokemuksista saatujen tietojen jakamiseen;

2) keinot, jotka on suunniteltu turvarikkomusten tunnistamiseksi, valvomiseksi ja havaitsemiseksi sekä asianmukaisten varoitusten välittämiseksi henkilöstölle;

3) keinot turvatoimiin liittyvien rikkomusten vaikutusten hallitsemiseksi sekä korjaavien toimien ja lieventämismenettelyjen määrittelemiseksi, jotta kyetään estämään tilanteen uusiutuminen.

c) Lennonvarmistuspalvelujen ja ilmaliikennevirtojen säätelyn tarjoajien sekä verkon hallinnoijan on tarvittaessa huolehdittava henkilöstönsä turvaselvityksistä ja toimittava yhteistyössä asiaankuuluvien siviili- ja sotilasviranomaisten kanssa tilojensa, henkilöstönsä ja tietojensa turvaamiseksi.

d) Tietoturvanäkökohtia on hallittava ATM/ANS.OR.B.005A kohdan mukaisesti."